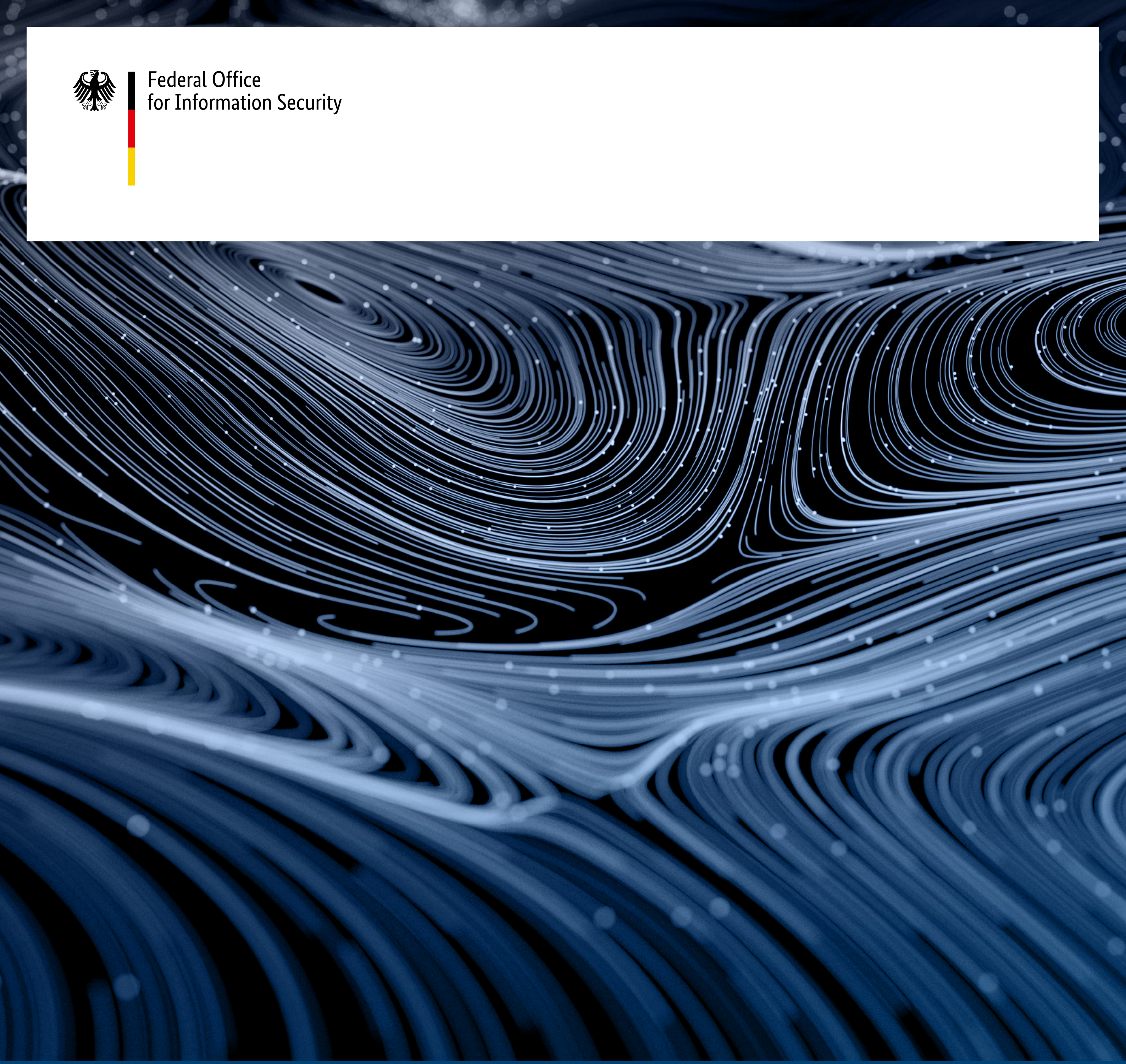
Federal Office
for Information Security



The State of IT Security in Germany 2018

Foreword

Our modern, high-tech society depends on the functional integrity of information technologies and communication systems, effective infrastructure and a secure supply of energy. These systems are the foundation for technical progress and economic development in our country.

As such systems grow more complex and all the areas of our information society become more interconnected, however, the risks posed by disruptions and attacks from within Germany or abroad are increasing as well. Threats in cyberspace are highly dynamic, and cyber attacks are becoming more adaptive and professional. Both IT systems and the methods used to attack them are constantly evolving at a rapid pace.

The Federal Government takes seriously its responsibility to ensure security also in cyberspace by maintaining a framework of IT security laws, pursuing a cybersecurity strategy and strengthening the relevant agencies.

Nevertheless, we cannot – indeed, we must not – rest on our accomplishments. Instead, we will further develop our IT security legislation (IT-Sicherheitsgesetz 2.0) as a way to strengthen the government's mandate to provide adequate protection in this regard. Our aim is to achieve a further expansion of the guidance and support the BSI offers to our federal republic, its states, citizens and companies.

Nevertheless, these matters demand more than just governmental action. When it comes to guarding against such threats in business and industry, companies themselves are called upon to enhance their IT security measures and adapt them to new challenges.

Cooperation and the sharing of information among all the entities involved are essential to address the dangers of cyberspace effectively. Security standards need to be established and enforced, and that requires a strong moderator. In addition to serving as the security service provider for Germany's federal administration, the BSI already offers a broad portfolio of security services for business and industry as well as society in general. I am committed to further expanding the BSI's capabilities and advancing it as our national cybersecurity authority.

In its 2018 report on the state of IT security in Germany, the BSI has presented a well-founded and comprehensive overview of the threats facing our country, our people and our economy in cyberspace. Above all, however, it illustrates the successful and indispensable efforts the BSI undertakes on our behalf. Germany, its residents, businesses and governmental agencies remain in the crosshairs of those looking to carry out cyberattacks. Taking on these challenges and devising rapid, efficient responses to the latest dangers in cyberspace remains the central task of the BSI and its employees.

Horst Seehofer
Federal Minister of the Interior, Building and Community

Foreword

With the increase in motorised traffic at the beginning of the industrial age, new regulations had to be created, new technical facilities implemented and new behaviour learned in order to guarantee road safety. For more than 100 years, traffic lights have regulated the traffic and road traffic regulations have been in place since 1934, providing rules of conduct for all road users. For some road users a required test was even introduced before they were allowed to use their vehicle. New professions were created, new rules laid down, and new institutions had to govern traffic.

Today, we are at the beginning of a new era again. Digitisation increasingly determines the activities of states and businesses, as well as the everyday life of citizens. And just as in the early days of the industrial age, we need to create new regulations, implement new technical facilities and learn new behaviours to increase cyber security. A few examples include the German IT Security Act, IT-Grundschutz standards and behavioural rules on how to handle smartphones, tablets and more are just a few examples.

In contrast to the start of the industrial age, however, we have less time to respond and adapt to this new technological foundation as a society. The pace of innovation in digitisation is breath-taking. New applications and new products are reaching the market in ever shorter cycles with new companies based on innovative digital technologies displacing the old established ones. And globalisation and technical networking mean that mistakes in development, gaps in regulations and negligence in behaviour often have immense consequences.

The more important digitisation becomes for governmental activities, our businesses and our everyday life, the more the associated challenges of cyber security must be tackled jointly by all those involved at national and international level.

Germany has made good progress in this direction. Important legislative and operational measures have been implemented in all areas. The networking of players at federal, state and local level has been driven forward, cooperation with industry has been expanded, and the BSI has been significantly increased in terms of personnel. We are well prepared.

But only as long as we as a society continue to increase our efforts for a stable and successful cyber defence at least proportionately to but ideally as a proactive response to the level of threat. The legal framework must be further developed, existing cooperation efforts intensified nationally and internationally, and affected protection measures continually put to the test. We need to remain open to new things, anticipate current threats and intensify our awareness of the importance of IT security.

We must stay clear on one point: the digitisation process cannot continue successfully without cyber security. BSI approaches this process in line with its own guidelines: as the national cyber security authority, the BSI is responsible for digital information security for the state, businesses and society through prevention, detection and reaction.

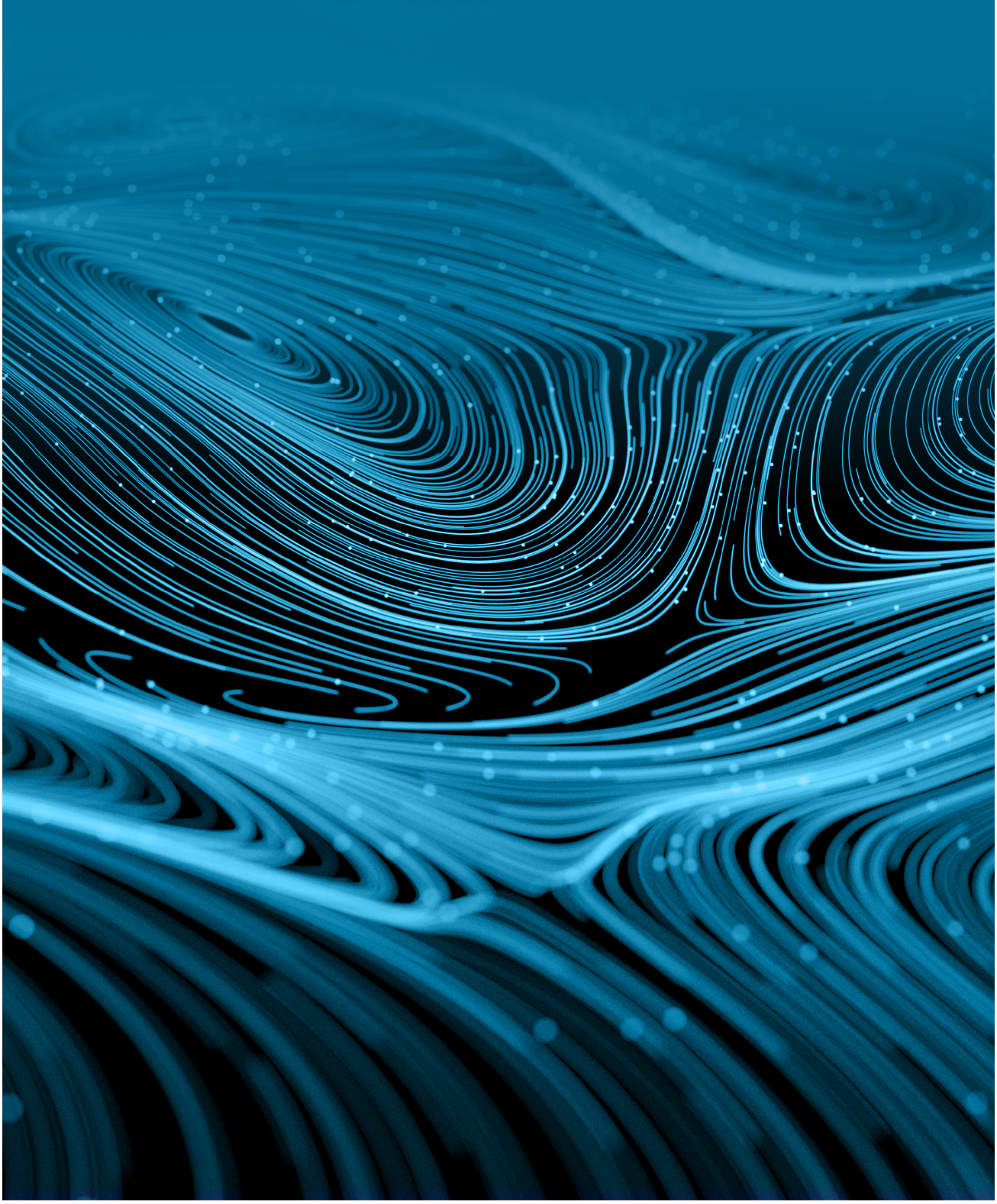
I hope you find the 2018 status report interesting and informative.

Arne Schönbohm

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

Content

1 The Level of Threat



1 The Level of Threat

This chapter describes the level of threat to IT security in Germany in the period from 1 July 2017 to 31 May 2018. It is divided into three areas: the Federal Administration, critical infrastructures/the business world and society. It also looks at the methods and means of attack used by perpetrators, in addition to the general conditions and causes, providing a number of examples of how attacks on IT security can affect life in a digitised society.

1.1 The level of threat to the Federal Government

To ensure that government institutions are able to carry out their constitutional tasks safely and sustainably, the state‘s information systems must be able to operate reliably and without disruption. This is the only reliable way to guarantee forgery-proof documentation of administrative activities and to allow the state to communicate with its citizens without gaps and protected against manipulation of any kind. If this is not possible due to impaired or non-functional information systems, confidence in the integrity of the state is shaken. In digital society, the information systems of the state authorities have thus become critical factors for the functioning of the community.

1.1.1 Insights from the protection of government networks

End-to-end encrypted communications and a robust, redundant architecture are the most important measures taken to protect the central government. Efforts are also undertaken to ensure regulated and reliable operations. In addition, ongoing improvements are made to the technical security configurations of the networks at hand, and close links are maintained among the networks of Germany’s federal states and municipalities.

The BSI has established a multi-level security system to protect the networks and IT systems as effectively as possible. Along with commercial security solutions, it comprises measures that the BSI has developed and adapted for its own specific purposes. These measures are continuously reviewed, advanced and adapted to changing threat scenarios. By combining these different defensive measures, the BSI maintains a solid overview of the current IT security status across the German government’s networks.

Protection against malware

Cyber attacks on the German government’s networks occur on a daily basis. In addition to arbitrary large-scale operations, these networks are exposed to targeted attack campaigns.

The most frequently detected attacks on the Federal Administration involve e-mails containing malware. Using automated anti-virus measures, an average of 28,000 e-mails of this kind were intercepted in real time each month before they reached the recipients’ inboxes. Of these, an average of around 6,000 malicious e-mails were collected each month using specially created anti-virus signatures alone. The decline in these figures compared to the previous year’s report can mainly be attributed to the sharp downturn in ransomware in 2017, which was also observed outside the government’s networks. In comparison to previous years, significantly more malware was distributed via links in e-mails rather than as attachments.

In HTTP traffic, an average of around 500 malware programmes were detected and blocked each month in 2017. This was another area in which the trend towards merely incorporating links to malware into e-mails rather than attaching the malware itself continued in 2018.

To supplement its automated anti-virus measures, the BSI operates an additional downstream system to detect malware in the government’s network traffic in accordance with the expanded authority granted to the BSI by German law (Section 5 of the BSIG). The manner in which it combines automated testing and manual analysis of exceptions makes this system particularly suitable for detecting targeted attacks and new types of malware. With it, BSI analysts were able to identify 40,000 attacks that were not detected or blocked by the commercial security products in use in the period under review. In addition, they prevented more than two million attempts to connect to servers associated with malicious code, fraud or data theft from within the government’s network.

1.1.2 Insights from IT security consulting

The working environment in the Federal Administration is characterised by numerous changes. In addition to centralising the required IT services within the scope of the Federal IT consolidation, the digitisation of workflows and internal administrative processes is also continuing.

The increasingly complex IT components are fundamentally vulnerable and can contain weak points. As a consequence, the Federal Administration must react in a planned and systematic manner to any vulnerabilities and attacks discovered. After the initial measures have been implemented, the information security management system (ISMS) should also be checked as to whether it is up to date and whether it conforms to the specifications; security measures should be adapted. Protection against APT attacks places high demands on security management and the implementation of measures. The *Spectre* and *Meltdown* processor vulnerabilities have shown that hardware also plays an important role in securing IT infrastructures. Corresponding countermeasures must be developed and implemented.

Cyber attack on German authorities

Situation
Towards the end of 2017, the BSI received indications of a successful cyber attack via the National Cyber Defence Centre, which purported to affect individual German federal authorities. The BSI started the incident handling process in coordination with the authorities involved in the National Cyber Defence Centre, informed the authorities that were potentially affected and began the analysis and verification of the information initially available.

Cause and Damage
The primary target of the attack was the Foreign Office. A learning platform operated by the Federal University of Applied Sciences was attacked in order to gain access to the Federal Foreign Office network via this intermediate step. This was because established protection measures had prevented attackers from accessing the network of the Foreign Office directly.

This put the attacker in a position to successfully infect some client systems at the German Foreign Office and to extract internal documents in small numbers. However, the attack was not directed against the government networks as a whole.

Reaction
In close cooperation between the authorities concerned, the National Cyber Defence Centre and BSI responded with the following measures, among others:

- analysis of the impact
- identification and protection of infected systems
- forensic analysis
- protocols and log data evaluation for those affected and at central points in government networks

In addition, the BSI has deployed a mobile incident response team (MIRT, within the meaning of Section 5a of the BSIG) to support incident handling on site for those affected, at weekends as well.

In consultation with those affected, the attack was observed undercover in order to first analyse the attackers‘ actions and then to maximise the effectiveness of the measures to be taken. The findings gained have already been incorporated into the Federal Administration‘s protective measures during the analysis.

After press reports had publicised CLASSIFIED information on the incident on 28 February 2018, immediate corrective action was taken. Additional protective measures to prevent attacker communication have been established. The affected systems of the Federal University of Applied Sciences were subsequently also switched off.

Recommendation
The situation clearly shows the current threat potential posed by targeted attacks on the Federal Administration. The financial, time and technical resources invested by the attacker in the preparation and execution of the attack demonstrate the attacker‘s great interest in its target.

The incident underscores the need for multi-level protection concepts and consistent implementation of protection measures against targeted attacks. However, the incident also proves the effectiveness of these measures: Similar incidents have had a far more serious impact on those affected in the past.

The challenges facing the departments and federal authorities as well as the state and local administrations lead to a greater need for advice from the BSI security consultancy.

In practical security consulting, more complex security measures must be the response to the advanced attack methods. From the point of view of security consultants, the detection of and defence against malware becomes a task that can no longer be handled simply by installing an antivirus programme alone. Constant levels of demand are also generated by required compliance with regulations and renewed information security standards, which are becoming more complex against the background of more complex IT.

To move away from a purely reactive approach, the existing information security management system (ISMS), the security concept and implementation of update security measures are of great importance.

Together, the modernised IT-Grundschutz standards and the renewed Guideline For Information Security of the Federal Administration (see section 2.1) provide an up-to-date set of instruments. These are the foundation for corresponding requirements and options for action, allowing existing and future challenges to be met effectively.

1.1.3 Insights from notifications from the Federal Administration

According to Section 4 (3) of the BSIG, federal agencies are obliged to immediately inform the BSI if they have information that is significant for fending off threats to information security. The details of the reporting procedure, particularly regarding which information is relevant to the work of the BSI or to the protection of Federal Government IT, have been laid down by the German Federal Ministry of the Interior (BMI) in the general administrative regulations on the implementation of Section 4 (3) of the BSIG, following consultation with the Council of Chief Information Officers of the federal ministries (IT Council). It came into force on 1 January 2010.

This task is performed by central reporting within the National IT Situation Centre, as an organisational part of the BSI. It aims to establish a reliable picture of the current IT security situation in Germany at all times. This means it should be able to quickly and effectively assess any need for action and the options available at the state and commercial levels in any IT security incidents.

IMMEDIATE notifications

IMMEDIATE notifications are incident related and therefore irregular in frequency. In principle, however, the number of notifications is also an additional indicator for assessing the level of threat.

In 2017, a total of 157 IMMEDIATE notifications were reported to the Central Reporting Office and National IT Situation Centre.

Ransomware was the main topic of the notifications in 2017. There were reports of the exploitation of telephone/video conference systems for malware infections. In the middle of the year a cyber attack took place with the encryption Trojan *NotPetya*. This shows that, with regard to All-IP connections and VoIP PBXs, experts should always ask whether configurations are secure and whether there are regular security updates handled by specialised personnel.

Only half as many notifications of DDoS attacks were received compared to the previous year. The *Mirai* botnet, which was strongly represented in 2016, lost significance after the first quarter of 2017.

1.2 The level of threat to critical infrastructures and the business world

Critical infrastructures (KRITIS) are organisations and institutions of vital importance to the community. Their systems and services, such as the supply of water or heat, their infrastructure and their logistics are increasingly dependent on information technology that runs smoothly. A disruption, impairment or even a failure due to a cyber attack or an IT security incident can lead to lasting bottlenecks in supply, considerable disruptions to public security and other dramatic consequences. Other commercial enterprises are also interesting targets for cyber attacks due to their technological know-how and their foreign activities. The financial consequences of production stoppages, damage to machinery, patent theft or cyber extortion are what make increased IT security precautions necessary.

1.2.1 Insights from critical infrastructure notifications

The overall risk situation in the critical infrastructures is at a high level, but varies in the individual sectors. During the reporting period the BSI received 145 reports from the KRITIS sectors, most of them from the IT and telecommunications sector and the second most from the financial sector.

KRITIS operators such as energy providers (see EnBW/Netcom Incident) are exposed to new or more advanced attacks in addition to normal attacks from the Internet. Other sectors are less in the spotlight. They are confronted with attacks that have already been observed in the more exposed sectors. However, the methods used have now been automated and can now be used by attackers across the board.

Although the division into exposed and less exposed sectors is relatively stable, it cannot be assumed that this will always be the case. Social and political events can change the motivations of attackers, meaning that all KRITIS companies can become the focus of more progressive attackers and must arm themselves against it.

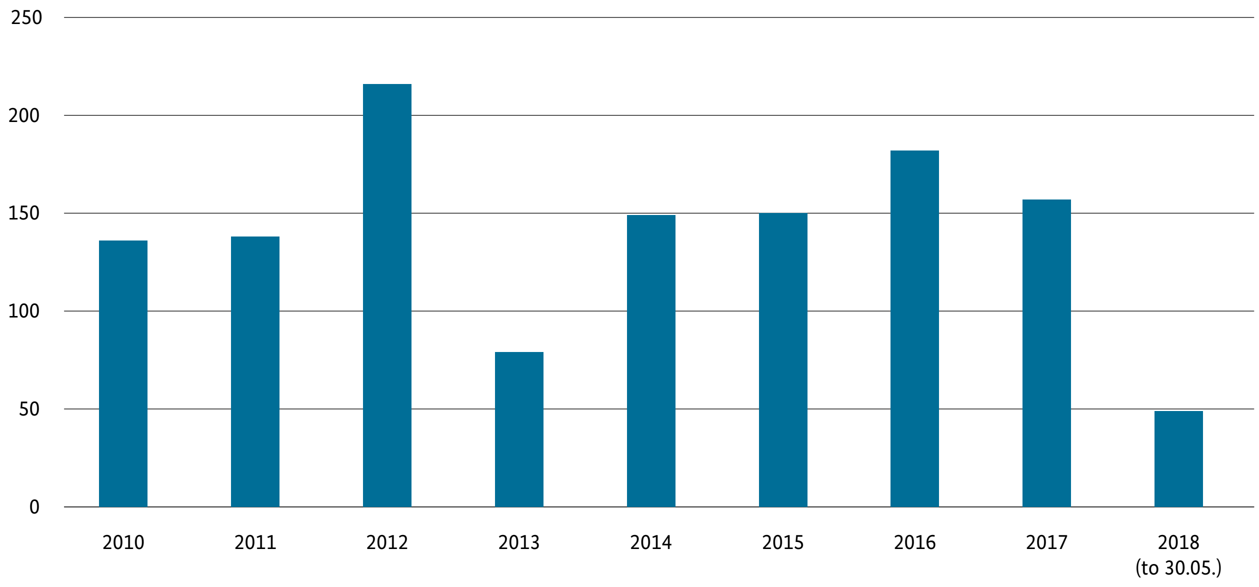


Figure 01 IMMEDIATE notifications submitted, in line with Section 4 (3) BSIG

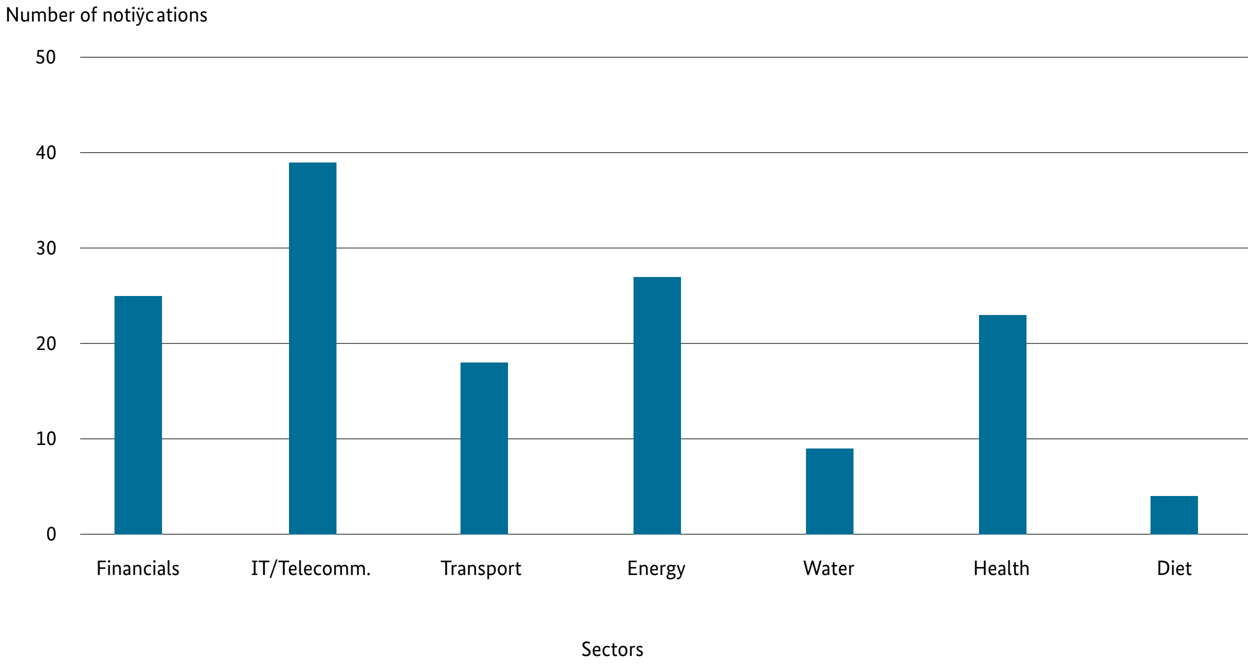


Figure 02 Reported occurrences by KRITIS operators (voluntary and obligatory notifications) in the reporting period from 1 June 2017 to 31 May 2018

Attack on the network of a regional telecommunications company

Situation

It has become apparent in recent years that one or more groups are developing malware that is specifically aimed at attacks on industrial control systems (ICS). The malware Havex was discovered as early as 2014, leading to infections worldwide and searching networks for ICS systems and information about their configuration: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf. The exact purpose of this campaign was not clear at the time, as there was no evidence that economically or politically exploitable information was stolen. There were also no reports of destructive actions of this malware.

Since 2015 there have been several attacks on critical infrastructures in Ukraine using modified variants of Black-Energy. Although this malware had no ICS-specific functions, it was used to give the perpetrators access to the control systems of power network operators. The perpetrators also had sufficient knowledge of the systems and processes of the operators to cause large-scale power failures through manual changes https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

In mid-June 2017, a malware called Industroyer or CrashOverride https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf was reported for the first time, which has the functionality to command control systems via ICS-specific protocols. This was used at the end of 2016 for attacks against Ukraine‘s power supply. The modular, extendible architecture and the detailed implementations of ICS protocols suggest that this group of offenders has extensive test environments and the long-term goal of penetrating ICS networks to sabotage these where possible.

Reports of spearphishing and watering hole attacks on American and European energy companies and nuclear power plant operators https://www.ci-project.org/blog/2017/7/10/document-indicates-campaign-may-have-targeted-european-energy-and-critical-infrastructure-in-march-2017 also fit into the overall picture. Even if only office networks have been compromised through this to date, the selected watering holes are relevant for the ICS supply chain. It can be assumed that information will be collected in the office networks initially and used for further attacks.

The BSI believes that all these attacks are from two specific groups that may share the same strategic objectives. In media and analysis reports these groups are called *EnergeticBear/Dragonfly* and *Sandworm/VodooBear*. The security situation was exacerbated when a man was arrested in May 2017 who appears to have sold confidential information about European energy transport routes to a Russian spymaster.

Finally, in the summer of 2017, unknown hackers entered the network of a regional telecommunications company, a subsidiary of an electricity company. The operator received a warning about the attack from the Federal Office for the Protection of the Constitution (BfV), the domestic intelligence service within the Federal Republic of Germany. The operator reported the security incident to the BSI and asked for support. The incident was analysed and dealt with by the BSI within the framework of the National Cyber Response Centre in cooperation with the company concerned.

Cause and Damage

There is currently no evidence to suggest that critical supply services have been impaired in the incident described above.

Nevertheless, the level of threat must be taken seriously. Attacks systematically carried out with the appropriate expertise and resources have the potential to endanger the energy supply. Consistent safeguards that already exist must also be kept up to date in order to counter successful attacks such as those on the electricity supply in Ukraine in 2015 and 2016.

Reaction

The BSI provided early information about attack campaigns against energy companies.

Based on further information provided by affected companies and partner agencies over time, the BSI was able to upgrade this warning with new findings and make it available across all sectors.

In addition, the BSI supported the operator in the technical analysis. BSI does not publish names of affected companies without their permission.

Recommendation

As soon as operators discover any irregularities that could indicate an attack, they should forward information about them to the BSI as soon as possible. This helps other operators to protect their installations, as the BSI passes on this information in a sanitised form, as in the case detailed above.

To protect ICS systems and networks, the BSI continues to recommend the implementation of the measures in the following documents:

- BSI Grundschutz: IND - Industrial IT (modules and implementation notes in particular) https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/IND/IND_Uebersicht_node.html
- BSI, ICS Security Compendium, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/ICS/ICS-Security_compendium.html
- Remote Maintenance in Industrial Environments https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_108E.html;jsessionid=3AE8D73338C2E9B908985A118076E3B8.2_cid360?nn=6656412

1.2.2 Insights from notifications from the business world

Companies are basically exposed to the same risks as any other IT and Internet users. In addition, however, they are exposed to attacks that do not occur in their private lives. These include cyber blackmail and cyber espionage.

The cyber attacks *"WannaCry"* and *"NotPetya"* attracted a great deal of attention in mid-2017. *WannaCry* first appeared on 12 May 2017 (see also JLB 2017), *Petya* (also: *NotPetya, ExPetr, DiskCoder.C*) in late June 2017. These attacks impressively demonstrated how vulnerable many companies are to the risks of digitisation and what the consequences are if cyber security is not understood as an indispensable prerequisite for successful digitisation.

Analyses by IT security researchers suggest that in the case of *Petya/NotPetya* different malware variants have already been distributed in several waves since April 2017 via the update function of the accounting software M.E.Doc, which is widely used in Ukraine. Thus companies could also be affected by this cyber attack if they use M.E.Doc, even if they were not affected by the widely publicised *Petya* encryption Trojan. The different types of malware enable the spying out of data from the affected company networks.

Russia and Ukraine were largely affected initially by the spread of *Petya*. Computers were next infected in Poland, Italy, Great Britain and France. Later, the blackmail software reached the US and spread to Asia. Companies in Germany were also affected. The consumer goods company Beiersdorf confirmed that it had become the target of the attack and that IT and telephone systems had failed.

Although it was possible to limit the harmful effect of *WannaCry* by registering a URL ("kill switch"), malware like *WannaCry* continues to be virulent. At the beginning of 2018, the BSI received notifications from industry that computers were infected with *WannaCry* malware (see info box on page 14). These late-stage infections clearly lag behind the first *WannaCry* wave, especially in terms of effects.

WannaCry has the ability to spread on its own. This means that sporadic but limited infections occur again and again as soon as infected computers that have not been detected get in contact with other networks. Unfortunately, all too often internal networks that are believed to be secure and rely on the security measures of their environment give the bug the freedom it needs to spread.

The cases show that they may well become a serious problem for individual operators. Embedded systems with older, possibly unpatched operating systems and controls for industrial plants can still be vulnerable to the distribution channels used by *WannaCry*. For some devices, an operator does not necessarily immediately see which processes are running on these devices; this also applies to patch statuses or configuration.

Overall, however, the damage *WannaCry* has caused is immense: estimates range from several hundred million dollars to four billion dollars worldwide. More than 200,000 computers in 150 countries have been infected. In comparison, the blackmail proceeds of the attackers are low. After the deadline for the ransom payment had expired, bitcoin payments worth almost €93,000 were received by the anonymous hacker group in the three digital bitcoin wallets.

Ransomware attacks such as *WannaCry, NotPetya* and *Bad Rabbit* put pressure on many companies in 2017, including critical infrastructures such as healthcare and logistics companies. According to published estimates, ransomware incidents cost companies more than $8 billion worldwide in 2017.

This threat is still present in 2018, albeit to a lesser extent, with a shift to or supplementation by cryptocurrency mining observed on the one hand and more diversified, targeted attacks on the other. This increases pressure on companies to develop appropriate reaction strategies in order to be able to better limit the effects of an attack.

Infections with *WannaCry* malware

Situation

At the beginning of 2018, the BSI received a notification from a critical infrastructure operator in the food sector. Several computers in a production plant had failed repeatedly and had to be restarted. A few days later another case was reported to the BSI, this time by a plant manufacturer responsible for maintaining plant at several locations. Another report reached the BSI in February 2018. *WannaCry* infections occurred in medical equipment at several sites in a hospital network. Numerous clinics were also affected in the United Kingdom.

Cause and Damage

In this case, the plant manufacturer had configured the computers in such a way that they were reset to a defined original state after a restart. This facilitates the resumption of operations in the event of a fault. The operator quickly established that the *WannaCry* malware was behind the multiple failures. A computer infected with *WannaCry* managed to reach one of the control computers via the network. The worm infected the control computer, spread from there and started the encryption of the file system, leading to the failure of the computers. The operator was able to restart the control computer to a productive state, although this did not eliminate the actual cause of the error. Then it happened again, probably by the infection of another control computer in the same network. Thus the control computers could be reset to a productive state again and again, but *WannaCry* could continue to infect control computers until a coordinated cleaning of the entire network.

In the second case, a Mobile Incident Response Team (MIRT) of the BSI investigated the situation on site in consultation with the operator concerned and the company providing support. After detailed analysis by the plant manufacturer in particular, it became clear that there was a common cause. An error was found in a network component that was part of the plant manufacturer's maintenance infrastructure. Because of this, the network separation did not work as configured, but made it possible for *WannaCry* to compromise it. The plant manufacturer then made contact with the network component manufacturer in order to fix the problem.

In the hospital network, analysis of the infection path clearly showed that a test device provided by the manufacturer was infected. *WannaCry* could spread from the test network to other locations because the firewalls were not all configured to prevent retransmission. According to the hospital operator, only the devices were infected, fortunately, and there were no harmful effects, i.e. *WannaCry* did not encrypt the file systems. Nevertheless, it still took a considerable number of working hours to clean the devices.

Recommendation

The BSI advises special caution when devices are newly integrated into networks or new communication links are established between networks or individual devices. The distribution path of *WannaCry*, even within closed networks, should not be ignored or left unchecked.

1.2.3 The level of threat to the business world: insights from the Alliance for Cyber Security survey

Cyber attacks have series consequences for business. This is the finding of the 2017 Cyber Security Survey conducted by the BSI as part of the Alliance for Cyber Security. Since 2014, the BSI has been conducting an annual cyber security survey to investigate the perceived threat and impact of cyber attacks on German institutions and the implementation status of appropriate protection measures. In the period from 4 October 2017 to 30 November 2017, almost 900 companies and institutions took part in the public online survey at www.allianz-fuer-cybersicherheit.de. The survey was anonymous; it is not possible to draw any conclusions about the participating institutions. The results of the survey clearly show that cyber risks are perceived as one of the biggest threats to the success of digitisation.

Almost 70% of companies and institutions in Germany fell victim to cyber attacks in 2016 and 2017. In nearly half of the cases, the attackers were successful and were able to gain access to IT systems, influence the functioning of IT systems or manipulate companies' Internet sites, for example. Every second successful attack led to production or operational downtimes. In addition, there were often costs for investigating the incidents and restoring the IT systems as well as damage to reputation.

Of the various types of attack, malware infections were the most common. Nearly 57% of reported attacks were infections in which malware invaded corporate IT systems to carry out malicious operations. Hacking attacks such as sabotage of industrial control systems, data theft or the manipulation of Internet sites accounted for 19%; DDos attacks, which lead to the failure of websites and other network infrastructures due to overload, amounted to 18% of the successful attacks.

There is a high level of awareness about the dangers facing companies in cyberspace. Around 92% of respondents rated the dangers as critical for the operability of their institution, for example. Only close to 42% of respondents believed that they could implement replacement measures and continue to operate in the event of a cyber attack. Large corporations considered themselves particularly at risk. Of these, just under 38% believed their operations could continue in the event of a cyber attack.

Many companies have already implemented comprehensive cyber security measures. 89% of respondents took measures such as segmentation or minimisation of gateways to secure the networks. Virus control measures were also frequently used (86%). They employed both central detection measures, such as scans at the security gateway and mail servers etc., and decentralised measures such as scans on client/server systems.

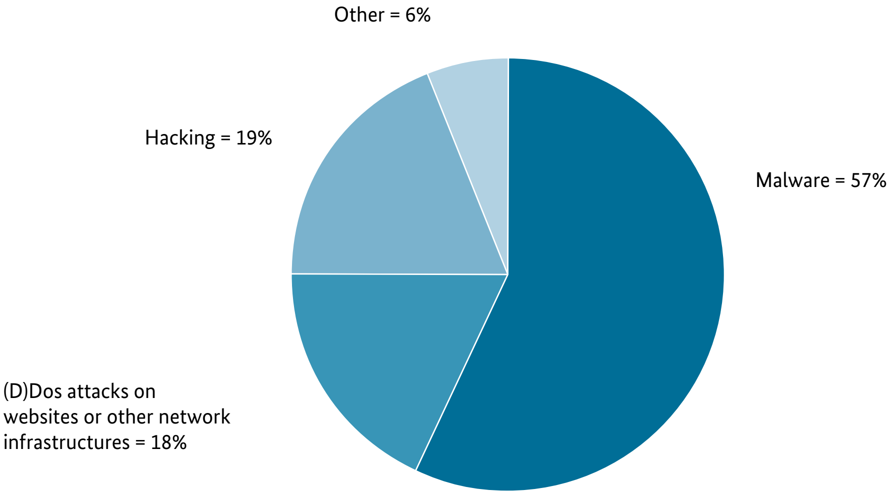


Figure 03 What kind of attacks were they?

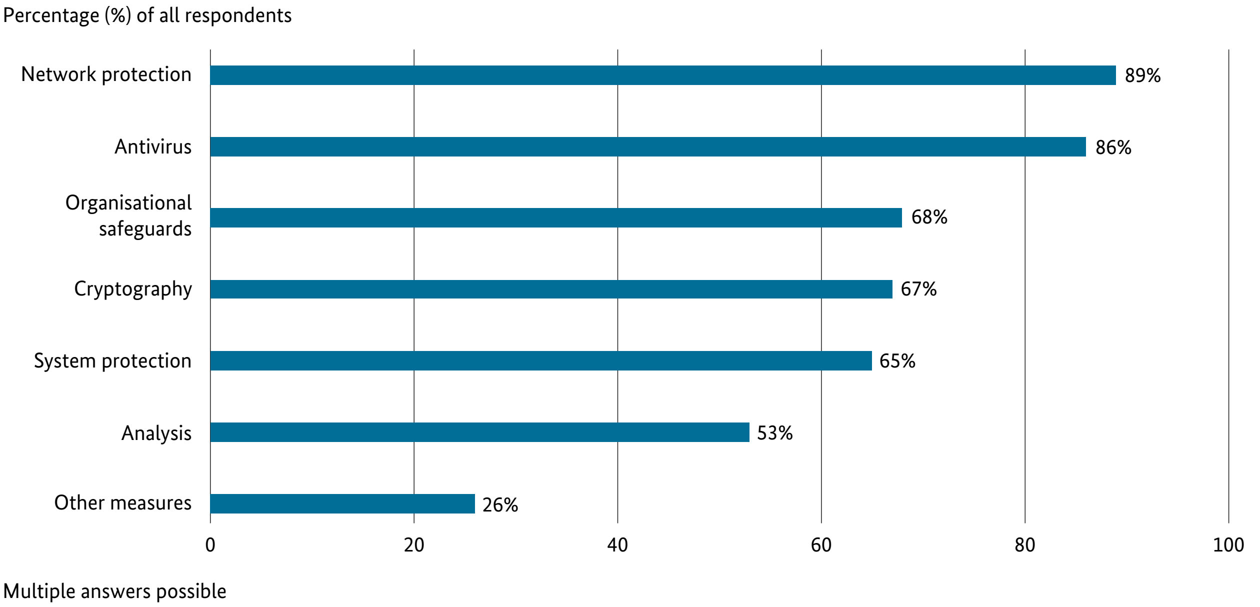


Figure 04 What measures are currently being implemented at your institution to protect against cyber attacks?

In addition to the measures already implemented, many companies (71%) are planning further improvements in cyber security. Of these, around 13% even indicated that urgent short-term improvements were planned for critical areas. Some companies have recognised that the human factor is also important when it comes to a holistic approach to information security. More than half of the companies regularly train their employees on cyber security issues. Of the remainder, almost 20% of the companies surveyed were planning corresponding measures. However, almost 30% of those surveyed said that there was no IT security training or plans for this.

A quarter of the companies surveyed have cyber security monitoring in place; 29% of large companies and 23% of small and medium-sized enterprises (SMEs) evaluate log

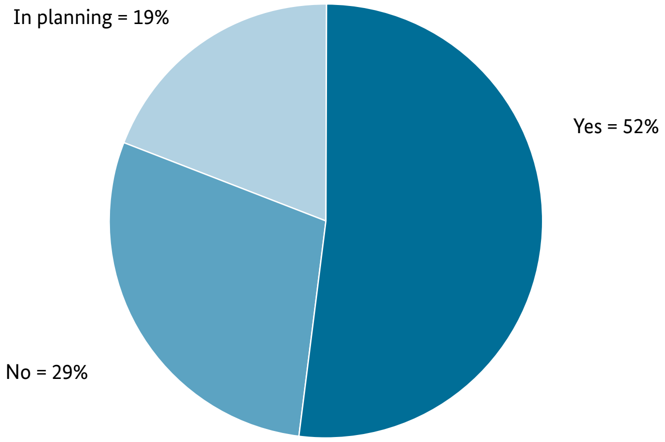


Figure 05 Is personnel trained in IT security at regular intervals and are these training courses documented?

files regularly and systematically. More than half of all companies only examine log files on specific occasions. The need for small and medium-sized enterprises to catch up is apparent in their planning activities. While around 17% of large companies plan to use log data, the figure falls to 11% for small and medium-sized companies.

These companies report that they are particularly focused on reactive measures to respond to a cyber attack. For example, around 58% of respondents reported having guidelines such as contingency plans or emergency instructions describing how to restore operations after a serious malfunction. There were once again differences between small, medium-sized and large companies in this area. While two out of three large companies have such a directive, the ratio for small or medium-sized companies was just over one in two.

Adequate and up-to-date emergency plans are a particularly important measure for increasing the level of security. Ultimately, the quality of resilience is crucial here. The key factor of resilience will become increasingly important in future for large companies and SMEs alike. Incident training is an important factor here. The proportion of well-positioned companies must grow further, a cause continuously supported by the Alliance for Cyber Security and the BSI.

1.3 The level of threat to society

Digitisation is increasingly pervading everyday life. It offers new opportunities for civil society, but the system and the technology also pose risks. As a result of the increasing networking of almost all areas of life, citizens have ever greater access to digital infrastructures, services, terminals and data sources with which they interact on a daily basis. IT solutions come easily to many areas of societal life. They facilitate medical care, control the power grids, improve the use of renewable energies and make our vehicles more environmentally friendly. In addition, digitisation opens up individual possibilities for action. This includes design possibilities such as the dissemination of information, but also destructive activities such as manipulation or data theft. Cyber security understood in terms of comprehensive IT security precautions is therefore the prerequisite for successful digitisation.

1.3.1 Results and findings from surveys

As part of their cooperation, the BSI and the Police Orientated Crime Prevention by the Federal Government and the States programme (ProPK) were able to ascertain whether and how respondents protect themselves from Internet dangers and whether they had ever been a victim of Internet crime in a representative online survey in October 2017. The results showed that 97% of Internet users in Germany attach great importance to security when using the Internet, although the information behaviour and the protective measures actually used sometimes appear to completely contradict the asserted importance of high security.

The high importance attached to information security does not necessarily lead to security-conscious behaviour in users. Only around one in three (30%) access information on data security. People are particularly interested in secure surfing when it comes to financial aspects: for 71% of all respondents, security is particularly important in online banking, and only 45% are concerned about secure online shopping. Secure use of social networks (11%), cloud services (8%) and networked home appliances for building automation (4%) was of little or no importance to respondents.

More than half of those surveyed only engage with the issue of IT security when facing a problem. While two thirds of respondents use antivirus programmes and a firewall, significantly fewer users implement other essential protection measures. For example, less than half ensure the secure transfer of personal data (45%), and only 37% install available updates immediately. Only around one in five users (21%) back up their data regularly.

According to their own statements, 59% of those questioned have never been victims of crime on the Internet. 19% say they have been victims of malware, 8% of online shopping fraud and 6% of phishing. Of the 823 respondents who were victims of Internet crime, more than half (52%) resolved the problem themselves, around a quarter (24%) asked family, friends or acquaintances for help and only around one in five (19%) reported the crime to the police. The results of the survey will be incorporated into the future educational work carried out by the BSI and the police.

1.3.2 Safety of medical devices

As digitisation progresses globally it is also finding its way into the healthcare system. More and more network-connected medical products are developed and placed on the market of medical devices. These products have different types of interfaces that can be integrated into networks in various ways and can sometimes be linked to mobile applications (apps) for managing personal data. Enhanced functionality and increased convenience speak in favour of this development as networking guarantees almost unrestricted and location-independent access to the patient's own data. Wireless technologies make it much easier for medical doctors to access documented patient data and communicate with the system itself. Active implantable medical devices such as pacemakers, defibrillators (implantable cardioverter defibrillators, ICD), neurostimulators and cochlear implants have clear advantages over older systems because wireless communication means additional surgical intervention is no longer required, for example to adjust parameters of the device. Such active medical devices demand for high safety requirements, as they normally have a relatively long life or retention time in the patient's body, performing vitally important functions. Hence, it is mandatory to identify and evaluate possible security threats in an early stage to allow for the development of appropriate countermeasures to guarantee safety over a long period.

As the degree of networking and distribution of "smart" medical devices increases, it can be assumed that both the product and application portfolio and the risk of cyber attacks possibly endangering patient safety will rise. Several tests under laboratory conditions, predominantly in the US but also in Germany, have shown that a variety of medical devices (pacemakers, defibrillators, respirators, infusion pumps) are vulnerable to malicious attacks. For example, a defibrillator was able to be controlled and reprogrammed remotely to release unwanted electrical shocks, even if just the model and serial number were known. Cybersecurity must therefore be integrated and implemented from the outset in the development and manufacture of medical devices ("security by design" and "security by default"), in order to guarantee for a secure use over as long a period as possible.

Often the authentication mechanisms for digitised medical devices are not sufficiently secured and the data encryption techniques for communication and storage are weak or non-existent. Under these circumstances, it would be possible to obtain unauthorised access and manipulate the device without the patient's knowledge. However, to give medical doctors the quickest possible access to devices such as implanted defibrillators in an emergency, the safety mechanisms were kept deliberately low in some cases; safer access mechanisms usually take time and any delay or complications in using a medical device under pressure in an emergency could be detrimental to a patient's well-being in the worst cases. Moreover, it can be problematic to implement stronger security features using the example of implantable defibrillators. Such a defibrillator has the size of a matchbox and is battery-powered. With a battery life of about four to six years, ICD patients have to schedule regular surgical procedures for replacement. If more storage space or better encryption techniques were used, this would be at the expense of the size of the defibrillator and battery life: the retention time of the device would be shortened and additional surgery required. Here, the compromise between functional medical devices and mature cybersecurity technologies becomes eminently clear.

As the level of threat is considered critical for medical devices, more suitable cyber security mechanisms will have to be developed in the future. The BSI responds to these developments in cooperation with the responsible regulatory authorities. Projects are currently scheduled to identify additional security features in medical devices and examine these in more detail.

1.3.3 Security of mobile banking

A very wide variety of payment services is offered on the Internet. There are providers of payment accounts for merchants and customers such as Paypal, credit card solutions such as 3D-Secure, direct debit-based solutions like on Amazon as well as variants such as Giropay or iDeal, which forward customers to a bank website. This also includes the Sofort transfer from Sofort GmbH (now Klarna), which forwards the payment order to the payment service provider managing the account.

However, Internet payments are no longer confined to PCs; they are increasingly made with mobile devices such as smartphones or tablets.

More and more banks are offering online banking applications (apps) for mobile devices. In addition to the apps offered by the larger banks, there are also free multibank-capable apps that allow customers to manage accounts with different banks. These banking apps are often combined with a second application, known as the TAN app. This generates a transaction number (TAN) to secure the transaction executed in the banking app.

The individual payment methods involve a wide variety of risks for the user, the merchants and also the customer's credit institutions. Mobile banking users rank security and convenience as the most important aspects they expect from their payment process/banking app.

The log-in method for a banking app and the type of transaction security clearly impact the safety. One-device banking is often used on grounds of convenience. The banking app and the app that generates the TAN run in the same device in this scenario. However, installing the banking and TAN app on one device carries risks: if the mobile device is compromised, an attacker may be able to access both apps and have full control over the account.

Hack of Promon Shield solution

During the 34. Chaos Communication Congress (34C3) in Leipzig in December 2017, the Erlangen-based security researcher and doctoral student Vincent Haupert showed how Promon's security solution, the so called Promon Shield, can be easily circumvented.

Situation
Promon Shield is a security solution from the Norwegian company Promon that can be integrated directly into applications, web services or apps. It is intended to ensure that these are protected against attacks by malware. No malware signatures are required for this.

The security solution is used by various banks to protect a total of 31 banking apps. Hardening should allow the corresponding apps to be protected against attacks or the software should prevent banking on compromised devices and interacts with the TAN app. The built-in protection mechanism becomes effective immediately and enables secure access.

Cause and Damage
Through a hacking attack with the tool Nomorp, German computer scientists succeeded in deactivating Promon Shield‘s protection mechanisms using security holes and manipulating transaction processes. A sample code developed by the hackers made it possible to take control of a victim‘s banking app and change transactions.

Reaction
In a project recently started, the BSI will examine with the variety of different mobile and online payment methods. The aim is to examine the general security features in a safety assessment and to formulate recommendations for action.

Recommendation
The BSI therefore recommends the use of two-factor authentication for online banking, in which the transaction number (TAN) is generated by a separate device. Using a banking app and a TAN app on the same device is not secure. If you want to use mobile banking, you should use a second device, like a TAN generator, to generate a TAN. In this case, secure two-factor authentication is only possible if the TAN is generated on a separate device.

1.3.4 Smart Home and the Internet of Things

The Internet of Things (IoT) allows more and more items to be connected to each other, and to people, through ever more affordable hardware and longer battery power while also reducing power consumption. Popular areas of application for IoT devices are household appliances, home monitoring and health management, e.g. wearables. New applications and networked devices are constantly put on the market, connecting the digital worlds with those that were previously analogue. A growing number of manufacturers are beginning to expand their product range with smart solutions. For the user this can often contribute to increased convenience and control in their environment or home.

Key factors in the customer's purchasing decision tend to be the device functionality and the associated convenience as well as the price. The decision is less often based on IT security. However, frequent reports of IT security incidents among consumers and manufacturers have noticeably contributed to a growing awareness of the risks posed by networked devices. Many frameworks and protocols used in the Internet of Things are now offering increased security functions and implementing them. There is also a faster response to device vulnerabilities. However, the sheer number of devices connected to the Internet that are not sufficiently secured continue to be lucrative targets for cyber criminals.

Unlike traditional Internet-connected devices such as PCs, laptops and servers, IoT devices often lack their own attack

Open OBD II interface in vehicles

Situation
The OBD II interface (on-board diagnostics) is an interface that has been available in all motor vehicles manufactured and registered in Europe since 2003. It provides access to the CAN buses that connect all electronic components of the vehicle. The original function of the interface was to monitor exhaust emission regulations; since then it can and has been used for further vehicle inspections, e.g. for manufacturer-specific fault diagnosis in workshops.

It can also be used to connect dongles. These are attached to the OBD-II interface and send diagnostic data to insurers or car rental companies e.g. via mobile phone connection during the journey. This gives the vehicle‘s internal network a wireless interface in addition.

Cause and Damage
Due to its design, OBD II can not only read out data from the vehicle, but also import commands into the internal network. However, the dongles are not subject to any authorisation checks. Since they offer interfaces into the vehicle that cannot always be covered by the safety concept of the vehicle manufacturer, this opens up additional risks. In 2015, researchers showed that they were able to send manipulated SMS to certain dongles, thus influencing braking functions at low speeds. In 2017 it was proven that the Bluetooth connection of a dongle could be attacked, again influencing driving functions.

Reaction
No immediate response from the BSI was required in this case. In order to assess the threat situation more precisely in future, the BSI will carry out corresponding security analyses of the interfaces of motor vehicles. The aim is to detect and eliminate security gaps in close coordination with the manufacturers before they can be exploited.

Recommendation
In principle, vehicle owners should be clearly informed about the possible consequences of integrating uninspected accessories such as OBD-II dongles into vehicle electronics. It is recommended that the dongles in particular be inspected in the same way as other vehicle components in the context of type approval. One option here would be the use of certification standards such as Common Criteria.

prevention systems. Compared to PCs, they generally have significantly less resources available for security mechanisms to reduce costs and increase battery life. In addition to being easier to compromise, detecting problems with IoT devices is also significantly more difficult. Owners of infected IoT devices often fail to notice any changes while the device is still operating as normal.

IP and port scans with special search engines, among other things, can identify sufficient numbers of IoT devices through the Internet with modest effort. These devices can be compromised in order to build powerful botnets, for example. There is also evidence of the use of attack tools that automatically exploit vulnerabilities. In addition to attacks via the Internet, local wireless or cable interfaces can also be misused by an attacker for a variety of purposes.

Two threat scenarios

A distinction must be made between two dangerous situations. In the first threat scenario, the IoT device is compromised in order to cause the user direct or indirect damage. Threats in this context include:

- Data manipulation:
  An attacker can, for example, modify the access control to gain unauthorised access to a building or cause damage to the air conditioning system by manipulating data.

- Data espionage:
  IoT devices can be equipped with various sensors. A compromised device can forward data to the attacker, providing access to sensitive information in this way.

- Sabotage of IoT devices:
  The device can be put out of order by the attacker and can, at least temporarily, not be used by the owner. Depending on the device, this can also lead to relevant restrictions for the owner.

- Using IoT devices as a backdoor:
  Insufficiently secured IoT devices can be used as backdoors to gain access to home or corporate networks.

In the second threat scenario, the IoT device is compromised to prepare for attacks on further targets. Web services or third party infrastructures are the attacker's main target, not the device itself. The attack on the device often goes unnoticed as the functionality remains unchanged. Threats in this context include:

- Construction of botnets:
  The mass hijacking of inadequately secured IoT devices enables the creation of large botnets that are capable of disrupting third party websites and web services using DDoS attacks.

- Identity concealment:
  Compromised devices can be used as proxies to disguise further attacks.

- Cryptocurrency mining:
  It is possible to use the collective computing power of all captured IoT devices to mine crypto currencies, such as bitcoins. This was tried, for example, with the well-known *Mirai* botnet, but apparently discarded due to lack of efficiency. However, it is conceivable that with increasing computing power this potential could also increase further. Misuse like this is easier to detect, however, because the devices have to run at full load and the response time for their intended use is noticeably slower.

- Click fraud with advertising banners:
  The attacker uses lots of different IP addresses from hijacked IoT devices to generate clicks on advertising banners, videos or social media content. In this way an unauthorised commission can be obtained with click-based billing. In addition, the advertiser suffers direct damage through the payment of a commission for simulated clicks.

Thus, the possible effects of attacks on IoT devices are as diverse as they are on PCs. All the IT protection goals such as confidentiality, availability and integrity can be compromised. DDoS attacks or the manipulation of data can lead to high commercial losses for those directly affected and third parties or even to impairments of critical infrastructures.

1.3.5 Identity abuse through remote identification procedures

Banks, telecommunications companies and other service providers are increasingly offering online procedures to identify their customers in online transactions. While a high level of security can be achieved with the online identity card or electronic residence permit function, procedures are still being used where the security does not match this level of personal identification and identity document verification.

Insecure identification via video channels

Procedures using video chats to confirm identity, which are still offered in some application areas, are particularly open to abuse. In terms of uniqueness and security, a video image of the user and their identity card recorded with a smartphone cannot be compared to identification in the flesh. Besides, the most a video channel can be used for is to check security features that change when the ID card moves under certain lighting conditions, such as the holographic portrait or the changeable laser image on the

An example of ID theft

Situation

On 5 July 2017, the Federal Criminal Police Office (BKA) published a short report detailing the discovery of nearly 500 million data records comprising e-mail addresses and associated passwords https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Kurzmeldungen/170705_HackerSammlung.html. The origin of the data set found and its age were not known.

Cause and Damage

If the data discovered is the access data for an e-mail account, an attacker could use it for different purposes, such as sending spam messages or malware in the name of the attack victim. Furthermore, the addresses stored in the contact book can become the target of spam, malware or social engineering attacks. If the published data are also access data for shops, social media or other platforms, an attacker could, for example, read chat history and obtain deposited credit cards or other personal information such as telephone number, address, etc.

Reaction

The BSI often receives pointers to identity data finds on the Internet, e.g. by law enforcement agencies or through its own surveillance. However, in most cases it is not apparent to what extent the discovered data are out of date or no longer relevant for other reasons. This is because the data often originate from different data leaks already published elsewhere and have been simply merged and passed off as “new”, resulting in large databases with several million entries.

Recommendation

The BSI recommends using the services of the Internet service providers to secure the accounts: many Internet services offer their customers additional security measures to protect themselves from uncontrolled access. Using two-factor authentication, for example, (usually mobile phone number or via app) to ensure that access can only be granted by the account owner. If you are informed that your data have been discovered, check the service for which this data was or is valid. Different services store data leaks published on the Internet and thus enable interested users to check whether their own e-mail address has already occurred in a leak. Various protection mechanisms can be used to protect digital identity in the network https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/ID-Diebstahl/Schutzmassnahmen/id-dieb_schutz_node.html. It is also helpful to use different passwords for each service https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html. It makes sense to use a password manager to manage the different access data more easily https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/Umgang/umgang.html.

back of the German ID card. Haptic features or even the security features that only appear in infrared or ultraviolet light cannot be checked remotely.

Within the scope of its security analyses, the BSI proved that it is already possible to create a forged ID card with standard equipment and use it to create the impression of corresponding individual, optically variable security features within the scope of a video transmission in real time. The mandatory countermeasures in place previously are no longer sufficient to prevent successful attacks or detect attack attempts, according to the latest findings.

Possible development of remote identification methods

The BSI has informed the responsible regulatory authorities about the changed level of threat and is working on the development of effective countermeasures in cooperation with the identification service providers. Based on past experience, however, it cannot be assumed that successful attacks at a high level can be prevented in the long term.

The BSI therefore recommends and promotes the use of more secure alternatives that meet the level of trust required for notified electronic identification systems. For example, the eID function of the ID card will be mandatory for all public institutions in the European Union from 29 September 2018 – particularly user-friendly with the mobile version of the ID card app. With the amendments to the Identity Cards Act introduced in 2017, the barriers for service providers to introduce the eID function have also fallen significantly, and guaranteed interoperability makes it possible to connect all eID systems notified abroad without additional effort.

1.4 Attack methods and means

Effective protection against cyber attacks is only possible if there is at least an overview of the general dangers in cyber space and the specific individual threat scenario. This knowledge is required to select suitable preventive and reactive measures and as the basis for the user's own risk analyses.

An essential component of cyber security is the defence against attacks. Due to the dynamic development of the cyber security situation, this aspect must be regularly and specifically reassessed. Attack tools and methods are easy and cheap to find and obtain. Time and again the latest findings on vulnerabilities in software and hardware are quickly exploited for cyber attacks. However, despite the large number of different attack targets and possible attack methods, trends and tendencies can be identified and that can be taken into account for successful defence.

1.4.1 Advanced persistent threats (APTs)

Advanced persistent threats (APTs) are targeted cyber attacks on selected institutions and organisations in which attackers gain persistent (long-term) access to a network and the spread the attack to other systems.

Compared to other security areas, APTs usually focus on the latest methods and developments, even if these are not necessarily representative of the overall situation.

The use of installer and update hijacking has increased in the initial phase of attacks. Installation archives with malware are placed on the websites or update servers of software manufacturers. When users download and install the programmes, an infiltrated malware programme is also run that can subsequently download additional modules.

This is an efficient method for the perpetrators because the users install the inserted malware (unknowingly) themselves and a larger number of targets can be compromised, depending on the type of legitimate programme. However, the latter feature also increases the probability that the campaign will be discovered by security companies. This path of attack can be prevented in the long term primarily by software manufacturers protecting their websites from attacks, signing the software and only storing the signature keys on isolated systems. Examples of installation hijacking attacks include Shadowpad, *NotPetya*, CCleaner, and two other legitimate programmes (an administration tool and a word processor). This approach is also sometimes referred to as a supply chain attack. Strictly speaking, however, this means that the perpetrators first attack suppliers of the actual target in order to then use its network accesses to reach the actual target network. This is another approach used currently by groups such as APT10 as part of the Cloud Hopper campaign.

In addition to these current trends, spearphishing e-mails with malicious links or attachments are still common in the initial phase of an attack. The links are either to malicious code or to phishing sites for access data of webmail mailboxes or VPNs. There have been several cases in the Middle East where supposedly legitimate smartphone apps were infected by malicious code in third-party app stores.

One of the later phase APTs is the lateral movement, in which the perpetrators spread within the affected network. The trend over recent years to work with the resources that are already available on the compromised computers is continuing here. The perpetrators use legitimate administration tools such as PowerShell and Windows Management Instrumentation (WMI). This makes their activities less conspicuous. Another trend is the use of publicly available tools which, unlike the administration tools, do not exist on standard installations. For example, several groups of offenders use publicly available versions of the penetration test tool Cobalt Strike independently of each other. This can be used as a convenient backdoor. Other publicly available tools are Powershell Empire and Koadic. This has two advantages for the perpetrators: on the one hand they save development effort, on the other hand it makes it harder to classify attacks.

However, this trend should not be exaggerated. According to the BSI, publicly available malware will never completely replace in-house programmes. Perpetrators continually have special requirements for carrying out targeted attacks as efficiently as possible; on the other hand, the use of known malware increases the probability of detection by security products. In response, groups of perpetrators are continuing to develop their own malware and use it in parallel with publicly available tools.

The only protection against APTs is a holistic security concept that includes some of the following key measures.

- Two-factor authentication for VPN and webmail is suitable as protection against phishing.
- Blacklisting document directories can make the initial execution of malware from mail attachments or the browser more difficult.
- Restricting communication between clients to functions that are absolutely essential makes lateral movement more difficult for the perpetrators.
- A layer model in the Active Directory ensures that highly privileged access data is not used on low-privileged systems, so that offenders require great effort to obtain highly privileged access data.

Organisations should consult professional and reliable specialist information in order to assess their own risk situation. The media is increasingly reporting attacks that have political relevance. The ongoing attacks on companies for the purpose of industrial espionage,

However, they receive little attention. Public reporting is not necessarily representative or comprehensive.

To defend against APT attacks, companies and institutions should ideally first implement general (perpetrator-agnostic) standard IT security techniques. It is important either to achieve a uniform level of security across locations and countries, or to consistently isolate network areas with different levels of security from each other. If the standard techniques have been implemented across the board, additional (perpetrator-specific) measures can be implemented if necessary, based on the industry-specific and region-specific level of threat. The following graphic provides an overview of the groups of perpetrators that are relevant in different industries.

Gov. organis.	Milit./armaments	Opposition	Media	Energy	Finances	Video conf.	NGO	Universities	High tech	Trans./logistics	Aeron. & aerospace	Health	Law offices
APT12/NumberedP. APT28/Sofacy APT29/CozyBear APT32/OceanLotus APT37/Reaper Bahamut BlueMushroom Cadelle/Chafer Callisto CharmingKitten DarkCaracal DarkHotel DroppingElephant EmissaryPanda ExtremeJackal Gamaredon GazaCybergang Greenbug HammerPanda Infy KeyBoy Lapis/TransparentTr. Longhorn LotusPanda Machete Micropsia MuddyWater Naikon/OverrideP. Leviathan OilRig OperationCleaver ProjectSauron Shamoon Snake Sowbug Tick TidePool/Ke3chang Tonto TransparentTribe TropicTrooper/PirateP. Vermin ViceroyTiger	APT28/Sofacy APT37/Reaper AridViper BlueMushroom Callisto CharmingKitten C-Major/PureStrike DarkCaracal DroppingElephant Gamaredon GazaCybergang HammerPanda HelixKitten LotusPanda Machete Naikon/OverrideP. Leviathan OilRig OperationCleaver ProjectSauron Snake	Ahtapot APT32/OceanLotus Bahamut BlackOasis Bookworm CharmingKitten DarkCaracal EnergeticBear FlyingDragon Group5 Infy Neodymium OperationCleaver Operation Manul Promethium ScarCruft Sima StealthFalcon SunTeam TemperPanda ZooPark	APT28/Sofacy APT32/OceanLotus Bahamut BlackOasis BugDrop Callisto CharmingKitten DarkCaracal DarkHotel DroppingElephant GazaCybergang Infy OlympicDestroyer Operation Manul Sandworm ScarCruft ShroudedCrossbow StealthFalcon SunTeam Tick	APT10 APT18/Wekby APT29/CozyBear CharmingKitten ElectricPowder EmissaryPanda EnergeticBear GazaCybergang Greenbug HelixKitten Kraken/Laziok Longhorn Machete MuddyWater OnionDog OperationCleaver Sandworm Shamoon TropicTrooper/PirateP.	APT18/Wekby APT29/CozyBear BlueMushroom DarkCaracal DroppingElephant EmissaryPanda EnergeticBear EquationGroup GazaCybergang HammerPanda Longhorn OilRig Sandworm	APT18/Wekby Codoso EmissaryPanda HammerPanda HelixKitten Longhorn Machete MuddyWater OilRig ProjectSauron Thrip	APT29/CozyBear APT37/Reaper Callisto CharmingKitten DarkHotel HammerPanda Honeybee Infy NilePhish OperationCleaver RocketKitten	APT10/menuPass BugDrop CharmingKitten Codoso DarkCaracal DarkHotel Greenbug DarkHotel Longhorn Leviathan RocketKitten	APT18/Wekby CharmingKitten Codoso LEAD/Winnti Tick	Cadelle/Chafer NanHaiShu OilRig OnionDog ProjectSauron Shamoon	APT28 DroppingElephant EmissaryPanda Leviathan HammerPanda Greenbug Longhorn	APT10/menuPass Leviathan LEAD/Winnti	APT29/CozyBear Codoso DarkCaracal DeepPanda Leviathan

Figure 06 List of APT groups that were active in various industries between 1 January 2017 and 31 May 2018 (source: BSI, evaluation of public reports)

1.4.2 Attacks on industrial control systems (ICS)

Production systems have frequently fallen victim to undirected attacks in the past year. In many cases, operator stations or other control components were infected by ransomware. This is not uncommon and not specific to Industrial Control Systems (ICS), yet nevertheless led to outages in the corresponding production systems, some of which lasted several weeks. Entry vectors were mostly, as in office environments, phishing mails or removable media. There were also cases where there was propagation as a result of incorrectly configured remote maintenance systems. The malware uses known vulnerabilities in outdated software and insufficient segmentation between office IT and production networks or within production networks to spread. This type of incident will continue to pose a significant threat to ICS in the coming years. This is partly due to very old systems for which there are no more updates or no approval for the available updates provided by the manufacturer or integrator/machine/plant constructor. Measures for the protection, also of existing plants, are given in the IT-Grundschutz modules for industrial systems and the ICS Security Compendium. Specifically, information is given on how to separate systems and segment the network in order to prevent unauthorised access.

Targeted attacks on ICS to manipulate them are the exception. At the end of 2017, the first documented attack on a safety system became known as TRITON. The aim was to reprogram a control system that was responsible for functional safety and thus the prevention of damage to people and the environment. This failed and the system was shut down to a safe state.

Exposure of existing systems is rising due to the increasing networking in the context of digitisation. Many

Triton – cyber attack on the safety system of an industrial plant in the Middle East

Situation

On 14 December 2017, FireEye and Dragos released a report (https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html; https://dragos.com/blog/trisis/TRISIS-01.pdf) describing the attack on a Safety Instrumented System (SIS) of an industrial plant in the Middle East. On the same day, Dragos confirmed the incident in a report (https://dragos.com/blog/trisis/TRISIS-01.pdf) that named the Middle East as the location of the attacked facility. SIS are designed to protect people, plant and the environment and are therefore subject to special functional safety requirements. In industrial automation systems, which are also used in critical infrastructures and the process industry, SIS are normally set up separately from the control system, i.e. they observe and only intervene when required. There are currently three names for the malware used: FireEye uses the name *Triton*, Dragos calls it *Trisis* and the NCCIC (formerly ICS-CERT) *HatMan*.

Cause and Damage

The attackers first gained access to the victim‘s IT servers. They then moved mainly through the Demilitarised Zone (DMZ) of Operational Technology (OT) and the computers of OT to the SIS network using tools developed in-house. The engineering workstation there, i.e. the computer used for programming the safety controllers, was infected. The forensic artefacts detected during the analysis suggest that the attack had been prepared for a long time and the attackers were in possession of or had access to a structurally identical safety controller. The individual safety controllers were then infected from the infected computer. The attack was two-stage: first, additional code was appended to the regular application programme, which obtained the required extended rights. In a second step, the firmware of the safety controller could be changed and a non-persistent Remote Access Trojan (RAT) installed. The attack process was favoured because the key switch, which was intended to protect against a change in the memory contents of the Safety Controller, was in “Programming” status. As a result, the first step was permitted. However, in the course of the attack, a validation of the application programme between the independent, redundant processors failed for at least one safety controller. An error status was then detected and the safety system switched the system to a safe state, i.e. despite manipulation of the control programme, the devices were able to fulfil their function.

Reaction
The plant operator concerned then initiated an investigation in which both the manufacturer of the safety controllers, Schneider Electric, as well as numerous analysis companies and the NCCIC were involved. The study was followed by a coordinated publication on 14 December 2017. The BSI then sent a cyber security warning to the operators of critical infrastructures presenting and evaluating the facts with recommended measures. A broad discussion of the incident among experts took place at the S4x18 in Miami, which was also attended by a representative of the BSI.

Recommendation
Attacks on safety systems pose a serious threat due to their potential impact on people and the environment. Although Triton has been tailored for certain firmware versions of Schneider Electric‘s Triconex 3008 model, the release of the framework has lowered the threshold for such attacks. It can be assumed that attacks on SIS from other manufacturers will also take place in the near future.

The BSI therefore recommends that the SIS network is operated completely separately from the OT network and the Internet. The operators should check whether the protection options already integrated in the safety system of the application programme and its parameters are activated to an appropriate extent. In particular, any physical protection against changes to the controller that may be present on the device should be activated. This may only be switched off during programming or configuration of the controller, which should also be signalled automatically in the control room.

As practical recommendations, the BSI has published the basic protection module “Safety Instrumented Systems” and other modules for the safe operation of industrial plants https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html. It is also recommended that the OT network is separated from the IT network as effectively as possible and a defence-in-depth strategy is pursued. In addition to monitoring the IT network, this also includes the establishment of IT security in the OT network. The BSI also provides Snort rules for the TriStation protocol for monitoring communication in the SIS network. https://www.bsi.bund.de/RAPSN_SETS

Furthermore, the User Association of Automation Technology in Process Industries (NAMUR) has developed a method for IT risk assessment of process control and instrumentation safety equipment with worksheet 163 https://www.namur.net/de/arbeitsfelder-u-projektgruppen/af-4-betrieb-und-instandhaltung/ak-418-automation-security.html, which is subject to a fee. A concrete assessment checklist is freely available at www.namur.net/fileadmin/media_wwww/Dokumente/AK-PRAXIS_4.18_NA163_Checkliste_DE_2017_12_15.xlsx.

systems are operated with outdated software. Attackers can use existing attack tools, which considerably reduces the effort. It can be assumed that initial attacks with no specific know-how of the production process will increase. With increasing knowledge on the attacker side, targeted manipulations of machines or systems that have an influence on the process or the products will also increase.

The progressive introduction of Industry 4.0 also offers new starting points for criminal activities for attackers. In conjunction with the increasing exposure, the protection and trustworthy operation of ICS represents an important challenge and plays a key role in the further success of the digital transformation.

1.4.3 Botnets

By using botnets, cyber criminals can access foreign computer systems on a large scale to steal personal data or misuse resources, such as computing power or network bandwidth, for criminal purposes. It is not necessary to set up your own botnets to do this. Professionalism in the cybercrime environment means that even technical amateurs can fall back on ready-made solutions and rent botnet capacities comparatively simply and cheaply.

The malware used on the client side is usually designed modularly and has the option of flexibly downloading individual functionalities from the command and control server (C&C server) at a later point. This allows a botnet to dynamically change or extend its purpose.

During the reporting period, botnets were mainly used for information theft, distributed denial-of-service (DDoS) attacks on computer systems, and for sending spam and distributing malware. What is striking in 2017/2018 is the increased emergence of IoT botnets that compromise Internet-capable home electronics and misuse them as bots.

During the period of this report, security researchers registered up to 10,000 bot infections in German systems daily and reported them to German Internet providers via the BSI. The providers then inform their customers about the infection and in some cases also offer assistance in cleaning up the systems. Detection takes place using sinkhole systems, which receive contact requests from bots instead of the regular command and control servers. The level of visible infections is influenced by various factors such as the selection of the observed botnets and the associated control domains and therefore varies greatly. Based on experience from successful botnet shutdowns, it can be assumed that the number of unreported cases is significantly higher and the total number of infected systems in Germany is at least in the six-figure range.

Focus on IoT botnets

Networked devices and assistants in the Internet of Things have a large attack surface that cyber criminals have been actively exploiting for years (see Chapter 1.4). In addition to attacks on the availability of the devices, complete control of the compromised systems is also possible through customised malware. The acquired devices are merged into a botnet, which receives its commands from a central location. Due to the modularity of current malware, the functions required by the bots, such as components for information theft or spam distribution, can be flexibly downloaded subsequently. IoT bots typically have worm functionality and are therefore able to find and infect other potentially vulnerable systems.

One of the first IoT-specific malware programmes to be discovered in January 2012 was the malware known as *"Linux.Aidra"*. This spread actively via insufficiently secured telnet logins and received the functionality to generate bitcoins in a later version. At the time, security researchers found a large number of infected end devices of different device classes such as home routers, televisions, TV receivers, DVRs, VoIP devices, IP cameras and media centres. In the following years there were a large number of other larger IoT botnets that were primarily used to generate cryptocurrencies and to execute DDoS attacks; but these were primarily only noticed by security researchers.

In August 2016, the *Mirai* botnet received great media attention with massive DDoS attacks of unprecedented bandwidth. The IT security blog https://krebsonsecurity.com written by security researcher Brian Krebs was hit by a massive DDoS attack with about 620 gigabits per second, for example. The publication of the *Mirai* source code in autumn 2016 has since led to the development of numerous *Mirai* variants that contain additional functionalities. In the period under review, the *Mirai* successors *IoT-Reaper, Satori* and *Okiru* attracted particular attention. These variants use advanced dissemination methods by employing specific exploits to maximise potential target system vulnerabilities, in addition to simply trying out passwords for the Telnet service. In the case of *Okiru*, ARC processors were used to attack another target platform that had not previously been the focus of IoT malware.

Apart from *Mirai*, new IoT botnets such as HNS (*Hide 'N Seek*) have also come to light, which bring with them new, unique features. Thus the HNS bot could permanently anchor itself on a part of the infected systems and survive device restarts.

These examples show that there is continuing development in the area of IoT malware programmes and existing functionalities for compromising and exploiting vulnerable systems are constantly being expanded and refined. As the number of IoT devices connected to the Internet continues to increase incessantly, the target area for attacks is also widening. Even though these botnets are reported to have high infection rates in the six-figure range, the direct impact in Germany is low. This is due to the fact that Internet access for end customers is typically via home routers, which seal off the internal network from the Internet and any existing IoT devices in the home network cannot be accessed directly from the Internet without the end user's active involvement. Nevertheless, this does not protect against the threats indirectly posed by IoT botnets such as DDoS attacks or spamming.

Abuse of *memcached* instances for DRDoS attacks

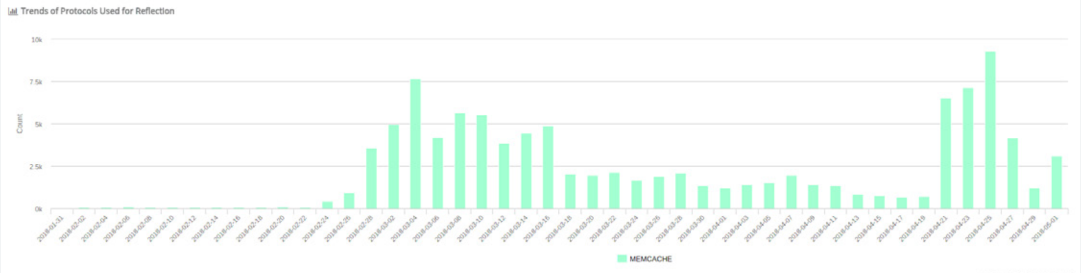
Situation

Memcached is an open source cache server for easy storage and retrieval of data from the memory. It is often used in conjunction with web applications. Since the beginning of 2018, *memcached* instances that can be accessed openly from the Internet have been widely abused for DRDoS attacks. In these attacks, *memcached* is accessed via UDP instead of TCP. Accessibility via UDP was included in the standard configuration up to and including version 1.5.5.

Cause and Damage

For common protocols that are abused for DRDoS attacks (such as DNS or SSDP), the amplification factor can reach values slightly above 50. With *memcached*, the factor can be 51,000. An attacker can therefore generate an enormous bandwidth for an attack with just a few small queries. Using *memcached*, for example, a new record for DDoS bandwidths was set at 1.7 Tbps.

It is therefore unsurprising that *memcached* has been very popular with attackers since this feature became known: The misuse of UDP-based protocols for DRDoS attacks is not, however, new.



Quelle: ddosmon.net

Figure 07 memcached

Reaction

The BSI has been informing German network operators about openly accessible *memcached* instances in their networks since the beginning of 2015. Up to now, the focus of the information provided by the BSI has been on the accessibility of instances via TCP.

At the end of February 2018, the BSI expanded its notifications to include *memcached* instances that are openly accessible via UDP. All major German hosting providers reacted quickly, so that the number of *memcached* instances that can be used for attacks in Germany shrunk from more than 2,700 initially to less than 130 (as of 31 May 2018). Nevertheless, the all-clear cannot be given, as numerous instances are still available worldwide and continue to be used for attacks.

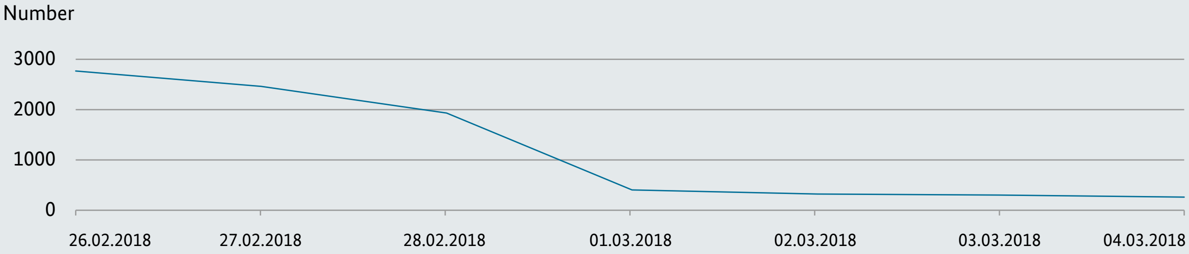


Figure 08 Rapid decline of open memcached instances in the first week of notifications

Recommendation

Accessibility via UDP is not absolutely necessary for memcached to function. This should be checked on your own systems and switched off if necessary https://www.bsi.bund.de/EN/Topics/IT-Crisis-Management/CERT-Bund/CERT-Reports/HOWTOs/Open-Memcached-Server/open-Memcached-server_node.html. In principle, *memcached* instances should not be accessible from the Internet.

Focus on Android

The reported infections were distributed among more than 130 different botnet families during the reporting period. It is noticeable that more and more botnets are targeting Android systems (approx. 25%) compared to the same period last year, while the remaining bot infections are predominantly on Microsoft Windows systems. The following graphic shows a distribution of the versions of infected Android devices using a sample at the end of May 2018. The botnet families that transfer the operating system used by the victim system to a sinkhole server are used as the database.

A closer look at the botnet families shows that they all have the functionality to extract information such as International Mobile Equipment Identity (IMEI), International Mobile Subscriber Identity (IMSI) or location and also to subsequently download other malware. Some of the families access data for online banking or are able to send high-priced premium SMS.

The majority of Android infections can be traced back to malicious apps obtained from third-party sources. However, besides the active installation of dubious apps, infections are also possible without the user's intervention. For example, many manufacturers of Android systems ship the devices ex works with an outdated software installation; if there are any security updates, they are only available temporarily. As they become older, these devices offer a larger attack surface due to the increasing number of existing vulnerabilities. Thus, the majority of infected systems (> 40%) still run with a version of Android 4, which has not been supported by Google for some time. Current variants such as Android 7 are only represented in 3.7% of cases. Infected Android 8 systems make up the smallest share with approx. 0.2%.

As in previous years, the infected operating systems also include Linux-based web servers and occasionally compromised systems based on Mac OS X.

The level of threat situations remains high

Current developments show that the threat posed by botnets remains high. Until a few years ago, attackers primarily focused on traditional computer systems (often based on Windows) but a reorientation towards mobile end devices and devices from the Internet of Things is now evident. The attackers are thus adapting to current market developments and expanding the spectrum by several million potential victim systems.

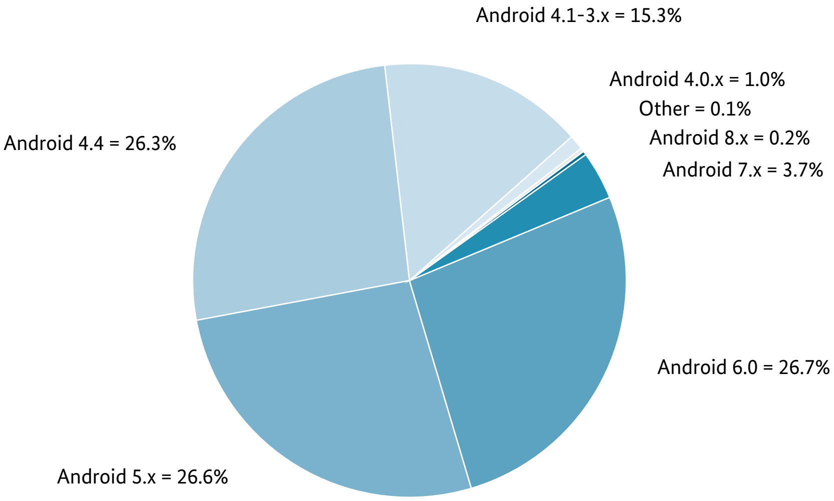


Figure 09 Versions of infected Android systems, Source: BSI, 22 May 2018

As early as 2016, the IoT botnet *Mirai* impressively illustrated the threat posed by the Internet of Things in this context. The reported high occurrence of further IoT botnets with botnet capacities in the six-figure range further increases the probability of occurrence and the potential impact of DDoS attacks.

Avalanche: extension of protection measures

One year after the dismantling of the world's largest botnet infrastructure, Avalanche, which was initiated on 30 November 2016, the BSI has enlarged and extended the protection and information measures. Analyses had shown that despite being notified by Internet providers, a large number of infected systems still exist: In Germany, the number of infections found has fallen by 61 percent after one year, which is a great success compared with the global trend (a reduction of 45 percent). On the other hand, this does mean that many affected users have still not cleaned up their systems.

In addition to extending the measures, the sinkholing system set up in the course of the Avalanche shutdown was extended to include domains of the Andromeda botnet. Analyses have shown that a very high number of systems worldwide were infected, particularly with the Andromeda malware. The main targets of the malware known as Andromeda or Gamarue have been identified in Asia, North America and in Europe, particularly in Romania, Italy, Germany and Poland. This global botnet was broken up by investigators in an international collaboration on 30 November 2017. The European judicial cooperation unit Eurojust coordinated the activities of the public prosecutors involved worldwide. The Luneburg Central Criminal Investigation Inspectorate was responsible in Germany, under the direction of the public prosecutor's office in Verden.

By extending and expanding protection measures, systems with active infections continue to connect to the sinkhole servers and no longer receive control commands. Information on the infections recorded at the sinkhole for German IP addresses is made available to the relevant Internet providers, who use this as a basis for informing their customers. Information on affected foreign IP addresses is forwarded via CERT-Bund to the relevant national CERTs (Computer Emergency Response Teams) in over 80 countries worldwide, so that users affected there can also be informed.

On 5 December 2017, almost 1.5 million infections were detected and reported worldwide in a single day. After six months, the daily notifications in Germany show a decline of 35%. A drop of 42% has been observed globally to date.

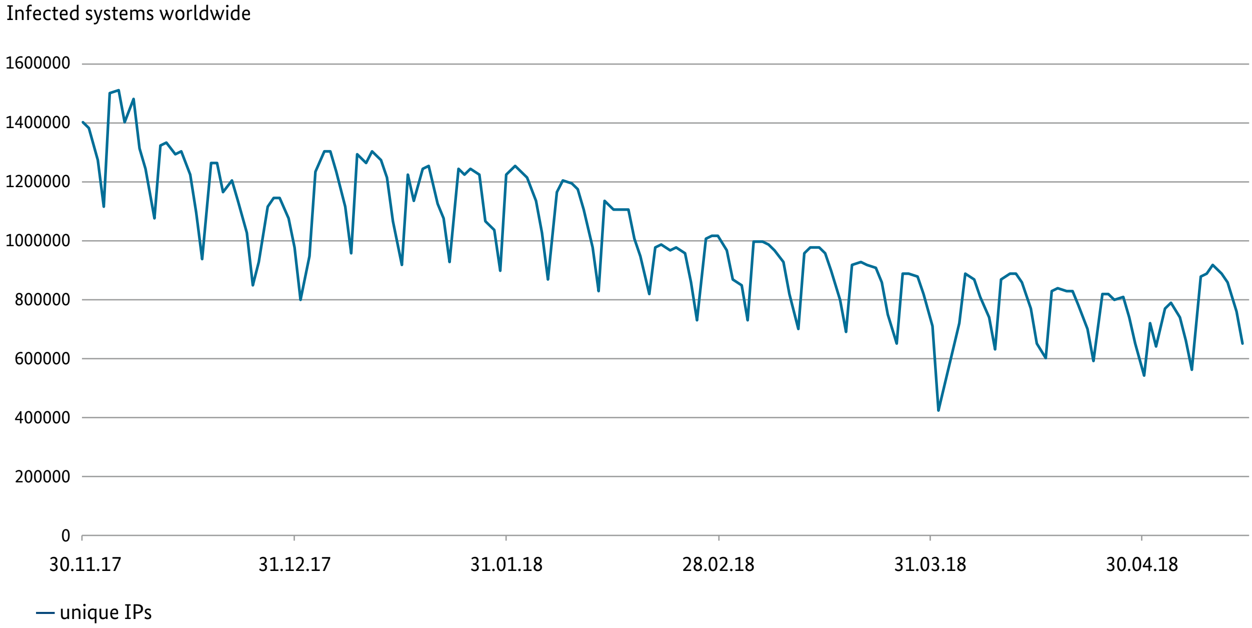


Figure 10.1 Infected systems

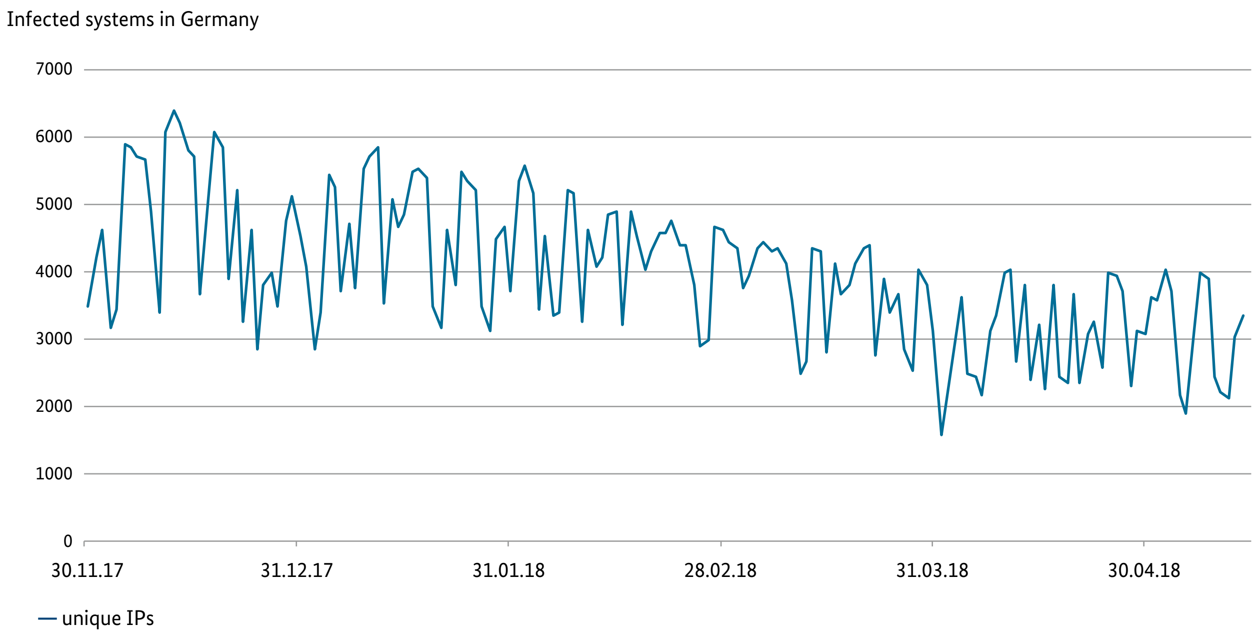


Figure 10.2 Infected systems

DoS attack on VPN router of a KRITIS operator

Situation

An operator from the KRITIS water sector reported a problem with VPN routers to the BSI. The devices were apparently vulnerable to a Denial of Service (DoS) attack. An existing IPsec connection could be interrupted by an attacker at any time. The operator received an error message in the control centre because measured values were reported missing and could no longer be controlled remotely.

Cause and Damage

The IP addresses of the VPN router were scanned from a university in the US and successfully attacked. For a short period of time, no measured values of the pumps were available in the control centre of the KRITIS operator. According to the operator, there was no impairment of critical supply services. However, the problem could recur at any time.

Reaction

The operator contacted the router manufacturer. The manufacturer acknowledged the existence of the vulnerability, but made no statement as to whether or when the vulnerability could be expected to be rectified.

When the BSI asked the router manufacturer for support, it created a firmware update. The BSI informed the public about its release by publishing information for managers.

Recommendation

Access to devices that need to be accessible from the Internet should only be possible from certain IP addresses (white list). The BSI continues to provide support in contacts with manufacturers.

The extension of the protection measures for a further year until 30 November 2017 took account of approximately 848,000 botnet domains so that the infected systems cannot be controlled by criminals. After the expiry of the protection measures on 1 December 2018, full coverage of all botnet domains will no longer be possible, as only freely available domain names can be used for sinkholing measures without judicial decisions. Warnings to users with infected systems that connect to sinkholes should continue afterwards. However, domain names that have already been assigned and registered will no longer be accessible, but there is a danger that criminals will regain control over infected computers.

1.4.4 DDoS attacks

Media reports about distributed denial of service attacks with record bandwidths remain high in 2018. In February 2018, attackers discovered that very high amplification factors could be achieved by using memcached (see Incident Box memcached). Arbor Networks reported an attack with a bandwidth of 1.7 Tbps (1700 Gbps). Attacks of this magnitude are a serious threat. Up to now, however, these attacks are exceptional. In the first four months of 2018, only 0.16% of the attacks known to the BSI in Germany exceeded 100 Gbps. The majority of DDoS attacks still have a bandwidth of less than 1 Gbps. While the maximum deflections for bandwidth, packet rate and duration vary greatly, the average values are largely constant. However, there has been an increase in the number of attacks. Appropriate measures can be taken to protect against the effects of most DDoS attacks. The BSI has compiled information on this on a topic page: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Informationspool/Themen/DDoS/ddos.html

However, 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 at application level, such as TCP connections or HTTPS requests, can cause significant damage even with low bandwidths and low packet rates.

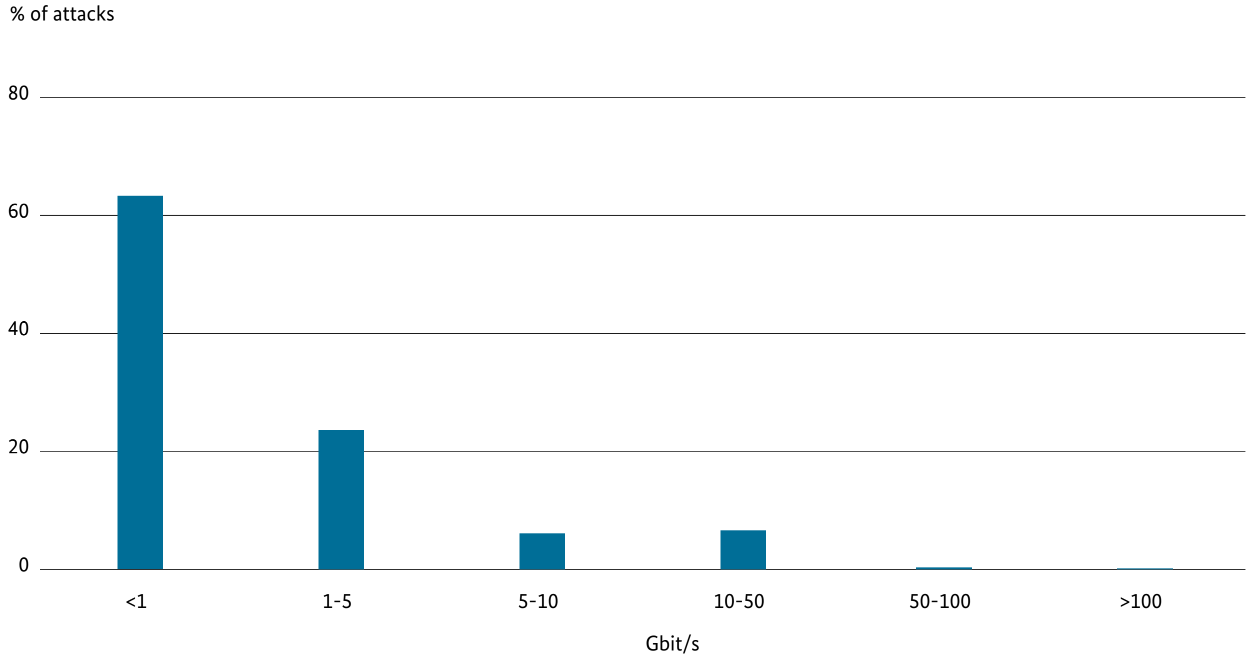


Figure 11 Distribution of attacks by bandwidth (1 January to 30 April 2018)

1.4.5 Cryptography

Cryptographic mechanisms are the basic building blocks for the effectiveness of many IT security products. State-of-the-art cryptography, such as the symmetric encryption method AES or the asymmetric Diffie-Hellman key exchange, provide excellent security guarantees. The BSI recommends a series of cryptographic algorithms and protocols in its Technical Guideline TR-02102, which are generally regarded as secure, based on the mathematical analyses (cryptanalysis) received. However, a number of assumptions are made with these analyses. For safe use in practice, it is important to verify that these assumptions are met and ensure further safeguards where necessary.

Various aspects can cause a cryptographic system to fail. These can include:

- Security holes in the hardware (e.g. *Spectre* and *Meltdown*)
- Errors in implementations
- Errors at protocol level
- Use of outdated standards (e.g. ROBOT, see box)
- Weaknesses in key generation (e.g. ROCA, see box)
- Insufficient random number generators.

A typical example is a device that encrypts data with a secret key. There are a number of common procedures for this and it is generally assumed that an attacker with access to the encrypted data will be unable to calculate the secret key or the plain text. However, if the attacker has network access to the device or is in close proximity, he can try to collect information about the secret data by observing the device behaviour in terms of calculation times, power consumption or electromagnetic emissions. These side channel attacks have been included in the security considerations for IT systems for a long time. Intensive research on this subject has produced a series of countermeasures and new attack vectors. The latest development is the use of Machine Learning (ML) techniques to recognise patterns in measurement data. Known as pattern recognition, data mining or artificial intelligence, ML has become a standard tool in other IT areas but ML attacks have yet to be established within the security considerations of IT systems.

Another prerequisite for the use of cryptography, which is very important in practice, is the generation of random numbers that meet certain quality criteria. The large number of products with a physical noise source certified in line with the German CC scheme is worth mentioning here. Due to the structural reduction of semiconductor products and the ever-increasing performance at low power consumption, newer products have integrated cryptographic post-processing of the random numbers, which completely prevents the theoretical exploitation of the already very small remaining statistical weaknesses of physical noise sources.

Post-quantum cryptography

However, the security guarantees of the cryptographic mechanisms used today apply at most until a “sufficiently large” quantum computer is available (measured in the number of entangled logical qubits). Since the 1990s, quantum algorithms have been known that approximately halve the security level of classical methods (Grover algorithm for symmetric cryptosystems) or completely break these methods (Shor algorithm for asymmetric cryptosystems). Another quantum algorithm of Brassard, Hoyer and Tapp finds a collision of an n-bit hash function after about 2^(n/3) steps.

Post-quantum cryptography offers an alternative. These are cryptographic mechanisms based on mathematical problems that probably cannot be solved with a quantum computer. However, there is no proof of the quantum computer resistance of these methods. As a result of the increasing probability that a quantum computer of sufficient size can be realised, research and standardisation activities in the field of post-quantum cryptography have increased massively in recent years (see Section 2.4). An important task for the BSI in the coming years will be to actively support these activities and implement its own projects.

Quantum computers: development status

In order to obtain a sound assessment of the current development status and the potential future availability of a quantum computer, the BSI commissioned the study “Development of Quantum Computer” from researchers at Saarland University and the Florida Atlantic University. In concrete terms, the report examines current technological approaches and quantum algorithmic innovations in detail and discusses their implications in the context of public-key mechanisms currently in use. The study and a summary can be downloaded from the BSI website at http://www.bsi.bund.de/qcstudie

ROCA

In November 2017, Czech researchers published a vulnerability in RSA key generation used in a cryptographic library provided by smart card manufacturer Infineon under the title „Return of Coppersmith‘s Attack" (ROCA). For RSA encryption or signature two secret, large (e.g. 1024 bit) prime numbers are required whose product forms the publicly known RSA module. Infineon‘s affected library generates prime numbers with a very special structure. This means that the primes generated in this way can be reconstructed from the public module using a method developed by Don Coppersmith in the 1990s. The special shape of the prime numbers is also transferred to the module, making it possible to quickly determine whether a public RSA key was generated in this way and is therefore vulnerable.

ROBOT

The acronym ROBOT stands for „Return of Bleichenbacher‘s Oracle Threat". The attack published by Hanno Böck, Juraj Somorovsky and Craig Young in December 2017 describes a vulnerability in current TLS implementations that uses RSA encryption in conjunction with an outdated padding procedure (PKCS#1 v1.5). The attack originally described by Daniel Bleichenbacher is already 20 years old. Bleichenbacher had used TLS error messages as oracles to determine whether the padding of a message was correct or not. Using an adaptive chosen-ciphertext attack, he was able to successively decrypt encrypted messages. As a result, the TLS standard contained recommendations on how implementations can be protected against the Bleichenbacher attack. The authors of ROBOT have shown that a large number of TLS implementations are still vulnerable.

1.4.6 Ransomware

The term ransomware includes malware that denies or restricts access to a computer, or pretends to do the same. Such software promises in a text message to release the resources again when a ransom is paid.

A distinction should be made between the following variants:

- Ransomware that blocks access to or use of the system by manipulating the operating system and instead displays the text with the request (lock-screen).
- Ransomware that encrypts user data in the form of files of certain formats and offers the prospect of decryption after payment of the ransom money. Encrypted files include a variety of formats for text, audio, video and presentation content, but also for spreadsheets and databases, which usually have a high value to the user. The general operability of the system is normally not affected.

Ransomware is now circulated through various attack vectors:

- Spam mails with malware that is attached or referenced via URLs.
- Drive-by exploits use vulnerabilities in browsers, browser plug-ins or operating systems that are triggered by accessing an infecting web site or advertising placed on it (possibly without further interaction by the user).
- Exploit kits that manage various vulnerabilities in different products and make both the type of attack and the transport of the malware available to the perpetrator at the touch of a button.
- Exploiting vulnerabilities or guessing weak passwords in publicly accessible web servers. There is also software for spying out additional passwords in the internal network.

- Vulnerabilities in remote administration tools (RATs) are also used to access the systems to be maintained. This often means that the attacker is equipped with extensive rights from the outset.

- After the target system has been infected, the malware sometimes uses vulnerabilities in the operating system to appear as a legitimate process and avoid early detection.

Ransom payments are often made in digital (virtual) currencies such as bitcoin and ethereum or via anonymous websites in the Tor network to make prosecution more difficult.

Threat development

There has been a sharp increase in the risk associated with ransomware since 2016. We cannot forget, particularly, the major ransomware campaigns from 2017 such as *WannaCry* and *NotPetya/ExPetr*. The latter was probably more an act of sabotage than real ransomware, as the people concerned did not receive any blackmail messages and users were not given the opportunity to decrypt the encrypted files.

Recent incidents in 2018 have not reached the public to the same extent as previous attacks, but point to various developments:

- On 26 January 2018, a new blackmailing software called *GandCrab* was discovered for the first time. In addition to locally active campaigns (Magniber), it is the first to be widely distributed via an exploit kit.

- The *SamSam* ransomware attacks via vulnerabilities in publicly accessible software components (web servers) or by guessing weak passwords in the user management. The city of Atlanta, Georgia (USA) was attacked with this ransomware on 22 March 2018 and large swathes of external and internal services paralysed.

- Ransomware *XiaoBa* also contains software that operates coin mining (or cryptocurrency mining), i.e. changes executable programmes so that they take over infrastructure tasks for cryptocurrencies and thus earn (secure) money.

- In April 2018, ransomware was observed that does not require ransom money but encourages people to play computer games.

- The ransomware *RanSIRIA* claims to use the ransom money to support Syrian refugees.

- Also in April 2018, ransomware used vulnerabilities in *HPE Integrated Lights-Out* to blackmail bitcoin payments.

- The ransomware *SynAck* was the first spotted using a technique called “Process Doppelgänging” in May 2018. Various other techniques are also used that make both detection and analysis more difficult (deleting protocols, computing jump addresses, using a hash instead of the original string).

These incidents and other information from the IT security industry point to the following developments:

- Similar to the botnet services available for DDoS attacks, there are now Ransomware-as-a-Service offerings. The service user no longer has to understand all details of the attack vector and can use a modular approach to create variations of existing ransomware. Contract work for special properties is also possible. This makes it easier for a larger group of attackers to perform individual attack scenarios.

- There are signs of fragmentation in the ransomware families. This does not necessarily make individual attacks more dangerous for the entire population or the entire economy, but contributes to a confusing threat landscape, which makes it harder than ever to exclude serious consequences. In addition to the attack procedures becoming more and more complex, the precautions for concealment or to prevent detection by AV software are becoming more and more sophisticated. Malicious processes are disguised as operating system processes, traces in the form of log entries or required intermediate files are deleted and jump addresses are outsourced or only generated in the calculation process, making forensics more difficult.

- The target groups and individuals are diverse. Individual users are less in the spotlight as ransom payers than they were in the past, as monetisation seems more difficult here. The demands vary with a business-like view of the monetary power and the relevant values of the computer contents. New target groups are being sought, e.g. potential players as buyers or possible victims for other online players or persons who are receptive to social issues. Regardless of whether the claim to use the ransom for refugees, for example, is true or not, there is a strong innovative power at play here to increase the target area.

CEO fraud – BSI warns companies specifically against acute risk

Situation

CEO fraud is the term used to describe social engineering attacks in which the fraudsters pass themselves off as the chief executive officer or board member of a company. The attacks, which usually take place via e-mail, specifically address employees of the finance departments of companies and attempt to get them to transfer large sums of money from the company‘s business account to a foreign account. The victims are often put under time pressure and instructed to maintain secrecy, as this is supposedly a secret or confidential company project.

Cause and Damage

The contact details of the target person and the bogus sender are often obtained through publicly available information on the company‘s website, in online career portals, in social networks, in commercial register entries or even through direct calls within the company. The attackers use this information to credibly imitate the content of the e-mail and the style of communication in the company and to trigger the recipient to transfer high sums of money. According to the Federal Criminal Police Office (BKA), damages in the multi-digit millions have been caused by CEO fraud in recent years.

Reaction

In July 2017, as part of an investigation into organised crime, law enforcement authorities succeeded in obtaining a list of around 5,000 potential targets for CEO fraud attacks. This list was sent to the BSI to warn those potentially affected. On 10 July 2017 the BSI published a press release on this subject https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2017/CEO_Fraud_10072017.html. The people and companies who were potential targets were also informed directly. Some companies confirmed that they had recently fallen victim to CEO fraud attacks. A sample conducted by the BSI showed that many of the target persons on the list had profiles in career portals or social networks in which the name of the company and the employee’s position in the finance department were detailed.

Recommendation

The public disclosure of company contact information should be limited to general contact addresses. Companies should raise employee awareness of this and other digitisation risks and provide regular training on the safe use of IT. In the case of unusual payment instructions, control mechanisms should kick in before the payment is initiated. The request for payment should be verified by callback or written inquiry with the alleged client and the sender address and the plausibility of the contents of the e-mail should be checked carefully. The management or the line manager and the IT security officer should be informed of any such attacks. Companies affected by (attempted) CEO fraud attacks should file criminal charges.

The Federal Criminal Police Office (BKA) has compiled a brochure with further information and recommendations https://www.bka.de/SharedDocs/Downloads/DE/IhreSicherheit/CEOFraud.html.

- At the same time, there are signs of diversification in the attack vectors. Different families spread via spam, exploit kits, drive-by exploits, worms, remote maintenance software. Ransomware seems to decrease to the extent that other models – such as cryptocurrency mining – are more financially worthwhile or promise more constant profits. On the other hand, changes in the initial situation could, conversely, lead to an increase again, such as falling exchange rates for cryptocurrencies or the higher willingness to accept ransom payments, since not only the withdrawal of data but also its publication can have unpleasant and expensive consequences.

As a measure against ransomware attacks, regular, external backups (including recoverability tests) are essential. However, the connection to the backup medium should not be permanently writable, or the ransomware can also encrypt the backup. Updates for operating systems and applications should be installed regularly and promptly. It is also important to be extremely careful when dealing with e-mails and links from unknown sources. Maintaining vigilance (awareness), updates and backups should be a matter of course. Due to the newer distribution channels for ransomware and the focus on “more valuable victims”, however, strict password guidelines must apply for publicly accessible endpoints and remote access must be reduced to a minimum (both in terms of time and number of accesses) and explicitly authorised. The server software used must also be subjected to particularly intensive monitoring with regard to its vulnerabilities and exposure.

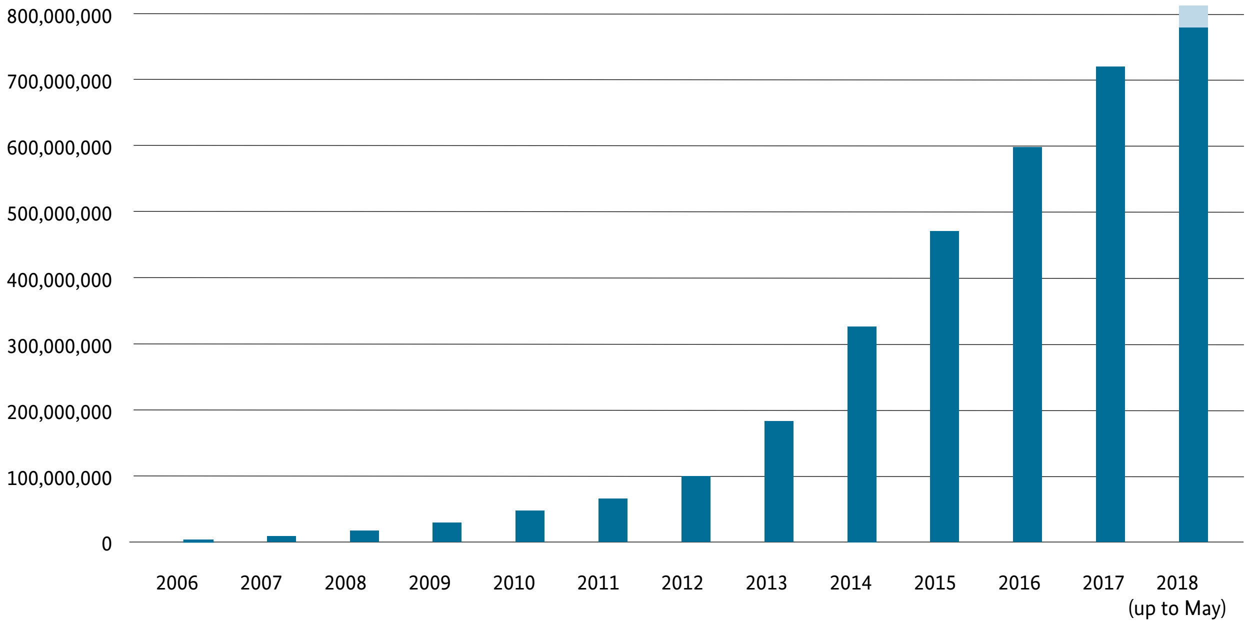


Figure 12 Known malware (2018 up to May), source AV-Test

1.4.7 Malware

Malware refers to all types of computer programmes that perform unwanted and malicious functions on a computer system. The terms Trojans, viruses, worms, etc. are usually used synonymously for all types of malware. Malware is an integral part of most attack scenarios – for example, when a client is infected by ransomware, in botnets and in APT attacks.

In the reporting period, the IT security company AV-Test (https://www.av-test.org/de/) observed an average of around 390,000 new malwareprogrammes per day.

In addition to malware for PCs, an average of approximately 690,000 new malware programmes for the Android mobile operating system were observed per month during the reporting period (source: AV-Test). The number of malware programmes for Android is expected to rise to over 30,000,000 in 2018.

Paths of infection

In the reporting period, there has been an increasing change from the path of infection via an e-mail attachment to e-mails in which the e-mail text contains a link to malware. This way, the malware is not stored directly on the mail server, where appropriate security measures could detect and remove it; instead, the malware is transported directly to the client. This can be done either by downloading the malware and running it manually or by using a drive-by infection.

Cryptocurrency mining

A current trend is the upsurge in software used to 'mine' crypto currencies. These 'crypto miners' use the resources of the affected systems to generate monetary gains in the form of cryptocurrencies. These systems then become part of a network which jointly provides a computing and resource-intensive service in the area of block chain calculations (validation of transactions) and is reimbursed for this service in the form of cryptocurrencies. A distinction must be made between voluntary and involuntary (hidden) mining. In the first case, the user voluntarily provides the computing power of his system. Different methods have been observed in the hidden use of these techniques:

- Crypto miners force visitors to a website to participate in the mining with the help of JavaScript libraries, which are executed by the browser.
- Malware that allows affected systems to mine cryptocurrencies as part of a botnet.

In addition, criminals use existing malware to steal the mined or otherwise obtained cryptocurrency from users by spying out the access data for storing this currency (known as crypto wallets).

Cryptocurrency mining can take place on a wide variety of devices and systems. In addition to normal PCs, incidents were also observed on servers, mobile operating systems, smart TVs and ICS during the reporting period. Company servers in particular offer very attractive targets for criminals due to their usually larger resources and the constant availability of these resources. It can be assumed that further targets and platforms will be used in future (e.g. webcams, smart home devices) and these should also be monitored with regard to criminal use. This is especially the case since crypto miners often remain undetected in affected systems for a long time – other than declines in performance and possibly increased power consumption, their behaviour remains inconspicuous. These "abnormalities" are usually so marginal that they are not suitable indicators.

Threat remains critical

As in previous years, malware continues to be one of the biggest threats to consumers, businesses and public agencies in the current reporting period. This was also shown in the 2017 Allianz for Cyber Security Survey, in which malware infections were again named as the most common type of attack.

1.4.8 Vulnerabilities in chips

Security elements store key cryptographic material and implement numerous algorithms. They serve as anchors for security-critical applications such as secure authentication, encrypted communication or electronic signatures.

The algorithms used are usually tested and sometimes even mathematically verifiable. However, the secure storage of the key and in particular the processing of key material remains major challenge, as measurable physical phenomena inevitably arise that allow conclusions to be drawn about the key.

With older chip generations, for example, the content of the ROM could be read simply with the aid of a digital microscope, since a stored ‘1’ is optically significantly different from a ‘0’. Measuring the power consumption during processing can also be used to attack a key, as the power consumption varies depending on different bit sequences. Although today’s security elements implement numerous countermeasures against such side channel attacks that make attacks significantly more difficult, multiple research findings also show the attack techniques have improved. While side channel attacks are relatively easy to implement, invasive attacks on the hardware, in which physical manipulations of the chip, for example by error induction through laser bombardment or even modification of the circuits, are not widespread due to the associated effort.

Algorithmic weaknesses are another problem. Although the methods used have been tested, sometimes cryptographically secure algorithms cannot be implemented due to the limited computing and storage capacity of security elements.

Key Reinstallation AttaCK (KRACK) on WLAN vulnerability

Situation

In October 2017, security researcher Mathy Vanhoef published a research paper describing an attack on the Wi-Fi Protected Access protocols (WPA, WPA2) called the Key Reinstallation AttaCK (KRACK). WPA2 is the current security standard for wireless networks, which is integrated in almost every WLAN-enabled device. The underlying vulnerability is a design flaw in the IEEE 802.11i standard whose security features have been implemented in WPA2.

Cause and Damage

The current IEEE 802.11i security standard has defined a multi-level handshake procedure as a network authentication protocol that provides greater security for setting up and using WLANs. The steps of the four-way handshake procedure consist of a communication between client and access point, in the context of which important crypto elements are calculated and exchanged. The core objective of this exchange is that the client can authenticate itself to the access point and ensure secure encryption. The procedure will generate and install a common session key for both parties. Data can then be encrypted with the key to ensure data confidentiality and data integrity.

KRACK starts at the point after the “installation” of the session key. Once the session key access point message has gone to the client, the client installs the jointly generated key and confirms this step to the access point. However, since messages in the network can occasionally be lost or deleted, the access point sends the message again if the client does not confirm. In this case, the client may also reinstall the session key. At the same time, the incremental transmission packet number (known as the nonce) and the playback counter used by the data confidentiality protocol are reset. With KRACK, the attacker forces repetitions of the message from the access point to initiate the reset of the nonce. This way a new encryption with the same keystream (because it depends on the nonce) can be forced, through which data packets can be played back, decrypted and/or forged, for example, if the attacker is within range of the wireless network. The attack works similarly with other WLAN handshake methods (Peerkey, Group Key, Fast BSS Transition).

Reaction

The BSI swiftly published technical information and a press release on the attack. In addition, the BSI monitored and evaluated the provision of patches from the various manufacturers and continuously updated the information provided to business, citizens and public agencies.

Recommendation

WPA2 should continue to be used and security updates provided by the manufacturer should be applied. Furthermore, additional secure wireless connections using VPN encryption are also recommended.

macOS security problems

Situation

The operating system macOS High Sierra (version 10.13) from Apple was affected by security problems related to passwords from October 2017 to March 2018.

Known as the "root" hole, it enabled an attacker on an unlocked macOS device to overcome the security settings of macOS by entering the user name "root" and an empty password line. Then, without entering a password, the attacker could log on to this machine as the "root" user with full administrative rights. Under certain conditions, this process was also possible via Apple's own Remote Access Tool without physical access to the device.

It was also possible to open the system settings of the Mac App Store with any character string. Subsequently, an attacker could also open and change other system settings. This also included network settings, for example to manipulate the DNS settings of the system to redirect the victim to untrustworthy websites (e.g. phishing websites).

Apple introduced the new Apple File System (APFS) in the operating version macOS High Sierra. There were further security problems in this regard: firstly, the password for encrypted APFS partitions was stored in plain text in the "password hint". Secondly, when creating encrypted APFS partitions, the password could be found in plain text in the log files.

Cause and Damage

Apple reacted quickly to the security problem of the "root" hole in particular and has provided both help and corresponding security updates. In a statement, Apple regretted the security issue and promised to review the development processes.

Reaction

The BSI is in direct contact with Apple Germany and discussed this topic immediately after the „root" hole became known. Practical recommendations for action to mitigate the problem were identified and published on the BSI website as quickly as possible.

Recommendation

The BSI recommends assigning a strong password for the root account of macOS devices. Furthermore, the automatic updates of the operating system should be activated to enable security updates in particular can be installed as quickly as possible.

The limited resources of hardware security elements mean complex cryptographic operations must be accelerated by function modules implemented in hardware. However, very complex operations, such as key generation in RSA, remain very time-consuming depending on the key length, since large prime numbers have to be searched for randomly. Using FastPrime, a proprietary algorithm for constructing large prime numbers, accelerates key generation. However, it has become apparent that the keys generated in this way, with few exceptions, are cryptographically significantly weaker than expected.

Proprietary processes, while being considerably faster, are also not subject to testing in the context of research and security evaluations. A security certification in line with the Common Criteria, for example, only evaluates the secure implementation (side channel resistance) on the chip. It does not evaluate the mathematical strength of a cryptographic process itself.

The ROCA (Return of the Coppersmith Attack) weakness reported at the end of 2017 by a research team concerns exactly such a procedure that was used in an Infineon crypto library on smart cards. Insufficient entropy meant the private RSA key could be reconstructed from the public key with some computational effort (see also ROCA incident).

ROCA is not a new problem in principle; it is the result of the fundamentally complex RSA key generation. With the help of the Coppersmith attack, an RSA modulus can be efficiently factorised if the uppermost bits of one of the prime numbers are known. This effect occurs not only due to the way prime numbers are constructed in line with the proprietary FastPrime algorithm, but also when bad random number generators are used. The problem of poor random numbers, for example, led to a successful attack on some Taiwanese ID cards in 2015.

The longer development and usage scenarios for security elements also pose a problem. While known weaknesses in software products can be fixed by short-term patches, security elements usually do not provide for the option of updates in the field. When they are used over several years – during which attacks are clearly developed further – it leads to security holes that are difficult to fix where there is insufficient preparation.

Side channel analyses in the field of symmetric algorithms (AES) and classical asymmetric cryptography (RSA) are a constant subject of research. Older safety elements often show weaknesses in terms of side channel resistance. Even if their safety was originally successfully certified in line with the Common Criteria, such certification is always only a snapshot of the current technology status. This means that side channel attacks also pose a practical threat to certified security elements as the hardware ages.

The validity of security certificates is generally limited to five years for chip cards and similar products for this reason. For security-relevant applications that are in the field for a longer period of time, there should be update mechanisms for implementing the crypto procedures at least. The BSI develops and provides appropriate security standards in line with the Common Criteria. To support developers in the secure implementation of applications that use security elements as building blocks in an overall system, there is also a trend towards modularised components in which cryptographic services are provided encapsulated via defined interfaces. Using such interfaces sufficiently guarantees that side channels are not unintentionally created in the implementation.

1.4.9 Vulnerabilities in software and hardware

The number of known vulnerabilities in software products regularly reviewed by the BSI remained high in the reporting period. There are no signs that this situation will change in the coming years. This also applies to other software products and combined hardware and software products that are considered occasionally rather than continuously by the BSI. Although software development tools (compilers, IDEs, source code analysers) have improved and can alert software developers to certain sources of error, several trends simultaneously undermine security in the end product:

- Massively increased complexity of end-use applications,
- Containerisation with only partially updated software components,
- Unchecked integration of more and more external dependencies,
- Speed optimisations at the expense of safety,
- Abandonment of troubleshooting with reference to mitigation measures and
- Security update refusal by many manufacturers.

Furthermore, when purchasing a software product or combined software/hardware product, it is almost always impossible to make a qualified statement about the security or the amount of known vulnerabilities present in the product before purchasing and often afterwards too.

For the period under consideration, it is noticeable that the Linux kernel seems to have an above-average number of vulnerabilities. This is due to the fact that many vulnerabilities were found in driver modules that are also used in Android smartphones. Unlike Microsoft Windows, these vulnerabilities are added to the Linux kernel because they are patched together with the Linux kernel. With Microsoft Windows, the driver manufacturer is obliged to publish the required updates, which must also be individually installed manually by the end user.

As in previous years, security updates in the operational environment were often delayed or not implemented at all or the products in use no longer received security updates from the manufacturer. There are often delays in the installation of security updates, as this must be aligned with operational processes (such as half-yearly maintenance cycles) and in some cases is subject to additional regulatory requirements. This also applies to areas where human lives depend directly or indirectly on the software product concerned (e.g. safety systems, medical devices) or industrial processes in which errors during

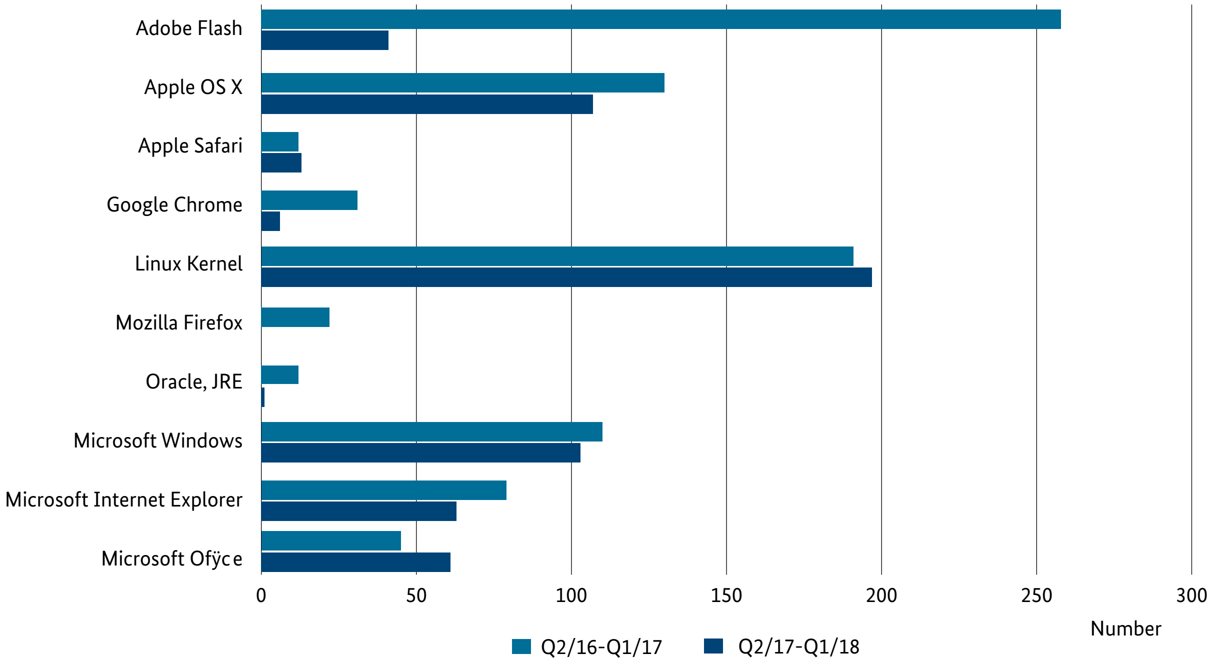


Figure 13 Critical CVE entries, version dated 31 Mar. 2018

Spectre, meltdown – attack on hardware architectures

Situation

In early 2018, a new class of attacks on central processing unit (CPU) architectures became known to a wider public. The vulnerabilities known by the names *Meltdown* and *Spectre* are novel in that they cleverly combine the architectural properties of modern CPUs in order to read out protected memory areas. Almost all current CPUs of the manufacturers Intel, AMD and ARM are affected.

Cause and Damage

The vulnerabilities exploit hardware features that have increasingly been built into processors since the mid-1990s. The primary goal was to increase performance and minimise the associated resource expenditure. These include technologies such as out-of-order command execution or speculative code execution. In connection with the constantly expanding cache storage areas this led to a largely unknown and incalculable risk for the platform operator.

Depending on the vulnerability exploited, an attacker can overcome the security mechanisms provided by the operating system and/or hardware and read data. If hardware-based problems occur, the necessary mitigating measures are often associated with considerable financial and personnel costs or noticeable losses in performance.

Reaction

The novelty of this attack class disproves previous assumptions about platform properties. This must be taken into account in the safety analysis of existing and future systems and products. Analyses carried out earlier must be checked to see whether they can continue to be applied even after the necessary correction of underlying assumptions.

Recommendation

Due to its deep structural roots in the hardware, this problem class will remain for the time being. At the moment, what changes CPU manufacturers will take to eliminate this vulnerability are unclear. Newly purchased hardware will remain vulnerable until the end of 2018, as newly developed CPUs from Intel and AMD were not announced until early 2019.

It can be assumed that further attack methods of a similar kind will be discovered as the underlying problems are progressively analysed. Due to the practical relevance of these types of attack previously seen as more theoretical, the methods of attack will gradually make their way into the realm of “usual” and “market-ready” techniques through further development. On multi-processor platforms, security gains can be achieved in certain cases when processes (or virtual machines) to be isolated are pinned to the execution context of different processors. This can make attacks significantly more difficult.

Modern processors and chipsets are highly complex; many internal mechanisms are company secrets of the manufacturers and are therefore not disclosed. As a result, these central components cannot be fully trusted and it is impossible to estimate the future risk. Whether and, if so, how an application is affected and by which measures this threat can be counteracted depends on the individual case and must be carefully examined. Until suitable solutions and sufficient transparency are provided or manufactured by the hardware manufacturers, the effects on installed systems can be partly mitigated or eliminated by software changes. This is achieved by quickly installing available patches for firmware, microcode, operating system and application programmes.

updates create high costs. Furthermore, devices with high investment costs are often used for so long that the manufacturer no longer offers support.

Even more serious are the cases where the manufacturer of a software product is no longer active on the market, cannot be identified or refuses any support. In addition, there are problems where the security updates cannot be installed in the operating system for example, because software dependent on it would no longer work correctly.

In addition to security updates that are delayed or not implemented, the manufacturers' unwillingness to provide information about the security status of their products and to maintain it, at least during the warranty period, contributes significantly to the precarious security situation.

Buyers generally lack the money, time or expertise to assess the IT security of a product and must either rely on manufacturer statements or third-party tests. How-

Features specific to Mozilla Firefox and Google Chrome

Anomalies can be observed over the past observation period for the two software products Mozilla Firefox and Google Chrome, which are regularly reviewed by the BSI. Since October 2016 Mozilla does not appear to have maintained any entries in the MITRE CVE database for Firefox. CVE entries are still referenced in its own publications (*Mozilla Foundation Security Advisories*) but these are not entered into the public database. No description of the vulnerability is given, nor is any reference made to the Firefox browser as the affected product. There is no assessment of the vulnerability or a base score.

Google seems to have been proceeding similarly with its Chrome browser since the end of October 2017 and has also failed to maintain entries in the CVE database, although Google still provides CVE numbers as it did previously in the release updates for Chrome. The corresponding entries in the MITRE CVE database are empty, however. Google does not give a description of the vulnerability either, nor does it refer to the Chrome browser as the affected product. The assessment of the vulnerability and a base score are also missing.

Furthermore, it is striking that CVE entries maintained for Google Chrome during the period under review are almost exclusively rated with a CVSS v2.0 base score of 6.8 *medium*. Thus, the reported vulnerabilities do not appear to be critical vulnerabilities which are based on a CVSS v2.0 base score of 7.0 or greater.

For Google Chrome it remains to be seen whether the CVE entries reserved initially will be updated after an internal blocking period in the MITRE CVE database or whether Google, like Mozilla for Firefox, will no longer maintain any official CVE entries.

Update-capability of smartphones

Smartphones with publicly known vulnerabilities are also sold as new without the availability of appropriate security updates. As a result, there are sometimes serious security problems for consumers when using the system.

One example are the „Stagefright" security holes in the multimedia framework of the same name in Google's Android operating system, which came to light in July 2015. It is virtually impossible for consumers to see if the software is current and whether there are any update options. Transparent information is necessary to make an informed purchase decision but this is often lacking from vendors. After the BSI found security holes in a smartphone, the Consumer Association of North Rhine-Westphalia used its authority to take legal action and initiated an injunction against the seller of the affected device as a result of insufficient consumer information. The legal action is still ongoing and The coalition agreement between the CDU, CSU and SPD intends consumer protection to be established as an additional task of the BSI.

ever, manufacturer statements on the IT security of SoHo products (small office and home office products), most of which are manufactured abroad, are often incomplete. This applies particularly to the creation of security updates and not just to statements about the current vulnerability of the product or the existence of publicly known weaknesses. Third-party product testing often focuses on functionality, not product security. There is no overview of the actual update and security situation for all market-relevant devices of a certain device class (e.g. smartphones, media players, etc.). Customers therefore have no realistic way to use product security as a criterion for a purchase decision before buying a product. This means that manufacturers with safer products have no advantages in the market.

A product that contains publicly known vulnerabilities at the time of purchase must be considered defective from an IT security perspective if the vulnerabilities are not expressly identified or no appropriate security update is available. The same applies to vulnerabilities that become known during the warranty period of the product. Software maintenance by the manufacturer, including the elimination of vulnerabilities, should not only be to "state of the art" standard, it should also be demanded by the consumer as a standard service.

1.4.10 Spam

Unsolicited e-mails are generally referred to as spam, which in turn can be divided into three categories:

- Conventional spam is often used to advertise products, securities or services, as well as in attempts at fraud (including advance fraud).
- Malware spam ("malspam") is used by attackers to infect recipients' systems with malware. This malware can be attached directly to an e-mail or introduced indirectly through a link in the e-mail body or attachments. The link then leads to the malware or a website containing drive-by exploits.
- Phishing messages encourage users to enter their login information (e.g. for Internet banking, payment services, social networks, or shopping portals) on websites controlled by those seeking to misuse such information.

In most cases, spam is sent either via compromised servers and infected client systems or from legitimate e-mail accounts using stolen login information. Systems that distribute spam are often assembled into a botnet, which makes it easier for cyber criminals to market their spam activities as a service.

The use of personal information found in data that has been stolen from large service providers, contacts from e-mail clients in infected systems or even researched data is being observed more and more frequently at present. This significantly increases the likelihood of infection.

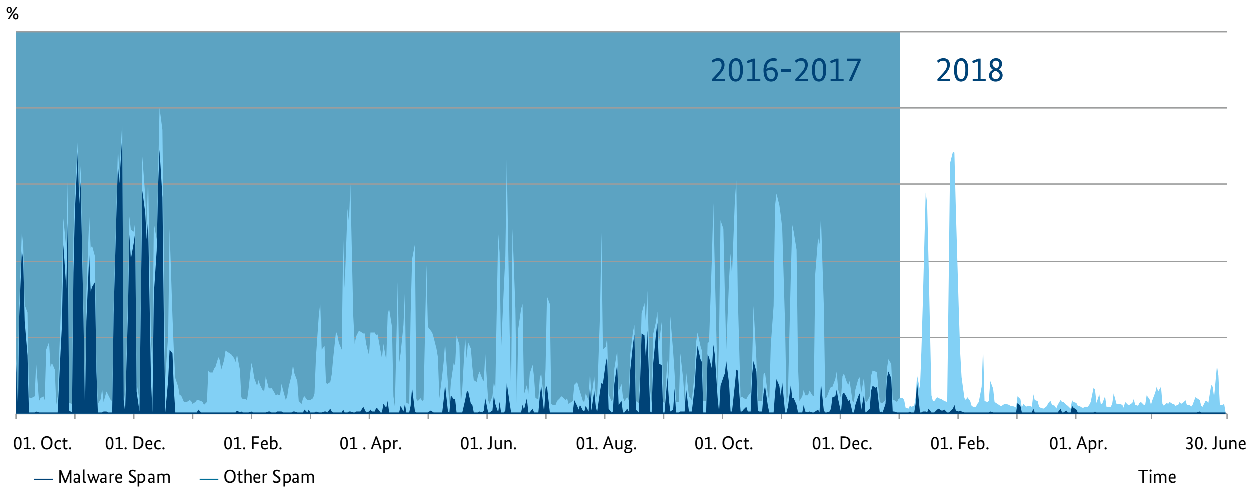


Figure 14 Qualitative tracking of spam and malware activity in Germany from 1 October 2016 to 31 May 2018.

Phishing with BSI sender

Situation

The BSI was notified at the beginning of 2018 that there were fake e-mails with BSI senders in circulation. They contained information on the topic "*Spectre/Meltdown*", as well as a link to a replica of the BSI for Citizens [BSI für Bürger] website. The URL was similar to official BSI URLs. This bogus website offered the user malware disguised as an update tool. The website itself was a copy of the "BSI for Citizens" website including a valid SSL certificate issued for this fraud site itself. At first glance, this site gave the impression of being an official BSI website. The website itself contained a download link to an alleged "Windows tool" to remove the "*Spectre*" and "*Meltdown*" vulnerabilities.

Cause and Damage

At the beginning of this year, the processor vulnerabilities *Spectre* and *Meltdown* became known to the general public. However, information about these vulnerabilities leaked to the public too early for some software manufacturers, which meant that they had not yet provided appropriate updates for their software. Some manufacturers subsequently delivered updates, some of which were recalled; other systems were not offered any updates at all.

Attackers took advantage of the general desire to update users and distributed e-mails with bogus senders purporting to be from the BSI suggesting that the BSI would provide an update for the *Spectre* and *Meltdown* vulnerabilities.

Reaction

When the falsified BSI e-mails and the bogus BSI website became known, several measures were taken at the BSI to prevent the spread of the malware as soon as possible. The malware was analysed by specialists. Domains used for malware communication were immediately blocked within the Federal Administration and announced to the public. At the same time, action was taken against the fraud site with the aim of removing it from the network. Contact was made with the host, the domain registrar and the certification authority. The website was then marked as phishing in Google's Safe Browsing service and therefore only displayed by Firefox and Google Chrome after a phishing warning message.

Recommendation

It is clear that counterfeit e-mails and websites are becoming more and more professional and so e-mails and websites should always be viewed critically. It is important to particularly check e-mails to see whether the sender address and the e-mail text match the displayed sender in form and content.

Faking websites is not a big challenge; it is therefore important to check website URLs closely. Attackers often use URLs that look similar e.g. with transposed letters or using other top-level domains, for example ".biz" instead of ".de". It is advantageous if the website can be accessed via HTTPS. In this case, there is a certificate that is usually issued by a third party and contains information about the domain name and the holder. If the issuing authority is trustworthy – the browser manufacturers check and remove conspicuous sites from the lists supplied – it can be assumed that the domain has also been checked cleanly. Depending on the browser, the trustworthiness is indicated by a lock symbol or coloured background in traffic light colours.

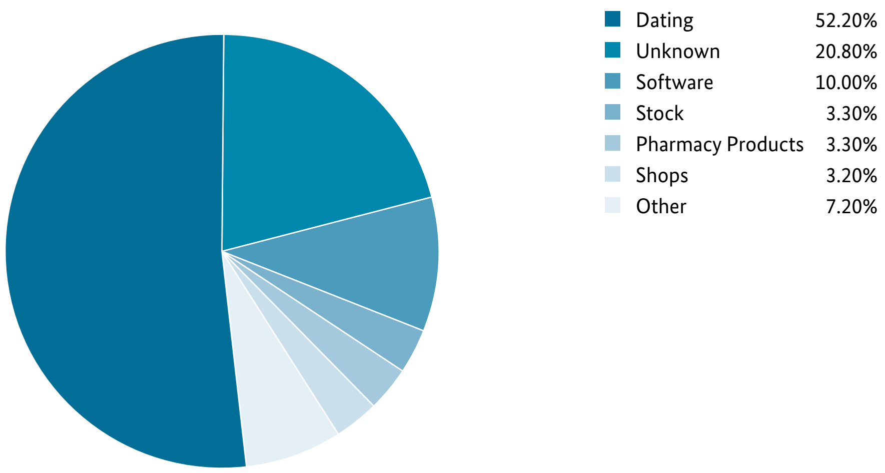


Figure 15 Distribution of spam topic areas

Necurs continues to dominate

The *Necurs botnet* remained the largest sender of spam messages. The third quarter of 2017 saw a further increase in the number of *Necurs* e-mails sent with malicious attachments. At its peak, however, this botnet achieved only about one third of the volume it registered at the end of 2016, which remains the all-time maximum in terms of malspam. In the fourth quarter, its output stagnated initially and then rose slightly in December. After the usual Christmas break (in line with the Orthodox calendar) there was only one larger wave of spam, in mid-January. Distribution then dried up almost completely.

During the period under review, *Necurs* was mainly used to send conventional spam. It primarily promoted Russian dating sites, with some smaller waves also attempting to manipulate the price of shares (penny stocks).

Overall, spam distribution seems to have the botnet operating at less than full capacity. While the graph below displays several peaks over the course of the year that give an impression of the botnet's total capacity, this point is not reached for much of the year.

Minor malspam campaigns

As in the previous year, smaller malspam campaigns continue to be observed outside of the *Necurs* network. Of particular note in this context are spam waves seeking to spread *Emotet*. This malware uses Outlook data obtained during an infection to send an e-mail that purports to be from a person with whom the potential victim has already communicated. While a large number of corresponding recipients (including IT-savvy individuals) have described this attack as targeted, it was actually a mass operation designed to persuade the targets to activate a macro execution in an attached MS Office document. In most cases, the macros then proceeded to download the malware itself *(Emotet)*.

The dominating issue at present is the sending of RTF files that exploit a vulnerability in MS Equation Editor (CVE-2017-11882, which was addressed by Microsoft in November 2017) to run malicious code that subsequently downloads additional malware.

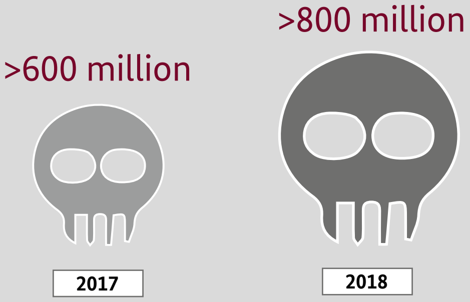
The Year in Review

Insights from the 2018 BSI Management Report

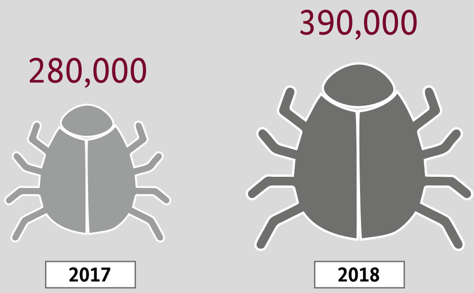
In its report on the state of IT security in Germany, the BSI provides a comprehensive overview of IT security in Germany each year. This page shows a summary of some of the findings in the 2018 report.

THREATS ON THE INTERNET

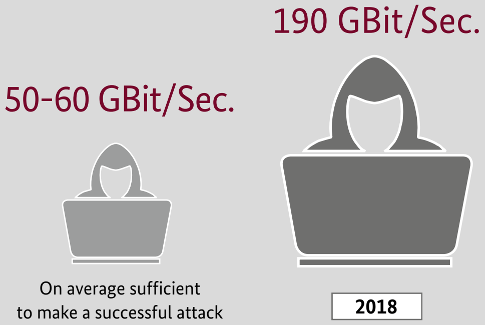
Malicious programs in circulation



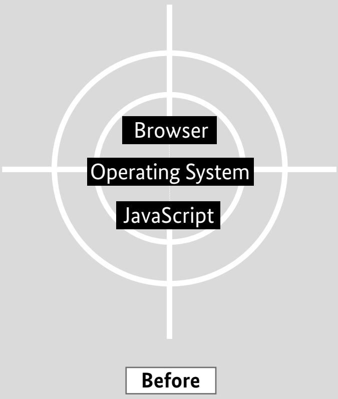
New malware types per day

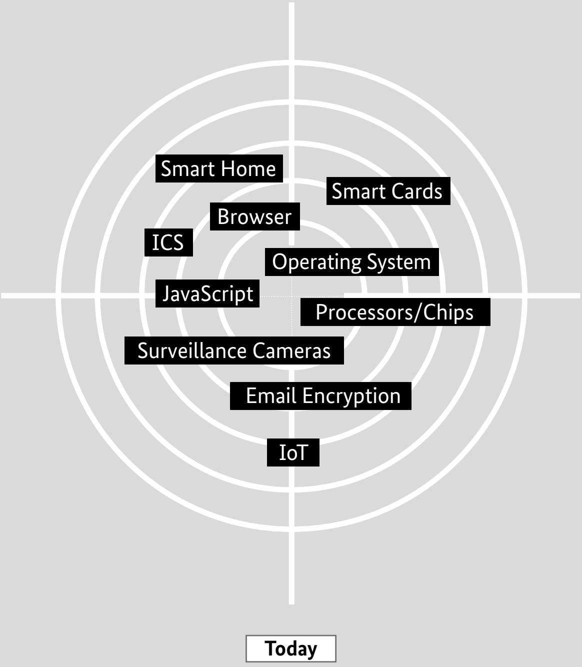


Speed of attacks



FOCUS OF ATTACKS BROADENING



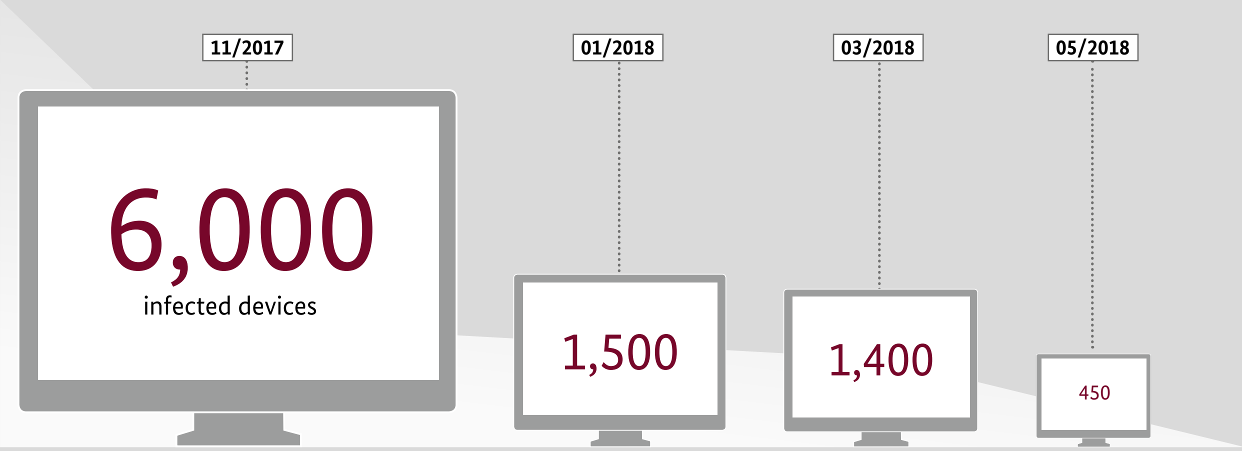


WARNINGS ARE EFFECTIVE

More than

16 million warning mails

were sent by the BSI to draw attention to dangerous situations.



(Example: Cisco Smart Install; The number of infected devices declined from more than 6,000 to around 450 following regular warnings by the CERT-Bund of the BSI to German network operators. Compare 2018 Report, p. 85)

NETWORKED COOPERATION

Allianz für Cyber-Sicherheit

More than

2,700 institutions

are connected to the Alliance for Cyber Security in order to increase the level of information security in companies and effectively protect against cyber threats.

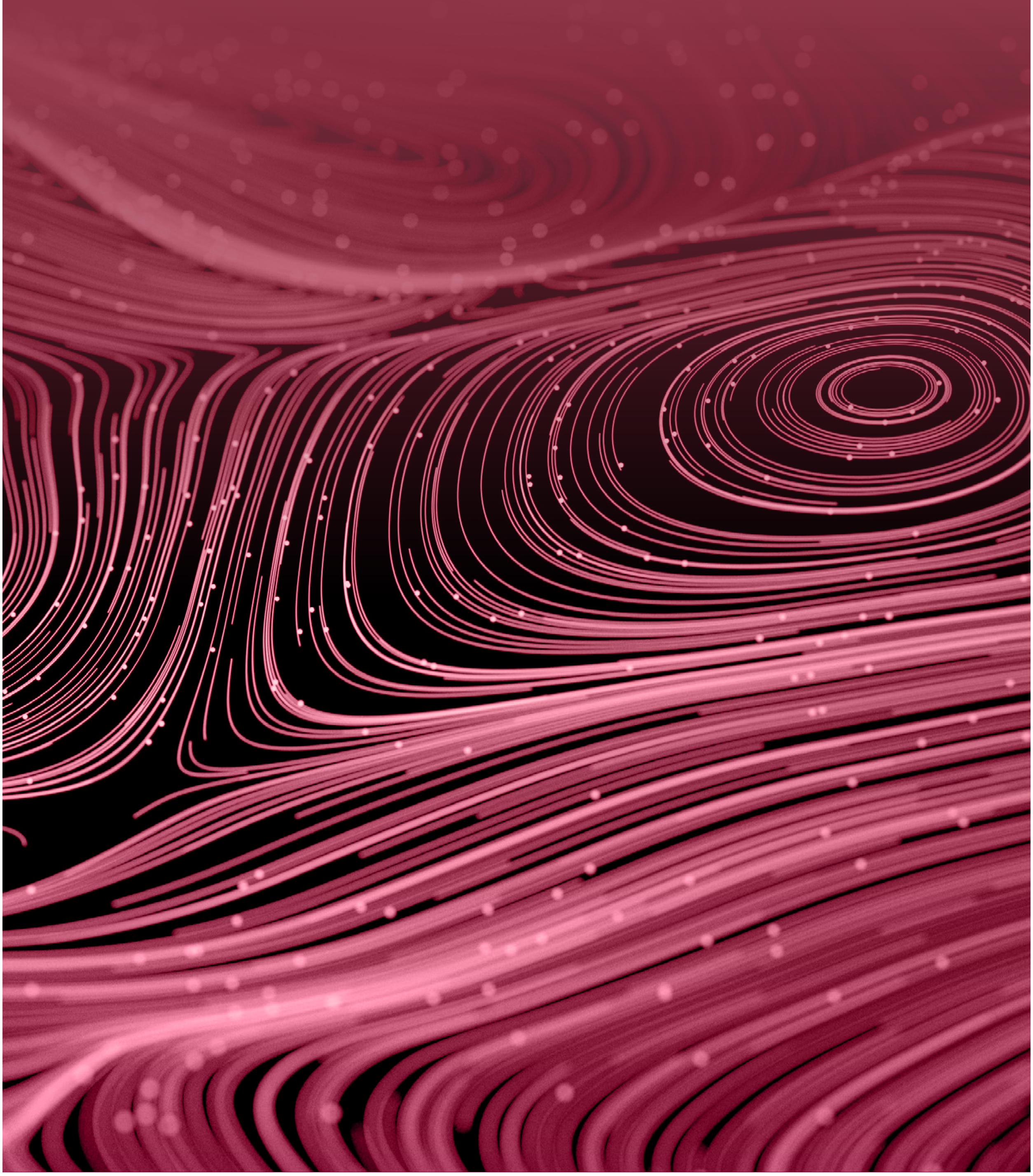
BSI FÜR BÜRGER
INS INTERNET - MIT SICHERHEIT
www.bsi-fuer-buerger.de • www.facebook.com/bsi.fuer.buerger

More than

100,000 citizens

seek information on threats on the Internet from the BSI on a regular basis.

2 BSI Solutions and Services



2 BSI Solutions and Services

This chapter will present BSI solutions and services using selected topics in the context of the current threats to IT security, focussing on three key areas: the state/administration, critical infrastructures/the business world and society/citizens. Links are provided to numerous publications and Internet packages provided by the BSI to enable the practical use of these services.

2.1 Target Audience: State and Administration

The scope of the BSI with regard to the target group of state and administration is defined by the Act on the Federal Office for Information Security (BSI Act – BSIG). The BSI is responsible for the protection of Federal IT systems. This concerns the defence against cyber attacks and other technical threats against federal IT systems and networks.

Since the amendment of the BSI Act 2009, the BSI has been the central reporting office for IT security for Federal authorities. In this function, the BSI collects information about security gaps and new attack patterns on the security of information technology. This enables it to create a reliable picture of the current situation, detect attacks at an early stage and implement countermeasures in good time. In addition, the BSI is authorised to collect, evaluate, store, use and process protocol data and data arising at interfaces of federal communications technology. The BSI is also authorised to define uniform and appropriate security standards for the Federal Administration. As the federal government's central IT service provider, it can also have suitable products developed as necessary or to put them out to tender and make them available.

This prevents manipulated IT components or unsuitable products with vulnerabilities from being used in the Federal Administration and government networks. The BSI advises other authorities and, in accordance with Section 3 (2) of the BSIG, the German states. It can also provide comprehensive support to the federal states and make its technical expertise available to them.

Product and service portfolio

In order to systematically support its target groups – the state, business and society – with specific information, technical products and services, the BSI created in a product and service portfolio during the reporting period. It is aimed at

- the Federal Government, the federal states, the local authorities and international partners in the state sector,
- operators of critical infrastructures (KRITIS), IT manufacturers and service providers as well as companies of all sizes across all industries in the business sector,
- political parties and political foundations as well as all citizens.

Six categories were standardised in the product and service portfolio. Starting from the category "Information", which includes standards such as IT-Grundschutz in addition to status reports and warnings, increasing effort is required to ensure provision in each category (see the target group example for federal states in Figure 16). In addition to "basic and advanced training" in the field of IT security and "cooperation platforms" such as the Alliance for Cyber Security, the BSI also offers "consulting services" on various matters relating to the implementation of IT security. The BSI can only perform specific technical services, such as support or even the adoption of technical protection measures, upon request – even if the legal requirements are met – due to the high effort involved.

By providing proven methods to protect against cyber attacks (e.g. using a malware information sharing platform) or consulting services, duplicate structures, for example at the state level, can be avoided.

The clear composition of the portfolio facilitates access to the expertise of the BSI. The National Liaison Service advises the target groups of the state, business and society on the individual products and services of the BSI and takes their requirements on board. For example, the portfolio forms the basis for the expansion of cooperation with the federal states.

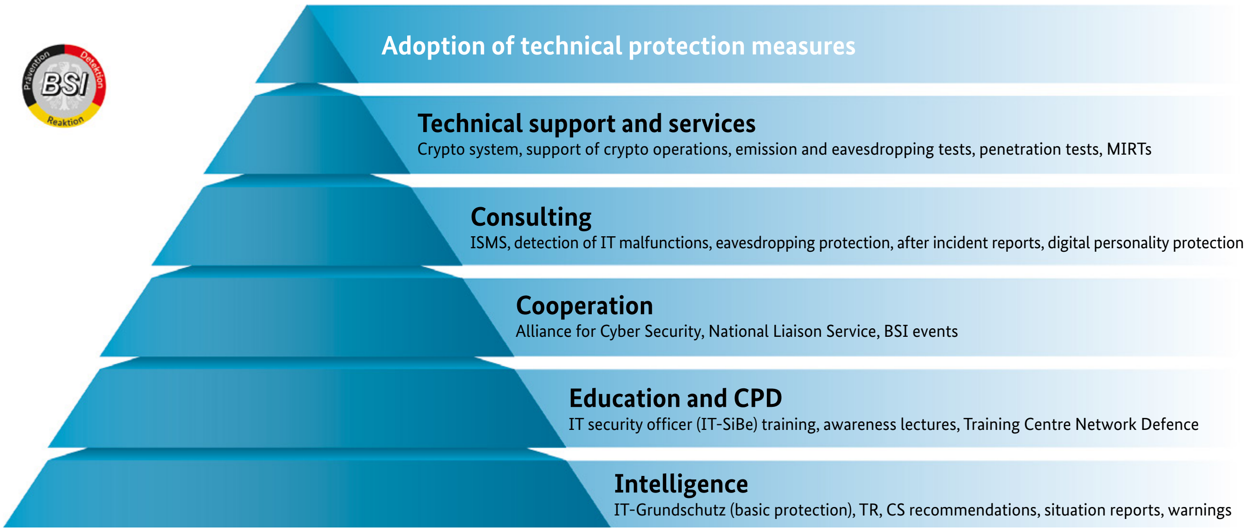

Prävention
Detektion
BSI
Reaktion
Adoption of technical protection measures
Technical support and services
Crypto system, support of crypto operations, emission and eavesdropping tests, penetration tests, MIRTs
Consulting
ISMS, detection of IT malfunctions, eavesdropping protection, after incident reports, digital personality protection
Cooperation
Alliance for Cyber Security, National Liaison Service, BSI events
Education and CPD
IT security officer (IT-SiBe) training, awareness lectures, Training Centre Network Defence
Intelligence
IT-Grundschutz (basic protection), TR, CS recommendations, situation reports, warnings

Figure 16 BSI solutions for federal states

2.1.1 CERT-Bund and National IT Situation Centre

The Federal Government's Computer Emergency Response Team (CERT-Bund) collects information on security incidents relating to IT systems in Germany from partners and other trusted external sources in its role as the national CERT and based on its own analyses. This includes information about malware infections, insufficiently secured server services and compromised systems or access data. Every day, several million such events are automatically evaluated and assigned to the relevant network operators based on the IP addresses of the affected systems. The network operators are then informed about the anomalies in their network areas and, in the case of a provider, asked to inform the customers concerned accordingly.

The BSI's National IT Situation Centre continuously monitors the IT security situation. To this end, a large number of public and non-public sources are evaluated daily, from specialist media and analyst blogs to information from IT manufacturers. This procedure ensures a prompt response to newly discovered vulnerabilities or IT security incidents that come to light. These findings are supplemented by the evaluation of information from various sensors, e.g. in government networks, as well as further analyses. The National IT Situation Centre acts as a central reporting office for IT security incidents related to the federal and state administration and the critical infrastructures, in line with recent legislation.

In serious IT situations, the National IT Situation Centre can evolve into an IT Crisis Response Centre.

Exercises

The necessary processes are regularly practised at the BSI – both internally and as part of participation in international cyber exercises such as “Cyber Europe” organised by ENISA. The key process in cross-agency exercises is the exchange of information; so that the volume of contributions can help to quickly provide and disseminate an overview of the situation and tips for coping with it.

In various training offered to the state and the administration, the BSI continuously promotes exercises and planning discussions in order to check that internal processes are up to date and work. Keywords here include emergency management, business continuity management (BCM) and crisis management.

For simple, smaller exercises, the BSI has created templates for IT emergency exercises, which are available to the Federal Administration and to members of the Alliance for Cyber Security, for example. Based on such models, organisations or organisational units can develop their own exercises, for example to check and test their own emergency management processes.

The transition from emergency management for incidents in IT operations or successful cyber attacks with low to medium impact to crisis management, where there is serious impact after IT incidents or cyber attacks, represents a particular challenge. When the malware *WannaCry* caused damage across the world in 2017, many of the parties affected were able to fall back on experience from crisis management exercises in addition to IT emergency and

BCM measures in place. In addition to established internal processes, the cross-organisational exchange of information is also relevant.

2.1.2 Cyber Response Centre

The National Cyber Response Centre (Cyber-AZ) is operated under the aegis of the BSI, based on administrative agreements between the agencies involved. The BSI provides the head, the office, including staff and the premises for its own staff and the liaison officers of the other public agencies involved. Fast channels between the Cyber-AZ and the National IT Situation Centre/IT Crisis Response Centre, the CERT-Bund and the mobile incident response team of the BSI (MIRT) ensure efficient cooperation even in crisis situations.

In addition to exchanging cyber-relevant information, the work of the Cyber Response Centre focuses particularly on coordinating the processing of cyber incidents in Germany and agreeing the operational measures taken by the responsible authorities. In implementing the coalition agreement, cooperation between the federal and state governments in cyber defence will be further expanded, improved and structurally reorganised in future. The case handling is taken over by the authorities involved within the framework of the respective tasks and powers of their appropriate specialist units. The results are continuously consolidated in the Cyber-AZ, evaluated and reported to the appropriate bodies. In this respect, the Cyber-AZ has access to the human resources of all the public agencies, if their involvement becomes necessary. The availability of these resources was reinforced last year by all Cyber-AZ authorities.

One of the most prominent cases discovered during the reporting period was the cyber attack on the Federal Foreign Office. The working group immediately set up in the Cyber-AZ involved several public agencies that invested considerable human resources in investigating the incident. At the BSI alone, these amounted to about 75 person months. Another major case was the worldwide impairment of companies' IT systems caused by the "*NotPetya*" malware software. In addition, the Cyber-AZ handled a large number of incidents that did not become public knowledge during the reporting period.

2.1.3 Detection

In addition to prevention and reaction, detection is the crucial building block for countering cyber attacks at an early stage and minimizing the extent of damage. Detection can thus be understood as the quality assurance of prevention, which determines where attempts are actually made to circumvent preventive measures. Due to its factual orientation, detection differs from vulnerability detection or penetration tests, but can only ever act backwards after or during an attack.

During the reporting period, a large number of attacks on the Federal Administration were successfully detected and averted with the aid of the detection options available under Section 5 of the BSIG. Both the decentralised and the central detection components of the BSI use statistical analyses and machine learning methods to detect previously unknown attacks.

A minimum standard for logging and detection has been created in order to make the detection of attacks even more effective in future. Particular emphasis was placed on taking account of the requirements of data protection and telecommunications secrecy while maintaining the same high detection level. The standard was developed in tandem with a reference architecture.

Based on this minimum standard, the BSI can offer efficient detection of attacks as a service to other authorities.

2.1.4 Protection against eavesdropping

The BSI provides counter eavesdropping concepts and services to federal and state authorities at risk of eavesdropping. This includes the publication of technical guidelines, consultation on new and reconstruction measures as well as conducting initial and repeat counter eavesdropping audits. In addition, it also supports conferences and bilateral meetings at a higher level where the discussions are required to be wholly or partially confidential.

The eavesdropping audit teams ensure that there are no eavesdropping devices and that no other means, such as manipulated or accidentally activated mobile phones, can be used by unauthorised persons to obtain call information.

2.1.5 Extension of cooperation between the Federal Government and the federal states

The 2016 Cyber Security Strategy for Germany defined the strengthening of cooperation between the Federal Government and the federal states in the field of cyber security. The legal basis for this is Section 3 of the BSIG, according to which the BSI can advise and warn the federal states in matters of information security and support them at their request in securing their information technology and averting dangers. In order to strengthen cooperation with the federal states, the BSI further developed the relevant structures and resources during the reporting period. Of central importance in this context were the development of the product and service portfolio for the federal states target group, the strengthening of information security consulting and the expansion of liaison services. The BSI has also steadily expanded its involvement in the AdministrationCERT Association [VerwaltungsCERT-Verbund] and supports the establishment and use of the MISP (Malware Information Sharing Platform) for the exchange of risk indicators in the federal states, for example.

The overriding goal of better cooperation is the creation of a uniform IT security level, which is gaining in importance in view of the progressive digitisation of the administration and the increasing networking of IT structures between the Federal and State governments. The security consulting and liaison services are jointly shaping the expansion of the BSI's cooperation with the federal states.

During the reporting period, the BSI identified the federal state requirement for support services from the BSI through intensive bilateral discussions and targeted needs assessment surveys. Since mid-2017, exploratory talks have been held to identify the federal states' individual cooperation and support needs and discuss models for their implementation. The talks aim to reach concrete agreements to strengthen cooperation as a basis for its expansion. A first step in this context is the signing of declarations of intent setting out areas of cooperation and support. The BSI initiated such model partnerships with the states of Hesse, North Rhine-Westphalia and Rhineland-Palatinate during the reporting period.

Further development of this cooperation in the form of administrative agreements are in the pipeline. The BSI offers these offers of cooperation to all German states equally, whereby the focus and support services are adapted individually and in line with requirements. In this way, the establishment and expansion of structures to strengthen IT security in the federal states is specifically supported by the BSI expertise available.

The BSI has structures at various levels in terms of cooperation with the federal states:

- The security consulting of the BSI is the central contact point for consulting requests from the federal and state administrations in the context of information security management. It is the central point of contact for the information security officers of the respective authorities. The employees within the Security Consulting division gain a good insight into the information security situation "on the ground" through committee work, close contacts with public agencies and an efficient exchange of information relevant to IT security. Security consulting supports the information security officers within the authorities in implementing an ISMS and in finding balanced solutions to information security issues.

- The BSI's liaison offices shape the BSI's relations with national partners in the fields of government, business and society and in particular with the federal states. A special feature of the liaison service is its regular regional presence in selected regions of Germany. This facilitates direct exchange and creates concrete accessibility to the BSI on site – to the benefit of customers and partners in all parts of Germany. The expansion of cooperation with the relevant contact persons in the federal states is an important focus of activities of the BSI's liaison officers. Regular meetings, participation in local events and lectures are part of the range of services offered by the liaison service in the federal states. The presence of the BSI at regional events was significantly increased during the reporting period.

- Operational cooperation with the federal states is established via the AdministrationCERT Association [VerwaltungsCERT-Verbund (VCV)]. Through the VCV, the CERTs (computer emergency response teams) of the Federal Government and the federal states aim to exchange information in order to be able to react more effectively and more quickly to IT attacks. In 2018, the IT Planning Council decided on a mandatory reporting procedure for the exchange of information on cyber attacks and thus created a reporting obligation between the Federal Government and the federal states. The BSI uses CERT-Bund to provide warnings, situation reports and threat indicators from a wide variety of sources processed at the BSI Situation Centre. By contributing to the overview and incident notifications, the federal states play a role that is fundamentally important in establishing a complete picture. The mutual reporting obligation is the basis for this.

The municipalities are also involved in strengthening co-operation between the federal and state governments. Due to the large number of municipalities, multipliers must be used to bundle or integrate the activities. The BSI also enables a direct connection between all municipalities to the Alliance for Cyber Security.

2.1.6 Federal Government Implementation Plan 2017

The Federal Government Implementation Plan (IP) 2017 is the Guideline for Information Security in the Federal Administration. The implementation of the included requirements and security measures guarantees information security in the Federal Administration. In the Federal Government IP 2017, the implementation plan originally drawn up in 2007 was revised and approved by the Federal Cabinet at its meeting on 19 July 2017. The Federal Government IP 2017 came into force on 1 September 2017 and implements targets from the 2016 Cyber Security Strategy in various action areas. It is binding for all departments and federal agencies. The growing dependency on IT and the increasing vulnerability of the Federal Administration's digital infrastructure make it essential to have a functioning information security management and a systematic achievement of the protection goals of information security in the Federal Administration. The Federal Government IP 2017 created the basis for this.

2.1.7 Information Security Consulting

Support and consulting for developing information security management systems (ISMS) is one of the essential core tasks of information security consulting at the BSI. The target groups for these services were expanded during the reporting period.

For example, the BSI advised political parties and foundations during the 2017 federal election. This will now be continued as a permanent service, as the security of the IT systems involved will also play an important role in future elections.

In 2017, planning also started on an expansion of the consulting services for the federal states and municipalities. The BSI standards 200-1 and 200-2 were tested for their practical application. The new BSI guideline on basic security in line with the IT-Grundschutz standards represents an introduction to information security that is quick to implement and matched to the state-specific and municipal sector in particular.

Individual advice to departments and public agencies as well as other federal institutions has become increasingly important. The update of the IT-Grundschutz standards, the implementation of the newly designed Federal Government IP 2017 and IT consolidation are important fields of consulting. In addition, there are projects in which the BSI advises on issues of information security.

For example, maturity models are examined by security consultancy in order to meet the need for better control of ISMS. Thus the strengths and weaknesses as well as the need for action in ISMS can be identified more precisely and presented more effectively.

In addition, security consultancy provides brief, subject-specific information, for example on secure messenger services, and answers questions on security-related topics. The aim here is to condense the topic to two pages, similar to a quick guide, balancing brevity and understandability and referencing other important documents with more information.

Based on the Federal Government IP 2017, the BSI cooperates with the Federal Academy of Public Administration (BAköV) to ensure up-to-date training for IT security officers in public administration.

2.1.8 Federal Administration IT consolidation

In the German government's major IT consolidation project, it is bringing its information technology together by consolidating operations, concentrating services and bundling procurement in a network of IT service providers. As a result, the IT landscape of the Federal Administration is undergoing considerable change, resulting in both new opportunities and new risks. For example, economies of scale can be used to professionalise IT processes. However, if IT systems are concentrated on IT service providers, there are also potential IT risk concentrations among IT service providers.

The BSI regularly and intensively advises the overall project management for Federal Administration IT Consolidation on strategic and operational issues of information security in IT consolidation. In particular, the BSI is intensively involved in several measures of subproject 6 "Joint Federal Government IT", for example in the measures Federal Cloud and Federal Client, and is also involved in the steering committee of the subproject. In addition, the BSI advises committees of the federal IT service providers on questions of information security.

Furthermore, the BSI continues to analyse all data centres of the Federal Administration on the basis of the "HV benchmark" standard for the Budget Committee of the German Bundestag. In addition to the results of the previous partial audits, it was possible to gain new insights into the effect of various individual measures in the information security management of data centres. The study based on the HV benchmark thus proved to be an effective tool for continuous improvement of data centre security.

2.1.9 Services and security measures during the 2017 Bundestag election

The BSI supported the Federal Returning Officer in questions related to information security during the federal elections in September 2017. For this purpose, relevant threat scenarios and protection requirements were discussed and the security concept was analysed at a technical level. Furthermore penetration tests were carried out. In addition, the BSI advised state returning officers on aspects of information security for their IT-related tasks during the Bundestag election.

The BSI created a range of services to ensure the cyber security of the Bundestag elections and provided the corresponding personnel resources. Key elements of this range of services included:

- Advising political parties and foundations on the development of management systems for information security (ISMS),
- Support in creating verified accounts on Twitter and Facebook,
- Digital personality protection in the form of an information and consulting service for top politicians,
- Penetration tests and web checks as well as
- Investigation of social bots.

During the relevant period before the Bundestag election, the BSI carried out a large number of activities, some of which are mentioned here:

- Focused monitoring of the situation with regard to the Bundestag elections
- 24/7 operation of the National IT Situation Centre during the critical phase of the election process
- Advising of the Federal Returning Officer and the State Returning Officers on information security issues
- Advising of almost all parties represented in the Bundestag
- Processing more than 700 requests to verify social media accounts.

In summary, the BSI has recorded and examined a number of relevant events in connection with the Bundestag election. With regard to cyber attacks on the Bundestag election, no influence on the Bundestag election could be determined.

2.1.10 Minimum standards

The BSI establishes minimum standards for the security of the Federal Government's information technology in accordance with Section 8 of the BSIG. These minimum standards to guarantee information security within the Federal Administration must be observed in accordance with the Guideline for Information Security in the Federal Administration (Federal Government IP 2017). In order to ensure a high quality of the standards, minimum standards are developed according to a standardised procedure: each minimum standard undergoes several examination cycles including a consultation procedure with the Federal Administration. In addition to active participation in the development of minimum standards, the Federal Administration can also contribute to the development of technical subject areas for new minimum standards or contact the BSI about the need for amendments to existing minimum standards. In connection with the development of minimum standards, the BSI advises the Federal Administration on request on the implementation of and compliance with the minimum standards.

The minimum standards already published cover a broad spectrum of information technology:

- Use of the SSL/TLS protocol,
- Secure web browsers
- External cloud services,
- Mobile device management,
- Application of the HV Benchmark compact,
- Interface controls.

Further minimum standards are being developed currently covering the topics "Logging and detection of cyber attacks", "Federal Government IT-Grundschutz" and "Federal Networks User Obligations".

The minimum standards provide concrete help to ensure secure IT operations. The ROBOT attack discovered in December 2017, which intended to exploit vulnerabilities in TLS implementations, had no effect on institutions that had already implemented the minimum standard "Use of the SSL/TLS protocol", for example. Due to the secure configuration of the TLS protocol specified by the minimum standard, the attack could be completely prevented.

2.1.11 Secure mobile communication in the Federal Administration

Mobile communication has undergone enormous development in recent years. The technical innovations and the rising performance of mobile systems make it possible to communicate and work independently of time and place. The use of mobile devices presents the Federal Administration with various challenges. Their deployment must meet the requirements of business processes as well as the security of government and public agency networks.

Together with security product manufacturers, the BSI has developed and approved various mobile solutions for the Federal Administration for processing and transmitting classified information ("VS"/"classified") of the "VS-NUR FÜR DEN DIENSTGEBRAUCH"/"RESTRICTED" ("VS-NfD"/ "restricted") security classification level. One example is Secusmart, who previously developed the SecuSUITE solution for BlackBerry 10. With SecuSUITE for Samsung Knox, it provides secure smartphones and tablets based on modern Samsung devices with the Android operating system. Since the end of the first quarter of 2018, public agencies have had access to a secure mobile solution for transferring data in the Apple iOS environment covering the current range of iPhones and iPads in the SecurePIM Government SDS product from Virtual Solution.

SecurePIM Government SDS

In cooperation with the BSI, the SecurePIM Government SDS solution was developed for the secure processing of classified information marked as restricted (VS-NfD – RESTRICTED) with iPhones and iPads. SecurePIM Government SDS synchronises e-mail, address books, notes, tasks, calendars and documents from an agency's internal network to iPhones or iPads for secure mobile access to public authority intranets. The solution uses a smart card as a security anchor, which is coupled to iOS devices via a smart card reader.

Study on secure telephony with iOS-based devices

Secure voice transmission is a central requirement for secure mobile solutions. The technical options and the effort involved in implementing secure telephony to meet the required level for information classified as restricted on iOS devices were examined in 2017 in the "Study on implementing secure telephony on iOS". A rough concept for the implementation of SNS was developed and is now being implemented by the device manufacturer.

2.1.12 Secure identities in eGovernment

In the context of digitising processes, the trustworthiness of identities in the digital world is of particular importance: where people no longer appear in person, their identity must be ensured reliably other ways. The BSI therefore deals with the secure implementation of identification and authentication procedures, particularly with regard to eGovernment.

The coalition agreement provides for the creation of a digital "citizen portal" for individuals and companies in which centralised and decentralised administrative portals are networked. This citizen portal (also described as a portal network in the Online Access Act) is intended to link all the portals of the Federal Government and all the federal states intelligently by the end of 2022 and make online administrative services easier to find.

The portal network is one of three sub-projects of the IT Planning Council's project "Administration portals at all levels intelligently linked".

The other subprojects are the federal portal and the citizens' account (now the service or user account).

In the portal network, the federal and state governments provide user accounts that provide standard identification for users for the electronic administrative services of the federal and state governments available in the portal network. Since both already had user and service accounts to some extent, the IT Planning Council decided not to provide a standardised federal service account, opting to set up a federation network of "interoperable service accounts" instead, so that citizens and companies only need a single service account to be able to identify themselves for the administrative services of the other members of the federation.

In the area of interoperable service accounts, the BSI supports the "eID Strategy" project group set up by the IT Planning Council and will develop a technical guideline on this topic based on the pilot phase.

In the context of the Online Access Act (OZG), security requirements for the pilot operation of the portal network/online gateway are currently being drawn up and agreed with the bodies participating in the pilot.

2.1.13 Smart borders and sovereign identity management

At the end of 2017, the EU regulation establishing a uniform entry/exit system (EES) came into force across Europe. The overall system consists of a central European register, a biometric background system for over 100 million travellers and integration into the national border control and other security systems of the Schengen states.

Under the EES, every border crossing of a third-country national across one of the external Schengen borders is recorded in a European register for three years, and in exceptional cases for up to five years. A biometric photograph and four fingerprints are stored along with the biographical data. This enables a significant improvement in the identification of travellers, as multiple identities can be uncovered by biometric comparison. Overstayers, i.e. travellers who have exceeded their authorised length of stay, can thus be easily identified and recognised during checks.

Furthermore, the legal framework for the new European Travel Information and Authorisation System (ETIAS) is currently being established. It is intended as a pre-registration system for visa-free travellers, similar to the US ESTA system. The new systems, combined with existing systems such as the Visa Information System (VIS) and the European Asylum System (EURODAC), enable secure identification of persons, even if they no longer have any documents. The BSI thus plays a decisive role in shaping important building blocks in the European system of migration control.

The digitisation of the European border control architecture is focusing closely on the functionality and IT security requirements of the new systems. In future, most border control steps will be automated as self-service solutions. Technical systems will provide the information required for decisions on border crossings and those responsible expect a high degree of reliability from these systems.

The BSI, together with its partner authorities the Federal Office of Administration and the Federal Police, is responsible for the national implementation of the EES and the ETIAS to follow. In its technical specifications, the BSI ensures that both the document verification of the optical and electronic security features and the biometric procedures are always state-of-the-art. In close coordination with the Federal Police, the BSI checks the border control systems for vulnerabilities and also operates the necessary background infrastructure within the framework of the National Public Key Directory.

The BSI thus makes an important contribution to sovereign identity management in the border control process. Ensuring a high level of security is a central concern of the Federal Government and continues the Schengen concept: a uniform and reliable system for controlling the common external borders.

2.1.14 Emission security

In fulfilment of NATO and EU treaties, BSI has the role of the National TEMPEST Authority (NTA). TEMPEST is a collective term for all electromagnetic effects that occur as a side effect of all kinds of electrical and electronic data processing. Compromising emanations like this can be misused under suitable conditions to reconstruct the processed information.

In its role as NTA, BSI has statutory responsibility for the development, implementation and control of defensive measures against the exploitation of compromising emanations in the processing, transfer and storage of classified information. Security standards and measurement methods in use are adapted to the protection requirements of the classified information as well as the environment in which it is processed. The highest security level for hardware, known as "Level A", implements the internationally agreed TEMPEST standard directly by employing complex signal analysis procedures. The National Zoning Model was developed by BSI for processing classified information in environments with a particular security level. Some of the security requirements for devices processing classified information are assigned to the operational environment. This enables the use of test procedures that are optimised for the series production of hardware intended for processing classified information. The procedure consists of a speciment certification of a set of devices with subsequent production of identically construcded hardware, with a test coverage of 100%. During the reporting period, ten TEMPEST approvals were issued for Level A devices and 549 TEMPEST approvals for devices in line with the National Zoning Model using these procedures.

Attacks on ePassports

Situation

At the end of 2017, a team of researchers published details of the attack known as ROCA (Return of the Coppersmith Attack). The attack targets RSA keys generated on Infineon smart cards. Using the public key, the private RSA key can be reconstructed with some computational effort.

The RSA process forms the basis for numerous applications, but the effects of ROCA are still manageable. ROCA signature cards mainly affected a number of foreign ID cards. In the context of the possible notification of such ID cards under the EU eIDAS regulation on electronic identification, mitigating ROCA will play an essential role in the countries concerned.

The electronic signatures of passports in some countries (Document Signer keys) are also based on RSA and can be affected. This signature guarantees the integrity of the data stored on the ePassport and is therefore much more critical. German travel documents are not affected by ROCA, as they use signatures based on elliptic curves.

Cause and Damage

During a check of all RSA-based Document Signer keys of other countries by the BSI (within the meaning of Section 3 (1) Sentence 13(a) of the BSIG, two problems were identified:

- Malaysia has been using keys affected by ROCA since 2016.
- Liechtenstein has been using keys since 2016 that were probably generated by incorrect configuration with weak random numbers.

The affected passports remain valid regardless of the electronic function and offer a certain degree of protection against forgery through their physical properties. With Document Signer keys, however, a complete electronic falsification of a passport can be generated with any passport data. This has significant effects, especially for ABC (Automated Border Control) stations.

Reaction

The BSI immediately informed the affected countries Malaysia and Liechtenstein. After the notification, Liechtenstein reacted in a prompt and exemplary manner and was able to identify the technical cause in cooperation with the BSI. The responsible authorities in Liechtenstein have started the free exchange of approximately 5,500 affected passports and recalled the corresponding incorrect certificates.

Malaysia has immediately replaced the signature cards affected by ROCA so that passports produced now are no longer threatened. However, the associated Document Signer keys were not recalled and the passports in the field were not exchanged.

Parallel to the affected member states, the BSI informed the Federal Police about the situation and agreed to block the affected keys in the border control system as a result.

Recommendation

Because Document Signer keys are blocked in the border control systems in Liechtenstein and Malaysia, problems may arise when entering the country using the passports of these countries. Citizens in these countries are therefore recommended to exchange affected passports for a new one. This can be done free of charge In Liechtenstein.

2.1.15 Approval

According to the BSI Act (Section 3 (1) Sentences 1, 14 and 17), the BSI is legally authorised to test IT security products as part of its evaluation and to make binding statements with regard to their security standard. This applies to IT security products that are used for the processing, transmission and storage of officially classified information within the scope of the General Administrative Regulation of the Federal Ministry of the Interior, Building and Community for the substantive and organisational protection of classified information (Classified Information Directive – VSA) or at companies within the scope of public administration contracts with reference to classified information. This applies mainly to IT security products that contain encryption functions, known as cryptosystems. The application for approval for an IT security product can only be submitted by a governmental user in principle.

According to Section 37 of the Classified Information Directive (VSA), approval must be provided by the BSI for products used to create encryption, for the encryption itself, for securing transmission lines and for separating networks with differing maximum classification levels for the classified documents to be processed. As in previous years, the BSI again issued or extended over 50 approvals in the reporting period. This increases the number of VSA-compliant products and product versions to 190. An up-to-date list of generally approved IT security products can be found in BSI publication 7164, which is available on the BSI website (https://www.bsi.bund.de/DE/Themen/Sicherheitsberatung/ZugelasseneProdukte/zugelasseneProdukte_node.html)

In order to continue to meet the public administration's need for approved products, the BSI is currently dealing with more than 60 ongoing procedures seeking approval.

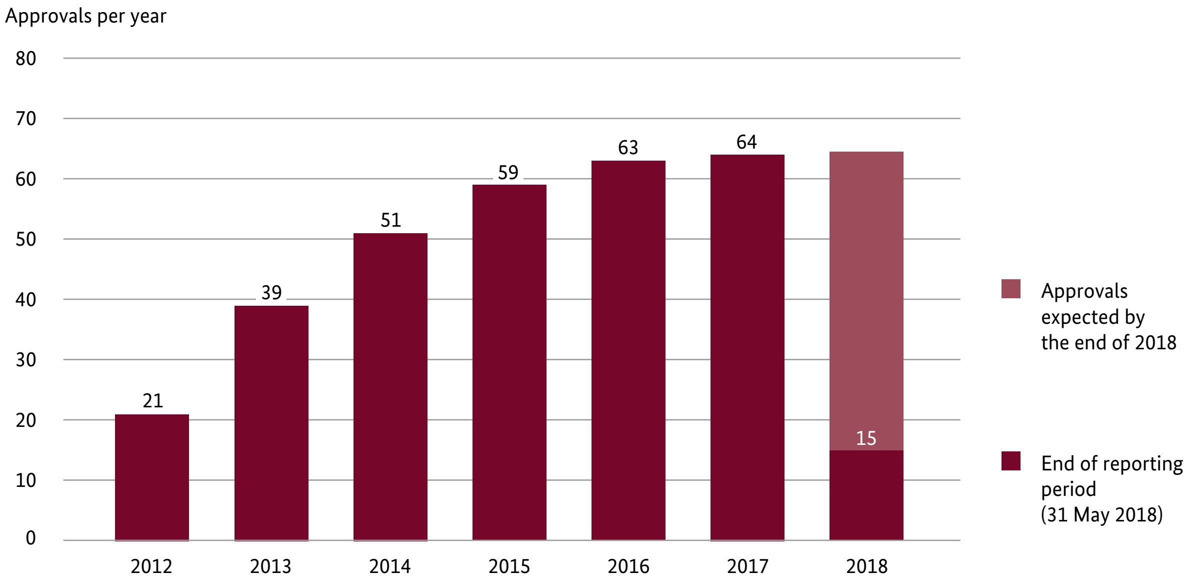


Figure **17** Approvals of the past years, version dated 31 May 2018.

2.1.16 VS requirements profiles

In order to accommodate the rising demand from the Federal Administration for secure IT solutions, the BSI is optimising the approval process. In terms of the processing, transmission and storage of classified information (VS), the creation of VS requirement profiles (VS-APs) for information security systems significantly accelerates evaluation and approval. This is reflected not least in the increasing number of approved VS-IT systems.

VS requirement profiles (VS-APs) describe IT security requirements for specific product classes and types. On the one hand, they are directed at users and operators, such as agencies who want to use products when dealing with classified documents and therefore need the basic requirements to be met by suitable products. On the other hand, VS-APs address the manufacturers of such products in order to give them a general technical guideline for the implementation of relevant IT security requirements.

Standardising new basic security functions is an important prerequisite for approving systems dealing with classified information. Numerous manufacturers have already been involved in round-table talks to help shape the future-proof design of information security systems in the VS sector.

The objectives for defining VS requirement profiles should meet the following key criteria:

1. Design of information security systems and components for the VS area by the BSI

2. Harmonisation of IT security requirements for certain product classes and types

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

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

The BSI published seven VS requirements profiles in the reporting period. A further four are in progress. 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 (nPPs) are being prepared for use in the VS area for the standardisation of further IT security products.

The BSI decision to integrate product manufacturers, users and operators at an early stage in the active 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.

2.1.17 Technical Guidelines TR-ESOR and TR-RESISCAN

The legislator requires electronic file management to be “state of the art” (Sections 6 and 7 of the Act to Promote Electronic Government (eGovG), Sections 298a of the Code of Civil Procedure (ZPO) and 32e of the German Code of Criminal Procedure (StPO)).

The BSI publishes technical guidelines that make it possible to implement corresponding state-of-the-art eGovernment solutions. Adherence to the BSI technical guidelines ensures regular compliance with “state-of-the-art” technology.

- BSI-TR 03138 Replacement Scanning (TR-RESISCAN) defines requirements for the proper and risk-minimising design of the scanning process for legally compliant electronic file management. The TR RESISCAN is intended to serve users in the judiciary, administrative, industry and healthcare sectors as an action guideline and aid to decision-making when it comes not only to scanning paper documents, but also to destroying them after the scanned product has been created.

- With the technical guideline BSI-TR 03125 “Preservation of Evidence of Cryptographically Signed Documents” (TR-ESOR), the BSI defines a guideline for users in administration, justice, but also in business and in healthcare for the preservation of archived data and documents until the end of the legally prescribed retention period based on the international standards RFC 4998 and RFC 6283 and the ETSI-AdES or ASCII formats as well as the eIDAS Regulation and the Trust Services Act.

Both with the ArchiSig model which is based on TR-ESOR, and with a digital copy produced in accordance with TR-RESISCAN, it has also been legally proven in simulation studies that the respective probative value can be optimised and the evidence can be simplified accordingly in court if there is compliance with the TR recommendations.

2.2 Target audience: the business world

Networking and exchange are important elements of digital shift in the industry. These elements are also important factors for productivity and economic growth in Germany. Intelligent and networked machines exchange information directly with each other in real time. In the "Smart Factory", the production facilities organise themselves independently and coordinate processes and deadlines amongst themselves. This makes production more flexible, dynamic and efficient. In addition, the machines communicate directly with all IT systems of the company and thus directly with the employees. But this also increases the susceptibility of the economy to hacker attacks and cyber attacks. The BSI has already set impulses in many ways on its own initiative and through its partner networks in order to fulfil its mission with regard to the economy as well.

2.2.1 Alliance for Cyber Security

The Alliance for Cyber Security (ACS), founded in 2012, enables the BSI to pursue the goal of increasing cyber security in Germany. More than motto "Networks protect networks" ACS provides practical assistance to companies in the analysis of cyber risks and the implementation of suitable protection measures. The initiative now counts members amongst 2,700 companies, public agencies, associations, research institutes and other institutions from all over Germany are now members of the initiative.

Yet more register every day to benefit from the expertise of the BSI and its ACS cooperation partners from industry and research as well as the reliable exchange of experiences with other companies and institutions. The alliance aims to achieve further strong growth for ACS in small and medium-sized enterprises (SMEs). To this end, extensive measures are taken, described below.

Around a hundred partners and more than 50 multipliers are involved in the ACS and thus make a valuable contribution to increased cyber security in Germany as a business centre. Free of charge for ACS participants, offers of partner companies are an important added value in the Alliance for Cyber Security; especially for small and medium-sized enterprises that do not operate their own threat intelligence. This includes training and workshops, analyses and initial consultations or penetration tests. In 2018, ACS provided an offer, free of charge, to its participants almost weekly from a partner company.

In addition, important strategic partnerships, for example with the German Confederation of Skilled Trades (ZDH) and the German Retail Federation (HDE), were initiated in the period under review and took effect when the official declarations of intent were signed. Via the ZDH alone, ACS reaches around one million trade businesses with 5.45 million employees throughout Germany. The first concrete measures within the framework of these cooperative efforts are, for example, developed and deployed together with the ZDH for new IT-Grundschutz profiles for trade organisations and enterprises and at events designed for target audiences.

Another successful model is the "Training Centre for Network Defence", which was commissioned by the BSI. The training offered is always fully booked within a few hours. The Cyber Security Days, which the ACS organises in cooperation with partners or multipliers, are also very popular. These thematic or target group-specific events are now held six times a year to meet the high demand.

A strategic goal of the Alliance for Cyber Security is to promote a practical exchange of experience in business. The Alliance experience groups (ERFA), which were redesigned during the reporting period, have the objective of "learning from one another" and serve to facilitate professional, subject-linked or target-group-specific exchange within a protected and confidential framework. BSI cyber security experts and those at other institutions accompany and enrich the exchange process with their expertise.

Information exchange between the cyber security initiatives in Germany

In mid-2017, the BSI started a dialogue process with the cyber security initiatives in Germany. Networks and organisations are invited to take part, including associations, research institutions and public agencies involved in cyber security on behalf of companies and/or citizens. The aim is to exploit synergies, further increase awareness of cyber security in Germany and maximise the impact of individual awareness campaigns. The Alliance for Cyber Security has taken over the structuring and organisation of the exchange.

The exchange between cyber security initiatives is developing very positively and has led to productive and sustainable cooperative efforts in many instances. In the future, this exchange can form the starting point for the cyber security pact proposed in the coalition agreement under the leadership of the BSI.

2.2.2 IT-Grundschutz

IT-Grundschutz is the BSI's sound and practical management system for information security (ISMS) available to business and administration users. It helps to check the status of information security in an institution and improve it consequently. The updated IT-Grundschutz standards were presented at the it-sa security trade fair in October 2017, supplemented by topics such as detection and industrial control systems (ICS). The IT-Grundschutz recommendations can now be provided even faster and better adapted to the size and the required security needs of an institution. The new structure and streamlined publications on a wide variety of information security topics are helping to ensure that the content better corresponds to state-of-the-art standards.

Practical recommendations for more information security

The fundamentally revised BSI standards are the central publications of its IT-Grundschutz.

- In the BSI Standard 200-1, information security managers learn everything they need to know about setting up an information security management system.

- The BSI Standard 200-2 explains the IT-Grundschutz methodology and

- BSI-Standard 200-3 deals with risk analysis based on IT-Grundschutz.

With the help of the BSI standards, users learn how the relevant business processes, applications, IT systems, etc can be identified, how their protection requirements can be determined and how to proceed if a higher protection requirement is to be ensured.

Another integral publication of the IT-Grundschutz is the IT-Grundschutz Compendium, which contains practical modules. In the current edition of February 2018, the first 80 IT-Grundschutz modules are published, which are also the basis for certification according to ISO 27001 based on IT-Grundschutz. The modules allow users to deal with one topic at a time in detail. The module standards show information security officers the tools they need to raise security levels. Detailed information and measures can be found in the supplementary implementation notes published for most IT-Grundschutz modules. All content was updated in close cooperation with the IT-Grundschutz community. As a result, the current IT-Grundschutz contents are field-tested and application-oriented, as well as being technically sound.

From users for users: IT-Grundschutz Profiles

Another element of IT-Grundschutz are the IT-Grundschutz Profiles. These are security concept models that can serve as templates for institutions with comparable framework conditions. The BSI is supporting business and administration in launching the first IT-Grundschutz Profiles for specific sectors. This includes the publication of a guide to support interested parties through the process. Successful kick-off workshops were held with the first industry representatives; following these, the first IT-Grundschutz profiles were published. There is also close participation and cooperation in the implementation of the IT-Grundschutz Profiles. The IT-Grundschutz standards thus also make a sustained contribution to increasing the level of information security in Germany.

2.2.3 CIP Implementation Plan (UP KRITIS) and the IT Security Act (IT-SiG)

Implementing the German IT Security Act

In order to take account of the increasing importance of information and communication technology and to combat new threats in good time, the BSI has been granted legislative tasks and powers for critical infrastructure protection (CIP) through the BSI Act. For example, according to Section 8a of the BSIG operators of critical infrastructures must ensure IT security precautions meet state-of-the-art requirements and their implementation must be regularly verified to the BSI every two years. Furthermore, the BSI can check compliance with IT security on site and may demand the elimination of any security deficiencies that are discovered, in agreement with the responsible regulatory authorities.

Linking operators of critical infrastructures to the warning and reporting structures of the BSI

The deadline for registration and designation of a contact point for the operators of critical infrastructures from the CIP sectors of health, finance and insurance as well as transport and traffic (amending regulation of the BSI-KritisV from 30 June 2017, the second part of the regulation) was the end of December 2017. Across all CIP sectors, some 300 operators with 1400 installations have now registered with the BSI. These have been connected to the warning and reporting structures of the BSI and are regularly provided with relevant warnings and (situation) information on cyber security by the BSI Situation Centre.

Status of the industry-specific security standards of the various sectors

In order to implement Section 8a (1) of the BSIG, KRITIS operators must "take appropriate organisational and technical precautions to avoid disruptions". They can develop industry-specific security standards (B3S), which are tested for suitability by the BSI upon request. Creating and using a B3S

- facilitates the identification of appropriate precautions and the methodology for implementing appropriate measures in particular,
- takes into account industry-specific requirements and
- defines "best practices" for an industry or a critical infrastructure sector.

Users also gain confidence with regard to the interpretation of abstract terms used in BSIG such as "appropriate", "suitable" or "state of the art". B3S are mainly developed in the various industry working groups within the CIP Implementation Plan. B3S is currently under development in the following industries:

- Food production and processing
- Distribution of district heating
- Plants or systems for the control/bundling of electrical power
- Air traffic.

The BSI has already successfully determined the suitability of B3S safety standards in the following industries:

- Drinking water supply/waste water disposal
- Food trade
- Information technology, the plant category of data centre/server farms and content delivery network (CDN).

The BSI advises the authors of B3S on request during the creation and supports them with advisory discussions and workshops, up to the stage of advance suitability testing. These services have been in demand and in use by the critical infrastructure industries. Some industries that are not obliged to implement Section 8a of the BSIG are still planning to develop a B3S.

In order to support KRITIS operators and their associations with the general development of B3S, the BSI issued an orientation guide for B3S in December 2015. This defines criteria to establish the scope of a B3S appropriately and set CIP objectives, drawing attention to the need to observe particular aspects of risk evaluation and risk management. The orientation guide lists relevant subject areas for the safety precautions and measures to be taken and provides assistance on the level of detail, appropriateness and suitability of measures.

At the beginning of 2018, after a period of practical testing and drawing on the experience gained, the BSI completely revised the orientation guide and published the new edition on its website. The BSI has collaborated with the Federal Office of Civil Protection and Disaster Assistance (BBK), the Thematic Working Group (TAK) "Audits and Standards" of the CIP Implementation Plan and the B3S authors. In addition to many detailed improvements, the inclusion of general and industry-specific standards (IT-Grundschutz, ISO 27001, C5 Catalogue, ISO 62443 etc.) is now particularly taken into account when creating a B3S. In addition, the creation, submission and review process as well as the publication of a B3S are now described in detail.

The orientation guide is thus an aid for authors of industry-specific safety standards, but also offers KRITIS operators support in implementing the safety precautions and measures required in Section 8a (1) of the BSIG and may be a tool to support auditors in developing a suitable test basis.

With this in mind, the orientation guide does not contain hard specifications; instead it describes a qualitative framework that permits equivalent alternatives for the described procedure and criteria. It thus allows the conditions in the various critical infrastructure industries to be taken into account and enables KRITIS operators to create B3S adapted to their situation and thus to implement the necessary IT security that is as streamlined as possible.

End of the period for furnishing proof according to Section 8a (3) of the BSIG for operators in accordance with BSI-KritisV from 3 May 2016

By 3 May 2018, operators of critical infrastructures from the first wave of the BSI CIP Regulation (the water, food, energy, information technology and telecommunications sectors) had to take "appropriate organisational and technical provisions in order to avoid errors regarding the availability, integrity, authenticity and confidentiality of their information technology systems, components or processes that are decisive for the functionality of the critical infrastructures operated by them" (Section 8a (1) of the BSIG) and verify this to the BSI.

To support the verification process, the BSI has published an orientation guide in accordance with Section 8a (3) of the BSIG, which explains the most important framework conditions for both the operators and the auditing bodies: it describes the roles and responsibilities of operators, inspectors and audit teams and the qualifications required by the latter two. It additionally explains the tools available for selecting the test basis, how to derive the test topics and the special features to observe with regard to the test methodology, the test plan and documentation of the test results.

German legislation to implement the EU Network and Information Security Directive (NIS Directive) and effects on digital services

In August 2016, the EU Network and Information Security Directive (NIS Directive) came into force, which had to be transposed into national law by the EU Member States by 9 May 2018.

Through the IT Security Act, Germany had already implemented many of the requirements contained in the NIS Directive, particularly for KRITIS operators, in advance. The remaining adjustments and extensions required were made with the law implementing the NIS Directive into national law. The legislator has thus created the basis for the uniform regulation of providers of certain digital services throughout the EU in particular. Compliance with the provisions of this Act has been mandatory since 10 May 2018.

In addition to KRITIS operators, digital service providers (online marketplaces, online search engines and cloud computing services) will now have to report security incidents with significant effects to the BSI. Furthermore, the new regulations provide for a minimum level of measures for preventive IT security and for the reactive management of security incidents. The obligation to register a contact point and provide evidence of the implementation of measures is not anticipated for digital service providers.

As the national cyber security authority, the BSI was tasked with supervising digital service providers. During the reporting period, the BSI has not yet received any notifications of security incidents from digital service providers.

2.2.4 Mobile incident response team

With the Federal Government's Cyber Security Strategy 2016, the focus of the CERT mission increased on local support. The BSIG was therefore amended in June 2017 (Section 5a BSIG) insofar as the BSI is authorised, under certain conditions specified therein, to take measures – including on site – which are necessary to restore the security or functionality of an IT system affected. The BSI then set up mobile incident response teams (MIRTs) to deal with IT security incidents on site. The focus is on Federal Administration institutions and operators of critical infrastructures. In individual cases, MIRTs can also be used by other companies. This is exclusively at the instigation of the body concerned, which must make a corresponding request to the BSI.

Both the procedure and the support options have developed and evolved with the experience gained in these emergency operations.

Among the best-known public MIRT missions are the IT incident at the German Bundestag in 2015, the support of hospitals during the ransomware wave in 2016 and the IT attack on the Federal Foreign Office in 2018.

The seconded MIRT usually consists of an incident handler (IH) and additional experts from various subject areas. In addition to organisational and coordinating support, the MIRT priority is to provide technical support to remedy the detected IT security incident working closely with the operational and IT security personnel at the affected body. To this end, the experts at MIRT try to limit the problem and isolate the cause of the damage. In the event of a concrete IT attack, the objective is to find signatures, also known as Indicators of Compromise (IoCs). The issues that arise are traced in terms of how far and deep the attacker has worked through the network and whether central components have been affected.

The short-term goal of an MIRT mission is to take initial measures to limit damage and ensure emergency operation on site. It is often the direct cooperation and the exchange of information and experience on site with those who look after the affected IT systems on a daily basis that enables the BSI to achieve this goal.

Any long-term clean-up work that may be necessary, such as replanning, expanding or updating the IT systems, is the responsibility of the unit affected. The BSI can provide support within the scope of its advisory work here, but not with an on-site team.

2.2.5 Trends in IT security certification of products

Certification of the IT security of a product by the BSI means that it was tested by an independent party on the basis of public test criteria and in a transparent process (https://www.bsi.bund.de/EN/Topics/Certification/certification_node.html).

For procurement specialists, BSI certification also indicates the following:

- Transparency regarding the effectiveness of the security-related performance
- Decision support for the usability of the product,
- Comparability of the security performance and
- Conformity with national or international standards.

The Common Criteria (CC) test criteria, which were drawn up and maintained by the nations represented in the Common Criteria Recognition Agreement (CCRA https://www.commoncriteriaportal.org) at the time, have now been adopted by the International Organisation for Standardisation ISO. The standard is currently being updated and expanded. The BSI actively participates in this programme together with experts from testing bodies and industry via the German Institute for Standardisation (DIN). The aim is to extend both the concepts for specifying security requirements and the evaluation methodology in order to improve the applicability of the standard to new technologies.

The demand for certified products has already been enshrined in numerous laws and regulations in recent years. For example, the coalition agreement also calls for manufacturers and providers of IT products that are of particular national interest in addition to critical infrastructures to assume greater responsibility. In many cases, this concerns the German government's digitisation projects, e.g. in the areas of eHealth, sovereign documents and smart metering, as well as digital signatures for many years. Since mid-2016, EU countries have been subject to the updated and expanded EU regulation on electronic identification and trust services (eIDAS regulation). Among other things, it regulates the necessary certification for IT products for generating digital signatures. In line with the national Trust Services Act (VDG), the BSI is the public body that verifies the conformity of signature-creation units with the requirements of the Regulation. Certificates issued in this regard will be notified to the EU Commission.

The Mutual Recognition Agreement (MRA) is now actively supported by 15 nations: Croatia, Estonia, Luxembourg, Poland and Denmark have been added (https://www.sogis.org). The member states of the Senior Official Group Information Systems Security (SOGIS) form a strong alliance to promote proof of trustworthiness for IT security products supported by public authorities.

The EU Commission has taken up the issue of certification as part of its efforts to promote cyber security in Europe. The legislative package on cyber security, which will also enshrine an EU-wide certification model, will be voted on at the end of the reporting period (31 May 2018). The European Council and the European Parliament have already discussed the package. The final bill will then be negotiated together with the EU Commission. With SOGIS-MRA, the EU member states already have a strong, well-established certification concept in operation, which is expected to be enshrined under the new EU umbrella.

Product certification is supported by new Protection Profiles (PP). They describe a standard of safety requirements for a particular product type. Examples of new protection profiles used in product certifications are:

- PP for a FIDO token,
- PPs for digital tachographs in line with to current EU regulations,
- PP for database management systems.

Manufacturers are increasingly moving the safety testing of development and production sites from the product certification process to a separate site certification. This streamlines the process of product certification and makes it more efficient.

Conformity testing and certification of IT security components and services

Functionality and interoperability as product features are described as standard within the technical guidelines (TR) of the BSI in terms of functional requirements and can be implemented accordingly. The conformity of an IT product or system to a TR can then be confirmed by the BSI with a certificate.

In the course of this procedure a conformity test is carried out by a neutral testing body on the basis of the test specifications defined in the TR. The test is monitored by the responsible certification body in the BSI and confirmed on completion with a notice of conformity and a certificate. Certification is handled by the German National Accreditation Body (DAkkS) for some TRs. Within the scope of certification in line with the technical guidelines, 60 certificates from 13 test areas were issued between 1 July, 2017 and 31 May, 2018, with 27 initial and re-certifications and 24 maintenance procedures carried out.

In addition to product certification, certification of management systems is also offered, based on the commonly used certification according to ISO/IEC 27001 and is carried out on the basis of the IT-Grundschutz developed by the BSI. The IT-Grundschutz procedure and the recommendations of standard security measures contained in the IT-Grundschutz now represent a de facto standard for IT security.

A total of 38 “ISO 27001 certificates based on IT-Grundschutz” were issued and 73 monitoring audits were conducted in the reporting period.

The BSI is the accreditation and supervisory body for De-Mail providers, whose De-Mail services provide an infrastructure for legally compliant electronic communications in Germany. The following accredited providers have been active in the market since 2012: Mentana-Claimsoft GmbH, Telekom Deutschland GmbH, T-Systems International GmbH and 1&1 Mail GmbH.

European Citizens’ Initiatives (ECIs) need to collect one million statements of support and have reached the minimum levels in at least seven member states for the European Commission to decide on the follow-up action. In order to collect statements of support via the Internet, organisers must make an online collection system available on their website, compliant with the technical specifications set out in Implementing Regulation (EU) No 1179/2011. They must then have their system certified by the relevant authority. The BSI is the national authority responsible for issuing certificates of compliance of online collection systems with the ECI Regulation (Regulation (EU) No. 211/2011). The following certificates were issued from May 2017 to May 2018:

- BSI-EBI-0008-2017 “Stop Extremism”
- BSI-EBI-0009-2018 “We are a welcoming Europe, let us help!”

The BSI is the national supervisory authority for trust service providers in the area of “creation, verification and validation of certificates for website authentication” in accordance with eIDAS regulation and the Trust Services Act (VDG) and is responsible for the qualification of trust service providers in this area. From May 2017 to May 2018, one qualified trusted service provider was certified here.

2.2.6 Investment controls

The Federal Ministry of the Interior, Building and Community (BMI) involves the BSI as part of its competence in proceedings for the control of investments by foreign investors in domestic companies and production facilities in accordance with Sections 4 ff. of the Foreign Trade and Payments Act (AWG) and Sections 55 ff. and Sections 60 ff. of the Foreign Trade and Payments Regulation (AWV).

The standard of review is whether essential security interests or the public order or security of the Federal Republic of Germany are endangered by the intended acquisition. This applies, for example, in cases where the target company manufactures or has manufactured products or essential components for VS-approved systems, where the target company operates critical infrastructures or where the target company manufactures industry-specific software for operating critical infrastructures.

Taking into account the respective economic, legal and technological situation of the buyer and the target company, the BSI analyses and assesses possible risk situations with regard to IT security. The risk assessment is incorporated into the security policy vote of the BMI.

Three factors have led to a significant increase in the audit procedures in which the BSI has been actively involved:

- The number and volume of non-EU investments in German target companies has been increasing for years.
- Foreign investment controls increasingly became a political focus, for example through the takeover of the Swabian robot manufacturer KUKA AG by the Chinese company Midea Group Co Ltd.
- The amendment of the AWV changed important procedural rules in 2017 and also introduced a notification requirement for planned acquisitions in the KRITIS sector, meaning that parties must now generally report or apply for more procedures in order to obtain legal certainty for the planned investment.

The number of individual audits accompanied by the BSI in connection with investment control procedures rose from four procedures in 2015 to 15 in 2016. In 2017, 23 procedures had already been examined by the BSI and it had carried out 31 audits by July 2018.

2.2.7 Export controls

The BSI supports the Federal Office for Economic Affairs and Export Control (BAFA) with applications for export/shipment authorisations based on the submission of export license applications for goods with characteristics or functions of information security 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 of 5 May 2009 (Council Regulation (EC) No. 428/2009). It focuses on the field of cryptographic export control and is structured as follows:

1. Support and (self-)protection of the German cryptology industry
2. Protection of approved IT security products, components such as smart cards and specific technologies against re-engineering, manipulation, etc.

The processing of these applications is a cross-cutting task that requires close cooperation with external authorities, applicants and manufacturers as well as between the various specialist departments of the BSI.

A new approach has been developed for the current bilateral cooperation between the BSI and the BAFA that enables a more comprehensive, faster and quality-oriented processing of applications compared to previous years. This includes the focus of export control on approved IT security products, the impact of which on BAFA applications is clear in Fig. 18.

The BSI processed 102 applications in 2017.

In addition, the BSI became involved in 2017 in the following topics related to BAFA:

- Participation in the revision of the EC Dual-Use Regulation
- Assessment of preliminary requests (applications) for information requiring protection, for example, test reports from the common criteria environment.
- Participation in the sale and acquisition of companies in the field of information security
- Processing of export requests in connection with the BSI encryption software Chiasmus

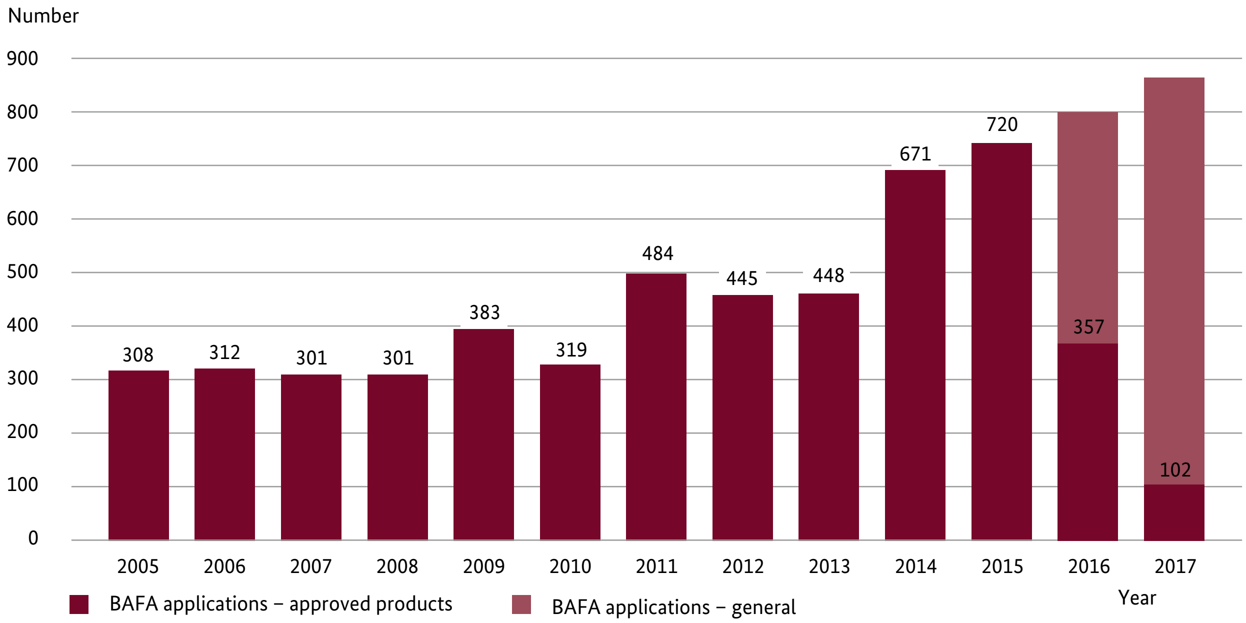


Figure 18 Number of BAFA applications processed at the BSI from 1 May 2005 to 31 Dec. 2017

- Supporting the BAFA with the advice on the list of goods (AzG) to determine the export obligation of a product in the context detailed above

- Securing of concluded Memorandum of Agreements (MoAs) for the export of approved IT security products (classified as VS-CONFIDENTIAL)

- Agreeing optimised cooperation with the BAFA, particularly regarding the revision of national and EU general authorisations (AGG16, AGG24, EU001, EU004 and EU009)

2.2.8 Other solutions and services for business

Securing ad servers

To fund free content on websites (such as news portals), website operators often use online advertising. A typical advertising medium for online advertising, advertising, are banners. They are usually shown at the top or side of the website. From a technical point of view, the advertising is delivered by ad servers: when the user visits an ad-financed website, the website first establishes a connection to the ad servers. The ad server then selects advertising media tailored to the user based on a complex process (real-time bidding) and sends it back directly to the website visitor.

There have been repeated incidents of malicious programmes being hidden and distributed in advertising banners (malvertising) in the past. Examples include attackers compromising existing, poorly secured ad servers or using stolen credit cards to purchase advertising space from marketers in order to spread harmful advertising material. For attackers, online advertising is a promising attack vector: linking an ad server to multiple web pages can achieve a potentially high reach for the distribution of malware. In particular, attackers have the opportunity to place malware on reputable websites if they succeed in compromising the ad servers linked by the website operator.

In order to make online advertising safe, the BSI has created a discussion paper for securing ad servers. It is aimed at those involved in the online advertising industry, particularly ad server operators and marketers. The document includes recommendations, which state-of-the-art measures must be taken into account in order to technically secure IT systems in the online advertising industry. This includes an encryption method that is recognised as secure, so that, among other things, the delivery of advertising material between the web server and client is encrypted.

As ad servers are treated as telemedia providers in business terms, their operators must, among other legal requirements such as Article 32 of the General Data Protection Regulation (GDPR), implement the security measures according to Section 13 (7) of the German Telemedia Act (TMG), which have been introduced within the framework of the IT Security Act (IT-SiG). The recommendations in the discussion paper are intended to support the online advertising industry in implementing these security measures.

Members of the German Association for the Digital Economy (BVDW) and Bitkom have commented on the discussion paper, which is currently at the final agreement stage. Publication is expected in the course of 2018.

Cloud Computing: Compliance Controls Catalogue C5/ Attestation in line with C5

With the requirements catalogue for assessing the information security of cloud services (Cloud Computing Compliance Controls Catalogue or C5), the BSI has published an auditing standard that defines a minimum security level for cloud services (see https://www.bsi.bund.de/C5). In line with BSIG Section 8, the minimum standard "Use of external cloud services" (https://www.bsi.bund.de/DE/Themen/StandardsKriterien/Mindeststandards/Nutzung_externer_Cloud-Dienste/Nutzung_externer_Cloud-Dienste_node.html) demands this level and the corresponding proof (attestation) for the use of external clouds for all federal offices.

The cloud market has taken up this requirement for federal agencies and companies are now also using C5 attestation for cloud use. This is evident from the wide range of attestation issued during the reporting period:

- August 2017: Attestation for Microsoft Azure Services from Germany

- November 2017: Attestation for the Dropbox Services Business and Education

- December 2017: Attestation for the services of Alibaba Cloud from the regions Frankfurt and Singapore

- March 2018: Attestation for Microsoft Office 365 from Germany

- April 2018: Renewal of the C5 attestation for the services of Amazon Webservices from Frankfurt

- May 2018: Attestation for IBM's Infrastructure-as-a-Service services worldwide

2.3 Target audience: society

An important task of the BSI is to provide information and raise the awareness of citizens to ensure secure handling of information technology, mobile communications and the Internet. To this end, the BSI has developed a comprehensive range of information under "BSI for Citizens" (https://www.bsi-fuer-buerger). The BSI is also involved in numerous digitisation projects ranging from the eID card function to autonomous driving, where it brings its expertise to the table. It works with relevant social groups and scientists. The German Federal Government's coalition agreement between the CDU, CSU and SPD in February 2018 also stipulates that consumer protection should be established as an additional task of the BSI.

2.3.1 Coalition agreement: new consumer protection task

The addition of consumer protection strengthens the BSI profile as a citizen-orientated cyber security authority. The BSI wants to support consumers in order to increase their resilience against cyber threats of all kinds. The BSI makes an important contribution to the design of information security and contributes to the success of digitisation.

As a manufacturer-independent and competent technical body, the BSI already supports consumers in the risk assessment of technologies, products, services and media offerings. To increase risk awareness, assessment ability and competence in the field of information security, already at the BSI existing activities are to be bundled and new measures introduced.

Cooperation with strong partners is necessary to achieve these goals. This is the starting point for the planned intensification and expansion of activities to support consumers in Germany.

The BSI has already approached established and recognised players in the area of consumer protection to establish cooperative efforts. A Memorandum of Understanding between the BSI and Verbraucherzentrale NRW (the Consumer Association of North Rhine-Westphalia) was concluded in March 2017. An example of this cooperation is the joint approach regarding the lack of update capability of smartphones that are sold as new with an outdated operating system, which can lead to serious security vulnerabilities when they are used. With the support of the BSI, the Consumer Association of North Rhine-Westphalia has initiated legal actions against a seller of such devices on the basis of insufficient consumer information. The process was ongoing at the end of the reporting period.

2.3.2 BSI citizen services

The BSI has run the website www.bsi-fuer-buerger.de for over 15 years. Users can find articles and information on current topics as well as check lists and, most recently, more descriptive explanatory videos and information graphics on Internet risks and the safe use of IT. In the reporting period, the range of information available about the Internet of Things was expanded and this information is now available on the website, including recommendations for smart-home applications. In October 2017, this information was published as a brochure entitled "Internet der Dinge – aber sicher!" ["Internet of Things - securely, of course!]. Information and recommendations on wearables are also available.

The free warning and information service "Bürger-CERT" is also part of the information service on www.bsi-fuer-buerger.de. The BSI uses this service to provide fast and competent information on the website and by subscriber e-mail – either in the form of "technical warnings" or through its fortnightly newsletter "Secure + Informed" ["Sicher ° Informiert"] – about vulnerabilities, security vulnerabilities and other risks, providing specific support information. Around 105,000 subscribers currently take advantage of this offer.

With the Facebook page www.facebook.com/bsi.fuer.buerger and the Twitter channel www.twitter.com/BSI_Presse, the BSI is also represented in social networks, providing information for users and offering an opportunity for dialogue. As of 31 May 2018, 34,160 people followed the BSI on Facebook and 11,715 on Twitter.

Private users can call the BSI Service Centre on 0800 2741000 or send an e-mail to mail@bsi-fuer-buerger.de with their questions on IT and Internet security issues. On average 600 requests from private users reach the BSI every month. In addition, private users and organisations can obtain copies of the BSI citizens' brochures free of charge.

European Cyber Security Month (ECSM)

In October 2017, the European Cyber Security Month (ECSM) took place for the fifth time throughout Europe under the leadership of the European Network and Information Security Agency (ENISA). As in previous years, the BSI assumed the role of the national coordination centre in Germany. In total, 104 partners were inspired to participate in over 216 events over the month. An overview of these events – from awareness events and live hackings to webinars and online campaigns – can be found at www.bsi.bund.de/ecsm.

The BSI participated in the weekly main topics "Cyber Security at the Workplace", "Security and Protection of Personal Data", "Cyber Security at Home" and "Communicating Cyber Security – to Professionals and Users" with its own events in the form of a press release, topic-related Facebook postings and a statement video in which an expert from the BSI explained a central question from the topic area.

The issue of secure smart homes also came under scrutiny at www.bsi-fuer-buerger.de during the ECSM: in addition to two current information texts, an animated explanatory video was published, giving website users the chance to test their knowledge in the online quiz "Smart home – are you sure it's secure?". In addition, a brief expert discussion was recorded and made available to radio stations as a broadcast-ready service via a service provider.

At its Bonn location, the BSI took part in the Bonn Cyber Security Days from 23–27 October 2017, participating in the "Dark Cyber Monday" action day with an information stand with live robot hacking and giving a specialist lecture.

Cooperation with ProPK

The cooperation between the BSI and the Police Crime Prevention (ProPK) of the Federal States and the Federal Government continued in the reporting period. Among other activities, the two partners communicated together on secure networked homes and the regular creation of back-ups. The BSI and ProPK published the results of a joint representative online survey of citizens on the topics of Internet security and Internet crime experiences at the Safer Internet Day on 6 February 2018 (see separate chapter on survey results).

2.3.3 Institutionalisation of social dialogue

The BSI has been involved in intensifying social dialogue in the area of information and cyber security since 2016. By establishing the "Secure Information Society Ideas Workshop" it has ensured open and trusted exchange on questions of cyber security between the state, business, science and civil society. This work was strengthened and extended in the "Digital Society: Smart & Secure" project. Among other things, it jointly developed findings on "inspiring a smart and secure digital society" which were presented to the public in September 2017. The fruitful discourse has motivated the BSI to continue on this path and a follow-up project entitled "Institutionalisation of Social Dialogue" is currently extending and strengthening this dialogue of trust. It is developing and testing opportunities for institutionalisation involving participatory approach.

BSI in Dialogue

BSI in Dialogue is a series of events launched in mid-2016 for the target groups of politics, business, associations and society aimed at stimulating dialogue on strategic issues of cyber security. This should raise the BSI profile with the target groups, make the tasks of the BSI more transparent and increase public awareness of the BSI and information and cyber security in general. Further BSI in Dialogue events on various focal points with different target groups are planned in future.

The format of the event further promotes a personal exchange on an equal footing, creating associated synergy effects for the cyber security situation in Germany.

Special electronic mailbox for lawyers (beA)

Situation
Security problems with the special electronic mailbox for lawyers (beA) became apparent at the end of December 2017. A member of the Chaos Computer Club had analysed the "beA Client-Security" software required for mailbox access, encryption and decryption of messages and, in addition to outdated software libraries with security holes, had also discovered the private key of a TLS certificate that was delivered with the software.

The Chaos Computer Club first reported the problems to the German Federal Bar (BRAK), which maintains the beA, and the CERT-Bund of the BSI. At the same time, he informed the certification authority that issued the TLS certificate about the obvious compromise of the private key. The company withdrew the corresponding certificate in accordance with its certification guidelines.

Cause and Damage
The delivery of a private TLS key in the client software was necessary for the intended architecture of the beA mailbox: the beA Client Security runs an HTTPS server on a local port and communicates with the webmail interface of the beA mailbox in the user's web browser.

In order not to endanger the usability of the beA mailbox for passive use from 1 January 2018, BRAK provided information about the invalidity of the certificate and provided a self-signed TLS certificate (again including the associated private key as a matter of principle) in exchange. Lawyers should now install this certificate manually on their systems.

However, this certificate was a root certificate that could be used to issue certificates for any web domain. On affected lawyers' computers it would have been possible to read or manipulate the communication traffic in encrypted Internet connections.

Based on information from the IT security sector, BRAK stopped the distribution of the certificate and the corresponding installation instructions immediately and requested the certificate be uninstalled again.

Reaction
BRAK switched off the beA mailbox on the server side until further notice after the security holes were discovered and organised a "beAthon" in January 2018 to discuss the security problems with the original discoverer and other security researchers. In addition, BRAK commissioned an independent expert report from an independent IT security service provider.

At the same time, the contractor commissioned by BRAK with the development worked on solving the security problems. On 4 July 2018, BRAK will make a new version of beA Client-Security available to the attorneys for download, in which the identified vulnerabilities are verified as corrected by the IT security service provider; according to current planning, the beA mailbox is to be put back into operation on 4 September 2018.

The BSI was in contact with BRAK and the contractor responsible for beA Client Security at an early stage.

From the BSI's standpoint, the withdrawal of the vulnerable software was the correct reaction on the part of the provider, even if a statutory requirement could not be met as a result. Data security correctly took precedence over functionality in this case.

Recommendation
Where it still exists, the self-signed TLS certificate provided by BRAK on 22 December 2017 should be immediately removed from affected computers.

BRAK also recommends the complete uninstallation of the old version of beA Client-Security and will release a new version of beA Client-Security on 4 July 2018, for which BRAK affirm that the security problems will be rectified. The certificate provided on 22 December 2017 will automatically be deleted in this version.

2.3.4 Digitisation projects in Germany

Digitalisation and energy transition/ smart metering systems

A successful digital transformation in the energy industry can only succeed with the early national development and provision of compulsory security standards and measures to ensure the trustworthiness of digital infrastructures ("privacy & security by design"). Consequently, a national reference market with secure product components, systems and communication infrastructures is crucial initially in order to play a leading role in the digitisation of the energy sector and, based on this, to shape European and international standards.

On behalf of the Federal Ministry for Economic Affairs and Energy (BMWi), the BSI develops protection profiles and technical guidelines as well as test methods for the Smart–Meter-Gateway as a central communication platform for intelligent measurement systems. Together with the technical standards of the BSI, the Digitalisation of the Energy Transition Act creates a binding framework for the secure and privacy-compliant use of charging stations and already shows how the minimum requirements must be designed to securely integrate the charging station infrastructure of electric cars into the smart power grid.

The use of the batteries of electric vehicles for electricity storage and the generation of control energy, which is used to compensate for the fluctuating supply from wind farms and solar systems, will play an increasingly important role. The future integration of the Smart-Meter-Gateway into the charging station thus enables secure charging and billing in compliance with data protection requirements, which is a basic prerequisite for the increasing spread of electric mobility. According to the BMWi-BSI roadmap ("Standardisation strategy for cross-sector digitisation in line with the Digitalisation of the Energy Transition Act"), the three main clusters for the further development of standards will be the application areas smart meters & submetering, smart grids & smart mobility and smart home & building & services.

Autonomous Driving, Strategy Paper BMVI

The German government's strategy for automated and connected driving defined IT security as a key area of action. In view of increasingly complex information technology and the numerous communication interfaces in modern vehicles, suitable measures must be identified to prevent hacker attacks, for example. In the joint IT security and data protection working group and the associated IT security sub-group, the Federal Ministry of Transport and Digital Infrastructure (BMVI), the BSI and other stakeholders from public agencies and industry have developed a series of corresponding recommendations for action in this context. It includes consideration of the following aspects:

- Type approval:
  In view of the possible effects of IT-based attacks on vehicle occupants and other road users, IT security mechanisms must be designed and implemented at an early stage in the development of (connected and/or automated) vehicles. These should then be checked in the context of type approval, which is a prerequisite for approval in road traffic. Suitable requirements and test criteria shall be established for this purpose. The United Nations Economic Commission for Europe (UNECE), which carries out the international harmonisation of type-approval regulations, is currently discussing the basics of such requirements.

- Certification:
  In the field of traditional IT security products, Common Criteria have been established for many years as the basis for internationally recognised certifications. Testing this type of certification is also recommended for IT components in vehicles with dedicated safety functionality and high protection requirements (e.g. central communication interfaces or components for vehicle-to-vehicle communication), as part of the type approval process, for instance.

- IT security in the field:
  Given the complexity of the software in vehicles required for the new functions and the experience gained from traditional IT, it can be assumed that some weak points and security vulnerabilities will only be discovered once the vehicle model is already on the market. Procedures must be established to minimise the resulting hazards. There must be discussion on the structure of suitable reporting channels for IT security incidents and how to ensure update management by the respective manufacturers. Furthermore, public agencies should be enabled to monitor IT security on a random basis even after approval, by means of penetration tests, for example.

eID: Europe-wide recognition of the online identification function

The secure identification of people and things is of crucial importance for the implementation of digitisation. 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 digitisation 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 at EU level. With its expertise, the BSI participates in its further development and technical implementation in all areas.

In September 2017, Germany was the first EU member state to successfully complete the notification of the online identification function of the ID card and electronic residence permits at the highest level of assurance in accordance with the eIDAS Regulation. Within the framework of the notification, the German eID system was peer reviewed by the other member states of the EU/European Economic Area (EEA). In the decision by the Cooperation Network – the EU body responsible for coordinating eID issues – the German system was certified on the basis of the final report of the peer review as meeting the eIDAS requirements at a "high" assurance level. The BSI carried out the technical preparatory work for the notification of the online identification function and accompanied the entire notification process from a technical point of view.

This requires all EU/EEA Member States to recognise the online identification function for public sector applications, particularly in eGovernment, from September 2018. Companies in other EU countries can also recognise electronic identity verification on a voluntary basis.

In terms of the recognition of electronic identities of other Member States in German eGovernment, preparations are also in full swing with the support of the BSI. The infrastructure for technical integration into the German eID system was created in the EU-funded TREATS project. This infrastructure is currently being integrated into the eGovernment applications to ensure Germany complies with the eIDAS identification regulation by September 2018.

In the first quarter of 2018, five more countries – Estonia, Spain, Croatia, Italy and Luxembourg – have started the notification of their eID systems and further notifications are expected in the course of the year.

Two-factor authentication

Secure authentication is required in many areas of electronic business processes - from online shopping to home banking. Up to now, single-factor authentication has been used in many areas, which usually relies solely on the knowledge factor in the form of a password. However, this involves several disadvantages:

- On the one hand, possession of this one factor is enough to break the authentication mechanism.

- On the other hand, itis extremely time-consuming for users to create and memorise a secure and individual password for each service.

Secure two-factor authentication can help here. Instead of one factor, two factors are used for authentication. These two factors must belong to different categories (ownership, knowledge, biometrics) to ensure that the strengths of the factors complement each other and are interlinked so that the two factors cannot be attacked independently. Instantiating such secure two-factor authentication is a security element. Here, the knowledge factor (in the form of a password or a PIN) is securely combined with the possession factor (the security element in the form of a smart card, for example) – the PIN is used to activate the card, on which the security element then uses cryptographic methods to prove ownership to the authentication server.

Secure two-factor authentication solutions have not been widely used to date. The Fast IDentity Online Alliance (FIDO) was formed in 2012 with a variety of stakeholders to develop open and license-free industry standards for worldwide authentication on the Internet. According to FIDO, two standards have been developed so far:

- The Universal Second Factor (U2F) fits seamlessly into existing web infrastructures in the form of a USB token.

- The FIDO UAF standard (Universal Authentication Framework) also allows the possession factor to be replaced by biometric procedures and thus implementing a secure two-factor authentication with simultaneous waiving of any passwords.

However, proof of the security of the U2F token used or the implementation of the UAF standard is necessary to ensure a secure implementation of the protocols in products.

As a member of the FIDO Alliance, the BSI is involved in the definition of verifiably secure authentication tokens. Proof of a high level of security can be provided by Common Criteria certification. The BSI has published such a protection profile with high test depth (EAL4+, AVA_VAN.5) for secure FIDO-U2F tokens (BSI-CC-PP-0096-2017), according to which a FIDO-U2F token developed by the BSI is currently being certified. After completion of the certification, the necessary manufacturer documents are published to enable other manufacturers of FIDO tokens easier access to the certification of their own products.

Technical security device for electronic recording systems

In the course of digitisation, electronic cash register systems or cash registers (electronic recording systems) are generally used today for the sale of goods and services. As a result, the technical environment for taxation procedures has changed considerably. Subsequent tampering with electronic cash register system recordings (digital primary accounting records) without appropriate protective measures can only be detected with a great deal of effort.

The Digital Primary Accounting Record Anti-Tampering Act [Gesetz zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen] therefore aims to make tampering with such records significantly more difficult. The central technical component for implementing the draft law is the introduction of a technical security device.

From 2020, electronic recording systems must have a certified technical security device consisting of three components:

- Security module:
  This ensures that cash register entries are logged at the beginning of the recording process and cannot be changed later without detection.

- Storage medium:
  The individual records are stored on the storage medium for the duration of the statutory retention period.

- Standardised digital interface:
  this should ensure seamless data transmission for verification purposes.

The standardised digital interface for the technical security device is also intended to simplify integration into existing and future electronic cash register systems. In particular, no special requirements on the physical interface are planned for the digital interface, so that common standard interfaces such as USB, Ethernet, SD cards, etc. can be used.

Once the legal framework is established by the adoption of the law, the technical requirements for the security module, the storage medium and the digital interface is defined by the BSI in technical guidelines and protection profiles.

The technical guidelines were agreed with the Federal Ministry of Finance and relevant professional associations and published in June 2018. This leaves sufficient time to develop and market technical safety equipment.

2.3.5 Electronic Passport

The first generation of electronic passports was introduced in Germany on 1 November 2005, followed two years later with the second generation integrating fingerprint images. The third generation was launched on 1 March 2017, updated with a completely revised external look and new physical security features. The most striking change is the introduction of a flexible cover, which replaces the familiar hardcover passport book, and the introduction of a polycarbonate data page similar to the identity card and electronic residence permit. As a result, the chip has also moved from the front passport cover to the data page.

The electronic component, the chip, will also undergo a fundamental revision. Under the leadership of the BSI, the chips currently maintained separately for passports, identity cards and residence permits are being transferred to a common platform ("family concept"). This reduces the logistical costs. On the other hand, it is ensured that the latest chip generation can be used in all documents.

Recent incidents (e.g. ROCA, see info box on page 35) show that even in the area of chip cards – especially with ten-year validity as in the case of German sovereign documents – it is important to react to security incidents, even if German documents are not affected by ROCA itself. The BSI is therefore working with the manufacturers to look at the option of a post-issue chip update. The update option would also to be introduced as part of the new chip platform. In addition to the introduction of an appropriate chip-side option, the update also requires the corresponding infrastructure, which is also being prepared.

At European level, too, the requirements for passports and residence permits are currently being updated with the intensive cooperation of the BSI. In addition to the technical update this would also make it possible to finally replace the aging access protection Basic Access Control (BAC) with the Password Authenticated Connection Establishment (PACE) developed at the BSI.

2.3.6 Seal of approval/ IT security identifiers

In the Cyber Security Strategy for Germany published in 2016, the BMI announced the introduction of a seal of approval for IT security. This security identifier is intended to enable consumers to make IT security an integral part of their purchasing decisions. The plan was confirmed in the 2018 coalition agreement. At the same time, an expansion of the BSI portfolio to include the topic of consumer protection is planned. The IT security identifier is embedded in the BSI's expanded task of consumer protection.

The certification of IT security products is already one of the BSI's established procedures. Manufacturers can have their products certified by the BSI and use this certificate to prove that their products comply with a specific IT security level depending on the test depth in terms of IT security. Previously, the certificates were aimed at professional users and products certified by the BSI are usually used in federal digitisation projects.

A solution for the wider market of consumer products that impacts consumers is a departure from this established certification procedure.

As a consumer purchasing decision is at stake here, the IT security identifier must be easy to understand and designed in a transparent manner. Consumers must be made aware of the IT security identifier either visually on the product (or in a web shop) accompanied by security information. The IT security identifier must also have a dynamic design, meaning that it must be able to communicate whether the security statements are up to date and valid. Manufacturers will be incentivised to use the seal voluntarily as this will distinguish their products from the competition. The IT security of products must be a selling point.

The prerequisite of a voluntary IT security identifier are transparent technical criteria on which basis the IT security identifier can be used. To date, these criteria have been published by the BSI in the form of Protection Profiles or technical guidelines and will be extended in future by requirements for IT products on the consumer market. This allows BSI to define what is state of the art.

In the context of the use of an IT security identifier, it will be necessary to establish a legal framework that allows manufacturers' requirements to use the IT security identifier transparently and quickly (manufacturer's declaration). However, the legal framework must guarantee that the informative value is sufficient and that manufacturers comply with the IT security characteristics promised to consumers. As different IT security requirements will apply to different product categories, the IT security identifier will be offered for the relevant products in the consumer market gradually over time.

2.3.7 Biometric Evaluation Centre

Biometric systems are reliable and easy to use. As a result, they have become established within IT security systems for user authentication. They have been part of everyday life in the consumer sector for many years and are also becoming increasingly important in public applications.

However, the actual quality of a biometric system can still only be determined with great effort. Extensive tests with significant numbers of test subjects and far-reaching attempts to overcome them are the only way to make reliable statements about the functionality and vulnerabilities of a biometric system.

The BSI also strives to contribute its expertise in the entire spectrum of biometric procedures, from the development of new technologies and consulting with manufacturers to the support and monitoring of biometric procedures in operation – with efficient and independent evaluation methodologies as the basis of every project. The higher the requirements for IT security and reliability, the more extensive the evaluation has to be – and this every time software and hardware is changed.

For example, biometric authentication technologies for personal identification in connection with electronic ID cards also play a central role in the European entry/exit system (EES). The systems in place must be highly reliable and secure. This is vital for the practical implementation of the EES objectives.

In cooperation with the Federal Police, the BSI has taken on the task, among other things, of continuously checking the performance and security of the biometric EES systems used and of advancing the development of new, secure technologies and corresponding test and certification procedures. In particular, this requires suitable laboratories in which the test systems can be assessed with larger groups of test subjects under controlled conditions.

These tests are carried out in the new Biometric Evaluation Centre (BEZ), which is currently being established on the campus of the Bonn-Rhein-Sieg University of Applied Sciences (HBRS) in St. Augustin. The BEZ provides the appropriate test and analysis infrastructure to conduct regular "performance", "security" and "usability studies on biometric systems with large user groups". The BEZ is a publicly funded institute at the HBRS and is operated under the close cooperation of the BSI and HBRS. In this way, the BSI can carry out all necessary investigations within the framework of the EU-EES project in the BEZ. This cooperation will be systematically expanded in future.

An important task in promoting the harmonisation of EES systems in Europe will be training measures for police (Federal Police or Frontex), testing laboratories and manufacturers.

Centralising these test competencies in the BEZ enables the evaluation of biometric systems to be undertaken much more efficiently and reliably than was previously possible. With the BEZ, the BSI supports manufacturers, developers and users alike and generates the greatest possible synergy for the Federal Government as a whole.

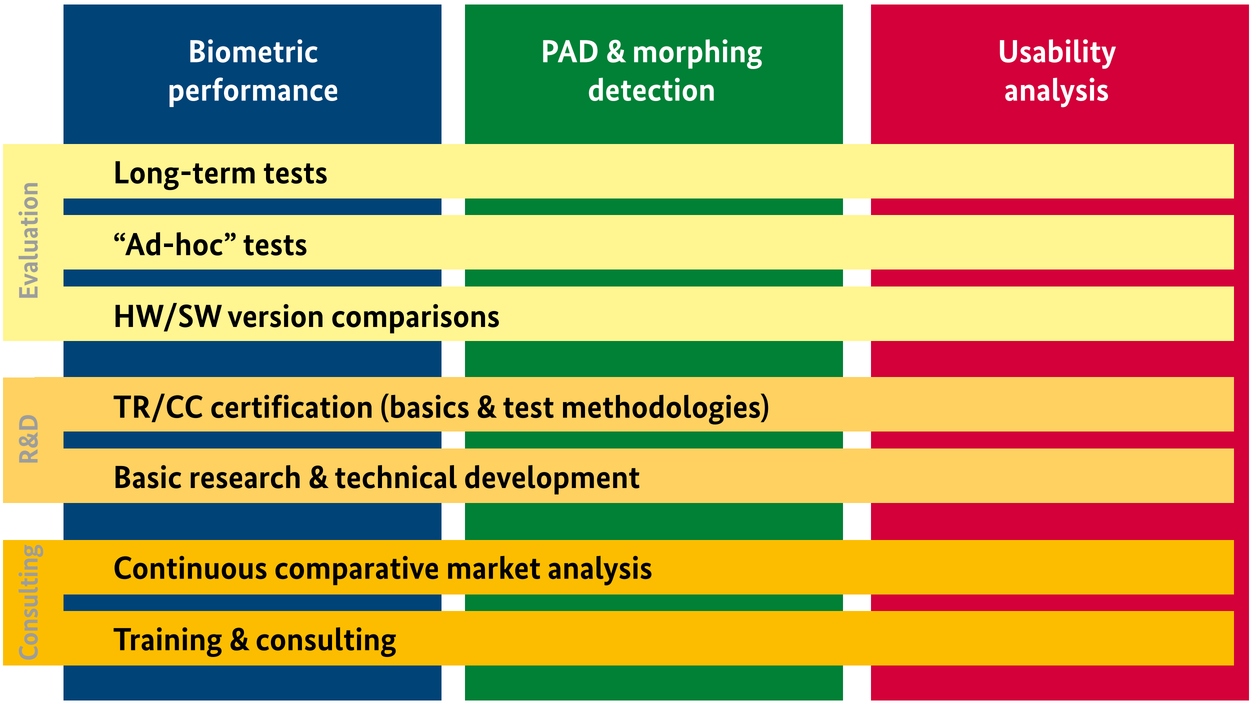

Biometric performance
PAD & morphing detection
Usability analysis
Evaluation
Long-term tests
"Ad-hoc" tests
HW/SW version comparisons
R&D
TR/CC certification (basics & test methodologies)
Basic research & technical development
Consulting
Continuous comparative market analysis
Training & consulting

Figure 19 Action areas and activities of the BEZ

2.3.8 Blockchain key issue paper

For some time now, blockchain has been developing as a new technology for decentralised, tamper-proof and consensual data storage in distributed networks. Blockchain technology is currently viewed as having great potential – not only for use in the financial sector (where cryptocurrencies such as bitcoin were the classic blockchain applications), but also in healthcare, the energy market, the public sector and in many other industries. At the same time, spectacular errors and crises in bitcoin and other blockchain applications are repeatedly made public that test trust in the new technology.

At present, many security, regulatory, legal and socio-technical questions remain unanswered with regard to the use of blockchain. Establishing IT security is particularly essential for the long-term success of blockchain technology in the various application areas.

Many of the classic challenges facing IT security such as network security, endpoint security or implementation security are also relevant when using blockchain technology. The use of strong cryptography and secure protocols is also of great importance for all applications, especially where blockchain is used to secure state or other critical services. Particularly in applications that store security-relevant (e.g. personal) data in a blockchain, the long-term confidentiality and integrity of the data must be ensured by cryptography.

In February 2018, the BSI published five key issues on the subject of blockchain and IT security that are intended to stimulate dialogue between the state, business and society and are to be continuously developed further. The key issue paper is available at https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Eckpunktepapier.pdf.

2.3.9 Secure e-mail transport

Much of today's digital communication still takes place using the speed and convenience of e-mail. In practice, however, the consistent application of IT security is often neglected. To counteract this, the BSI has defined a uniform standard by the Technical Guideline "Secure E-Mail Transport (BSI TR-03108)", which serves e-mail service providers as a blueprint for the secure operation of their e-mail services. The requirements of the technical guideline aim in particular at the functionally and cryptographically secure configuration of the communication interfaces in order to guarantee high-quality transport security, using modern standards such as DANE that have been tested in practice already. The requirements are to be implemented solely by the e-mail service providers. Users of e-mail services thus benefit from a high level of IT security without having any additional efforts.

The first draft of the technical guideline, published in 2015, was prepared in dialogue with e-mail service providers in the market. The concept on which the design is based has been constantly developed, with the focus on IT security, practicality and user acceptance. The core of the concept is that the technical guidelines does not create a new self-contained system, but instead increases the IT security of the already existing e-mail infrastructure. In addition to the use of high-quality cryptographic methods, signed DNS queries, mandatory encryption and trustworthy certificates are main requirements of the technical guideline. These requirements were chosen in a way that a secure connection between e-mail service providers is always established when both parties fulfil them.

The majority of e-mail service providers operating in Germany have already implemented the requirements of the technical guideline. It was also met with great international interest and has many supporters. A close contact with the Dutch National Cyber Security Centre (NCSC) was established for example and a joint endeavour to promote the use of modern e-mail security standards in Europe and beyond was started. With every e-mail service provider that meets the requirements of the technical guidelines, the network of secure e-mail transport expands globally.

2.3.10 Security standard for broadband routers

Broadband routers are used to access the Internet in many households. As well as providing access to the Internet, they are widely used to manage a private home network. Thus, they can be attacked from both sides – locally (via cable or radio interfaces) and from the Internet. This means that routers carry a particular threat potential.

Broadband routers are relatively powerful integrated systems. This gives them the potential to successfully defend digital attacks. Attacks can be initiated by taking control of the router itself, e.g. DDoS attacks. In 2016, for example, attackers attempted to infect almost one million routers with malware via a remote maintenance port and to integrate them into the *Mirai* botnet. This failed because the routers crashed when attempting to install the malware. However, infections with malware often suceed unnoticed, which makes it important to provide basic protection. In the best case, infection of the router can be prevented in advance.

Establishing the technical guidelines for broadband routers the BSI created a basis for protecting broadband routers and making them resistant to certain attacks.

They include the following distinct attack scenarios and threat types:

- The router is attacked to gain control of it.
- The router is attacked to access the owner's private network.
- The router is attacked to gain unauthorised Internet access.

The technical guideline for broadband routers sets effective security requirements for router functions and interfaces. For example, the ability to install updates is mandatory. For better transparency, the manufacturer of the broadband router should specify in the configuration interface, for example, the deadline for providing updates. Likewise, the router should only ever open the ports that are absolutely essential for the functions it currently offers. Remote maintenance ports should only be opened if the router has been configured in advance. The technical guideline also requires that the configuration interface can only be accessed with sufficiently strong authentication and recommends, for example, using multi-factor authentication.

The requirements were developed in cooperation with manufacturers, associations and other representatives from business and society. The Technical Guideline has been completed and can be used as a basis for national and international use.

2.3.11 Cooperation with science

The BSI is constantly in contact with German cyber and IT security researchers. For example, representatives of the leading IT security research locations discussed the challenges in the field of IT and cyber security, looking at possible solution approaches, with representatives of the BSI at the "BSI in Dialogue with Science" event organised by the BSI. The participants included the CISPA – Helmholtz-Zentrum (previously the Center for IT Security, Privacy and Accountability, Saarbrücken), Center for Research in Security and Privacy (CRISP, Darmstadt), Fraunhofer Institute for Applied and Integrated Security (AISEC, Munich), Competence Center for Applied Security Technology (KASTEL, Karlsruhe), Fraunhofer Institute for Communication, Information Processing and Ergonomics (FKIE), Cyber Defence Research Institute (CODE, Neubiberg) and the Horst Görtz Institute for IT Security (HGI, Bochum). The BSI has been and continues to be represented in the advisory boards of various research projects, such as the EU Horizon 2020 project Hardware Enabled Crypto and Randomness (HECTOR). This addresses the interaction between mathematical security, implementation security and the efficiency of cryptographic systems using a holistic approach. The BSI is also represented on the Advisory Board of the EU Horizon 2020 project Robust and Efficient Approaches to Evaluating Side Channel and Fault Attack Resilience (REASSURE), which enhances the efficiency, quality and comparability of side channel analyses in the context of security assessments. The BSI uses its involvement to meet its commitment to the EU as a national cyber security authority. In addition, the BSI specifically promotes promising approaches to the further development of IT/cyber security through letters of support.

Furthermore, the BSI is also involved in supporting the establishment and design of the "Agency for Disruptive Innovations in Cyber Security and Key Technologies" (ADIC), which is laid down in the coalition agreement and is intended to undertake tasks similar to US DARPA and to promote security-relevant key technologies.

On behalf of the Federal Ministry of the Interior (BMI), the BSI also supports the Federal Ministry of Education and Research (BMBF) in arranging research calls. For example, the BSI was involved in the content design of the research programme of the EU Commission "Horizon 2020 – secure societies" for the years 2018 to 2020 and the Federal Government's research framework programme on IT security "Self-determined and secure in the digital world 2015-2020".

Representatives of the BSI regularly hold technical discussions with the cyber and IT security research locations in Germany in order to stay up to date with the latest research results. Over the past year, for example, it has visited CISPA and the Fraunhofer Institute for Telecommunications (Heinrich Hertz Institute, HHI) in Berlin.

eFail – vulnerabilities in OpenPGP and S/MIME implementations

Situation

Security researchers from Münster University of Applied Sciences, Ruhr University Bochum and KU Leuven (Belgium) have found serious weaknesses in the implementation of the widely used e-mail encryption standards OpenPGP and S/MIME which they published on 14 May 2018 at https://efail.de/ Attackers can manipulate encrypted e-mails in such a way that the content of the message is forwarded to them in plain text after decryption by the recipient. However, the title of the research work is misleading, since the vulnerabilities related less to the standards than their implementation in the respective mail clients. This led to misunderstandings following the publication.

Cause and Damage

To exploit the vulnerabilities, an attacker must have access to the recipient's transport route, mail server, or mailbox. In addition, active content on the recipient side must be permitted, such as the execution of HTML code and, in particular, the subsequent downloading of external content. This is currently the default setting, especially for mobile devices.

Reaction

Since November 2017, the BSI has been involved in the process of Coordinated Vulnerability Disclosure by the research team detailed above. In conjunction with the publication of the eFail vulnerabilities, the BSI has therefore published recommendations and informed its national and international partners, the Federal Administration, the federal states and numerous KRITIS companies about suitable measures for the secure use of e-mail encryption.

Recommendations

The e-mail encryption standards mentioned can, in the estimation of the BSI, still be used securely if they are correctly implemented and configured for security. The standards are currently being adapted and implemented by the respective applications in the medium term. Most e-mail client vendors have already taken action against eFail as well as against the direct extraction of data, i.e. without encryption, in their products.

As a rule, the BSI recommends more security in the e-mail communication with regard to avoiding the display and generation of e-mails in HTML format. In particular, the execution of active content, i.e. the display of e-mails in HTML format and reloading remote content should be deactivated. In this way, users can prevent espionage of e-mail plain text via eFail vulnerabilities. If an e-mail provider uses the settings of its Webmail application and offers the possibility to do so, appropriate measures should be implemented. Independently of special security updates, protection is also provided by secure configuration.

The respective manufacturers also explain on the following websites how users of common e-mail programmes are able to prevent remote content from being reloaded:

- Microsoft Outlook - Block automatic picture downloads in e-mail messages
  https://support.office.com/en-us/article/block-or-unblock-automatic-picture-downloads-in-email-messages-15e08854-6808-49b1-9a0a-50b81f2d617a?ui=en-US&rs=en-US&ad=US
- Mozilla Thunderbird - Block remote content in messages
  https://support.mozilla.org/en-US/kb/remote-content-in-messages
- Apple Mail - Show or hide remote images
  https://support.apple.com/kb/PH4873?locale=en_US

Regardless of any vulnerabilities found, the type of connection is important in the context of communication with the e-mail service provider and the exchanged data. For example, if Internet Message Access Protocol (IMAP) is used, data are synchronised between the server and the client on the mobile device.

Depending on the mail client and its configuration, an e-mail can be decrypted locally and a decrypted copy then returned to the server, where it is stored in plain text.

2.3.12 Social networks

In March 2018, criminals sent mass messages in Facebook Messenger disguised as messages from Facebook friends containing a link to an alleged YouTube video. The link went to a bogus Facebook login page. As soon as a user entered his or her login details, the criminals were able to access the victim's Facebook account. This might also include the Facebook pages where the actual owner of the Facebook account had administrator rights.

Unfortunately, this incident is not an exception. Criminals use social networks to lure users to malicious websites, attempting to reach the access data of accounts or to infect the computer with malware.

Dubious companies also try to access sensitive personal data such as addresses, telephone numbers and hobbies from social networks in order to place targeted advertising, for example. They use the opportunity to systematically analyse data from personal profiles via the programming interface of the social network, disguised as an app.

Many of the current threats in social networks are due to users' lack of security awareness. They need to know the hazards better in order to protect themselves and their own data.

To protect against stolen passwords, social media users should use two-factor authentication. This prevents criminals from accessing accounts even if the password is intercepted. Furthermore, when using apps on social networks, users should carefully set up access rights for apps to make it more difficult to collect personal data.

In general, links or short links in Facebook, Twitter or other services should only be opened if you are absolutely sure that they come from a trustworthy source. If such content appears suspicious, users should check with the sender whether, for example, the message is genuine.

2.4 International cooperation

As the national IT and cyber security authority, the BSI represents national interests in the cyber security bodies of the EU and NATO and also designs cyber security at an international level. In addition, the BSI has sought to expand its scope and influence in 2018 through better networking and cooperation with players from business, politics and civil society.

European Union

In the past two years, the main focus of BSI's involvement in the EU has been on the implementation of the NIS Directive adopted in 2016. This has been legally effective in all EU member states since May 2018. Germany had already transposed the requirements of the NIS Directive into German law, on the basis of the IT Security Act adopted in 2015. The BSI is using its experience to support other member states in transposing the NIS Directive into national law.

The BSI has played an active role in the further development of the NIS Directive, in particular by participating in the two new bodies created by the Directive at European level:

- the NIS Cooperation Group
- the Cyber Security Incident Response Team (CSIRT) network.

In the CSIRT network, a working group led by the BSI has developed the basic standard procedures for significant cyber security incidents, which will serve as a basis for communication and cooperation between the member states in future. They were used for the first time in a Europe-wide exercise as part of the "Cyber Europe 2018" exercise.

Within the framework of the cooperation group, the BSI has contributed its experience from the implementation of the IT Security Act to various sub-groups, e.g. in the area of identifying critical infrastructures, designing minimum requirements and incident reporting obligations for operators of essential services and digital service providers. Currently, the BSI is also involved in a working group with the aim of guaranteeing the technical security of the 2019 European elections, contributing crucial experience from the 2017 Bundestag elections.

Cisco Smart Install

Situation

Cisco Smart Install (SMI) is an automatic configuration feature for Cisco network switches that is enabled on new devices by default. SMI does not provide access protection; authentication is not required. Access to SMI should therefore only be permitted from trustworthy networks and never openly from the Internet.

Cause and Damage

As early as February 2017, the CERT-Bund of the BSI warned that attackers with access to the smart install function of a Cisco switch (Bund 2017)

could misuse it to spy on sensitive information and possibly gain complete control of the device https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k17-0274.htm.

In August 2017 it became known that cyber criminals used the openly accessible SMI function on Cisco devices at various Australian organisations to read device configuration files https://acsc.gov.au/news/routers-targeted.html.

In November hundreds of other configuration files were discovered that, according to press reports, had previously been spied out by cyber criminals on affected devices around the world.

In early April 2018, cyber criminals used open access to SMI functions to compromise thousands of Cisco switches in different countries. In Russia and Iran, affected devices were deliberately decommissioned by the attackers. As a result of these attacks, many large network areas in these countries were cut off from the Internet for several hours.

Reaction

Since the beginning of November 2017, CERT-Bund has regularly informed German network operators/providers about Cisco devices with the active smart install function in their networks, which can be accessed openly from the Internet. Since then, the number of devices affected has fallen sharply from over 6000 on 1 November 2017 to just over 400 on 30 April 2018.

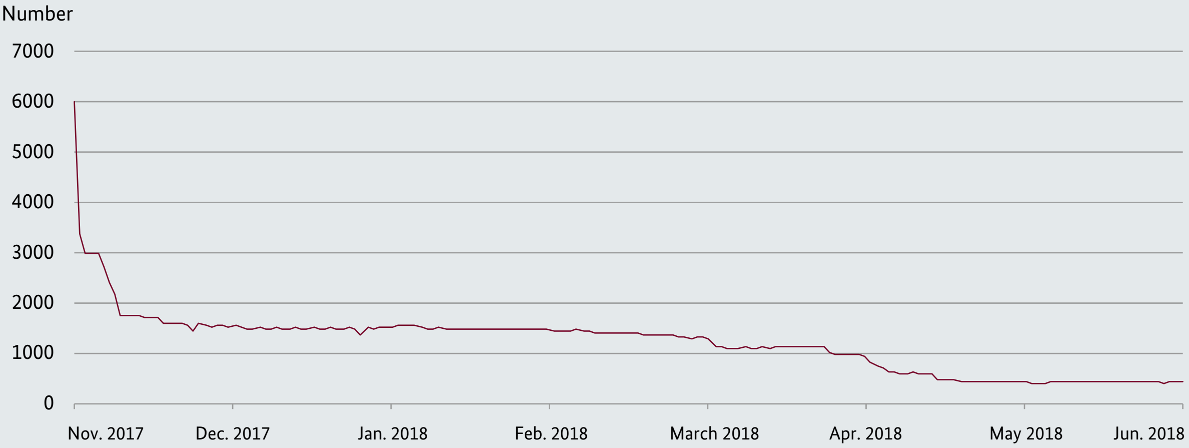


Figure 20 Number of Cisco devices in Germany with smart-install feature that can be accessed from the Internet.

Recommendation

Access to the Smart Install function (port 4786/tcp) should always be restricted to trusted source IP addresses (e.g. the internal administration network). After configuring a new device, the SMI function should be deactivated if it is no longer needed. Furthermore, the manufacturer's configuration instructions for SMI https://www.cisco.com/c/en/us/td/docs/switches/lan/smart_install/configuration/guide/smart_install/concepts.html should be observed.

Another central component of BSI's commitment in the EU is cooperation with the European Union Agency for Network and Information Security (ENISA), whose new mandate is currently being negotiated between the member states, the European Parliament and the Commission as part of the "Cybersecurity Act". The BSI President is the German representative on the Management Board, and the BSI also provides the German National Liaison Officer for ENISA. BSI experts also work continually in various ENISA specialist groups.

The new regulation defining the legal basis of ENISA is intended to be in line with the BSI's long-standing demand for a permanent mandate. It forms the basis for a further intensification of cooperation with the cyber security authorities of the member states. Cyber security is a national responsibility and ENISA can advise and support EU institutions and member states. One example is the redefinition of ENISA's tasks within the framework of the planned European certification framework for ICT security certification as a further component of the Cybersecurity Act. The BSI has significant expertise in the EU in the field of certification; the BSI Vice-President was the only representative of a national authority to speak at the meetings of the European Parliament's Committee on Industry, Research and Energy (ITRE) responsible for the Cybersecurity Act in 2017 and 2018.

With a focus on the planned European certification framework, it is key for the BSI to expand the scope of the European SOG-IS mutual recognition agreement as a European certification instrument, particularly in the field of high security, in order to be able to shape cyber security nationally and internationally.

NATO

The activities of the BSI as the national cyber security authority play a key role in Germany's commitment to NATO. As the national communications security authority, cyber security authority and approval body for crypto products, the BSI is a central contact for NATO in matters of information assurance and cyber defence. It represents Germany through active and advisory participation in the most important technical and political NATO bodies related to information and cyber security.

The issue of cyber defence has become increasingly important in NATO in recent years. At the NATO summit in Warsaw in 2016, the heads of state and government of the member states adopted its "Cyber Defence Pledge". Germany, too, has thus committed itself to constantly increasing its national resilience in cyber security in order to play its part in the Alliance's defence capability. This resolution is now being translated into concrete measures.

2017 was marked by the establishment of NATO's Cyber Operations Centre, ensuring the full competence of the Alliance and its member states in cyberspace operations. Since the signing of the Memorandum of Understanding (MoU) with NATO in 2011 and the confirmation of the MoU in 2016, the BSI has been the National Cyber Defence Authority (NCDA) for Germany within NATO. It is involved in this process in close cooperation with the responsible ministries of the BMI, the Federal Ministry of Defence (BMVg) and the Federal Foreign Office (AA), making a crucial contribution to Germany's security and defence.

In March 2018, Thomas Caspers, head of the evaluation and operation of cryptosystems at the BSI, was elected national co-chair of the NATO Cyber Defence and Information Assurance Capability Panel. In this role Mr Caspers will focus on improving communication and management processes in the alliance, enabling the much needed crypto modernisation of NATO forces, as well as enhancing NATO-EU cooperation. The fact that the vast majority of NATO nations spoke in favour of a BSI employee shows the great confidence the Allies have in the work of the BSI and at the same time reflects the great responsibility the BSI has to NATO.

Facebook account deletions

Situation

On 3 April 2018, Facebook deleted numerous accounts and pages on its social media platforms Facebook, WhatsApp and Instagram, which they assigned to the Russian Internet Research Agency (IRA). The Russian IRA is a "troll factory", thought to be state-owned, that distributes masses of non-authentic content on social networks and uses bogus accounts. The affected sites, in particular a site called IRA Open, are mostly Russian-speaking and disseminate false information or content that is intended to influence public opinion in line with the Russian government. In Germany this page was visited by 8,580 people and around 1,300 of these actively read this page. Adding up all affected accounts, pages and advertising banners that have distributed such content, Facebook estimates a total of about one million page views.

Cause and Damage

The major US operators of social networks, including Facebook, Twitter and Tumblr, have reported more often recently on Russian activities apparently aimed at influencing the US presidential elections.

In September 2017, Facebook announced that Russian players allegedly spent nearly USD 100,000 on advertising to spread misinformation on Facebook between June 2015 and May 2017.

In early 2018, Twitter announced that it had identified almost 4,000 user accounts connected to the Russian IRA ten weeks before the US presidential election. These were used to post some 180,000 tweets, 8.4% of which related to the US election. 13,500 automated accounts (known as social bots) with connections to Russia were reported identified, which had automatically sent tweets related to the US election.

Blogging platform Tumblr announced in March 2018 that it had also identified 84 accounts linked to the Russian IRA. The players did not rely on bots or advertising, but apparently defamed U.S. President Trump's then rival candidate Hillary Clinton in particular through regular posts.

No connection to or influence on the 2017 federal elections in Germany were observed with these accounts.

Reaction

The BSI is in contact with the providers of social networks in order to regularly exchange information on the security of accounts. For example, a direct communication channel to Facebook was established to escalate potential security incidents (e.g. irregularities in accounts of political decision-makers) to the Facebook security team. Furthermore, Facebook has agreed to inform the BSI in advance about actions (e.g. deletion of accounts that disseminate non-authentic content).

Recommendation

In addition to conventional accounts, accounts known as verified accounts also exist in social networks. Such verified accounts are marked with a white tick on a blue background ("blue badge") and confirm the authenticity of an account. Users of social networks can thus recognise whether a corresponding account actually belongs to the specified person (e.g. a politician, a party or a faction). Furthermore, users are urged to always critically question content from social networks.

2.4.1 Cryptography: International standardisation

In view of the threat posed to public-key cryptography by the possibility of future quantum computers, the standardisation of new cryptographic mechanismsthat are protected against this threat (known as post-quantum cryptography) is urgently required. In November 2016, the US National Institute for Standards and Technology (NIST) launched a standardisation process aimed at selecting quantum resistant key agreement, encryption and signature schemes. Proposals for such mechanisms could be submitted to NIST until the end of November 2017. There are still 64 candidates in the running: 19 signature schemes and 45 key transport and encryption schemes. A good overview can be found at www.safecrypto.eu/pqclounge/.

Other organisations such as the Internet Engineering Task Force (IETF) and the International Organisation for Standardisation (ISO) have also started standardising post-quantum cryptography. In addition, the IETF deals with the adaptation of cryptographic protocols such as TLS and IKE to the new methods, e.g. with the option of carrying out a "hybrid" key exchange (combining a traditional method with a post-quantum method). The European Telecommunications Standards Institute (ETSI) is also particularly active, both in the direction of quantum key distribution (QKD) and post-quantum cryptography (or quantum-safe cryptography). The working group on Quantum-Safe Cryptography established by the ETSI Cyber Security Technical Committee has already published several review papers (for example on key agreement procedures). Representatives of the BSI also take part in the meetings of this group.

The BSI exchanges information with international partners and helps develop standards such as ISO-20543 "Test and analysis methods for random bit generators" in order to establish uniform security levels and test criteria for these new procedures at an international level. The standardisation of post-quantum cryptography supported by NIST and the standardisation of TLS 1.3 are also worth mentioning in this context.

National recommendations or specifications for encryption algorithms and protocols, such as Technical Guideline TR-02102 "Cryptographic Mechanisms: Recommendations and key lengths", as well as commissioned studies, such as the continuous investigation of the Linux random number generator, are published by the BSI on its website and also offered in English in order to make them accessible to an international readership.

2.5 Cyber security needs IT professionals

Efforts to ensure reliable cyber defence can only succeed if sufficient experts and talented junior staff are recruited, actively shaping cyber security and anchoring it. For this reason, 180 new posts were allocated to the BSI in 2017 for the fulfilment of its tasks. Filling these positions in times of a shortage of skilled workers was a particular challenge, but one that it successfully overcame. At the end of the reporting period, almost all the positions were filled. Essentially, two challenges became clear:

- the recruitment of highly sought-after IT specialists

- the training and integration of the new colleagues.

The growth of 180 jobs in a workforce of around 650 employees meant that a noticeable influence on the structure and culture of the organisation was unavoidable.

The public sector needs STEM: attracting skilled workers

After the redevelopment of the career portal at the start of the year with the campaign slogan “What we want: your digital side” [“Was wir wollen: Deine digitale Seite”], efforts focused on keeping the campaign alive in the reporting period. The campaign underlined the ideal and reliable conditions the BSI creates for its employees in a challenging task that impacts society. This also included diverse options for working in a family-friendly and flexible manner. In addition, it focused on the authority as a very attractive employer, which enjoys an excellent reputation nationwide and internationally and where pioneering security projects are part of everyday life. In addition to an exciting working environment, the BSI also offers its employees a comprehensive training and further education programme. It is involved with international projects and conferences as well as regular collaborations with leading security experts in Germany and abroad. In addition, employees have first-class networking opportunities in politics, business and administration.

In order to promote the campaign, the BSI used its staff to present the employer brand in words, pictures and sound. These messages were presented in online channels, print advertisements, editorial articles online and in magazines, videos and brochures. Direct contact to students of STEM subjects was targeted through university fairs, excursions to the BSI, internships and the mentoring of final theses, to promote the national cyber-security authority as the ideal career-entry employer.

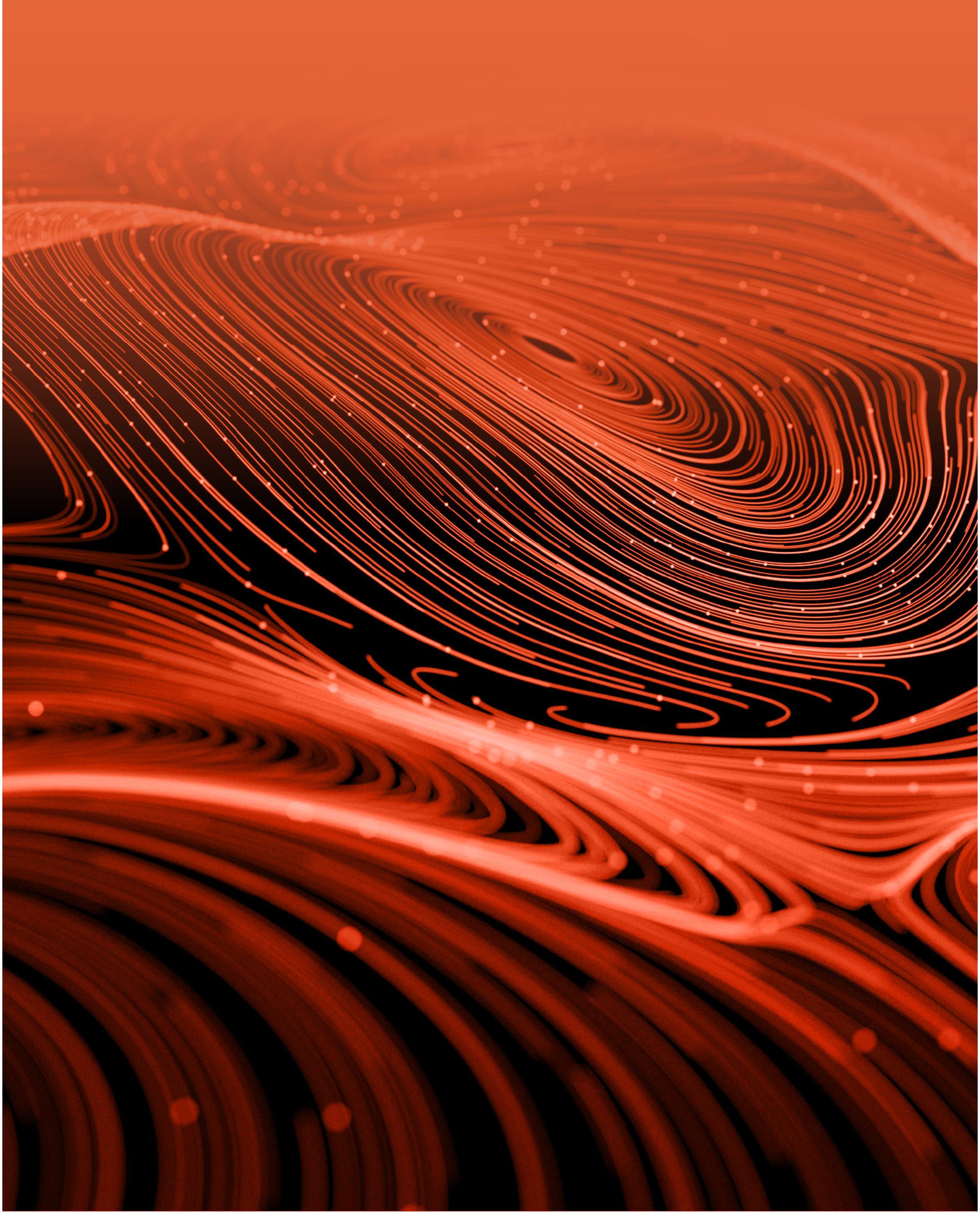
The extensive measures and a fully digitised recruitment process led to an increase in the number of applicants by approx. 47% in 2017 leading to the excellent staffing level described above. The campaign showed, despite the frequent focus on problems recruiting IT specialists, the public sector is also in a position to assert itself as an attractive employer vis-à-vis business and research.

The BSI sets standards in the public sector in its personnel work: at this year’s conference for digital government and modernisation [Zukunftskongress] in Berlin, the BSI won second place in the eGovernment competition on digitisation and modernisation of public administration for the project “Recruitment, training and retention of more than 260 new employees since 2016”.

Lots of new faces: on-boarding and integration

In order to integrate the new employees into the BSI, mandatory introductory events were initiated to make the employees more familiar with the specialist tasks in the different areas and thus to create an overview, as well as to provide the management basics in the public sector for these STEM specialists, who were often completely unfamiliar with these requirements. In-house training courses are also offered on topics such as project management, presentation skills, resilience, conflict management, time management, communication and cooperation, conducting negotiations and stress management. This reflects the different interdisciplinary requirements for new and more experienced employees: above all, it promoted cross-divisional cooperation and collaboration as well as familiarisation with BSI-specific procedures. In addition, training courses in conflict management, remote leadership, common goals, human resources law, feedback meetings and general management were offered specifically for executives, in addition to the established management trainee programme. Health management was always included in order to anchor this as a leadership task.

3 General Evaluation and Conclusion



3 General Evaluation and Conclusion

Threat level remains high

In the reporting period, the risk has become more diverse compared to the previous reporting period. An example of this are the hardware security vulnerabilities such as *Spectre/ Meltdown* and *Spectre* NG, which became known at the beginning of this year.

In 2018, there were no major new waves of ransomware. Nevertheless, ransomware must continue to be classified as a massive threat. This was demonstrated by the Petya/ *NotPetya* ransomware attacks in the second half of 2017, for example: the German economy alone suffered losses in the millions. New ransomware families are also emerging all the time (such as Bad Rabbit in October 2017). There is no reason for an all-clear in the area of ransomware.

Overall, the number of malware programmes has continued to rise: there are over 800 million known malware programmes. Around 390,000 new variants are added every day. In the mobile environment, there are already more than 27 million malware programmes for Google Android alone.

The methods of mass distribution of malware have also been further developed. For example, malware was distributed in 2017 in several incidents (e.g. with *NotPetya*) by compromising updates, update files or update servers (installation or update hijacking).

Well-known malware families are continuously modified, further developed and equipped with additional malicious functions. Since September 2017, the malware *Emotet* has attracted attention through frequent attacks in Germany. *Emotet* began as a banking Trojan in 2015 and has since evolved into a multifarious malware with loadable modules for spam, DDoS, data spying, identity theft, sandbox detection and other malware components.

IoT botnets are continuing to evolve but the new botnets like Hajime and IoT_reaper/IoTroop have not been as significant as the *Mirai* botnet. However, we should expect large new botnets to carry out high-impact attacks (spam, DDoS, etc.) as a result of the rapid growth of vulnerable IoT devices and mobile devices. In December 2017, the global Andromeda botnet was successfully dismantled in cooperation with the BSI. It had previously distributed malware such as banking Trojans to millions of computers.

There were only minor changes in the number of open critical software vulnerabilities compared to the previous reporting period.

The scale of credential leaks and threats from misconfigured cloud services also means there is no easing of the security risk from spam and phishing. The mass of credentials available allows for more targeted and personalised IT attacks.

Identity thefts are being reported with ever increasing frequency. Data collections involving billions of stolen digital identities are increasingly traded on the IT black market.

Although there are effective techniques on the market to ward off DDoS attacks, the threat level is still high due to high mitigation costs and new attack techniques („memcached amplification“). In the second half of 2017, however, there was initially no significant increase in the attack capacities used; typical peak values of 50 to 60 Gbps were recorded. In the first quarter of 2018, however, DDoS attacks of up to 190 Gbps were detected in Germany. A link with the misuse of the server software memcached as a DDoS reflection vector is thought to be very likely.

In early January 2018, serious and fundamental vulnerabilities were discovered in the hardware architecture of almost all Intel, ARM, AMD processors. This is a new class of vulnerabilities (*Meltdown*/*Spectre*) as a result of design errors in the processor architecture. Updates cannot close the security holes completely. Exchanging all the affected processors is also unrealistic. There remains a residual risk, therefore, that the vulnerabilities will be exploited for an unrestricted period of time. This is a new threat to virtual structures, such as cloud offerings.

Illegal crypto-mining has also been added. It is increasing significantly as a cyber risk because it is highly attractive in financial terms and the infections can remain undetected. The number and intensity of cryptocurrency mining incidents registered have increased since the second half of 2017. In several cases, the use of currently known infrastructures (e.g. botnets and exploit kits) can be observed for distributing crypto-currency mining malware.

The summary overview shows that the risk has not decreased at all compared to the previous reporting period; instead, it has increased slightly. It has become more complex, which increases the cost of protection. Attackers continue to be highly dynamic in the development of malware and attack routes, and this requires a high level of attention and flexibility to ensure information security. And there is a new calibre of vulnerabilities in hardware, gaps that cannot be completely closed without replacing the hardware.

Digitisation only at the beginning

At the same time, we are only at the beginning of an era of digitisation that will have a major impact on our daily lives and our society. In a digitised and networked world, attacks and threats that already pose extreme challenges to the state, the economy and society today will continue to increase. Without appropriate efforts to ensure the necessary degree of information security through prevention, detection and reaction, the state, economy and society in Germany are increasingly at risk.

The problem lies in the combination of growing vulnerability with the increasing dependence on information technology. The likelihood of successful attacks on digitised infrastructures increases as the number of points of attack increases, communication infrastructures become increasingly complex and the amounts of data to be processed multiply. Relevant security incidents from the reporting period clearly show this.

- Despite all the measures that contribute to the German government‘s IT networks and systems being regarded as especially secure, a successful hacker attack occurred in 2017. The attack took place via a web server of the Federal Academy of Public Administration. The Federal Foreign Office and the Federal University of Applied Sciences were affected. The BSI was able to observe the cyber attack on the Federal Foreign Office over a longer period of time by deploying a Mobile Incident Response Team (MIRT) and thus gain deeper insights into the perpetrators‘ intentions and procedures. Major damage or further spread could be prevented thanks to existing protective measures.

- In May 2017, hackers entered the network of a subsidiary of a German energy provider. They had access to a small part of the Internet traffic for a few minutes. The incident was analysed and dealt with by the BSI within the framework of the National Cyber Response Centre in cooperation with the company concerned. The BSI has information that proves that German KRITIS operators are increasingly in the focus of foreign cyber attacks and must expect the risk situation to change.

- Hardware security vulnerabilities such as *Spectre/Meltdown* and *Spectre NG* have the potential to make current business models and basic IT security concepts obsolete. The chips concerned are installed in millions of devices and form the basis of modern computers. Since these are vulnerabilities in the hardware, software updates cannot provide adequate remedies. Comparable products that are not affected by vulnerabilities need to be developed first. Until then, the vulnerability will remain acute, even if its exploitation is very costly and therefore its use as an attack method can only be expected in special cases.

These incidents – as examples of risk potential and attack variance – make it clear that cyber security must be considered and examined at a greater level. The security architecture of computer-supported workstations and company processes must be rethought just as fundamentally as the IT security of products and services. The security of the systems used in government administration, in business and by the end user must be guaranteed from the outset by „security by design“ and „security by default“. Germany must take a leading role in this area.

To remain a strong and secure location in future, more must be invested in information and cyber security.

Strengthening defensive efforts

Based on its in-depth technical expertise, the BSI already has an integrated value-added chain, from consulting and the development of security solutions and the prevention of attacks on cyber security to standardisation and certification. As the national cyber security authority, it designs information security in digitisation for all players in all areas through prevention, detection and response.

In this function, the BSI is required both to point out vulnerabilities and to design and implement new solutions.

- The Internet of Things is increasingly developing into a new source of danger for IT security. A key factor in this is that IoT devices are easy to attack and their security is not given sufficient prominence either in their manufacture or in the customer‘s purchasing decision. In implementing the Federal Government‘s Cyber Security Strategy and the coalition agreement of the 19th Bundestag, the BSI is working on introducing a security identifier for IT security in order to make it easier for consumers to assess the IT security of IT products and services in future. An important step here is the Technical Guideline for Routers, which the BSI jointly worked on with the industry.

- eFail vulnerabilities allow attackers to read encrypted e-mails. As a result, confidence in encrypted communication has declined. Germany must finally make encrypted communication available for mass use for citizens and to protect company secrets. This requires a central initiative to drive and accompany this process. The BSI and the Alliance for Cyber Security will take over this task.

- Incidents and vulnerabilities such as *WannaCry*, *NotPetya*, eFail and *Spectre* shake the foundations of global IT security architectures and take the threat scenario in cyberspace to a new level. This is why it is necessary for the required security measures to be checked by independent bodies and to create reporting and transparency obligations to the BSI for manufacturers and providers.

- Operators of critical infrastructures are increasingly the focus of cyber attacks. The BSI works closely with the KRITIS industries to improve security measures and ward off cyber attacks. However, the implementation of the IT Security Act against the background of the current level of threat make it clear that an update is urgently needed in order to continue to effectively protect other parts of the economy, and significantly increase the level of security.

Rethinking prevention

As important as it is to defend against concrete attacks from any part of cyber space is, it must not side line the fundamental concern of preventing potential attackers from attempting to attack through preventive measures.

This requires both the further development of the legal framework and the development of security standards for IT structures and the protection of critical infrastructures in coordination with the business community, the German government and its federal states. This also includes IT security research, which deals with the security of tomorrow‘s IT systems, but is equally concerned with the security of existing information technologies. In addition to existing competence centres for IT security research, the BSI is already contributing to Germany‘s digital sovereignty.

Prevention always means, on the one hand, raising the hurdles for an attack and, on the other hand, enabling the players in the state, business and society to recognise dangers more effectively and to behave more defensively. Digital consumer protection therefore plays an important role in prevention. According to the coalition agreement, this will be established as an additional task of the BSI. For many years, the BSI has been offering information and support to the population with its „BSI for Citizens“ („BSI für Bürger“) concept. Now the BSI, together with established players from consumer protection (including Verbraucherzentrale NRW, Verbraucherzentrale Bundesverband) and agencies from the related discipline of data protection, will significantly expand its range in this area. As a manufacturer-independent and competent technical body, the BSI supports consumers in the risk assessment of technologies, products, services and media offerings. This can increase society‘s resistance to cyber threats of all kinds.

Securing the digital future

The coalition agreement contains numerous items to meet future challenges in the prevention, detection and defence of cyber threats. This includes a number of items that may go beyond the tasks for which the BSI is responsible.

- Implementing a framework programme for civil security research and further developing of the competence centres for IT security research into internationally visible research and consulting centres.

- Establishing an „Agency for Innovation in Cybersecurity“ and an IT security fund to protect key technologies relevant to security.

- Developing simple and secure electronic identification and end-to-end encryption solutions that enable citizens to communicate in encrypted form with administrations using common standards (PGP, S/MIME).

- Promoting distribution of secure products and the development principle „security by design” as well as the developing IT security standards for Internet-enabled products.

- Developing and implementing an IT security standard in the form of a seal of approval for IT security that goes beyond the legal minimum standards.

- Establishing clear rules for product liability in the digital world with a balanced definition of risk and spheres of responsibility for consumers, manufacturers and providers.
- Strengthening financial supervision in the field of digitisation and IT security and intensifying cooperation with all relevant supervisory and security authorities.
- Involving all socially relevant groups, manufacturers, providers and users as well as the public administration in a National Pact for Cyber Security.
- Updating the IT Security Act to an IT Security Act 2.0 and expanding the regulatory framework to counter new threats adequately.
- Establishing digital consumer protection as an additional task of the BSI.

In addition, the central element for the BSI in the coalition agreement expands the organisation's position as a national cyber security authority and strengthens its role as an independent and neutral advisory body for IT security issues and as a central certification and standardisation body for IT and cyber security.

These requirements and plans must now be rigorously implemented. The BSI will contribute its expertise in both the traditional and new areas of responsibility:

- It protects federal information technology against cyber attacks and cyber dangers. The BSI will continue development of this proven concept and establish this as a basis for offers to federal states and municipalities, and for administrative and judicial digitisation.
- The BSI regularly and intensively advises the overall project management on strategic and operational issues of information security in IT consolidation and ensures the necessary centralised review of the topics and the project process. However, if IT systems are concentrated at IT service providers, there are also potential concentrations of IT risk among IT service providers.
- Even in times of crisis, it is the first point of contact for those affected, for national and international partners and for multipliers. Within the scope of the particular options available, the BSI provides active and transparent information and supports mobile incident response teams (MIRT) directly on site. The focus is on Federal Administration institutions and operators of critical infrastructures.
- The BSI exchanges information with national and international providers of IT products and IT services, while incorporating the IT security issues of users.
- It is a competence centre in the field of cryptography, which draws up recommendations and technical guidelines on cryptographic procedures and participates in the development of international crypto standards.
- In December 2017, the green light was given for a BSI-internal competence centre for Artificial Intelligence/ Machine Learning, where the topics will be intensively supported and promoted in future from an IT security perspective.
- Internationally, the BSI positions itself as a thought leader and competence centre for all issues related to information security in multilateral and bilateral cooperation. A particular focus is on cooperation in the EU and NATO.

Protecting business and local sites

Cyber security is the prerequisite for successful digitisation. The potential of digitisation is almost limitless. A study commissioned by the BDI shows: by 2025, Europe can generate up to €1.25 trillion in additional industrial added value. Nowadays, many process steps in industry are already fully automated. A new feature is the digital networking of machines. As machines and products communicate with each other, the flexibility of production increases considerably. Digital networking is an important factor for productivity and economic growth in Germany.

However, the increasing number of smart factories and networked objects will further extend the vulnerability of the economy to hacker attacks and cyber attacks. Industrial companies are also often victims of more complex cyber incidents. The risk of attacks from cyberspace must be considered the most significant risk that companies face in the long term.

The BSI has already taken important steps and given impetus to raise awareness of the dangers in the economy and to provide concrete support to companies in averting danger:

- Through the Alliance for Cyber Security (ACS), it manages the largest self-help network in German business with practical help in analysing cyber risks and implementing suitable protection measures. In doing so, the ACS works closely with partners/multipliers from industry and research.

- With the German Confederation of Skilled Trades (ZDH) and the German Retail Federation (HDE), important strategic partnerships were initiated during the reporting period and confirmed by the signing of formal declarations of intent.

- By updating the IT-Grundschutz, the BSI offers a sound and practical management system for information security (ISMS) available to business and administration users. It helps to check the status of information security in an institution and improve it in future.

The BSI as the central office for cyber security in Germany

With the National IT Situation Centre, the CERT-Bund and the National Cyber Response Centre, the BSI provides three essential building blocks of the national cyber security architecture. In the event of an IT crisis, the National IT Situation Centre becomes the National IT Crisis Response Centre. The BSI is also the independent competence centre for cyber security and the IT security service provider for all federal departments. The BSI aids these departments in designing information security in the major digitisation projects in order to guarantee the functionality and added value of a society that will be highly digitised in future. Examples include:

- Telematics infrastructure in the health sector/“eHealth“ (BMG)

- Digitisation in the energy revolution (BMWi)

- Intelligent transport systems (BMVI)

- Smart home/intelligent construction sites (BMWi, BMJV, BMUB)

- The Internet of Things/IoT (BMI, BMWi, BMJV)

- New technologies/blockchain (BMBF)

- Digital shipping (BMVI)

- Digitisation of cross-departmental encrypted communication (BMI, BMVg, AA, BKAmt)

The interdisciplinary function of the BSI is pronounced at federal level.

In addition, cooperation with the federal states and the municipal sector is being expanded. Cooperation agreements have already been reached with a number of German federal states with the aim of avoiding the establishment of parallel structures and to ensure a uniform level of security in the interests of the state as a whole.

This is a step in the direction of making the BSI the „Central Office for Cyber Security in Germany“.

The BSI is already approaching this with new strength and confidence. However, this 2018 report also shows what challenges still lie ahead.

As everyone knows, information security is the prerequisite for successful digitisation. It is for this reason that the BSI must systematically continue to be developed further in the coming years.

4 Glossary

Advanced persistent threats

Advanced persistent threats (APTs) are targeted cyber attacks on selected institutions and organisations in which attackers gain persistent (long-term) access to a network and the spread the attack to other 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.

Adware

Adware is defined as programmes that are financed through advertising. Malicious programmes that generate advertising for the author of the malware also belong to this category.

Application/app

An application, or app for short, is an application software. The term app is often used in relation to applications for smartphones or tablets.

Attack vector

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

Blockchain

Blockchain describes distributed, synchronised, decentralised and consensual data storage in a peer-to-peer network. A redundant hash-chained list of data blocks is maintained in all network nodes, which is updated by means of a consensus procedure. Blockchain is the technological basis for crypto currencies like Bitcoin.

Bot/botnet

A botnet is a collection of computers (systems) that have been attacked by a remotely controllable malware (bot). The affected systems are controlled and monitored by the botnet operator using a command and control server (C&C server).

CERT-Bund

The CERT-Bund (Computer Emergency Response Team of the Federal Administration) is located within the BSI and functions as the central coordinating body for federal agencies 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 is made up of IT specialists. CERTs have become established in many companies and institutions to handle defence against cyber attacks, respond to IT security incidents and implement preventive measures.

Cloud/cloud computing

Cloud Computing is understood as offering, using, and billing IT services dynamically adapted to the requirements via a network. Here, these services are only offered and used by means of defined technical interfaces and logs. 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.

Critical Infrastructures (KRITIS)

Critical infrastructures (KRITIS) are organisations and institutions of vital importance to the community. Their systems and services, such as the supply of water or heat, their infrastructure and their logistics are increasingly dependent on information technology that runs smoothly.

Cryptocurrency mining

In cryptocurrency mining, computing power is used to participate in the proof-of-work consensus process of a crypto currency and to mine corresponding currency tokens such as bitcoins.

DANE

DNS-based Authentication of Named Entities (DANE) is a protocol that 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 protecting 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, such as botnets.

DRDoS / DRDoS attacks

Many types of Distributed Denial of Service (DDoS) attacks are based on reflection and amplification. Reflection-based DDoS attacks are often referred to as Distributed Reflection Denial of Service (DRDoS).

The basic principle of DRDoS attacks is that an attacker sends a small data packet with a bogus sender address to a server. This server then responds to the bogus address belonging to the victim of the attack, so the attacker uses a server as a reflector. Since the server's response packets are usually much larger than the requests, the attack is intensified. The ratio of response to request is called the amplification factor. All DRDoS attacks use UDP-based protocols, since UDP works without connection and the sender address can be forged.

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 programmes (plug-ins) or the operating system which can then be exploited, thereby enabling malware to be installed on the PC unnoticed.

Embedded systems

[Source: Wikipedia] An embedded system is an electronic computer or a computer connected (embedded) in a technical context. The computer either takes over monitoring, control or regulation functions or is responsible for a form of data or signal processing, for example during encryption or decryption, coding or decoding or filtering.

Exploit

Exploits are malware that exploit vulnerabilities.

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 is software that is embedded in 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

A nonce is a „number used only once“ and represents a unique number in cryptography, i.e. a number that is only used once in a given context. Nonces are often generated with a random number generator and then used, for example, to create an electronic signature before being deleted so that the same number is not used again for another electronic signature. Nonces are also required to establish the TLS connection.

Patch/patch management

A patch is a software package that software manufacturers use to close security vulnerabilities in their programmes or to implement other improvements. Many programmes offer an automated update function to make the installation of these updates easier. Patch management is the term used to describe 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 attacker attempts to access the personal data of an Internet user via bogus websites, e-mails or messages and to misuse this data for their purposes, usually at the expense of the victim.

Plug-in

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

Ransomware

Ransomware is malware that restricts or prevents access to data and systems and claims to release these resources only upon payment of a ransom. It is an attack on the availability of a security target and constitutes a form of digital extortion.

Sinkholes

Sinkholes are 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 affected users.

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. In terms of both cybercrime and espionage, the perpetrators are skilful in exploiting perceived human weaknesses such as curiosity or fear to gain access to sensitive data and information.

Spam

Spam refers to 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 (malspam), links to infected websites or is used for phishing attacks.

Spearphishing e-mails

Phishing e-mails with malicious links or attachments that are sent to specific recipients.

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.

Trolls

Trolls are Internet users who disrupt/inflame discussions or disseminate false information through statements aimed at influencing others.

UP Bund

The Federal Government IP 2017 is the guideline for information security in the Federal Administration, intended to ensure information security across the administration. In the Federal Government IP 2017, the implementation plan originally drawn up in 2007 was revised and approved by the Federal Cabinet at its meeting on 19 July 2017. The Federal Government IP 2017 came into force on September 1, 2017 and implements targets from the 2016 Cyber Security Strategy in various action areas. It applies to all departments and federal agencies.

UP KRITIS

The CIP Implementation Plan (www.upkritis.de) is a public-private cooperation between critical infrastructure operators, their associations and government agencies such as the BSI.

Virtual private Networks (VPNs)

A Virtual Private Network (VPN) is a network that is physically operated within another network (often the Internet), but is logically separated from this network. In VPNs, the integrity and confidentiality of data can be protected and the communication partner can be securely authenticated with the help of cryptographic procedures, even when several networks or computers are connected to each other over leased lines or public networks. More: https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/VPN/VPN_Virtual_Private_Network.html

Legal Notice

Published by
Federal Office for Information Security (BSI)

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

Email
bsi@bsi.bund.de

Telephone
+49 (0) 22899 9582-0

Telefax
+49 (0) 22899 9582-5400

Version
September 2018

Print
Appel & Klinger Druck und Medien GmbH, Schneckenlohe

Layout
Fink & Fuchs AG

Content and editing
Federal Office for Information Security (BSI)

Image credits
all images: gettyimages.de/shulz

Graphics
BSI

Item number
BSI-LB18/507e

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