Federal Office
for Information Security

The State of IT Security in Germany in 2020

Foreword

The Federal Office for Information Security (BSI) is the federal cyber security agency and is tasked with ensuring Germany's digital security. This report on the state of IT security in Germany in 2020 once again highlights the importance of this task, as well as the diversity and complexity of the associated challenges.

Cyber attacks are becoming increasingly sophisticated. At the same time, businesses, government and private citizens are now increasingly dependent on IT, which increases the potential scale of damage.

The coronavirus pandemic has once again underlined the unequivocal importance of IT infrastructure that is both functional and secure. In all of our digitalisation activities, IT security must therefore be a focus that is actively considered and implemented from the outset.

The malware Emotet constituted a major threat to the state, the industry and civil society in the reporting period. This sophisticated combination of a digital toolbox and social engineering makes it possible to infect even professional users. Everyone has their digital vulnerabilities. Once a system is infected, the perpetrators then analyse it with the aim of extorting money from their victims either by encrypting data or threatening to go public with it. For a commercial enterprise, the impact of such an infection can range from temporary reductions in work or production capabilities to complete stoppages lasting several weeks or even months.

I am pleased that we have capable teams of experts at the BSI and other security agencies who do their utmost each and every day to protect private users, businesses and government agencies against threats from the digital sphere.

Alongside its role as a provider of security services to the federal administration, the BSI also offers a broad portfolio of services for businesses and private citizens. In doing so, it acts as a central point of contact and clearing house for IT security in critical infrastructures and is also developing security requirements for the 5G networks of the future. With its 'BSI für Bürger' programme, the BSI also provides a wide range of information about online risks and the precautions that should be taken. Shortly after the COVID-19 outbreak, the BSI provided an information pack about safe mobile working. To make the software as secure as possible, the BSI has also been involved in developing the German Corona Warn App from the start.

We must ensure that we can adapt to an ever-changing threat situation. This is why I intend to further expand the BSI's remit and strengthen its role as the government's cyber security agency. Part of this work will involve passing the IT Security Act 2.0 during the current legislative term.

I have also requested a review of the Federal Government's cyber security strategy over the next few months. This strategy, originally issued in 2016, sets out many important objectives in national and international cyber policy. These goals and their associated measures will now be reviewed and reformulated with an eye towards the future.

The field of IT security boasts a very wide range of ongoing projects. This is reflected in the present report on the state of IT security in Germany in 2020, in which the BSI describes the current threat landscape and the activities it is engaged in to contain these dangers.

Horst Seehofer
Federal Minister of the Interior, Building and Community

Foreword

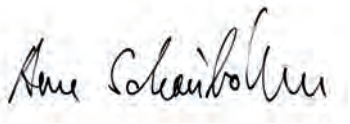
Germany – Digital – Secure – BSI

In the mid-19th century, the Bavarian pastor Sebastian Kneipp promoted and popularised the hydrotherapy treatment that was later named after him. This was based on the idea that ice-cold water on the human body stimulates or promotes certain processes in the body that are capable of facilitating healing. During the first six months of 2020, we have observed a similar effect, with the coronavirus pandemic requiring many people to stay at home for months on end and many types of familiar routines at home or in the workplace being suddenly stopped overnight (or reorganised entirely). For many people, COVID-19 has come as a real shock in more than one sense.

The pandemic has also brought about many changes in information security. Once again, cyber criminals have demonstrated a talent for adapting to new situations and circumstances and exploiting them for their illicit purposes. At the same time, however, the BSI itself has responded with remarkable alacrity to this crisis situation and was able to respond effectively with appropriate recommendations and countermeasures in terms of prevention, detection and reaction.

While we had been deeply involved in topics such as 5G, artificial intelligence, smart homes and autonomous driving 'pre-COVID', these became overshadowed as topics for public debate by the coronavirus as it reached pandemic proportions. The BSI has not lost track of these issues, however. On the contrary, we have continued to work very hard on designing and promoting information security in these areas, which are of specific importance for Germany on the international stage. In particular, our role as the German Government's cyber security agency - the 'cornerstone of security for the digital transition', as Head of the Federal Chancellery minister Helge Braun once described the BSI - requires us to help end users in government, business and civil society to utilise these new technologies securely while addressing the challenges of the threat landscape described in this report. One aspect of our work here involves defining security standards and ensuring widespread compliance. We also provide end users with relevant and practical recommendations that ensure their safe and secure interaction with their digital environment.

While we acknowledge the severe medical and epidemiological events in relation to COVID-19, the pandemic has underlined the importance of well-functioning, secure IT systems both in day-to-day life and for our global economic coexistence. The positive trends and accelerated development cycle that digitalisation has experienced in Germany because of the pandemic must be built on and further expanded over the long term in the post-COVID era. Only by continuing to take a proactive and preventive approach to risk assessment will we succeed in this endeavour. That is precisely what is enshrined in the mission statement we strive to uphold: 'Germany – Digital – Secure – BSI'.



Arne Schönbohm
President of the Federal Office for Information Security

Table of Contents

1 Threat Landscape

1 Threats to Cyber Security in Germany

The Federal Office for Information Security (BSI) monitors the threat landscape for IT security in Germany on a continuous basis. The present report covers the period from 1 June 2019 to 31 May 2020 (the 'reporting period'), although it also summarises events that occurred thereafter. The IT security threat situation has remained fraught in this period. The BSI has observed a continuation of the trend of attackers utilising malware for mass cybercriminal attacks on private citizens, commercial enterprises and other institutions. Leaks of personal data - which in this reporting period also included patient data - were also observed, as were critical vulnerabilities in both software and hardware products.

1.1 Malware

The term 'malware' encompasses all computer programs that perform damaging operations or enable other programs to do so. Typically, malware gains access to a computer via email attachments or links in emails. If a PC user opens such an attachment or clicks one of these links - which leads to a compromised web page - a malware program is installed. Other typical *attack vectors* include downloads that occur unnoticed in the background (known as *drive-by downloads*[1]), as well as malicious add ons to legitimate software programs. Malware commonly exploits vulnerabilities to infect host systems. These vulnerabilities can occur in software or hardware products, in gateways - for example, between office and production networks or to the public internet - or, in the case of social engineering, as a result of human error.

Individual malware programs differ in terms of their functionality, and a single piece of malware can also boast several different kinds of functions. One common type of malware is *ransomware*, which typically uses encryption to restrict access to data or systems to ultimately blackmail the user into paying a ransom fee (cf. chapter *Ransomware*, page 11). Malware that camouflages itself as a harmless software program or conceals itself in legitimate files is known as a 'Trojan' (cf. chapter *Emotet: New Quality of Advanced Attacks*, page 11), while malware that can be controlled remotely with the aid of command-and-control servers is called a 'bot' (cf. chapter *Botnets*, page 16).

Among others, antivirus software offers protection against attacks from these malware programs by detecting them, preventing their successful execution and removing them from the system. However, some kinds of attacks can make far-reaching changes to an infected system that cannot be simply rolled back without a considerable amount of effort.

1.1.1 Increase in Number of New Malware Variants

New variants of malware occur when changes are made to the program code. While detection methods do exist for known malware variants, new variants cannot be identified as malware programs immediately after their release - which makes them particularly dangerous.

In the current reporting period, the number of new malware variants increased by around 117.4 million (see figure 1; source for this and following data: BSI analysis of raw data supplied by the AV-TEST Institute). Growth in September 2019 was especially strong, with 14.1 million new malware variants and 1.1 million new variants of potentially unwanted applications (*PUAs*)[2]. A large quantity was also recorded around the New Year.

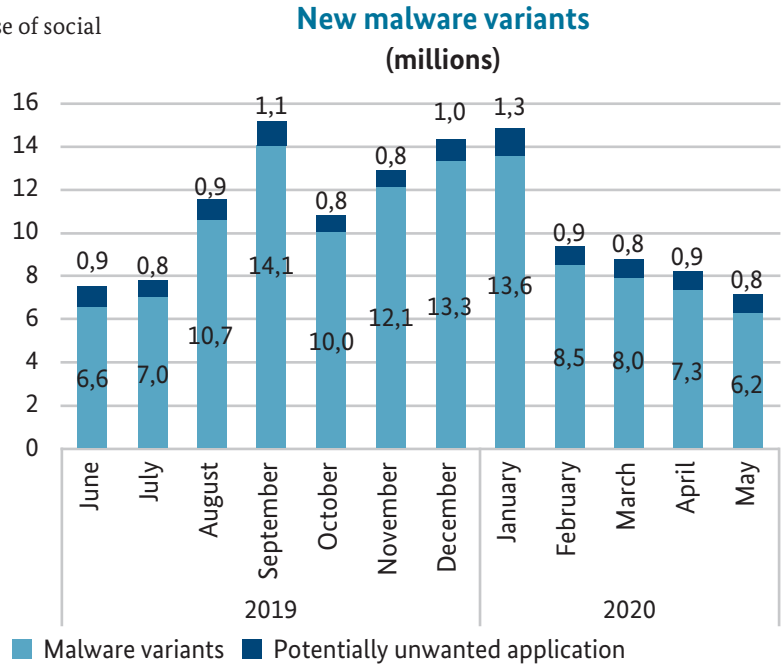


Figure 1 New malware variants,
Source: BSI analysis of raw data from the AV-TEST Institute

[1] Terms in italics are explained in the glossary.
[2] Application software that cannot be classified definitively as *malware*

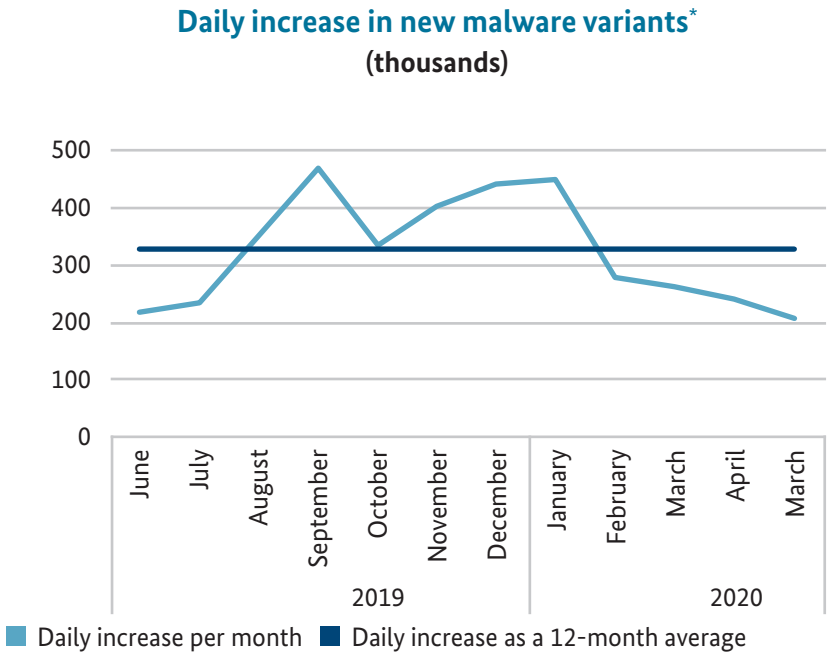


Figure 2 Daily increase in new malware variants,
Source: BSI analysis of raw data from the AV-TEST Institute
*Without PU

This was equivalent to an average increase of around 322,000 new malware variants per day in the reporting period (see figure 2). There was considerable variation in this trend, however. Mid-year 2019, this indicator was only at 220,000 new variants per day - 32 percent less than the average value during the reporting period. Much stronger growth was then seen in September 2019, with around 470,000 new variants recorded on average every day (46 percent higher than the average for the reporting period).

In February 2020, this wave of new malware variants tailed off abruptly before eventually settling at a below-average level.

Waves of new malware variants that start in the fourth quarter and continue until the first quarter of the New Year are a regular phenomenon. Compared to earlier reporting periods, the wave in the current period was flatter - although by no means less of a threat. This was largely attributable to new variants of the *Emotet* malware, whose deployment in cyber attacks started to pick up again in September 2019. The appearance of *Emotet* marks a change of tactics on the part of attackers. While random mass attacks on randomly selected targets used to be the method du jour, malware attacks are now becoming increasingly intelligent and - thanks to a sophisticated approach involving the combination of several malware programs - more targeted.

1.1.2 Emotet: New Quality of Advanced Attacks

Emotet was the dominant malware threat to IT security during the reporting period. This former banking Trojan embodies a wide range of malware functions. The software 'bundled' with this malware includes modules for data espionage (cf. chapter *Theft and Misuse of Identity Data*, page 18), for sending unsolicited emails (cf. *chapter Spam and Malware Spam*, page 15) and for downloading additional malware programs. Emotet also includes worm and bot functionality (cf. chapter *Botnets*, page 16). As a result, the malware is not only capable of spreading autonomously in a network, but can also connect to a command-and-control server to receive server commands sent by an attacker and execute these commands in the infected network.

This versatile toolbox of malware functions offers attackers a wide range of new and advanced *attack vectors*. As a result, methods that had previously only been observed in targeted, complex and technically demanding attacks on carefully selected targets (e.g. during an APT attack affecting a single business entity - cf. chapter *Advanced Persistent Threats*, page 28) can now be deployed en masse. This is illustrated by the three-tiered attack strategy using Emotet, the malware Trickbot and the ransomware Ryuk.

1. Emotet infection using social engineering and the 'snowball effect': Emotet is propagated by email. As an email attachment, the malware is disguised as an application letter or hidden in manipulated images, for example. As a link, it is hidden on compromised web pages and installed once the link is clicked. Advanced social engineering techniques are used to induce users to click on the link. Following a successful infection, Emotet spies out the victim's email communication (known as 'Outlook harvesting') and uses what it finds there to attack the victim's correspondents - such as their business partners. The victim's correspondents then also receive emails containing malware attachments that install Emotet when clicked. By exploiting the email communication history that it acquired earlier, Emotet automatically generates deceptively realistic replies to emails apparently sent by the victim and propagates these on a huge scale. Since the subject lines are familiar and the email content has been properly quoted, recipients can often be tricked into clicking. This type of attack can be executed automatically by the malware with virtually no further intervention by the attacker.

2. Espionage and persistence with Trickbot: After successfully infecting a system, Emotet downloads other malware payloads. In the reporting period, this was often Trickbot, a piece of malware that features modules for espionage and sabotage and can compromise the victim's network comprehensively and automatically. This can even include core systems such as the Domain Controller in Active Directory, which handles the primary *authentication* of users, as well as the assignment of rights and roles. This grants the attacker a complete set of rights, permitting them to create user accounts with administrator rights, for example, to view and exfiltrate data; or to set up *backdoors* to facilitate a longer-term presence within the infected system. Trickbot also autonomously collects information about the victim's systems, users, installed software, and sends it back to the attackers.

3. Monetisation with the ransomware Ryuk: As a next step, the attackers presumably use the information collected by Trickbot in order to decide whether or not to exploit Trickbot's remote access functionality to execute a manual attack on the victim's network. If the target appears to be solvent, the Ryuk *ransomware* is then deployed simultaneously on all of their accessible servers and systems. Since Trickbot is able to obtain such extensive system rights, *backups* are also often encrypted. The typical next step is then a ransom demand.

The damages caused by this strategy are enormous. Affected businesses, government agencies, scientific establishments and other institutions may find themselves saddled with punitive costs in restoring systems, mitigating production stoppages and offsetting lost revenue. In the reporting period, up to eight-figure sums were demanded as ransom.

1.1.3 Ransomware

For a number of years now, *ransomware* has constituted one of the most serious threats to users of IT systems - not least because the successful deployment of this kind of malware prevents access to data and systems stored locally or on the network. Typical practice for attackers is to encrypt user data (such as office documents or image, audio and video files) or even entire databases. The victim is then sent a message informing them that access to their encrypted files can be restored by payment of a ransom fee. A common practice is to set very short deadlines and to threaten victims with the successive disclosure or deletion of the encrypted data (cf. chapter *Theft and Misuse of Identity Data*, page 18). Ransom payments are usually demanded in (virtual) digital currencies (e.g. *Bitcoin*) in order to make law enforcement efforts more difficult. Alongside real cases of this kind of extortion, cases have also been

Emotet as a Point of Entry: a Ransomware Attack on the Council Offices of a Mid-sized German City

Situation
On 6 September 2019, the IT department in the administration of a mid-sized German city discovered that their local systems had been compromised. To prevent the infection from spreading any further, IT management decided to take the servers temporarily offline. By this time, however, many of the council's databases and documents had already been encrypted - including their *backups*. A ransom demand was then made.

Emotet had been the point of entry for the *ransomware* attack. It had most likely been sent to the council's PCs as an attachment in an email made to look authentic with sophisticated *social engineering* methods. The council's virus scanners were unable to stop the infection.

The attackers rolled out the Ryuk *ransomware* to the infected systems and encrypted some 550,000 files, including parental pay applications, building plans and much more besides. All council business came to a virtual standstill. It took more than a week before the first systems could be brought back to service. Some services were still unavailable even as late as the first quarter of 2020.

Response
Since Emotet not only downloads additional malware payloads, but also eavesdrops on email communication for usage in subsequent attacks, the council phoned its external partners to explain that they should not open emails apparently sent by the city's administrative staff.

To clean the infected systems, the IT department was able to restore a clean and unencrypted *backup* of its accounting data. Other files had to be recreated from scratch - including building plans for a new development area. On recommendation of the BSI around 300 computers were reinstalled. These additional measures amounted to costs of approximately EUR 500 per computer.

Stricter rules for email attachments were also introduced in order to ensure that more attachments would be rejected automatically. In addition, the network was segmented more stringent with the intention to make propagation of malware throughout the network in the event of any future attack more difficult. Tape backups (offline *backups*) stored in physical safes were also reintroduced.

Recommendation
Regular *backups* are the most important precaution that can be taken to restore normal operations following a *ransomware* attack. To ensure that *backups* are not also encrypted in the event of an attack, they must be stored offline and separately from other systems. Backups should be checked regularly to ensure that they can be restored quickly as part of disaster recovery.

observed that appeared to be a *ransomware* attack but were in fact utilised as a diversionary tactic or simply carried out as an act of sabotage.

Ransomware is distributed using the usual malware *attack vectors*, either as an email attachment or a link that takes the user to an infected web page (cf. chapter *Malware*, page 4). One *attack vector* that is particularly dangerous for businesses and other institutions with larger-scale IT infrastructure is provided by vulnerabilities in remote administration/*VPN* gateways. These tools are used to access systems that require maintenance and/or to work on these systems remotely. Compromising such a tool often means that the attacker is subsequently granted an extensive set of rights from the outset. Further information on this topic can be found at www.bsi.bund.de/ransomware.

The current reporting period saw a continuation of the trend in targeted attacks on entire networks operated by companies or other establishments. Meanwhile, another trend emerged towards targeted attacks on financially robust victims such as car manufacturers and their suppliers, a number of airports and airlines, and less well-known companies with high levels of earnings. Smaller-scale

businesses - those with unique characteristics (a specialisation in producing specific machine parts, for example) or a simple lack of proper protection - were also the subject of such attacks.

Public-sector organisations, especially at the local authority level, have also found themselves the target of *ransomware* attacks. Other victims of such attacks during the reporting period included universities and healthcare facilities - particularly hospitals.

Alongside these targeted attacks, scattergun *ransomware* attacks (e.g. Sodinokibi) also continued. With this approach, attackers try to maximise their profits by having a large number of victims. With the aid of *social engineering* strategies in spam emails, many users are tricked into clicking malicious mail attachments or links. Common tactics here include leveraging personal trust in a familiar name or the appeal of trending topics. Typical processes associated with particular jobs are also misused, such as the fact that employees in HR are required to open application letters, which could then trigger a malicious macro. One particular *ransomware* of this type is Sodinokibi (also known as Sodin and REvil), which, like its probable predecessor GandCrab, is distributed as a special kind of 'service model' (*ransomware*-as-a-service).

The procedure used by this kind of extortion differs from that which is practised by network-wide attacks. In communications from attackers, victims are directed to a special web page that is hosted on the Tor[3] network. Typically, the attackers will provide all of the infrastructure required for the victim to pay the ransom fee, at which point the corresponding decryption program can then be downloaded. However, for *ransomware* like Ryuk that is deployed manually, attackers normally only provide one or more email addresses the victims should use to contact the attackers in order to negotiate the ransom fee.

The losses from ransom fee payments and system recovery costs are steadily increasing as entire networks become sabotaged and, in some circumstances, hundreds of thousands of people are affected - by the encryption of patient data, for example. Employees working at organisations that are the target of these attacks may also face drastic repercussions. The losses caused by *ransomware* may prove to be an existential threat.

The overall damage suffered by affected businesses and institutions is, as a rule, much greater than any ransom fee that these organisations may elect to pay. This is because IT outages, which may already entail considerable costs for data cleansing and system recovery, also trigger a wide range of secondary expenses. Lost revenue is naturally a direct business loss. Costs also increase, however, due to the installation of alternative business processes (such as when additional personnel must be hired) or outsourcing to third parties. During the recovery of IT infrastructure after an attack, hardware is often replaced in order to be able to implement the necessary reworked security concepts. This migration also causes disruptions and delays in the ordinary course of business and lead to further training requirements, as well.

For many affected organisations, a *ransomware* attack also means a loss of reputation. Even when the greatest care is taken and *backups* are available, data may nonetheless be lost (application-specific caches, for example). The quality and frequency of *backups* will therefore also determine the magnitude of the effort or damage caused by the loss of this data.

The most important countermeasure against the fallout from *ransomware* attacks is having viable *backups*. These *backups* must be checked regularly to confirm that they can be used to reconstruct the data. It must not be possible to simply change or delete these backups from the network (offline *backups*). However, since contemporary attackers do not merely encrypt data, but also take copies that they then threaten to disclose in order to force payment of a ransom fee, systematic, rule-based monitoring of all data transfers is also necessary. This could identify an unusually large outbound flow of data, for example, and terminate such a transfer in reasonable time.

To minimise exposure, the number and variability of externally accessible systems must be kept as low as possible, and prompt updates of operating systems and server and application software must be performed on a regular basis. Even in the event of a successful attack, appropriate segmentation of internal networks will help to limit the extent of the damage.

For companies and other organisations, the comprehensive and continuous training of all members of staff on the topic of information security (so as to raise awareness) should be a matter of course, as should taking steps to restrict the number of individuals with (remote) access to systems. Where access is necessary, stringent requirements must be applied in the form of policies on passwords and protocols.

To ensure an organisation is prepared in the event of an attack, response scenarios should be established in writing. These should cover all of the aspects of an attack as described above as part of crisis management, including damage to production facilities, the deployment of personnel and security firms, alternative business processes and a potential loss of reputation.

[3] Network for anonymising connection data

Ransomware in Hospitals

Situation
On Saturday, 13 July 2019, the core systems managed by a German Red Cross operating company (DRK Trägergesellschaft Süd-West) were encrypted by *ransomware*. This attack severely impaired the ability of associated hospitals in Rhineland-Palatinate and Saarland to provide healthcare services.

Response
The BSI learned of the incident from the National Cyber Response Centre and initiated what is known as 'coordinated case handling', which involves various agencies at the state and federal levels. After analysing the ransom note sent by the attackers to the affected organisation, the BSI was able to identify the Sodinokibi malware as the most likely cause. The BSI provided the affected service provider of DRK Trägergesellschaft Süd-West with a case-specific support package as an initial support strategy. This package contained the latest warnings and assistance, as well as information about the identified malware. Other services offered by the BSI included deployment of the Mobile Incident Response Team (MIRT) for on-site support, which was accepted on 18 July. A specialist team arrived at the organisation on 19 July. The BSI MIRT and the IT service provider succeeded in working together to identify the extent of the attack, determine the most likely point of entry, remove and block the attacker from the network, and restore the IT network to its normal operational condition. This work was completed on 26 July 2019.

In response to this incident, the Roundtable for Hospital IT Security - a project group staffed by a number of subject-matter experts - was established in August 2019 by the Ministry of Social Affairs, Labour, Health and Demography for Rhineland-Palatinate. The Roundtable was tasked with formulating recommendations and drafting specific measures with the aim of informing hospitals in Rhineland-Palatinate on the topic of information security and raising awareness of this subject. Alongside representatives of the Ministry of Health, other project group members included representatives of the BSI, the Rhineland-Palatinate State Commissioner for Data Protection and Freedom of Information, representatives of the hospital association Krankenhausgesellschaft Rheinland Pfalz e.V., representatives of the association of German hospital directors Verband der Krankenhausdirektoren Deutschlands e.V., and the Head of IT Management at DRK Trägergesellschaft Süd-West. The Roundtable adopted an action plan in March 2020.

Evaluation
The health sector is of fundamental importance to the proper functioning of any community and is therefore part of critical infrastructures. The BSI welcomes the initiative launched by the State of Rhineland-Palatinate to learn from this incident and take a joint approach to continually improving standards in hospital information security. The BSI is also keen to work with other state governments and operating companies (and corresponding associations) in the health sector.

Recommendation
A functional and well-rehearsed crisis management is a key success factor in handling cyber security incidents. In this case, an important role was played by the hospital's comprehensive management of the incident, which featured close cooperation between the business continuity management (BCM) team for patient care - using paper-based treatment documentation, for example - and the IT crisis management team. Rule of thumb for IT incident management: narrow down the problem, find the cause, and identify the measures required.

Ransomware Attack on a University

Situation
On 23 December 2019, a university became the victim of a *ransomware* attack. Immediately after detecting the attack, the university shut down all of its computer systems as a preventive measure in order to hinder the propagation of the malware within its network. The appropriate authorities and a provider of IT security services were brought in to analyse the attack and restore the systems. Owing to the direct impact on research and teaching, the university published regular (sometimes daily) updates to its website with contact details, news of new developments and recommendations for action.

In early February 2020, the university disclosed details of the attack and the inferences drawn from managing it. According to the analysis, the attackers had already penetrated the university network in October 2019 using malware-infected emails. Before executing the Clop *ransomware* in December 2019, the attackers spent time infiltrating the network. By using other malware and exploiting certain vulnerabilities, they ultimately achieved a comprehensive level of access and carried out an attack that restricted or directly affected 1,647 servers and around 7,307 workstations. The attackers also managed to encrypt the *backup* servers.

Response
The university later made a public statement confirming that they had decided to pay the ransom demand. Key factors in this decision had been the ethical aspects of making such a payment as a public institution and the potential repercussions regarding its ability to resume its tasks and duties as an institution of higher education. Since the attackers had encrypted critical systems and their *backups* and it was to be assumed that for example the results of research would therefore be irretrievably lost, a ransom demand totalling 30 *Bitcoins* (the equivalent of around EUR 200,000 at the time) was paid.

According to the forensic analysis, there were no indications that research results or other data repositories had been stolen from the university's networks during the attack. Both the university and its IT service provider however believe that such a theft may have been possible, however, and further investigations are ongoing.

Recommendation
Regular *backups* are the most important precaution that can be taken to restore normal operations following a *ransomware* attack. To ensure that *backups* are not also encrypted in the event of an attack, they must be stored offline and separately from other systems. Backups should be checked regularly to ensure that they can be restored quickly as part of disaster recovery.

As a rule, the BSI does not recommend paying ransom demands because this works to legitimise the *ransomware* 'business model' and may motivate further attacks on other targets.

1.1.4 Spam and Malware Spam

Unsolicited emails are generally referred to as *spam*. Apart from bulk advertising, some emails - like *malware spam* and *phishing* mails - may constitute cyber attacks. Spam mail can be sent from compromised or commercially rented server facilities, via legitimate email accounts stolen by the attackers (whose access credentials have been pilfered earlier) or via infected systems that have been consolidated into *botnets* and then used to provide *spam* services (cf. chapter *Botnets*, page 16).

The sending of unsolicited advertising email continued its downward trend in the current reporting period (cf. *Bibliography*[1]: www.bsi.bund.de). One reason for this decline is likely to have been the increasing quality of many *spam* filters. Their high rate of success makes advertising *spam* increasingly unattractive as a business model because many of these bulk mails no longer reach their recipients. In addition, a more efficient type of online marketing is now available in the form of 'targeting'.

Targeting analyses user behaviour data from websites, online shops or social media platforms, for example, in order to display personalised advertising to the recipient.

Malware spam involves the bulk sending of untargeted *spam* emails with malware payloads. While the sending of *spam* declined, the effectiveness of *malware spam* continued to improve in the reporting period. Notably, the *spam* component of Emotet saw further use as a successful means of distributing this malware. The potential scale of the resulting damage depends in particular on sophisticated social engineering techniques designed to trick the end user into executing the malware payload. The risk of infection should therefore be estimated as high (cf. chapter *Emotet: New Quality of Advanced Attacks*, page 11).

1.1.5 Botnets

The term *bot* refers to a type of malware that gives an attacker remote access to an infected system. Any piece of malware that can establish a connection to a command-and-control server operated by the attacker to receive commands from the server and execute them on the infected system is therefore a 'bot'. The wide distribution of bot software has given attackers access to a large number of third-party systems (computers, smart phones, routers, IoT devices, etc.), which they can then misuse for their own purposes. A cluster of multiple bots controlled from a master computer is referred to as a *botnet*.

The modular design of contemporary bot software lets attackers adjust the functionality of a bot flexibly to suit the particular attack goal and intended target. Apart from causing damage on the infected system itself (exfiltrating personal data, conducting online banking fraud, encrypting data, etc.), the infected systems themselves can be used to attack third-party systems. Attackers can therefore exploit the enormous computing and networking capacities offered by these aggregated infected systems to carry out high-bandwidth *DDoS attacks* (cf. chapter *Distributed Denial of Service*, page 29) or send *spam* mail, for example.

In the current reporting period, *botnets* were primarily used to steal information or download and propagate other types of malware (such as banking Trojans or *ransomware*). A significant decline was seen in the number of *DDoS botnets* compared to the previous reporting period. While it is true that new variants of the Mirai *botnet* (for instance) did continue to appear featuring additional infection mechanisms designed to extend the spectrum of victim systems to other device classes such as IoT devices and less widespread hardware platforms (e.g. ARM, ARC and PowerPC), these were not associated with high rates of infection or successful *DDoS* attacks.

The trend in attackers focusing more strongly on mobile devices such as smartphones and tablets was also observed once more in the current reporting period. In the Windows-based *botnet* segment, Emotet and Trickbot in particular were responsible for large waves of infection in Germany. Both of these malware families have been active for several years now, and they have also infected several larger institutions and companies in addition to private users. The deployment of the *ransomware* Ryuk, which attacks victims previously invected by Trickbot, has caused major financial losses (cf. chapter *Emotet: New Quality of Advanced Attacks*, page 11).

During the reporting period, up to 20,000 bot infections per day were registered in German systems and reported to German internet *providers* via the BSI. In such cases, the providers then notify affected customers of the infection and may also provide additional information about how to clean compromised systems. To detect *botnet* infections, *sinkhole* systems are deployed to accept contact requests from bots in place of the attackers' regular command-and-control servers. For a description of the sinkholing procedure, see www.bsi-fuer-buerger.de (cf. *Bibliography*[2]: www.bsi-fuer-buerger.de).

As in previous years, the threat posed by *botnets* remains consistently high. Infection numbers derived from sinkholing should always be seen as a lower limit because it is impossible to obtain a complete set of data for all ongoing *botnet* infections. Depending on the *botnets* selected for observation and the domains utilised for the control servers, figures on visible infections can vary greatly. However, the experience gained thus far in successful *botnet* shutdowns shows that the number of unreported cases is significantly higher and at least in the seven-figure range.

As the number of potential victim systems continues to expand as a result of inadequately secured *IoT devices* and mobile systems, one can therefore expect a continuous increase in infections, and thus in both the number and size of *botnets*, as well.

Avalanche: Protective Measures Extended

Situation

On 30 November 2016, the Luneburg Central Criminal Inspectorate (ZKI) and the Verden public prosecutor's office joined forces with other international partners to take down the 'Avalanche' *botnet* infrastructure. The BSI also played an important supporting role. The *botnet* infrastructure servers were shut down, the attackers were jailed, and the end users of the infected systems were informed by their internet *providers*. To ensure the ongoing detection of infected systems, *sinkhole* servers were set up to log contact attempts from the remaining active *bots* and identify their IP addresses. With these IP addresses and corresponding timestamps, internet *providers* are able to inform and warn the affected end users.

Response

Originally scheduled for one year, the measures to provide protection and information were extended in each of the following years to continue safeguarding infected systems. In November 2019, these measures were extended by a further 12 months. This involved checking and blocking third-party access to around 830,000 domains in order to prevent *botnet* takeovers by criminals. This naturally requires the active cooperation of the domain owners. The forwarding of infection data by the BSI to *providers* and other international partners enables the prompt decontamination of affected systems.

Infection volumes and their trends over time are measured using the unique IP index. This involves counting unique IP addresses per day both in Germany and around the world. The previous downward trend also continued in the current reporting period. As a result, the index generally remained below the average figure for 2019.

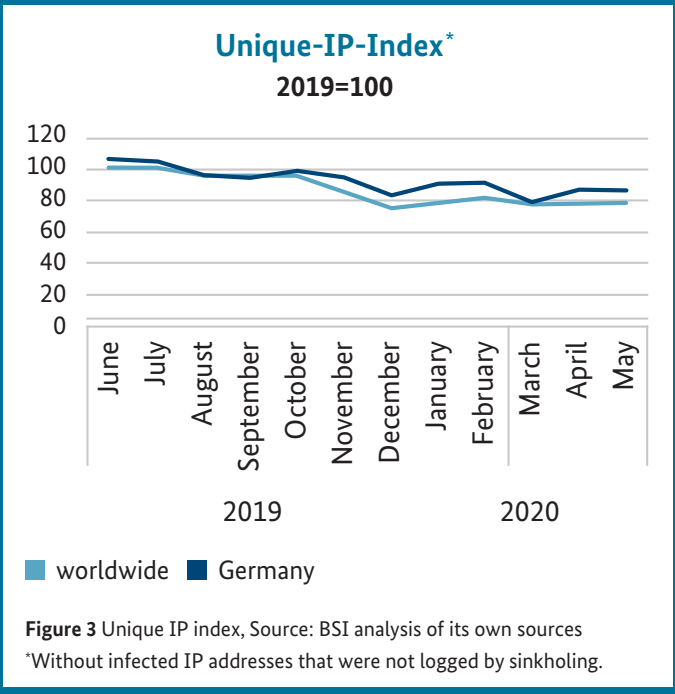


Figure 3 Unique IP index, Source: BSI analysis of its own sources
*Without infected IP addresses that were not logged by sinkholing.

Recommendation

The infection figures clearly illustrate the fact that, even after three-and-a-half years, many affected end users have yet to desinfect their infected systems. The BSI recommends doing so as a matter of urgency.

1.2 Theft and Misuse of Identity Data

In the context of information security, an 'identity' is understood to mean a set of attributes providing evidence that a person or thing is genuine. Accordingly, the identity of a person or thing can be defined by a single attribute, or by a combination of several discrete attributes. In the online world, the identity of a person is typically deduced from identification and authentication data - the combination of a username and password, for example. The concept of 'identity theft' is therefore defined as the illegal takeover of such data. If a stolen identity is then used by the thief or some other third party for an unauthorised purpose, this is referred to as 'identity fraud'.

As in the previous reporting period, notifications of leaks of identity data were observed on a regular basis. Regardless of the advantages promised by major digitalisation projects, these will only prove successful and enjoy an appropriate level of acceptance if they are designed to be secure from the outset and also provided with the resources this requires over the long term. On the part of internet service providers, the integration of procedures for secure identification during initial customer contact is an important step in this context. Only by identifying each user in accordance with the protection requirements at hand can a service ensure that sensitive data is restricted to authorised individuals.

However, the current cases of identity theft also show how the 'digital duty of care' incumbent on each and every one of us represents an important aspect of information and IT security over the long term. The sheer volume of compromised user information and the opportunities to misuse it have made personal information a widely available and valuable commodity, which in turn endangers the security and reputation of digital infrastructure as a whole. In the hands of an attacker, this kind of data greatly increases the chance of success for many hacks - from tampering with systems, blackmailing users and automating authentication attempts (known as 'credential stuffing') to direct access to third-party accounts.

The BSI therefore recommends taking great care when handling one's own personal information and setting up *two-factor authentication* for accounts as soon as this is offered by an online service. As one example, the FIDO2 (Fast Identity Online 2) standard has defined an *authentication* protocol that permits the use of key stores on mobile devices or an external hardware token as an authentication factor. As of this writing, FIDO2 has already been implemented in most browsers. The protocol is based on *public-key cryptography*, which means that users never need to share their private key with the service. Instead, key ownership is proven by means of a random number combined with a digital signature. This standard is already supported by many service providers, such as Google, Facebook and Microsoft. The use of authentication factors taken from separate categories (knowledge, possession or inherence (biometric attributes)) considerably reduces the possibility of identity theft and identity fraud.

One prominent type of identity theft is known as *phishing*. In this kind of attack, a set of sophisticated *social engineering* techniques are used to enforce the victim to disclose sensitive information (cf. chapter *Phishing and Other Types of Fraud*, page 18). Another potential attack vector for purloining identity data is the use of specialised malware (cf. chapter *Malware for Harvesting Identity Data*, page 20). Identity data can even be acquired without the direct involvement of the victim - when stolen from the victim's service provider, for example (cf. chapter *Data Leaks*, page 20).

1.2.1 Phishing and Other Types of Fraud

On the topic of *phishing* in Germany, attackers currently appear to be focusing not just on bank customers, but also on customers of online retailers like Amazon or payment systems such as PayPal. As has been seen before, the current spate of *phishing* campaigns closely tracks social trends and topical issues such as tax refunds or discounted offers for Black Friday. While attackers in the previous reporting period exploited uncertainty regarding the General Data Protection Regulation (GDPR), implementation of Payment Service Directive 2 (PSD2) was the primary focus during the current reporting period. The repercussions of the COVID-19 pandemic were also felt in the digital world, however. The air of uncertainty surrounding coronavirus countermeasures was exploited by attackers, as were objective and subjective time pressures and the dominance of the topic in society and the media. The BSI subsequently received reports of German-language *phishing* mails that were typically well-formulated, were careful to play to the recipient's emotions and addressed the all-important topic of COVID-19. Their content included (for example) temporary closures of bank branches, details on new opening hours, and information about applying for emergency help and short-time working money.

By exploiting human propensities to help, trust, worry, take urgent action and respect authority, victims were consistently lured onto *phishing* pages that were very hard to distinguish from the original websites.

The use of HTTPS links in *phishing* attempts is fast becoming the standard for these messages. Hypertext Transfer Protocol Secure (HTTPS) describes a type of data transmission that is encrypted and protected against outside tampering, which is how it enhances the impression of trustworthiness and respectability given by *phishing* websites. Joint analyses conducted by the BSI and the Consumer Advice Centre for North Rhine-Westphalia (NRW) based on reports to its Phishing Radar (cf. *Bibliography*[3]: Verbraucherzentrale.de) showed that more than half the links in *phishing* mails in Germany had begun using HTTPS (60%) in the current reporting period. The same figure was only 45 percent in the prior reporting period. This development may well be attributable to the fact that popular web browsers now warn users about sites that use 'plain' HTTP. The certificates necessary to establish an encrypted connection can be obtained free of charge on the internet and typically give no guarantees that the owner of the certificate should be trusted.

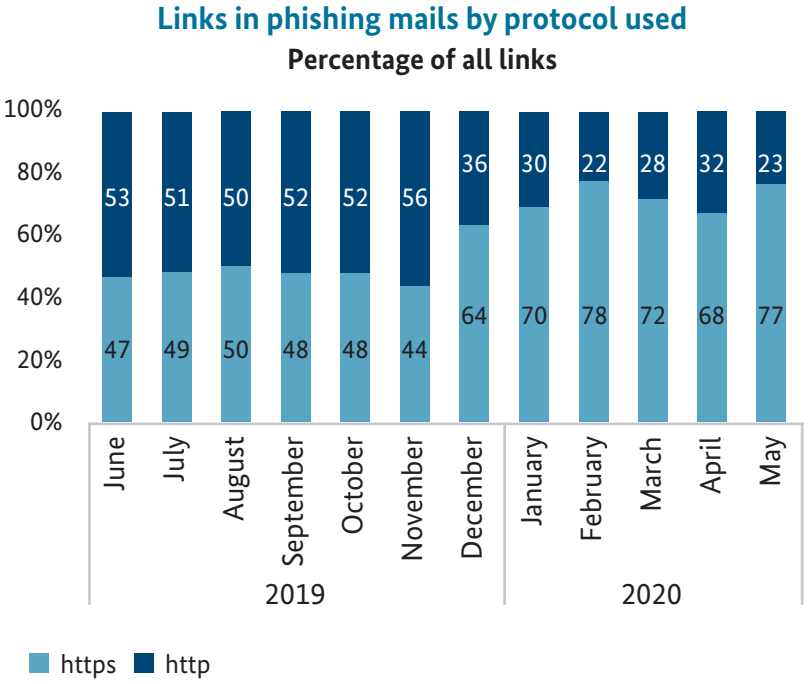


Figure 4 Links in phishing mails by protocol used
Source: BSI analysis of raw data from the NRW Consumer Advice Centre

Alongside conventional *phishing* emails, attempts at extortion were also observed once again in the current reporting period. In these cases, attackers reproduced the victim's (correct or alleged) passwords in counterfeit emails, for example, or claimed to have recordings of the victim visiting pornographic websites ('sextortion'). The attackers demonstrated a high degree of creativity in the wording of these extortion attempts. Whether they involved disclosing all of the victim's secrets, inflicting bodily harm, or infecting one's entire family with COVID-19, their threats typically involved some sort of financial loss for the victim. Alongside this exploiting of basic concerns, some mails also appealed to people's readiness to help out, such as by pretending that a supposed friend had got into trouble on holiday and was in need of financial support. Others requested donations in the cryptocurrency *Bitcoin* for the purported development of a COVID-19 vaccine.

In summary, the current reporting period once again demonstrated the versatility of attackers in latching onto events and current topics of public interest. The COVID-19 pandemic and the societal uncertainty it caused were a particularly popular choice in this regard.

1.2.2 Malware for Harvesting Identity Data

Alongside *phishing* attacks, malware designed for the theft and misuse of identity data is also deployed. In this respect, the malware Emotet offers a striking example of the huge value that repositories of identity data can have as the basis for subsequent attacks. Emotet retrieves contact relationships and email content from the mailboxes on infected systems. This information is subsequently used by the attackers to further propagate their malware. The great success of Emotet stems from the fact that its emails seem highly authentic and thus succeed in tricking victims into opening attachments (cf. chapter *Emotet: New Quality of Advanced Attacks*, page 11).

The theft of personal information can also play a major role in individual cases of extortion. The BSI has learned of a number of cases in which the blackmailers not only demanded a ransom fee to decrypt the data, but also threatened the victim with the online publication of personal information they had harvested. Examples of this particular approach have been attributed to the hacker collectives behind the Sodinokibi and Maze *ransomware* (cf. chapter *Ransomware*, page 11).

Meanwhile, malware does not need to be complex in order to constitute a threat. Even apparently simple programs such as browser extensions can pose risks to end users and result in the loss of personal data. Browser extensions are optional programs that can be used to add functions to the standard feature set offered by a web browser. During the reporting period, a large number of these extensions were banned by browser makers because they exhibited malicious properties. At the end of 2019, for example, the Mozilla Foundation (which develops Firefox) removed a browser extension published by a well-known manufacturer of IT security software. This extension had been collecting large amounts of data on its users' browsing behaviour and then using it for marketing purposes.

During the reporting period, it once again became clear how the growing volume of freely available identity data constitutes a dangerous basis for further attacks. Even apparently trivial programs such as browser extensions can nonetheless cause serious damage.

1.2.3 Data Leaks

As in the past, reports of customer data being stolen were a common occurrence in the current reporting period. The organisations affected by data leaks included prominent banking firms and payment service providers, technology companies, doctor's practices, hospitals and higher education institutions, as well as a company in the electronics retail segment and a car hire business (cf. incident on page 21). Along with the incident at the car hire company, the publication of large volumes of hospital patient records was particularly notable. Highly sensitive personal information of this kind - especially healthcare data - needs that much more effective protection.

The multitude and frequency of incidents in which sensitive data continues to be published accidentally is a matter of great concern. These events affect larger corporations, as well. At the end of 2019, security researchers discovered multiple unsecured databases containing customer and support information of a technology company that were publicly available online due to a misconfiguration (cf. *Bibliography*[4]: www.heise.de). These kinds of data offer an excellent starting point for fraudulent support requests. In this type of *social engineering* attack, criminals may pose as a company employee, for example, and use a purported phone call or counterfeit warnings displayed on the user's PC as a cover for attempting to deactivate security functions or acquire access to the victim's system. In light of the current COVID-19 pandemic, these kinds of attacks are once again becoming a serious threat: in such exceptional circumstances, they may be fortunate enough to target unprepared or inattentive individuals who see themselves forced to act quickly without exercising due care and attention (cf. chapter *Threats to Cyber Security due to the COVID-19 Pandemic*, page 33, cf. incident on page 34).

Tools and services are freely available for identifying exposed databases and systems that are publicly accessible over the internet. Attackers can utilise these resources to obtain unauthorised access to such databases and systems.

The degree of responsibility borne by service providers is clear from the regular reports of data leaks. In the healthcare sector in particular, the public disclosure of sensitive data can simultaneously have an adverse effect on the individual health of the patients affected - potentially with lifelong consequences. However, the current cases of identity theft also show how the 'digital duty of care' incumbent on each and every one of us represents an important aspect of IT security over the long term.

Data Leak at a German Car Hire Firm

Situation
Following an advisory notice published by the German Cybersecurity Society and joint research conducted by journalists from c't and ZEIT, the general public first learned in January 2020 that the sensitive data of three million customers of a German car hire firm had been freely available on the internet.

Due to a configuration error on a *backup* server run by the firm's provider, the server had not required a password to access it via the Server Message Block (SMB) network protocol. By connecting to the open SMB port 445, any internet user could have downloaded the 10 TB of data stored there.

According to the analysis completed by the journalists, the dataset included over nine million rental agreements, some of which dated back to 2003. Alongside the hirers themselves, the data listed details such as names, addresses, dates of birth, driving licence numbers and issue dates. Many hirers of vehicles had also provided their mobile phone numbers and email addresses. Furthermore, the dataset included detailed information about damage and accidents that had occurred during rental periods, as well as over 3,000 passwords from employees and customers - all of which was stored in plain text. Although credit card numbers were not found in the database, the data did include payment information and bank account details from scanned invoices.

Since the car hire firm also offered its vehicles via intermediaries, the data leak potentially affected individuals that had not even rented a car from the firm directly. The details provided in relation to accidents could also have resulted in data being collected on individuals that were not actually customers of the company.

The leaked data was thus considered to be extremely sensitive. The highly genuine nature of the data also meant that it had considerable potential for misuse by cybercriminals: from *phishing* to extortion or other threats, many types of criminal activity could be considered as feasible. In addition, these sorts of crimes would remain entirely possible even long after the incident had been forgotten.

Response
Unprotected access to the server was possible until the port was finally closed on 20 January 2020. The car hire firm reported the closure to its State Data Protection Authority. On 25 January 2020, the company published a statement confirming the incident, with details as required by Article 34 of the GDPR.

Recommendation
This incident clearly highlights the serious consequences that may result from a single configuration error. To ensure compliance with the BSI standards for internet security (ISi series), servers should always be configured as minimal systems whenever possible. This means that only the services, programs and functions that are actually required should be provided. Following server setup, an analysis should also be conducted of running processes, interfaces that are available on the network and other programs installed on the server to exclude any possibility of misconfiguration. Depending on the intended use of the server, the configuration should also be checked by a management component in order to detect any changes.

Patient and Medical Imaging Data Publicly Available Online

Situation
In September 2019, IT security researchers contacted the BSI with news that unsecured databases containing highly sensitive medical data had been discovered on the internet. The information in these databases was personal data such as first and last names, dates of birth, medical exam dates, information about the treating physician or treatment, and even high-resolution X-rays and other materials. The information was stored on systems known as PACS servers (Picture Archiving and Communication Systems), which are used in the healthcare sector to archive images created by radiological departments and make them available for viewing by treating physicians.

In Germany alone, around 15,000 datasets were publicly accessible during the period from July 2019 to September 2019. They contained a total of several million images (cf. *Bibliography*[5]: www.greenbone.net). Most of these were accessible without a password or other form of authentication. Many countries around the world were similarly affected. Overall, it is estimated that around 24.3 million patient datasets and several hundred million linked image files were publicly accessible on the internet.

Response
BSI informed the healthcare facilities of the problem. In three cases, it was possible to contact these facilities directly; in 14 other cases, the respective internet service *providers* were asked to identify and inform their customers based on the IP addresses in question. The BSI also informed 46 international partner organisations about the incident.

Many countries also responded to the situation by introducing corresponding measures as quickly as possible in order to protect the data. For example, 11 countries (including Germany) removed the PACS systems discovered by the original scan from the public internet. More publicly accessible PACS servers in other countries have since been discovered.

Recommendation
The BSI recommends making patient data available in cloud-based systems or other services accessible over the internet only if it can be ensured that all available safeguards - such as the encrypted transmission of data and encrypted storage - are appropriate for providing an adequate level of protection and secure *authentication* to guarantee the confidentiality of these patient records. The BSI has not yet assessed the IT security of PACS servers, which are classified as medical devices. In the BSI's opinion, all of the above requirements for protecting sensitive patient data apply equally to PACS servers.

1.3 Vulnerabilities

1.3.1 Vulnerabilities in Software Products

Modern software products are now responsible for handling many processes and areas of our lives. They can be used to solve complex problems or simplify various kinds of routine work, for example. To meet the growing challenges represented by these tasks, software products themselves are becoming increasingly complex and may now consist of several million lines of program code. This effectively makes it impossible to audit all of the contingencies that a software product may have to deal with (although it is true that there are many automated approaches for improving software quality). As a result, software products may contain undetected errors or faults that could lead to them no longer functioning as intended. If these faults or errors can be exploited by unauthorised third parties to execute routines that damage a computer system, the products affected are said to have 'vulnerabilities'.

When exploiting a vulnerability, an attacker causes a software product to carry out operations that were not intended by its developers. Examples of such operations include the disclosure of sensitive information (cf. chapter *Theft and Misuse of Identity Data*, page 18), the execution of malware planted on the system (cf. chapter *Malware*, page 9) or simply causing the software to crash. Software vulnerabilities are not merely undesirable; they frequently pose a major threat, as well. They should thus be patched as quickly as possible after detection.

Vulnerabilities differ in terms of their criticality, their individual potential as a threat and whether or not countermeasures - in the form of updates, for example - are already available. In simple terms, the criticality of a vulnerability is calculated using three factors: the relevance of the affected software product for end users; the effort or circumstances required to successfully exploit the vulnerability; and its potential impact on the security objectives of confidentiality, integrity and availability. Together, these aspects indicate the specific level of risk that a vulnerability poses to its end users. It can generally be assumed that the proper functionality of a piece of software is as important as the purpose for which it is intended. This kind of risk assessment can be made by following the BSI's 'IT-Grundschutz' code of practice, for example.

As soon as a vulnerability has been made public, it should be assumed that attackers will actively seek out ways of exploiting this vulnerability. It is therefore in the particular interest of all users of a software product that the manufacturer fixes the vulnerability with a security update as soon as possible.

Some companies have taken the step of offering 'bug bounty' programmes, which are designed to catch and patch vulnerabilities before they can be exploited. These programmes invite developers and IT security researchers to earn a reward by actively searching for vulnerabilities. Simply seeking out vulnerabilities without the manufacturer's permission is typically prohibited by law because the methods deployed may well breach the general terms and conditions of business that apply to the purchase and use of a software product. Such efforts can therefore have legal consequences for IT security researchers if they are not expressly commissioned to carry them out.

Critical vulnerabilities can be reduced by adopting an appropriate design philosophy during the actual software development process. To design software products to be more secure, the principles of *security by design* and *security by default* must be applied. The security by design philosophy starts at the beginning of the software development process and continues throughout a product's entire lifecycle. It attaches the same importance to the security of a software product as it does to its usability, for example. For software deployed in a high-risk context, however, security is considered to be significantly more important.

The security by default concept, meanwhile, focuses on how software is configured at the time it is shipped out. Many software products allow their users to change various kinds of settings and tailor them to the respective intended use, or to strike a particular balance between usability and security. When shipping out software that follows the *security by default philosophy*, the default settings represent the most secure configuration in which the software can be used. This is an important point because cases are increasingly coming to light in which an initial configuration was not changed, and its settings were then exploited by attackers.

The handling of vulnerabilities in software products is a crucial factor in ensuring a secure digital transition in Germany. The increasingly widespread and high-profile use of bug bounty programmes, CVD processes (cf. chapter *Computer Emergency Response Team for Federal Agencies*, page 67), *security by design* and *security by default* shows that the importance of such activities is being acknowledged by more and more software companies, IT security researchers and public-sector organisations.

On the subject of handling vulnerabilities, the current reporting period once again underlined the 'digital duty of care' incumbent on end users. Users are responsible for ensuring their software is up to date. This includes applying updates and following instructions from manufacturers if a *patch* is not currently available. Even in case of vulnerabilities that should be considered critical, the BSI has repeatedly observed situations where the available updates were only applied after some time had passed (if they were at all).

Corresponding action on the part of end users was also required in the reporting period after Microsoft ended support for its Windows 7 and Windows Server 2008 (R2) products on 14 January 2020. Since then, both critical and important security updates for these two operating systems have only been made available to customers of the company's premium Extended Security Update programme. Other users no longer receive security updates. Although it is now a decade old, the Windows 7 operating system is still in widespread use. It remains fully functional and can still be installed without support, but it has no protection against new risks.

The BSI recommends that personal users and businesses no longer use the affected Windows operating systems and instead switch to an operating system for which security updates continue to be offered. Before upgrading or changing their operating system, users should verify that their hardware meets the new system's technical requirements. The programs and specialised applications they use should also be supported, along with peripheral devices such as printers. As a final step, backups should also be made in order to avoid a potential loss of data. Since migrating an operating system can entail a significant investment of both time and human resources (especially in larger organisations), it should be treated with the requisite urgency.

Critical Vulnerability in Citrix Products

Situation

On 17 December 2019, US software company Citrix published information about critical vulnerabilities in several of its products and recommended countermeasures to prevent them from being exploited. The software products affected included *VPN* gateways that provide remote access to an organisation's internal applications, which were in active use at over 80,000 businesses in 158 countries. In their function as gateways, these software programs represent a critical junction that separates a company's network from the public internet and regulates the corresponding traffic. As a result of the vulnerabilities, attackers were able to execute arbitrary pieces of code - including malware - on these network traffic controllers. Depending on the other protective measures present in these corporate networks, this then presented the attackers with extensive options for further attacks in some cases.

From 8 January 2020 onwards, *exploits* started to become public - and were remarkable for their simplicity. As a result, a number of attackers were able to adapt and take advantage of these *exploits* for a range of purposes (cf. *Bibliography*[6]: www.trustedsec.com). A prodigious wave of attacks capitalising on these vulnerabilities was then observed (cf. *Bibliography*[7]: https://deyda.net, cf. *Bibliography*[8]: https://blog.dcso.de, cf. *Bibliography*[9]: www.fireeye.com).

Response

Since the *exploit* code was published, the BSI has identified some 5,000 separate systems that were vulnerable to the security vulnerabilities in Germany alone and reported these to the respective network operators and internet service *providers*, along with the details of the threat. However, these 5,000 identified systems presumably do not represent all of those that were at risk in Germany.

By 24 January 2020, the software manufacturer had provided a successive series of security updates that closed the vulnerabilities in the affected product versions. After these updates were posted, the number of vulnerable systems fell significantly - to around 230 at the last count. In addition, the BSI reported dozens of systems where attackers had installed *'backdoors'* to the respective network operators and internet service *providers*. *Backdoors* of this kind are designed to give attackers continued access to a system even after the vulnerability has been patched.

Recommendation

Users of affected products who did not follow the manufacturer's recommendations to temporarily address the vulnerabilities until a *patch* could be provided - before the widespread wave of exploits as reported - are advised to audit any Citrix systems they have connected directly to the internet, as these systems are likely to have been compromised.

Whether or not a vulnerability in a specific system has been announced, programs should only be installed and operated on a system when actually necessary. This type of hardening reduces potential exposure, and with it the risk of falling victim to a cyber attack

When security updates are published to close a vulnerability in a piece of software, they should generally be installed as a matter of urgency. If this is not possible - because of compatibility reasons, for example - the implementation of a workaround examined to prevent exploitation should be considered. In situations where neither *patches* nor effective workarounds are available, the temporary deactivation of the affected software should be seriously considered.

The extent to which the above measures can be implemented in a particular situation depends on the specific conditions in which the affected software is used and the associated risks. Every vulnerability requires a response, however; inaction will always result in a high level of risk.

Critical Vulnerabilities in the Windows Remote Desktop Protocol

Situation
The Remote Desktop Protocol (RDP) runs as a service on the Microsoft Windows operating system and enables remote maintenance, among other features. In May 2019, details were published of a critical vulnerability in this service termed BlueKeep, which enables remote attackers to execute arbitrary applications - including malware - on vulnerable systems (cf. Bibliography[10]: www.microsoft.com). BlueKeep affects older systems such as Windows XP, Windows Server 2003, Windows 7, Windows Server 2008 and Windows Server 2008 R2. Public *exploits* for BlueKeep have been available since June 2019. These pieces of malware search for publicly accessible RDP services on the internet so as to spread themselves automatically via the vulnerability. BlueKeep is therefore also referred to as 'worm-ready'. Scenarios such as those in 2017, when the WannaCry *ransomware* rapidly infected over 100,000 Windows systems and encrypted vast swathes of data, are therefore possible.

Two further vulnerabilities, termed DejaBlue, were announced as presenting a similar potential threat in August 2019. These affected more recent Windows systems as well, up to and including Windows 10 and Windows Server 2019. DejaBlue also permits attackers to execute arbitrary code remotely without *authentication* or any kind of user interaction.

These vulnerabilities are considered critical. While the RDP service is not active in default configurations, it is used for remote maintenance over the internet on a large number of servers and with a relatively low level of protection.

Response
Microsoft responded by publishing security updates for the affected systems, including updates for Windows XP and Windows Server 2003 - systems that the company technically no longer supports. Microsoft also worked with various German and international security agencies and service providers to provide information about vulnerabilities and the security updates available to patch them.

The BSI published cyber security warnings and press releases about both BlueKeep and DejaBlue (cf. *Bibliography*[11]: www.bsi.bund.de).

Recommendation
When setting up systems, only the programs that are actually necessary should be installed and operated. Reducing exposure in this way also lowers the risk of falling victim to an attack.

If a security update is available to patch a vulnerability, this should be installed as a matter of urgency. In cases where this is not possible, workarounds should be considered that are capable of preventing the vulnerability from being exploited. These kinds of temporary solutions will depend on the type of vulnerability and the service affected. It may be possible to temporarily deactivate the respective service, for example, or use an alternative software component for the time being.

1.3.2 Vulnerabilities in Hardware Products

Along with software-based attacks on the confidentiality of data or the integrity and availability of services, attacks targeting hardware are now increasingly becoming a topic of focus for both security experts and the general public. The Spectre and Meltdown vulnerabilities in processors, as well as reports of alleged espionage chips on motherboards - all of which emerged in 2018 - are just a few examples that have attracted considerable attention and clearly underlined the singular importance of secure hardware.

Common to all attacks on hardware is the fact that these typically occur at a low level in the respective architecture or organisational process. They may involve the physics of transistors in highly integrated circuits, the microarchitecture of a highly complex processor or even the production and supply chain steps when considering the life cycle of an IT product. Although the difficulty and complexity of these attacks are comparatively high, the same can be said of the potential rewards. Once the underlying hardware is compromised or the vulnerabilities it includes open a sufficiently wide chink in its armour, any security mechanisms based on this hardware are generally rendered useless.

Authentication Token Attacks

Even today, passwords are still the commonest method of authentication online. They have a number of disadvantages, however (cf. chapter *Two-Factor Authentication*, page 47). This is why services are now increasingly offering an additional layer of authentication protection using specialised hardware that adds another factor (possession) to the user's password (knowledge).

These kinds of security tokens can also contain vulnerabilities, however. During the course of a BSI project, a commercially available FIDO-U2F token (without Common Criteria certification) that is used as a key store for web applications was investigated for vulnerabilities by Fraunhofer AISEC. The manufacturer was informed of the results. (The number of the corresponding CVE entry is CVE-2020-12061.)

In particular, it was discovered that the security token's housing could be opened without leaving any corresponding visible evidence. It was then possible to use an oscilloscope to read out security-relevant, device-specific data from the token. New *firmware* could then be installed to create keys with very low entropy. Existing keys, which the earlier firmware had created with high entropy, could then be extracted using a *phishing* web page. It also proved possible to make a copy of the token. This invalidated the additional level of security assumed by the 'possession' factor.

This procedure is the equivalent of an attack known as the 'Evil Maid' scenario, whereby an attacker briefly obtains control over a device in order to tamper with it. Another scenario relevant in this case is the 'Supply Chain' scenario, whereby an untrustworthy manufacturer, supplier or dealer manipulates an arbitrarily large number of tokens before shipping them out to customers.

This attack combined two essentially independent kinds of vulnerability:

- Security-relevant data can be read out in an unencrypted format (weakness in design)
- Although the microcontroller has read-only protection against manipulation, this does not prevent write operations (weakness in the microcontroller used)

This investigation once again underlines the importance of thoroughly auditing security hardware and treating it as part of an overall system. If hardware and software are analysed separately, potential vulnerabilities could remain undetected.

Smartcard Vulnerabilities

Smartcards are plastic cards into which an electronic processing unit (a microchip) has been embedded. The components used for these microchips include specialised modules for message encryption. The long-standing Data Encryption Standard (DES) is still in use today, typically in the form of Triple DES (3DES, which applies the cipher algorithm three times). Researchers have recently discovered and published vulnerabilities affecting the implementation of this standard on smartcards. Since these research articles are complex and give the impression that the vulnerabilities can be exploited only with specialised lab equipment, it was unclear whether the vulnerabilities actually make the encryption insecure. After other experts failed to repeat the original research findings, the BSI joined forces with the Fraunhofer Institute for Applied and Integrated Security (AISEC) to attempt to replicate the lab setup needed to perform the attack and then to appraise its practicalities. These investigations have shown that the strength of the encryption can be significantly weakened - even with the 3DES algorithm used today. This weakening of key strength results in a data encryption standard that no longer meets the relevant security requirements. As a result, smartcards still based on the older data encryption standard using Triple DES should be replaced with cards utilising the more modern Advanced Encryption Standard (AES).

Attacks on Program Execution

The processing units found in contemporary computers do not always execute the commands sent to them by programs in the specified order. To improve performance, program commands are re-sorted to ensure that these computations utilise processing unit capacity as optimally and simultaneously as possible. As a result of this optimisation, however, commands may be executed incorrectly. For example, commands may be executed with the results of interim calculations that are not yet fully complete. Branches that use if/then conditions can then be incorrectly interpreted and commands can be executed in a different way than they would have been in the original processing sequence. If the processing unit notices such an execution error later on, it then rolls back the operations that it carried out. This corrects the error that occurred. Although these kinds of errors should not be visible outside the processing unit, researchers demonstrated in 2018 that the effects of incorrectly executed commands could still be found in the processor's cache, and also showed how these effects could be utilised to read out the data processed by a different program. Although these attacks on program execution are highly complex and must be customised for the respective architecture and the specific internal optimisation procedures used by the processing unit, they nonetheless represent a serious threat and must therefore be thwarted. To do so, the manufacturers have provided improvements to the firmware running on these processing units, although some of the patches have resulted in significant degradations in processor performance. At the same time, researchers worldwide have developed new attack methods based on similar methods, but different kinds of optimisations and caches used by a number of different processing units.

In retrospect, the expected development of speculative execution attacks has indeed taken place. Accordingly, the recommendations for action made in last year's State of IT Security report remain as current as ever: over the medium to long term, computing hardware should be designed so that data of an especially confidential nature - and key material in particular - should be processed only on entirely separate processing units. Virtualised *cloud* systems in particular should be protected from speculative execution attacks. Due to the high level of complexity involved in exploiting existing vulnerabilities, broad-based attacks are not as efficient and are therefore less likely.

1.4 Advanced Persistent Threats

Advanced persistent threats (APTs) are distinguished from other threats in relation to IT security as a result of the attacker's motivation and methodology. While most malware is typically untargeted and distributed by financially motivated attackers, APTs often prove to be attacks that were planned over a long period of time and with considerable effort to target a single, carefully chosen victim. The normal objective of an APT attack is not financial gain, but instead to obtain information about the target, in some cases with the objective of sabotage.

In terms of technical differences, the lines between criminal activities and targeted attacks are becoming increasingly blurred. One indication of this is that *ransomware* attacks may now be preceded by weeks of propagation in internal networks (cf. *Emotet: New Quality of Advanced Attacks*, page 11), which is a methodology formerly only associated with APT attacks. As a result, an increasingly important criterion in identifying them is the fact that targeted attacks always have a strategic background. Any consideration of the security threat posed by APT attacks must therefore take this dimension into account, which is why 'strategic threat intelligence' is becoming the term of choice. This strategic perspective makes it easier to understand the reasons - relating to a particular industry sector, product or geographical location, for example - for which one's own organisation can become a potential target for APT attacks.

As of this writing, hundreds of APT collectives are active worldwide. In Germany, the activities of just over a dozen such groups were observed in the reporting period. These ranged from straightforward attack attempts and *phishing* emails to successfully compromised systems. Ministries involved in foreign policy work constituted the primary target of attacks on government networks in Germany. Embassies were also the focus of APT groups with interests in the respective countries represented. Other attacks or attempted attacks targeted international non-governmental organisations, as well as companies in the chemical, automotive and machinery manufacturing sectors. This highlights the fact that APT collectives are deployed in a targeted manner and adopt a strategic position that is aligned with certain regions of the world or sectors of industry.

In the current reporting period, such activity was particularly intense in Southeast Asia, Central Asia and the Middle East. In these regions, a significant increase can be observed in the telecommunications sector. This sector offers attackers the chance to harvest personal data on individuals, as well as trade secrets or insider information about technologies. Many of the published reports also document the fact that spy programs are being used by many countries to keep track of critics in their own populations.

As before, most APT activities are designed to procure information from government agencies, military organisations, commercial enterprises or dissidents. Sabotage attacks are considerably rarer and restricted to individual sectors and regions. Cases have, however, come to light in which information has been gathered that would then be appropriate for use in a sabotage attack.

In technical terms, attack methods are becoming increasingly diversified. Although earlier APT attacks were launched from email attachments or links to web pages containing malicious code, attackers are now varying their *attack vectors*. These include compromising legitimate software products, exploiting vulnerabilities in remote management services and using stolen login credentials. An increasing number of APT collectives are also utilising input supplier infrastructure and access data to compromise their actual intended targets. The first step in this process is to attack the poorly protected network of a supplier company. The data and access accounts obtained are then used to penetrate the network owned by the actual attack target. As a result of this technique, even companies that actually maintain a high level of IT security and a professionally staffed security team can be compromised if they trust a supplier with poor security and integrate this supplier into their own network.

Several APT groups are also now developing and testing methods designed to compromise corporate routers. This is alarming because so far, only a few security products have existed for these routers that enable monitoring or are even capable of detecting attacks.

While most APT groups use publicly available tools such as Cobalt Strike or Empire, whose structures and specifications are well known, many collectives are now starting to develop their own additional tools. In particular, much effort is being invested in completing additional interim steps during the initial attack phase. Malware programs are not transferred to the target system directly but brought in gradually as separate payloads - in some cases after the attackers have verified that the compromised system is indeed a target of interest. This degree of effort highlights the attacker's familiarity with the detection methods and processes utilised by security teams, and how they are attempting to conceal their own malware from such analyses.

1.5 Distributed Denial of Service

A distributed denial of service attack (*DDoS attack*) is an attack that aims to overload an internet service. If a website such as an online shop or an internet platform is no longer reachable, network services go down or critical business processes cannot be accessed because they are overloaded, for example, a *DDoS attack* may well be the cause. *DDoS attacks* are typically used to damage specific targets, extort money from victims or attract attention to the attacker's cause - such as a specific set of political demands. They may also be used to conceal other kinds of attacks or even enable them in the first place. *DDoS attacks* are typically coordinated attacks involving a large number of computers, including servers in some cases (cf. chapter *Botnets*, page 10). With *DDoS attacks* having been observed for over 20 years, *DDoS* can be said to have celebrated a milestone birthday in the reporting period: the first DDoS is thought to have been an attack on the University of Minnesota on 22 July 1999 (cf. *Bibliography*[12]: www.link11.com).

The effects of *DDoS attacks* can be very serious indeed. They can entail both major economic losses for the institutions affected and considerable damage to their public image. For the world of digital business, they are one of the most significant cyber threats of all because they directly affect the availability of the services that these businesses offer.

As in the previous reporting period, the circumstances surrounding *DDoS attacks* were characterised by multiple developments, some of which had common elements. Cyber criminals continued to hone their attacks by developing and utilising new *attack vectors*. Current examples of this include WS-Discovery, the Apple Remote Management Service and TCP amplification. For the less technically savvy attacker, so-called *DDoS* 'booter services' also continue to be offered. These services make it increasingly simple for attackers who have neither technical expertise nor a criminal record (e.g. school pupils; cf. *Bibliography*[13] www.cambridgeuniversity.uk) to carry out attacks with the potential to cause significant damage (cf. *Bibliography*[1]: www.bsi.bund.de).

During the reporting period, an increased level of *DDoS* activity was also observed on certain key dates in the e-commerce calendar (the run-up to the Christmas season, Black Friday, Cyber Monday) and in the context of gaming.

In contrast, one new development observed in the reporting period was the perpetration of attacks of a quality that far exceeded the expected level of development by specialising in certain target groups. Unlike in earlier, 'scattergun'-style attempts, these technically sophisticated attacks are increasingly using smart, efficient strategies. Such attacks can even outwit the kinds of protective measures considered effective to date, and therefore make it necessary to develop an essentially new set of concepts and countermeasures.

There have been several reports of actively managed attacks in which the attacker responds to the victim's countermeasures to maintain the virulence of the attack despite this resistance. To do so, the attacker utilises information about the course of the attack, which can be taken from public sources (for example). One example of this is an attack launched against a major online bank with around four million customers in January 2020, which continued for several days. During this attack, the perpetrators used the public website allestörungen.de to gain information about the progress and effect of the attack on the victim. This website collects status and fault reports from customers, for example, and therefore acts as a kind of early warning system for service interruptions or disruptions affecting service providers in several industries (including banking, e-commerce and *ISP*s). As a result, the attackers were able to draw on the information they needed to respond effectively to the countermeasures that had been put in place. In an attack launched against a South African *internet service provider*, the perpetrators also monitored countermeasures in order to adapt their attack strategy. Since no protective measures had been put in place to handle these new attacks, the *ISP* remained offline.

During the second half of 2019, the increased use of another strategy was also observed, which has been known of since the end of 2017 and is referred to as 'carpet bombing' (cf. *Bibliography*[14]: www.datensicherheit.de, cf. *Bibliography*[12]: www.link11.com). With this approach, attackers bypass the conventional *DDoS* safeguards at the network boundary by targeting a large number of IP addresses within the network. The volume of data the attack uses per IP address is kept small enough so that it typically remains below the threshold of detection for anti-*DDoS* solutions. As a result, the attack is not detected and no defence is mounted. While the bandwidth used by the attack, expressed as a sum total of these individual attacks, equals the several dozen or hundred Gbps achieved by a large-scale *DDoS* attack, the attack remains undetected. This type of attack is especially dangerous for *internet service providers* and was exploited during the two-day attack on the South African *ISP* mentioned above for this very reason.

Though not directly connected to those described above, the new kinds of attacks also include 'multi-vector' attacks, which were first discussed in the 2019 State of IT Security report. These remained a popular kind of attack, accounting for 65 percent of DDoS attacks in the fourth quarter of 2019 (cf. *Bibliography*[12]: www.link11.com). Unlike conventional *DDoS attacks*, multi-vector attacks are characterised by their targeted combination of the *attack vectors* they utilise. This presents a considerably more complex threat to the victim, who requires a similarly advanced level of expertise in the various *DDoS* attack types to mount an effective defence. Multi-vector attacks also have the potential to be particularly effective against existing protective measures. The response times of static protective solutions that are based on static thresholds prove to be too slow and too inefficient in the face of attacks capable of changing vectors from minute to minute.

All things considered, the trend from the previous reporting period towards advanced *DDoS attacks* has further solidified, even if advanced attacks - with the exception of the already widespread multi-vector attacks - currently make up a comparatively low proportion of the total attack volume. Comparable lessons learned from other threats (such as malware) make it seem plausible that this trend will continue and advanced DDoS attacks will proliferate further in the future.

This trend towards advanced kinds of attacks means that defensive solutions will need to adapt accordingly. The effectiveness of static safeguards is limited in this context, however. In order to counter these kinds of advanced attacks on their own terms, a more dynamic approach to countermeasures is necessary - the automatic derivation of filter definitions from attack patterns, for example. Qualified *DDoS* mitigation service providers (as defined by BSIG section 3(3)) fulfil this requirement. A list of qualified service providers, including the selection criteria used for qualification, is available from www.bsi.bund.de (cf. *Bibliography*[15]: www.bsi.bund.de).

1.6 Attacks in the Context of Cryptography

Cryptographic mechanisms are important basic components for the implementation of security functions in IT products. State-of-the-art crypto-algorithms provide in principle excellent security guarantees. In Technical Guideline TR-02102, the BSI recommends a series of cryptographic algorithms and protocols that are generally regarded as secure based on thorough mathematical cryptanalysis.

Before a cryptographic scheme can be implemented, it needs to be designed and planned mathematically on paper. The security of such a cryptographic system is generally linked to certain conditions. For example, keys must be unpredictable and must not leak through intermediate results of computations or through side channels. If a practical implementation of a cryptosystem does not meet all these requirements, additional security measures must be taken. The following aspects can contribute to a cryptosystem failing to fulfil its intended purpose in practice:

- Weaknesses in cryptographic mechanisms (cf. box *Collision Attacks Against SHA-1*, page 31)
- Implementation errors
- Insufficiently mitigated side channels
- Hardware vulnerabilities (cf. chapter *Vulnerabilities in Hardware Products*, page 26)
- Weak random numbers, which can lead to predictable and therefore less secure cryptographic keys

In a typical application scenario, such as communication via an insecure network with protected endpoints, IT products operate in a secure environment and communicate with other devices over an open network. Various cryptographic protocols are available for confidential and integrity-protected communication that are commonly regarded as secure against an attacker with network access, i.e. an attacker can neither learn the secret keys nor decrypt or manipulate messages unnoticed. For cryptographic protocols to be effective, it is on the one hand imperative that the implementation is correct. On the other hand, it must be prevented that device characteristics observable at the network interface (e.g. error messages, response time) leaks information about processed secrets (see box *Runtime Attacks Against ECDSA*, page 32).

If cryptosystems need to resist attackers with physical access to the device, other information such as power consumption or electromagnetic radiation of the devices must be taken into account in addition to the runtime, because these can be used for *side-channel attacks*. Intensive research in this field has produced new *attack vectors* in addition to countermeasures. Artificial intelligence (AI) also plays an important role in cryptography, namely in side-channel analysis, i.e. the analysis of vulnerability to side-channel attacks, and as a tool in mathematical cryptanalysis (cf. chapter *Cryptography*, page 75).

An essential precondition for the secure use of cryptography is the generation of random numbers that meet certain quality criteria. Random numbers are required in cryptography, among other things, for generating cryptographic keys. As the name suggests, they must not

be predictable. The stronger the random numbers are, the harder it is to exploit them for attacks. In order to prevent this kind of attacks, the BSI defines functionality classes of random number generators for different purposes in the Application Notes and Interpretations of Schemes AIS 20 and AIS 31. Furthermore, the BSI has actively participated in the development of the standard ISO/IEC 20543:2019 for the evaluation of random number generators, which came into force in October 2019.

It should be positively emphasized that many products now have a physical random number generator certified according to the German Common Criteria scheme (cf. Chapter *Certification*, page. 16). Due to the increasingly efficient utilisation of semiconductor products and the ever-higher performance with low power consumption, newer products also have integrated cryptographic post-processing of the random numbers. This reduces the already very low probability of exploiting the already tiny remaining weaknesses of physical noise sources, and thereby prevents such attacks entirely.

However, the security guarantees of cryptographic mechanisms used today will no longer apply once a sufficiently powerful quantum computer is available. The chapter on cryptography (see page 75) shows ways of countering this threat and presents BSI activities in this area.

Collision Attacks Against the SHA-1 Hash Function

Cryptographic hash functions map messages of arbitrary length to hash values of fixed length and are used, among other things, for integrity protection. An important security feature of a cryptographic hash function is collision resistance. This means that is in practice impossible to find a collision, i.e. two different messages with identical hash values.

The collision resistance of the widely used hash function SHA-1 (Secure Hash Algorithm 1) was already theoretically defeated in 2005 by the researchers Xiaoyun Wang, Yiqun Lisa Yin and Hongbo Yu (X. Wang, Y.L. Yin, H. Yu: Finding Collisions in the Full SHA-1). A research team led by Marc Stevens were the first to calculate a collision in practice and published it in February 2017 (cf. *Bibliography*[16]: https://shattered.io). In the current reporting period, the known collision attacks against SHA-1 saw further improvement. In January 2020, the researchers Gaëtan Leurent and Thomas Peyrin published the first so-called chosen-prefix collision of SHA-1 (cf. *Bibliography*[17]: https://sha-mbles.github.io). The messages of a chosen-prefix collision no longer contain an identical, pre-selected initial segment as before, but two different pre-selected initial segments. This higher flexibility enables new attack scenarios.

Furthermore, the researchers were able to reduce the computing effort for collision attacks against SHA-1 roughly ten-fold. The researchers also estimate that the cost of generating a collision or chosen-prefix collision of SHA-1 with rented hardware has dropped significantly.

The BSI has not recommended the hash function SHA-1 for general use for many years. However, there are no objections to its use in constructions that do not require collision resistance for security (e.g. in one of the best known and most important use cases of SHA-1, the Hash-based Message Authentication Code, or HMAC for short) according to the current state of knowledge. Nevertheless, the BSI recommends using a hash function of the SHA-2 or SHA-3 family as a basic security measure in such applications as well.

Runtime Attacks Against the ECDSA Signature Scheme

In a runtime attack, the attacker uses the computing time of a cryptographic algorithm as side-channel information. In unprotected implementations, this runtime leaks information about processed secrets (e.g. secret keys).

In the reporting period, two research teams conducted investigations into runtime attacks against the ECDSA (Elliptic Curve Digital Signature Algorithm) signature scheme. These have been published under the names 'Minerva' (cf. *Bibliography*[18]: https://minerva.crocs.fi.muni.cz) and 'TPM-Fail' (cf. *Bibliography*[19]: https://tpm.fail). While Minerva looked at ECDSA implementations for smartcards and software crypto libraries, TPM-Fail investigated computer cryptoprocessors known as Trusted Platform Modules (TPMs).

The basic idea of runtime attacks are known since 1999. The first step is to initiate the generation of multiple signatures. The runtimes required to generate each of these signatures are measured. Then, a mathematical method combines these individual pieces of information in such a way that it is possible to calculate the secret signature key. Finally, this key enables an attacker to forge a victim's signature.

Various countermeasures are known to effectively prevent runtime attacks against ECDSA implementations. As part of AIS 46, BSI released guidelines for the evaluation and certification of implementations regarding their resistance to *side-channel attacks*.

1.7 Hybrid Threats

Hybrid threats and defending against them continue to gain relevance in both a national and international context. State and non-state actors alike are increasingly resorting to hybrid methods and approaches to bring a destabilising effect to bear on nations.

They typically involve a wide range of tools, such as cyber attack, covert military operations, economic pressure or disinformation, all of which can exert their effects across multiple domains while also benefiting mutually from one another. The intentions and initiators of such activities are often kept hidden to act below existing intervention options based on the rule of law.

As digitalisation continues worldwide, it is becoming an important catalyst for hybrid threats because it reveals potential vulnerabilities of nation states, the industry and civil society. The cyber dimension is therefore a key part of hybrid campaigns. Additionally, it is also playing a unique cross-sectional role because actions taken in other domains are often dependent on it. In a hybrid campaign, the physical (e.g. hardware and firmware), logical (e.g. virtualisation and operating systems) and informational (e.g. applications and data) layers of cyberspace can be utilised by an aggressor depending on the individual characteristics of the attack in question.

In the reporting period, the first few months of 2020 also saw actors exploit the COVID-19 pandemic to use disinformation - also a potential hybrid tool - to exert pressure on other nation states. It is assumed that the aim here was to exploit existing fears and insecurities within the population of the target state in order to use targeted disinformation to weaken the population's confidence in their national systems and democratic institutions.

To an increasing extent, this disinformation is being supported by technical resources that serve to manipulate authentic information. Examples of this include counterfeit photo, video and audio recordings, as well as attempts to falsely attribute information transmissions (such as an email or a post made on a social network) to a particular source. These kinds of technical tampering often leave behind a trail, and the forensic analysis of such trails can be supported by BSI given its technical expertise. The BSI also supports operators of critical infrastructures, helps with IT security in the context of elections, maintains a dialogue with social media platforms - for example through an initiative to develop security recommendations - and offers a number of services aimed at raising awareness of IT security issues in the general population.

1.8 Threats to Cyber Security from the COVID-19 Pandemic

Owing to the close-meshed global interdependencies in business, government and society, the COVID-19 pandemic has had far-reaching effects on almost every area of our lives. This also applies to the digital world, which now often plays a central role in providing the basic necessities of life to a country's citizens while also being an important tool for combating the pandemic itself. Digital systems not only ensure the essential transfer of research findings in the effort to combat the coronavirus; they safeguard the supply chains for vital goods and working environments for the vast majority of companies, as well. In light of these facts, a successful cyber attack could have devastating consequences for an organisation involved in managing COVID-19, for example - both for individual people and in terms of containing the pandemic and mitigating its overall impact on society.

Social engineering attacks exploiting the coronavirus pandemic

Social engineering attacks include attempts at fraud and manipulation that use premises based on unsupported facts or exploit human responses such as fear or a readiness to help to beguile their victims into acting against their own best interests. One example would be tricking a victim into clicking a link that installs malware (cf. *Theft and Misuse of Identity Data*, page 18). Perpetrators that utilise these kinds of methods typically respond quickly to topics that draw strong public interest in the media and adjust their attack campaigns accordingly. The BSI accordingly observed several campaigns during the COVID-19 pandemic that exploited the complex overall situation. These attacks have included *phishing* and malware campaigns, *CEO fraud*, and more straightforward scams utilising IT resources. Characterised as it is by fear, worry and uncertainty, the current mood in much of the population does make such attacks more likely to succeed, but unexpectedly large waves have not in fact occurred.

Difficult times for IT security

In normal circumstances, the IT security measures implemented within an organisation, the local availability of IT specialists and service providers and the presence of financial and infrastructural security safeguards provide for a multi-layered defence and response structure. However, since companies are now frequently being asked to relocate employees and business processes to home environments, there is the risk that IT security is being neglected in favour of a functional working-from-home setup. The necessary hygiene restrictions have also made it more difficult to ensure the availability and physical presence of IT specialists and IT security service providers.

'Going digital' increases exposure to attacks

From lockdowns and social distancing to the closure of schools and businesses, government policies designed to contain the coronavirus pandemic have led to far-reaching restrictions on day-to-day life. In many cases, digital solutions have been the method du jour for ensuring the maintenance of basic business processes and human social relationships. Working from home, virtual classrooms, online shopping and video chats with friends and relatives have resulted in an unparalleled wave of digitalisation in many areas of our lives. This sudden, widespread surge in the use of digitalisation products has given attackers a much broader range of targets for their criminal activities.

Use of insecure software and solutions with privacy problems

Almost overnight, communication platforms, *VPNs*, chat servers and video conferencing were set up for use in education, healthcare and government, as well as more generally for employees working from home. In personal environments, the well-known and familiar messenger apps and social networks were used more than ever before. For professional users, *VPN* and team solutions and other software for things like video conferencing were in great demand.

The need for evaluation

For security reasons, the use of a *VPN* solution to access work documents is to be preferred to other solutions, such as simply emailing files or using public cloud services. Even in a crisis, the need for careful consideration of security and privacy - as set out in the General Data Protection Regulation (GDPR), for example - should not be ignored. In cases where the applications themselves are based on *cloud* services, the possibility of setting up a data repository inside a private *cloud* for security reasons should be considered.

COVID-19 Rapid Relief Measures Misused by Cyber Criminals

Situation
Phishing campaigns attempting to exploit the COVID-19 relief funds rolled out at both the federal and state level in late March 2020 were observed almost immediately after the announcement of these measures. Here, fraudsters registered *phishing* domains and designed the corresponding websites to be virtually identical to the official assistance pages. These pages were then brought into circulation using a variety of methods, such as spam mail or the optimisation of search engine results. It can be assumed that the basic objective of these *phishing* attempts was to collect information on companies and private individuals experiencing financial problems. The attackers were then able to use these details to apply for payments in the victims' names from the official COVID-19 relief funds. This resulted in genuine applicants being refused their relief payments from those funds (at least temporarily) and caused considerable financial losses for the German Government. From a long-term perspective, the data gleaned during these *phishing* attacks may well be used in follow-up attacks on the original victims.

At the same time, these kinds of *phishing* attacks on COVID-19 relief funds were not restricted to Germany alone. Such attempts were also observed in other countries that had organised comparable types of emergency assistance programmes.

Response
To prevent cyber criminals from misusing the official COVID-19 relief fund pages with stolen identity data, some pages were temporarily taken offline, which meant that a number of payments to recipients were delayed. Once the affected systems had been audited and reworked, the application procedure was relaunched on the official websites and payment processes were restarted. The state police forces are investigating these cases.

Fraudulent websites identified in the course of these investigations have been taken offline. The BSI has provided support to government agencies in taking down fraudulent websites related to COVID-19. Both the BSI and official government announcements at the federal and state level have warned the public about this kind of fraud.

Recommendation
To guard against *phishing* campaigns and similar kinds of fraud, great care must be taken with emails, phone calls and web pages that request the disclosure of personal data. In cases of doubt, the authenticity of the sender of an email should be checked by telephone.

1.9 Summary and Assessment of the Threat Landscape

The state of IT security in Germany remained fraught during the reporting period. Attackers used malware for waves of cyber attacks on private individuals, companies, government agencies and other institutions, as well as for targeted attacks on carefully chosen victims. At the same time, the threat of data leaks took on a new dimension with the publication of millions of patient records on the internet. During the reporting period (and as discussed in previous chapters), a number of vulnerabilities - several of them critical - were discovered in software products that attackers were able to exploit for malware attacks or data theft. Attackers also made increasing use of the 'human factor' as a starting point for attacks that leverage social engineering to gain a point of entry for further incursions.

The section below provides an overview of some of the most notable examples from the reporting period:

- **A new wave of malware in autumn and winter: Emotet the dominant threat**
  The threat situation was dominated by the Emotet malware, which had already proven to be especially dangerous in the previous reporting period. Emotet enables a cascade of additional malware attacks that may culminate in targeted *ransomware* attacks

on handpicked and wealthy victims. The overall incidence of new malware variants in the autumn and winter was well above average (with as many as 470,000 being recorded on a day-to-day basis).

- **Cyber criminals using encrypted communication**
  Hypertext Transfer Protocol Secure (HTTPS) guarantees secure and encrypted data transmission on the web. In the reporting period, however, there was an increasing trend towards the use of HTTPS by cyber criminals. As a joint investigation conducted by the BSI and the Consumer Advice Centre for North Rhine-Westphalia discovered, more than half (60%) of the links in *phishing* emails now lead to HTTPS websites, which, in contrast to simple HTTP websites, appear secure and genuine while actually being used for fraudulent purposes.

- **Millions of patient records publicly available on the Internet**
  Reports of the theft of customer data were again observed regularly during the reporting period. Theft was not the only reason for such leaks, however. During the reporting period, databases holding highly sensitive clinical data were also found to be freely accessible online. Unlike actual data theft, these leaks were not the result of technically sophisticated attacks, but of inadequate protection or incorrect configuration. In Germany alone, around 15,000 data records from private citizens containing a total of several hundred million images were publicly available on the internet between July and September 2019.

- **Critical vulnerabilities in remote access services**
  Several critical vulnerabilities were discovered in the reporting period. The new vulnerabilities BlueKeep and DejaBlue in the Windows Remote Desktop Protocol have left many Windows systems - including Windows 10 - open to attack. They allow attackers to execute arbitrary code, including malware, on unpatched systems. The vulnerabilities also permit malware to propagate itself automatically and have therefore been described as 'worm-ready'. Microsoft has provided security updates for all the affected systems.

- **New APT collectives**
  In the context of *Advanced Persistent Threats* (APTs), more than a dozen groups were active in Germany during the reporting period. There are over a hundred such groups around the world. Meanwhile, more and more countries have publicly admitted to developing cyber capabilities, which means that the global number of active APT groups is likely to rise further. Unlike other kinds of attackers, APT collectives are uninterested in cyber criminality per se; instead, they pursue tactical and strategic goals such as espionage or sabotage.

- **Distributed denial of service (DDoS) attacks with intelligent strategies**
  DDoS attackers increasingly deployed technically advanced and strategically smart attacks in the reporting period. In particular, attackers were found to be utilising publicly available information - such as customer fault reports - in order to monitor their victims' countermeasures during attacks, which allowed them to adapt their strategies on the fly.

- **Social engineering attacks exploiting the COVID-19 pandemic**
  Cyber criminals specialising in online fraud typically respond quickly to socially relevant topics and trends in order to exploit these for their own campaigns. During the coronavirus pandemic, *phishing* campaigns, *CEO fraud* and straightforward IT-based scams were all observed in this context. In one example, fraudsters were able to exfiltrate emergency assistance funds by creating website mock-ups that were virtually indistinguishable from official pages. The corporate information entered by applicants on the fake websites was then used by the cyber criminals to impersonate them and misappropriate emergency assistance funds.

The State of Cyber Security in 2020

Action and Response

117.4 m new malware variants

2019: 114 m

average of **322,000** new **malware variants** every day

peaking at **470,000**

76% of mail received by all government NETWORKS WAS SPAM

▶ 2019: 69% ◀

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

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

419 **CI** notifications

▶ 2019: 252

▶ 2018: 145

52,000 WEBSITES containing malware programs were blocked by web filters protecting

35,000
mails containing malware were detected in German government networks on average every month

109,000
subscribers to Bürger-CERT
- 2019: 105.000
- 2018: 100.000

around **100**
products and sites were certified by the BSI according to the

over **4,400**
members in the Alliance for Cyber Security
- 2019: 3,700
- 2018: 2,700

over **1,700**
registered **CI** facilities

just under **7m**
reports of MALWARE INFECTIONS
forwarded by the BSI to German network operators

2 Insights and Services for Specific Target Groups

2 Insights and Services for Specific Target Groups

Information security issues are of considerable importance in all areas of our society. This in turn explains the sheer variety of activities dealt with by the BSI. The BSI provides information and advice to private citizens, businesses and the government, maintains an ongoing dialogue with researchers, and promotes information security as a topic within society as a whole. The extensive datasets that the BSI thereby acquires on the state of IT security in Germany are then analysed by its in-house experts in a range of technical disciplines. The results of these analyses are used to develop safeguards and solutions to all threat areas in this digital age - from consumer products and critical public-sector infrastructure to the government's own networks. The challenges the BSI faces are specific to each target group, and each one requires an individual response.

2.1 Civil Society

From online shopping to *wearables*[4], new payment and ID schemes, the digital transition is actively shaping our everyday lives. However, this degree of digitalisation is not without its risks and dangers. According to the 2020 Digital Barometer[5], one in four people have already been a victim of cyber crime. The BSI is therefore taking a number of steps to ensure that consumers stay safe and secure as they interact with the digital world. These include information services, events and warnings about critical products and services, as well as the general dialogue about information security that the BSI maintains with society as a whole. In the latter instance, the BSI actively engages with private citizens, researchers, government agencies and businesses alike to promote the development of digital consumer protection.

2.1.1 Insights from Surveys Aimed at Assessing the Threat Landscape in Civil Society

To be able to make statements about the threat landscape for IT security in society as a whole, the BSI cooperates with a variety of government agencies, institutions and organisations. Surveys and studies are carried out as part of these efforts, and their results provide a clear picture of the current situation.

Results and insights from the 2020 Digital Barometer
The BSI cooperates with the Police Crime Prevention of the Federal States and the Federal Government (ProPK) to ensure that citizens are comprehensively informed about online risks and the ways in which these risks can be minimised. This work is based on the Digital Barometer, a representative online survey conducted jointly by the two organisations. The survey collects data on the importance of online security for private users, and on the extent to which they protect themselves from vulnerabilities, risks and general hazards in the digital world.

One in four a victim
The general rate of cyber crime affecting citizens remains constant, with one in four respondents having been a victim of cyber crime - 25 percent of them during the last 12 months. The most common kinds of fraud that affect victims occur in the context of online shopping (44%) and third-party access to online accounts (30%). Protective measures are still in need of improvement. While antivirus programs (57%) and secure passwords (48%) are widely used, their uptake is still well below the level actually required. In addition, only one in four respondents uses automatic updates, and only a third of them make use of *Two-Factor Authentication* (see chapter on *Two-Factor Authentication*, page 47).

Acting quickly on security recommendations pays off
Just over half of the survey respondents are familiar with the recent security recommendations on protecting themselves against cyber crime. In most cases, these recommendations are acted on if doing so is convenient at that particular moment (41%) or the person in question has just learned of a particular piece of advice (39%). The data shows that people who have already been a victim on multiple occasions tend to act on advice only when a problem has already arisen (33%), even though they were already aware of the recommendations.

Most respondents stated that they read up on internet security once in a while (37%), although one in four never does so. The respondents consider security in online banking (60%) and online shopping (40%) as especially important. Roughly a quarter of them follows security recommendations published by the BSI and is familiar with the 'BSI für Bürger' (27%) website.

A plea for orientation in an emergency
For victims of cyber crime, self-help was the most common strategy among the respondents (36%). This is in line with their interest in information: over half of the respondents were keen to see a checklist published

[4] Intelligent electronic devices that are worn on the body, such as fitness-tracking armbands, smart watches or smart glasses.
[5] A survey of private citizens on the topic of cyber security, conducted jointly by the BSI and the State and Federal Police Crime Prevention Commission.

for use in an emergency. The respondents would also like to see more advice published in the future about identifying online crime (58%) and the actions that people can take as victims (46%). ProPK and BSI have already responded to these requests and created a series of checklists that can be downloaded from the respective websites (cf. *Bibliography*[20]: www.bsi-fuer-buerger.de). More checklists are being added over time.

Results and insights from a project to develop protective measures for online accounts

The development of effective protective measures for private citizens' online accounts is the focus of a joint project that the BSI launched with the German Federal Chancellery in July 2019. The aim of the first phase of this project was to obtain insights about password handling, barriers to action and risk awareness, and to identify the communication channels that private users would prefer to use to find out more about these topics.

Following ten group discussions involving a total of 100 participants (who were split into five age groups and stratified by gender), the project team garnered its first insights and starting points for these topic areas. These were included in a questionnaire for a representative online survey (n = 995, 16 years and older; survey dates: 26 October to 3 November 2019). The insights presented below on the protective measures applicable to private users' online accounts are based on these two surveys.

Risk awareness

On average, the respondents consider the risk of cyber criminals acquiring passwords to be moderately high (average = 2.9 on a scale ranging from 1 = very low to 5 = very high). The respondents also consider the theft of data from companies the route that hackers are most likely to use to obtain their personal passwords (average = 3.3 on a scale from 1 = very unlikely to 5 = very likely). The respondents tend to doubt that they themselves can adequately protect their passwords from hackers. At the same time, they are also unlikely to know when a password can no longer be cracked by a hacker.

Handling of passwords and available technology

The sheer volume of passwords that now need to be readily available in a variety of contexts both inside and outside the home is a challenge for most respondents. Around four-fifths of them (78%) make use of up to 20 online accounts that need to be protected with a password. Faced with this challenge, three quarters of the respondents (74%) simply remember the passwords themselves. Around a third (34%) note down their passwords on paper, while 15 percent store them in a password manager (more than one option could be chosen).

Two-thirds of the respondents (67%) stated that they choose completely different passwords each time. While 10 percent of the respondents use a personal rule for generating their passwords, around 6 percent of them come up with a random sentence and create a password from the words' initial letters.

Although 39 percent of the respondents are familiar with password managers, just under a third of them (27%) uses these kinds of technical tools to generate strong passwords and log into online accounts. The main reason why this kind of software is not used more has to do with related concerns (67%). One particular worry is that a hacker could gain access to all of their passwords in one fell swoop (78%), while many other respondents are sceptical about the integrity of the program developers themselves (58%; more than one option could be chosen).

A need for information

Two-thirds of the respondents would like more advice about how to protect themselves from data theft (66%). The kind of advice sought mostly concerns practical tips on issues such as ensuring secure passwords for a large number of online accounts (59%), followed by an interest in recommendations on suitable software for protecting personal online accounts (52%) and information about the advantages and disadvantages of password managers (49%; more than one option could be chosen).

A detailed interim report that provides further details about the surveys and their results has been published on www.bundesregierung.de (cf. *Bibliography*[21]: www.bundesregierung.de).

2.1.2 Digital Consumer Protection

The numerous cases of identity theft in the current reporting period are just one indication of the persistent threats and risks we as consumers are exposed to by the increasingly digital dimension of our day-to-day lives. Thanks to the activities of the BSI, private citizens are more aware of these cyber threats in the online world, which in turn increases the digital resilience of German society as a whole. In its activities on behalf consumers, the BSI focuses on enhancing their risk awareness, improving their judgement and increasing their knowledge of available solutions.

Promoting digital consumer protection

The BSI has stepped up its work in digital consumer protection by setting up a dedicated internal department at its new premises in Freital. The experts assigned to this new unit will engage in activities that include exploring how to design government cyber security policies to be more consumer-friendly, safeguarding the security of consumer products and services and taking a service-based approach to handling cyber security issues that are of interest to consumers.

Partnerships for new perspectives

Government, business and civil society must all work together to ensure an effective approach to consumer protection. In one such initiative, the BSI has signed a memorandum of understanding to strengthen existing partnerships with the Consumer Advice Centre in North Rhine-Westphalia in 2017 and the Federal Association of Consumer Advice Centres in 2020. This cooperative approach also includes maintaining a dialogue with researchers to incorporate viewpoints from a wide range of disciplines into the BSI's work and collaborate on innovative solution strategies. In September 2019, the BSI joined forces with the Consumer Research Network to host an interdisciplinary consumer research forum on the topic of *digital nudging*. During this event, a number of insights from behavioural economics were applied to issues relating to information security. Discussions during the event focused on the common goal of strengthening digital consumer protection in Germany.

2.1.3 The IT Security Mark – Reassurance for Consumers

On the basis of the 2016 Cyber Security Strategy for Germany and the German IT Security Act 2.0 (a draft of which is currently in deliberation), the BSI is working with the Federal Ministry of the Interior, Building and Community (BMI) on plans to introduce a labelling system for consumer products.

The IT Security Mark is intended to raise awareness among consumers and therefore result in an improved level of education about IT security matters in the general population. One aspect of the mark is to present clear details of product-specific features relating to information security. This is intended to give consumers the information they need to assess the security characteristics of products and services before purchasing them or subscribing to them. Requirements documents should also be explained clearly and intelligibly as part of the range of information services offered in the context of the IT Security Mark. In this way, the influence of IT security features on purchase decisions made by consumers should help to bring about a significant increase in the level of security offered by products in the consumer segment.

The IT Security Mark will also provide manufacturers of consumer-grade products for the Internet of Things (IoT) with a useful instrument for highlighting the various kinds of security features offered by their products, while simultaneously improving transparency in terms of the level of information security offered by products bearing this mark that are intended for consumer use. In addition, the IT Security Mark will be linked to a dynamic range of information services for consumers that not only guarantee full disclosure of product security characteristics, but also address any current security problems of interest while providing details of the corresponding solutions as recommended to users by the product manufacturers.

The IT Security Mark will be issued to IoT products that exhibit the security characteristics required by the latest technical standards in the respective product category. The BSI will work with manufacturers to establish these technical standards in requirements documents for specific product categories. They may include the BSI's own technical guidelines or requirements documents recognised by the BSI (e.g. DIN standards, VDE[6] technical rules or other industry-specific standards). According to current plans, manufacturers will need to submit a declaration confirming their compliance with these product-specific requirements. The requirements documents should also include test specifications that manufacturers are required to follow. The results of these tests must be documented, and the records must be submitted to the BSI.

In particular, the requirements documents should promote and establish *security by design* and *security by default* as parts of the product development process while also guaranteeing product compliance with general information security goals.

By working towards objectives in relation to both manufacturers and consumers, the IT Security Mark is intended to make an essential contribution to digital consumer protection. The mark will seek to provide manufacturers with a framework for implementing security characteristics in their products and make the details of these features clearly intelligible to consumers. Manufacturers will also be provided with support to ensure the *resilience* of their products throughout their useful life. A key aspect of this process is the immediate resolution of any critical vulnerabilities that might occur.

The first product category to be issued with the IT Security Mark will be broadband routers. The BSI published a

[6] German Association for Electrical, Electronic & Information Technologies (Verband der Elektrotechnik Elektronik Informationstechnik, VDE)

technical guideline for these products last year. The related test specification, which must be used to prove that the requirements have been met, will also be published shortly.

2.1.4 Dialogue for Cyber Security in Civil Society

Maintaining a dialogue with all areas of society is a key instrument that the BSI uses to promote the discussion of different perspectives on information security and thereby raise the profile of the topic in society as a whole. This approach breaks down the walls between various interest groups and facilitates a general discussion among all societal actors on the topic of designing a secure 'information society'. In this process, the BSI seeks to strengthen its dialogue with organised civil society in particular in order to obtain input it can then apply to its own work. The term 'organised civil society' is used to collectively describe areas of society apart from the government, the industry and the private sector. It encompasses the sum total of community engagement activities - whether in the form of clubs, associations or other kinds of initiatives and movements - and is characterised by the fact that its activities are neither profit-oriented nor dependent on party political interests.

On the basis of a participatory multi-stakeholder approach that includes actors from the areas of organised civil society, research, business, government, media and the arts, the 'Establishing a Community Dialogue' project, which was launched back in 2018, was extended into the reporting period and has since been completed. Up until the end of 2019, a core group of 15 specialists drawn from the areas and sectors mentioned above worked together in a range of workshops and sessions on topics such as the establishment of a dialogue within the community.

The participants in this dialogue have prepared a model (cf. figure 5) that demonstrates how the multi-stakeholder dialogue initiated by the BSI can be deepened and consolidated in the future. This model, which is based on participatory elements, includes the annual Think Tank Workshop as its substantive node. In the Think Tank Workshop, participants can themselves recommend topics for discussion, which are then worked on in participant groupings known as 'work streams' for up to nine months using agile methods.

Other key tasks that were focused on during the project included the identification of relevant actors in civil society who work in cyber security; their primary activities, objectives and networking structures; and the launch of an event intended to bring such actors together with others from the field of knowledge transfer.

Further details of the project and its results have been published at: bsi.bund.de/gesellschaftlicherDialog (cf. *Bibliography*[22]: www.bsi.bund.de/gesellschaftlicherDialog).

2.1.5 Educating and Raising Awareness Among Citizens

As criminals increasingly use social engineering techniques to exploit the 'human factor' as a point of entry for their attacks (cf. chapter *Summary and Assessment of the Threat Landscape*, page 34), the BSI has had to take steps to raise awareness of this trend among citizens. To achieve this, the BSI offers a broad-based portfolio of information and consulting services for private users entitled 'BSI für Bürger'. The focal point of this range of services is the www.bsi-fuer-buerger.de website (cf. *Bibliography*[23]: www.bsi-fuer-buerger.de), which publishes

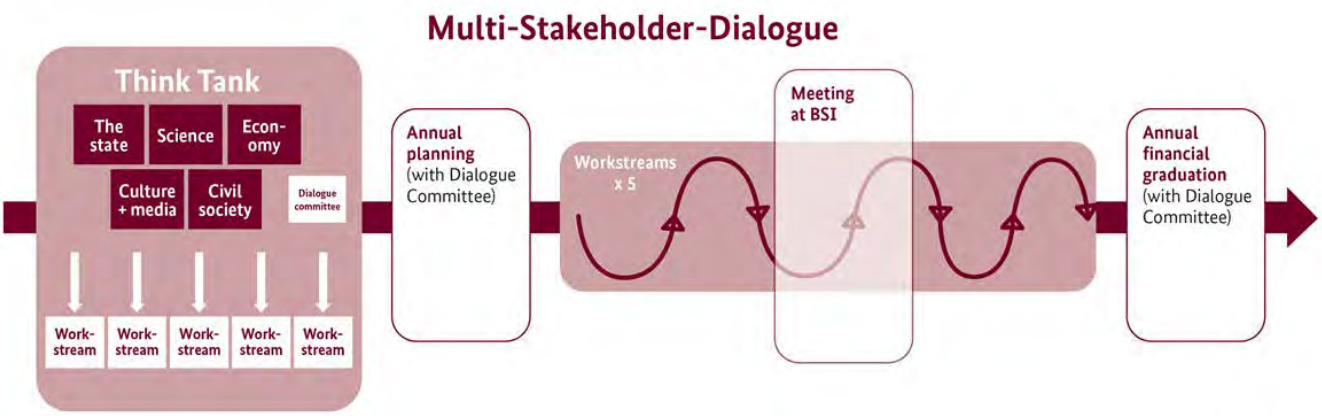


Figure 5 Dialogue process as an annual cycle. Source: BSI

information about the risks and protective measures relevant to the many ways in which the internet can be used. The primary focus is on recommendations on secure and self-determined conduct in the digital sphere. Current incidents are responded to promptly, including in the form of advice on how to respond to serious vulnerabilities or waves of malware. The topics are often complex and are presented in form of checklists, informative graphics and interactive quizzes in a way than can easily be understood. Expert interviews, animated explainers and podcasts are also used to make issues clearer.

BSI's free 'Bürger-CERT' warning and information service issues technical warnings and also includes the fortnightly newsletter 'Stay secure · Stay informed', which discusses vulnerabilities while offering appropriate help and advice. Around 109,000 people are currently subscribed to this service.

Meanwhile, a five-part brochure series covers the topics of basic digital protection while offering practical tips on browsing, staying secure on mobile devices, social media, the IoT and *cloud computing*. These brochures can be downloaded from the online media library and free print versions can also be ordered from the website. Since summer 2019, the printed materials have included a colouring and puzzle book that is specially designed for tech-savvy kids.

To support its presence on the web, the BSI reaches out to citizens through its Facebook and YouTube profiles, as well. A service centre also handles user enquiries on the topics of IT and internet security. It can be reached by phone at 0800 2741000 or by email at mail@bsi-fuer-buerger.de.

The Federal Ministry of the Interior, Building and Community (BMI) and the BSI are also planning a joint public awareness campaign on the topic of IT security for consumers, which is scheduled to start in early 2021. The BMI and the BSI will use the campaign to raise consumers' awareness while improving their judgement and solution skills. The campaign will also address specific topic areas where citizens typically require additional information and guidance according to the surveys conducted by the BSI.

Partnerships

To leverage synergy effects, 'BSI für Bürger' has joined forces with a large number of organisations and initiatives that also work in the field of cyber security. One example of this is its close collaboration with consumer advice centres, which has resulted in the joint communication of urgent warnings and the video series 'Cyber Security to the Max', where specialists from the Consumer Advice Centre in North Rhine-Westphalia and the BSI discuss issues relating to smartphone security. Following the principle of helping users to help themselves, ProPK and the BSI responded to the results of the 2019 Digital Barometer by publishing a series of checklists designed specifically for victims of cyber crime. *Phishing*, online banking fraud and malware infections are some of the topics the series has covered so far. Together with the 'Deutschland sicher im Netz' ('Germany safe online', DsiN) association, the handbook 'Cyberfibel' was also produced to provide orientation for key users and educators. In addition, the BSI has partnered with the German National Association of Senior Citizens' Organisations (BAGSO) on a number of initial joint activities. This approach is an example of the BSI's adaptation of its educational and awareness activities to specific target groups.

European Cyber Security Month

The BSI once again participated in the European Cyber Security Month (ECSM) as a national coordinator. The ECSM aims to cyber security into the focus of private citizens, companies and organisations and to draw attention to the importance of acting responsibly when engaging in online activities. With 183 initiatives and events organised by 123 partners, this campaign made it possible to present the importance of cyber security in Germany to a wider public. The participating partners included businesses, government ministries and agencies, chambers of industry and commerce, business associations, colleges and universities, and cybersecurity initiatives cooperating as members of the Alliance for Cyber Security (ACS). In Germany, ECSM got officially under way as part of the 29th Cyber Security Day, with this year's event ('Networks Protect Networks') attended by 300 representatives from government, business and society.

'BSI für Bürger' also participated with its own initiatives: on its website, Facebook and Twitter, the main focus was on helping users to help themselves in response to online threats.

2.1.6 Security of Wearables, Smart Homes and the Internet of Things

Wearables are intelligent electronic devices worn on the body that are now an essential part of day-to-day life for a great many people. Fitness trackers in particular are very popular. While wristwatches once only displayed the time or the current date, modern smart watches can help out with many everyday activities, from reading or writing messages to maintaining or improving personal

levels of fitness and helping their wearers to find their way around in unfamiliar surroundings. In a nutshell, smart watches offer an array of useful features and can even extend smartphone functionality to one's wrist.

Smart watches with GPS tracking are a particularly popular means of keeping tabs on children or other individuals who may need urgent assistance. However, the combination of an always-on internet connection and GPS tracking can also be exploited for criminal purposes. As one example, critical vulnerabilities in smart watches that infringe on the privacy of their wearers have been the subject of recent media coverage.

In the case of one smart watch intended for children, a security researcher discovered serious security problems and took the step of informing both the BSI's *Computer Emergency Response Team* (CERT) and the press at the end of 2019. The vulnerabilities were verified by an independent security audit and the manufacturer was asked to make a statement on the vulnerabilities identified in accordance with BSIG section 7a.

As a result of a failure to encrypt the communication between the smartphone app and the manufacturer's server, as well as deficiencies in the *authentication* procedure used, it was possible to eavesdrop on the data being transmitted and glean personal information about the wearer.

Moreover, by simply changing the device ID in an app configuration file stored on the smartphone, it was possible to connect the smartphone app to a smart watch owned by a different person. This gave the attacker access to the data stored on the other smart watch, including the individual's phone contacts and the person's current location. It also enabled the attacker to take over and control any number of user accounts without the legitimate account owners necessarily even noticing that this had happened. Device IDs were issued as sequential numbers, which made it easier to take over a user account because no *authentication* was required. Exploiting these vulnerabilities did not take any particular level of technical expertise.

After they were brought to the manufacturer's attention, the product was initially taken off the market.

The manufacturer then revised its smart watch and notified the BSI that the vulnerabilities had been patched. The watch was subjected to a further round of testing. These tests revealed that the known vulnerabilities had been closed with the aid of a software update for the smartphone app and a new interface on the manufacturer's server.

This was by no means an isolated incident; similar cases have occurred on multiple occasions in the past. As a preventive measure, security standards such as the European ETSI EN 303 645 standard can be followed during the design and development phase for smart products of this kind. For example, this standard requires the transfer of sensitive personal data (such as when communicating with external services) to be secured using state-of-the-art encryption. The standard also sets out basic protection requirements for consumer IoT devices - a category that includes smart watches. The BSI is involved in the development of this standard and its associated test specifications.

As a general point, it should be noted that smart watches and other devices in smart homes generate and store a great deal of personal and sensitive data. This data is an appealing target for attackers. Accordingly, ensuring that these devices have an adequate level of protection is sensible and important.

The BSI is working to establish an appropriate level of protection in the field of IT security for smart consumer products in particular. One of its most important goals in this work involves creating appropriate security standards and having manufacturers and developers follow them across the board. By ensuring that the principles of *security by design* and *security by default* are applied from the development phase throughout a product's lifecycle, significant security improvements can be made that greatly limit the attack options previously discussed. The BSI remains in constant dialogue with key stakeholders in this area while also offering an extensive range of online services designed to help ordinary citizens make conscious, self-determined use of smart products and services related to smart homes and the Internet of Things.

2.1.7 Security of Medical Devices

As the digital transition continues in the healthcare sector, it not only has important ramifications for the provision of healthcare itself, but also affects medical technology and the networking of medical devices in particular. Vulnerabilities in and on networked medical devices must be viewed as potential points of entry for criminal agents. Exploiting these vulnerabilities can affect the confidentiality, integrity and availability of data, with potentially adverse effects on the health of patients that could even prove fatal. Accordingly, the topic of cyber security in a medical device context is of interest not merely to manufacturers and operators, but also to patients themselves.

The BSI believes it has a responsibility to help shape and promote cyber security in the field of networked medical devices, which it does by engaging in publications, project

and committee work, and other activities. Since an investigation of this nature has not been conducted to date at the national or international level and the results may well prove to be of signal importance for this area of healthcare, the following section takes a look at the BSI project 'ManiMed' (manipulation of medical devices).

ManiMed (manipulation of medical devices)

Launched in early 2019, the ManiMed project aims to model cyber security threats to networked medical devices as realistically as possible by the end of the project (Q4/2020). Its other goals include promoting active cooperation among stakeholders (manufacturers, security researchers and government agencies) and ensuring the active and widespread use of the processes involved in a coordinated vulnerability disclosure (CVD). The idea is to raise awareness of vulnerabilities, make them easier to handle and thereby help to ensure that a high level of cyber security is maintained in the field of networked medical devices for the long term.

Two products from each of five separate device categories were selected for IT security testing. Ideally, these devices were to offer a large number of interfaces (thereby maximising their risk exposure) and to have been brought to market in Germany in just the last five years. Products from the following device categories were selected:

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

These products were subjected to in-depth IT security testing by *ERNW Research GmbH* and the vulnerabilities identified were communicated back to the manufacturer in the form of a detailed test report. As a last step, the reports were discussed in a confidential meeting attended by the respective manufacturer, security researchers and the BSI.

The manufacturer is now drawing up a risk assessment based on the test report received and initiating any internal processes that prove necessary. This project workflow is based on a CVD, whereby the IT vulnerabilities discovered are not published for an initial period (at least 90 days) so that the manufacturer has time to resolve them and develop corresponding security patches, which are then tested and rolled out. However, if the manufacturer is able to identify a risk to patients as part of its risk assessment of the vulnerabilities discovered, the German Federal Institute for Drugs and Medical Devices (BfArM) is brought in as the competent authority for medical device vigilance.

Apart from the high level of technical expertise involved, the ManiMed project's success fundamentally depends on communication among all the stakeholders and the guarantee of mutual confidentiality during the time they spend working together. The transparent and truthful handling of vulnerabilities and corresponding discussions in this context are necessary to build, maintain, and strengthen this trust over the long term. Vulnerabilities are published - and potentially presented at the relevant IT security conferences - only once they have been resolved in consultation with the manufacturer. Of a total of ten products that were investigated as part of this project, most were provided based on device loan agreement contracts with their various manufacturers. The BSI applauds the readiness of these manufacturers to have their products tested for cyber security readiness and to work together with security researchers and the BSI.

As the current set of (occasionally critical) findings have shown, vulnerabilities do exist that are not particularly uncommon. As a result, it will be possible to make concrete statements on the cyber security of medical devices at the end of the project. A final IT security report will present the findings of the ManiMed project using non-technical language. The project intends to improve the accuracy of assessments made about the threat landscape relating to the cyber security characteristics of networked medical devices. Ideally, the results produced by these tests will be incorporated into work on corresponding standards and will help the BSI to prepare its technical guideline documents and other publications.

2.1.8 Corona Warn App

As a result of the current pandemic situation that has been caused by the spread of the COVID-19 virus, Germany is only one of many countries around the world with an interest in a mobile application that can support contact tracing and help to break the chain of infection. To ensure the greatest possible level of acceptance within the population, such an app must not only fulfil its purpose in the sense of containing the pandemic, but must also meet stringent requirements in relation to privacy and data security. The German solution, dubbed the 'Corona Warn App' (CWA), was developed by Deutsche Telekom AG and SAP at the request of the German Government. The BSI has been closely involved in the development of the Corona Warn App, including by testing the app along with its backend infrastructure and providing advice on the drafting and implementation of the security model. The Corona Warn App has been available for Android and iOS devices since 16 June 2020.

The German Government elected to follow a fully documented procedure for the development of its app. Accordingly, the Corona Warn App is an open-source development project. This means that the code for the applications and the backend system is publicly available from a GitHub repository. The BSI has provided continuous support and testing for the app and corresponding backend system during the development phase - by conducting penetration tests on both aspects, for example. The BSI also acted in an advisory role during the preparation of the technical security model. All of the IT security vulnerabilities discovered by the BSI and its service providers were uploaded to GitHub by the BSI and patched by the development team. As a result of this close and constructive collaboration, the developers were able to continuously improve the overall system and deliver a final product that guarantees an optimum level of information security. The BSI will continue to provide IT security services for the CWA project.

2.1.9 eHealth and the Electronic Health Insurance Card

The electronic health insurance card (eGK) and the expansion of telematics infrastructure (TI), which seek to connect all the stakeholders within healthcare, offer good examples of how this increased level of networking - in connection with the continued advance of digitalisation - can contribute to improving efficiency in healthcare provision while achieving greater patient safety. The development and future deployment of new applications such as emergency data management (NFDM), the e-medication plan in conjunction with the safe use of medicines (AMTS) and the electronic patient record (ePA) are providing the users of this technical infrastructure with a wide range of new opportunities.

The BSI has drawn up a set of technical guidelines[7] based on specifications issued by the telematics firm Gesellschaft für Telematikanwendungen der Gesundheitskarte GmbH (gematik). These help to ensure that the existing connectors equipped with basic functionality for interfacing with the TI, which are certified by the BSI and currently deployed in doctors' practices and hospitals, can be safely extended to support the new functions. In the future, patients will be able to request that the data required for use in a medical emergency and e-medication plans be stored securely together with their electronic health insurance cards, where it will be ready when needed. In the context of e-medication plans, the attending doctor can compare new medicines prescribed to patients against their existing medication more easily than before, which will help identify any harmful interactions and thereby reduce potential risks.

Alongside its previous range of features, the eGK also offers patients with public health insurance the option of maintaining an electronic patient record. Once the consent and the approval of the insured party has been obtained, the attending doctor or hospital can access the respective record securely in order to view the patient's clinical data and amend it as necessary. With the help of a BSI-certified connector, medical interventions can also be coordinated efficiently between different healthcare facilities. Ideally, this will make it unnecessary for patients to undergo multiple medical examinations and deal with associated delays in their course of treatment.

Outside the context of a doctor's practice or a hospital, patients themselves will also have personal access to their own medical records, which they can browse through on their own computers or mobile devices with a software program approved by gematik.

2.1.10 Security of Payment Methods

Payment Service Directive 2 (PSD2), which has been valid since 13 January 2018 and has been transposed into local legislation in Germany by the Payment Services Oversight Act (ZAG), aims to increase security in payment transactions, strengthen consumer protection, promote innovation and increase competition in the market.

To flesh out the details of PSD2's requirements, the European Banking Authority worked with the European Central Bank (ECB) to draw up regulatory technical standards (RTS) on topics such as strong customer *authentication* in order to increase the level of security provided for digital financial transactions. Authentication solutions that are based on two independent elements from the categories of knowledge, possession or inherence (biometrics) are regarded as methods of strong customer authentication (SCA). These methods include authentication using a physical chip card (possession attribute) and a PIN (knowledge attribute). Combining systems such as chipTAN, text TAN and pushTAN (all possession attributes) with a person's online banking PIN (knowledge attribute) or a digital card (possession attribute) with a fingerprint (biometric attribute) also fulfils these requirements.

As a rule, the requirements of PSD2 relate only to authentication solutions for electronic payments that are initiated by customers themselves. These include transactions that are carried out using digital or physical cards, meaning not only cash machine withdrawals and payments at the point of sale, but e-commerce payments using things like credit cards or PayPal, as well. Direct debits and purchases on account are not covered by these requirements.

[7] TR 03154, TR 03155, TR 03157

As financial services undergo their own digital transition, this is leading to a fundamental change in payment procedures. Payments using mobile devices offer a good example here. As smartphones continue to grow more powerful and gain larger screens - along with an increasing number of connectivity options such as Near Field Communication (NFC), Beacon and Bluetooth Low Energy (BLE), as well as barcode and Quick Response code (QR code) scanners - user-friendliness is also improving. Meanwhile, mobile payment solutions themselves are becoming more feature-rich and simpler to use. Banks and payment service providers are increasingly offering banking apps to supplement their web-based online banking services. While some of these apps handle conventional bank business such as wire transfers or standing orders, they can also be used for point-of-sale and e-commerce payments.

At the same time, however, it is crucial that security remain the main priority and not be neglected in the name of usability. In cases where strong customer authentication is skipped in order to make transactions faster and easier for end users, this has a detrimental effect on security. As one example, the use of the 3-D Secure protocol for safeguarding online credit card payments is not yet mandatory for all kinds of online purchases. The matter is beyond the control of end users because online retailers decide how they will implement this authentication procedure. What users can do, however, is ensure that they only make purchases from online shops where credit card use is in fact secured by 3-D Secure.

Until fairly recently, the de facto standard for online banking involved entering a username followed by a four- to six-digit PIN for the initial login process, along with a TAN to approve each transaction. At the point of sale, payments have typically also been authorised by entering a PIN or providing a signature. Today, however, users can simply authorise payments with their mobile devices.

Users simply utilise the various unlock mechanisms - entering the device PIN or password, or making use of biometric procedures - to authorise their mobile device. The use of biometrics in particular, however, can lull the end user into a false sense of security. While biometric procedures are indeed suitable for identification and authorisation, the quality of the components built into a device, such as a fingerprint sensor or camera, plays a decisive role. To evaluate the quality of the sensors used and thereby improve the security of payment methods using mobile devices, the BSI has developed testing criteria for biometric authentication mechanisms. Since smartphones are devices that are not deployed in environments that can be effectively controlled, they are subject to particular risks that these testing criteria are designed to target.

Overall, these risks must be reduced to an acceptable level by security analyses and security appraisals that look at the overall architecture at hand. Insecure procedures must be detected by appropriate measures and also deactivated as necessary.

Essentially, it is important that users not be forced to use additional security methods but encouraged to adopt user-friendly and secure procedures. Further information on this subject, including on the security of payment methods both in e-commerce and at the point of sale, has been provided in the brochure 'Keeping E-Commerce Secure. An FAQ About Online Payment Methods'. However, choosing a secure online payment method is just one of the many decisions that need to be taken to improve one's personal security online.

2.1.11 Two-Factor Authentication

Even today, password entry is far and away the commonest form of authentication online. In this case, a single factor - knowledge of a password - is requested by the service in order to authenticate the user. Implementing passwords as an authentication mechanism is simple, but they have several disadvantages. First of all, only this single knowledge factor has to be known in order to break the authentication mechanism. Second, it takes a certain amount of effort to select a secure and individual password for each service, and then to memorise it or enter it into a password manager.

More and more services are now asking for a second factor in addition to a password for secure user identification. As one example, the service may request a second piece of knowledge in the form of a code sent to the user's smartphone. However, this approach only improves the level of security if the devices are actually physically separate and the factors cannot be attacked simultaneously. If a smartphone application were to use a password as the first factor, for example, and a code sent to the smartphone as a second factor, both of these factors could be intercepted by malware on the smartphone. The system is therefore insecure. Other usability problems can also arise, such as when the user switches to a different phone or changes their mobile phone number.

A better approach is to request two factors from different categories (possession, knowledge, biometrics) as part of *two-factor authentication*. Combining the strengths of these individual factors makes attacks much more difficult. In the process, biometric features should be used locally instead of being stored by the online service. One approach is to use unlocking the smartphone as one factor (possession) and then have the smartphone use cryptographic methods to authenticate itself to the online service.

The Fast Identity Online (FIDO) Alliance was formed in 2013 by a large and diverse group of government and industry stakeholders interested in developing open and licence-free industry standards for worldwide *authentication* online. FIDO has resulted in three standards being developed to date:

- The Universal Second Factor (U2F) fits seamlessly into existing web infrastructures in the form of a hardware token. Physical possession of this authenticator is proven after a password is successfully entered.
- The Universal Authentication Framework (UAF) permits password-less *authentication* by replacing the password with biometric procedures or a PIN used as part of secure *two-factor authentication*.
- The second release, FIDO 2.0, consists of the Web Authentication Standard (WebAuthn) from the World Wide Web Consortium (W3C) and various client-to-authenticator protocols (CTAPs) that a web browser uses to communicate with the FIDO token.

However, proof of the security of the FIDO authenticator used is necessary to ensure a secure implementation of the protocols within 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 published such a protection profile with an evaluation level for secure FIDO U2F tokens. It has since been used to successfully certify a FIDO U2F token developed by the BSI. Without testing and related security certification, there is a real risk of implementation errors being overseen (cf. chapter *Vulnerabilities in Hardware Products*, page 26). Certification according to the FIDO security standard will also be available shortly.

In addition, the BSI plans to publish the source code of the security-certified FIDO token in the near future as open-source so as to contribute further to the transparency and propagation of a secure U2F implementation. This open-source implementation can then be utilised by any interested developer as the basis for their own U2F implementation on JavaCard smartcards.

While the launch of the FIDO initiative was marked by many large corporations extending their services to offer the option of FIDO-based *authentication*, use of the FIDO token has since remained static and it has not yet managed to establish itself as a de facto standard.

2.1.12 Assessment of Electronic Identification Procedures

Online banking and shopping have been an indispensable part of everyday life for citizens in Germany for many years now. By the end of 2022, most of the services offered by local governments in Germany should also be available online. Common to all of these applications is the fact that they are based on a trusted system of mutual identification. If an attacker were to succeed in falsifying the identity of either the sender or the recipient, however, this could result in considerable financial losses or other repercussions. This kind of identity fraud has not only been suffered by private citizens; it has also caused serious problems in the public and private sector, such as in the case of fake websites set up to tap into the COVID-19 emergency assistance funds.

The BSI is working on a number of preventive strategies in order to minimise the risk of identity fraud for government, business and civil society. Apart from helping to design highly secure identification solutions such as the German online ID card service, the BSI has also prepared two technical guidelines that enable the systematic appraisal of a wide range of procedures for electronic identities and trust services for online processes, as well as their assignment to a specific level of assurance. Guideline BSI TR-03107-1 addresses assurance levels and mechanisms for electronic identities and trust services in e-government. This Guideline is supplemented by BSI TR-03147, which offers an approach to evaluating the assurance level of procedures used to check the identity of natural persons.

The BSI has now launched a project aimed at using these technical guidelines to evaluate the security of various electronic identification procedures from the private sector with an eye to their potential use in e-government. A differentiated grade is awarded by this evaluation based on the assurance levels of 'normal', 'substantial' and 'high' - which are defined in more detail in BSI TR-03107-1. During the reporting period the evaluation of two electronic identification procedures were started, one of them was concluded in the meantime. The BSI reported the results of these evaluations to the BMI, which, as the relevant authority for e-government, will render a final decision on approving these procedures for use.

Of particular interest here are electronic identification procedures capable of achieving at least the assurance level of 'substantial' as defined by BSI TR-03107-1. Both suitable procedures and established evaluation criteria are available for the cryptographic algorithms and protocols that are required. A more complex issue is assessing the level of assurance at potential interfaces to the analogue

world or in the case of media discontinuity. This is often the case during the initial identification or registration of individuals for electronic identification procedures. Along with procedures in which ID documents are still presented conventionally in person, video-based procedures are also frequently used in which individuals are filmed holding their ID documents. These recordings are then verified by the identification service provider. The BSI is currently working with the Federal Criminal Police Office to evaluate whether the video-based verification of ID documents can also achieve the assurance level of 'substantial'.

2.1.13 Smartphone-based Secure Electronic Identities

Much of contemporary life now takes place in the digital sphere. Many kinds of services are easily accessed with the aid of smartphones. In order to use many of today's online services, such as banking, shopping or social media, an electronic identity (eID) is necessary. To enable the secure storage of identities on smartphones and the phone-based use of services involving sensitive data, the BSI is working on user-friendly solutions to these questions as part of the publicly funded OPTIMOS 2.0 project.

The term 'eID' is itself highly generic and can represent a very wide range of online identities - ranging from the pseudonym by which someone may be known on an online forum to a profile on a social network, a customer account for an online shop or bank details used for online banking.

Each of these eIDs must be protected against misuse. This protection must also vary in strength depending on the type of electronic identity. While the entry of simple credentials (such as a username and password) is often all that is required, this kind of protection is not adequate for sensitive data. If a smartphone needs to handle bank business, for example, or the device actually authorises the holder to enter a company's premises, the corresponding eID needs stronger protection. The very highest level of security requirements does not need to be met for each and every use case, of course. However, users may rightly expect a level of protection that ensures their identity cannot simply be stolen or tampered with.

Protecting eIDs

As with any networked device, smartphones are continuously exposed to the risk of a cyber attack. Accordingly, particular requirements must be fulfilled in order to be sure that eIDs are being securely stored on the smartphone. A corresponding legal framework is provided by 'Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC' (known as the 'eIDAS Regulation') and its defined assurance levels.

The eIDAS Regulation distinguishes between three assurance levels: 'low', 'substantial' and 'high'. Each of these assurance levels is associated with the amount of resistance required to withstand a defined level of attack potential. In its technical guidelines, the BSI provides manufacturers with resources to help them fulfil security requirements in line with current industry standards. Technical Guideline TR-03107 is the national interpretation of the eIDAS Regulation for Germany. The Guideline offers a wealth of advice about the requirements that must be met to attain the stated assurance level and therefore achieve a certain capability to resist cyber attacks.

During the last few years, the BSI has talked to many manufacturers of mobile devices and contributed its expertise to a large number of standardisation bodies. These activities have been carried out to raise awareness among manufacturers about security requirements in smartphones, tablets and wearables, as well as to anchor the BSI's own requirements in international standards. Only standards can ensure that every user of mobile devices is provided with the security functions that are necessary to protect their personal eIDs.

OPTIMOS 2.0

In OPTIMOS 2.0, a research project funded by the Federal Ministry for Economic Affairs and Energy (BMWi), a consortium of universities, government agencies and businesses are developing solutions to ensure the secure and workable handling of eIDs on smartphones. OPTIMOS 2.0 is intended to create a non-discriminatory infrastructure that will be accessible to all *service providers* and will fulfil the highest security and privacy standards. The core element in this infrastructure is the Trusted Service Provider, which, as an interface between service providers and end customers, has the task of transferring eIDs securely to mobile devices. To achieve this, the BSI is engaging in the standardisation of the necessary components, interfaces and processes to ensure that the technology developed can be made available to as many end users as possible. At the 2019 Digital Summit, the OPTIMOS 2.0 team was able to demonstrate a number of successful prototypes involving various business partners.

2.1.14 Biometrics in the Age of Artificial Intelligence

Biometric security technologies are becoming ever more important across a wide range of government and commercial application scenarios. Their success is primarily based on the use of deep neural networks (DNNs), which are a component in artificial intelligence (AI) systems. These enable the achievement of truly ground-breaking accuracy, robustness and speed when performing 1:1, 1:N and N:N comparisons of biometric features. While previously inconceivable, frontal and profile shots of faces can now be compared with a high degree of accuracy.
The BSI regularly performs IT security evaluations of biometric systems used by the public and private sectors, and also develops technical guidelines for their procurement and deployment. To properly account for the special features of AI systems, such systems are examined in detail within the BSI. Key aspects and insights from these investigations are explained in the section below with reference to figure 6:

AI biometrics systems use sensor data to make decisions about the identity of individuals (figure 6 centre: blue illustrates the correct, normal operation, while red depicts an *adversarial attack* on the left and an instance of a *morphing* attack on the right). As a result of their complexity, these systems cannot be completely engineered by developers. Instead (figure 6, left to right), the systems are trained and tested using AI models, machine learning techniques and data in what is at times a complex process chain before being released as an end product. The high level of accuracy and robustness that AI systems need to achieve requires training and testing with a large amount of adequate input data, plenty of processor power and a wealth of expertise on the part of the developer. During the last reporting period, a corresponding internal test platform for analysing vulnerabilities in biometric AI systems was set up by the BSI.

Although both powerful and robust, AI systems also exhibit vulnerabilities of an entirely new quality compared to conventional IT systems - with potentially serious implications for IT security. One option for attackers is to manipulate the training data (figure 6, top left), which can, for example, lead to hard-to-detect backdoors being 'learned' by the AI system. Another approach is to manipulate the reference data, such as by blending separate faces into a single ID card photo (facial *morphing*, cf. red facial image in the reference data box in figure 6). In addition, attackers can manipulate live sensor data while the system is in operation by presenting it with artefacts, as in the case of adversarial attacks (figure 6, top centre), or by making use of 'deep fakes'. Adversarial attacks involve the perpetrator modifying sensor data so that the attack is not seen as such by a human (e.g. the targeted application of a slight amount of noise or

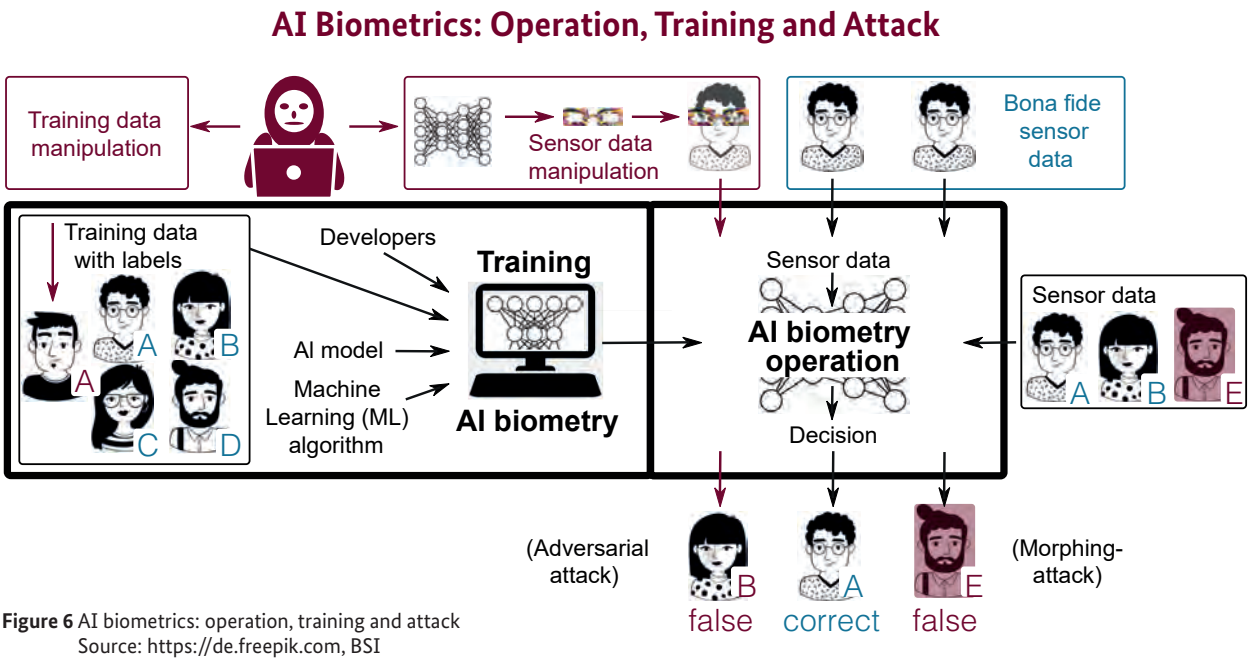


Figure 6 AI biometrics: operation, training and attack
Source: https://de.freepik.com, BSI

a sticker with a colourful pattern to an image), but the AI system nonetheless comes to a different decision than originally intended by the developer. These attacks exploit vulnerabilities inherent in AI systems. With deep fakes, sensor data is manipulated so that human subjects - and potentially even AI systems - can be fooled. AI systems themselves are often used in turn to generate these artefacts.

For attacks against facial biometrics, patches or spectacle frames can be prepared with specific patterns to trick the AI system into classifying the individual incorrectly - often as a specific person. (In figure 6, person A is identified as person B when wearing manipulated glasses; in the real-life data in figure 7, person 3 wearing manipulated glasses is identified nearly 80% of the time as person 1, and only <5% of the time as person 3.) The inherent properties of the main types of DNNs deployed at the moment make them very hard to interpret - which prevents us from obtaining logical explanations for their decision-making. As a result, the kinds of attacks discussed above are typically very hard to detect and new approaches are needed to obtain better interpretations of how AI systems 'work'. The BSI is currently engaged in investigating the various aspects of attacks and defence mechanisms as part of the research work it conducts in collaboration with leading national research institutions. Qualitatively new vulnerabilities specific to AI systems and techniques for their evaluation have been systematically addressed in a review article published by the BSI (cf. chapter *Artificial Intelligence*, page 74).

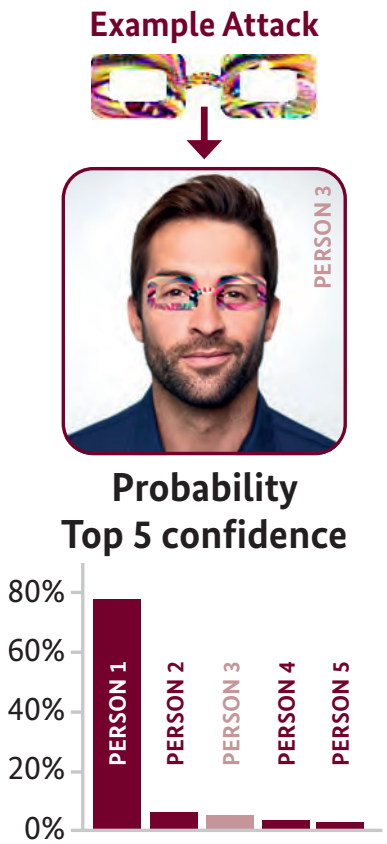


Figure 7 Probability Top 5 convidence
Source: GettyImages @ Morsa Images, BSI

2.2 Industry/Critical Infrastructures

The German industry is highly dependent on functional information technology. This applies in particular to the operators of critical infrastructures (CI). The BSI therefore monitors the situation continuously to determine whether protection is adequate while simultaneously creating the environment needed to improve the corresponding types of infrastructure. One example is its recent approval for the rollout of intelligent metering systems - an important step in the digitalisation of the energy transition, and one that will also help to ensure that networks are better protected against cyber attacks. In addition, the BSI is working closely with relevant manufacturers and operating companies to ensure an appropriate level of security for the introduction of 5G networks and intelligent driver systems. Together with its partners in the Alliance for Cyber Security, the BSI is also working to promote its dialogue with the business world and towards improving the development of IT security expertise.

2.2.1 Threat Landscape for the Industry – with a Focus on Critical Infrastructures

Critical infrastructures (CI) refer to organisations of vital importance to the wellbeing of our society. These organisations provide critical services such as supplying our food, water or power, and they also perform key functions in healthcare, data processing and storage in data centres and maintaining cashpoint networks. All of these types of service are now provided with the help of a vast amount of information technology. Accordingly, they are heavily dependent on IT systems that work without disruptions. Any fault, impairment or failure of these services due to a cyber attack or an IT security incident can lead to lasting bottlenecks in supply, considerable disruptions to public security and all sorts of other dramatic consequences.

This dependency on IT is naturally not restricted to critical infrastructures; it is also more or less true of the industry as a whole. Information technology is all around us - not just in office environments, but in manufacturing, as well. The consequences of cyber attacks, technical failures or other incidents are not limited to IT systems suffering damage or being taken offline. Further risks include data falling into the wrong hands or being tampered with.

Critical infrastructures – a definition

Published in 2009, the German National Strategy for Critical Infrastructure Protection (CIP Strategy) defines nine CI sectors: energy, information technology and telecommunications, health, transport and traffic, media and culture, water, finance and insurance industry, food, and government and public administration. All organisations in these sectors, regardless of their size, are considered to be critical infrastructures (CI).

The BSI Act (BSIG) builds on this basic definition with reference to the BSI Critical Infrastructure Ordinance (BSI-KritisV) in providing more details of the IT systems requiring protection in these various sectors. BSI-KritisV applies measurable and transparent criteria to determine the organisations that fall under the regulatory scope of the BSIG. Organisations are therefore considered CI operators as defined by BSIG section 10(1) and BSI-KritisV if they belong to one of the seven sectors in BSI-KritisV sections 2 to 8 (all of the sectors listed above except media and culture and government and public administration), provide critical services as stated in BSI-KritisV section 1(3) and also exceed the threshold values defined there.

From the perspective of the individual German states, CI operators are defined solely by the corresponding state laws and the criteria published by the competent public authorities in these states; these criteria are to an extent also oriented on the BSI Critical Infrastructure Ordinance.

In 2015, the German Federal Government adopted the IT Security Act (IT-SiG), which introduced new duties for CI operators in the BSI Act and other legislation. For CI operators, the BSI Act now prescribes measures for the prevention (section 8a) and management (section 8b) of IT security incidents or disruptions.

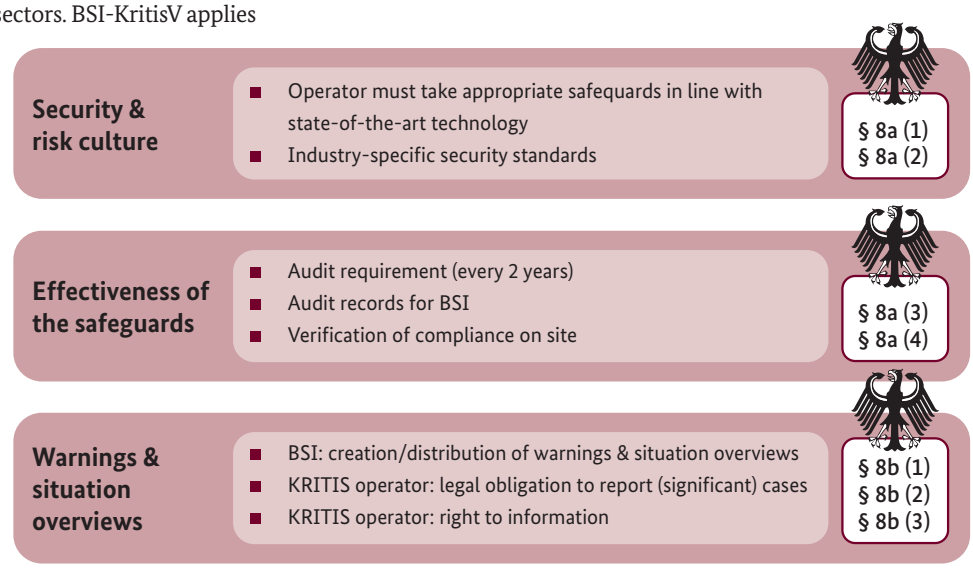


Figure 8 Overview of key provisions in the BSI Act for critical infrastructures

2.2.1.1 Preventive Measures for CI Operators (BSI Act, section 8a)

Industry-specific security standards

In order to comply with BSIG section 8a(1), CI operators must "take appropriate organisational and technical precautions to avoid disruptions." Operators must ensure these precautions are state-of-the-art. Industries can define and specify this 'state of the art' by creating industry-specific security standards (termed 'B3S'), which they can submit to the BSI for auditing to confirm they can meet the requirements of BSIG section 8a(1). Over 20 CI industries are now creating B3S or have already done so. Twelve of these have already been successfully audited for suitability by the BSI. The current list of B3S is available from the BSI website (cf. *Bibliography*[24]: www.bsi.bund.de).

The rapid pace of technical progress requires a repeat audit of the suitability of a B3S by the BSI every two years. Since the creation of the first B3S standards was over two years ago, these have been or will be revised and once again submitted for a suitability audit. In the reporting period, the BSI confirmed the suitability of B3S from the following industries:

- Water/waste water (repeat audit)
- Food trade (repeat audit)

Insights from evidence submitted by CI operators

Operators of critical infrastructures must implement appropriate security measures to protect their IT systems, components and processes, and also ensure that these measures are state-of-the-art. BSIG section 8a(3) requires proof of these measures to be submitted to the BSI every two years if the operator is not already required to submit evidence to another regulator - as is the case for operators of power grids or telecommunications networks, for example (BSIG sections 8a(3), 8d(2)). According to BSIG section 8a(3), such evidence must be submitted in the form of a record of the audit completed for a CI facility by an auditing body commissioned by the CI operator. To make it simpler for operators to prepare these records, the BSI published version 1.0 of its orientation guidance for evidence submitted in fulfilment of BSIG section 8a(3) in May 2019 (cf. *Bibliography*[25]: www.bsi.bund.de).

A total of 358 operators were required to submit evidence in 2019. The BSI received 350 such records in the reporting period. All of these records were subjected to a check for completeness and validated before being comprehensively evaluated in order to determine the main topics covered, as well as challenges and trends. An analysis of the security deficiencies discovered in the individual sectors reveals several important facts.

As a result of the pivotal importance of the information technology industry for other critical service providers, this industry is very much aware of just how important information security is. Many companies operating in this industry have long since established an internal information security management system (ISMS) and a business continuity management system (BCMS). Many operating companies in this industry are themselves audited as part of customer audits. This has resulted in existing IT security defects being discovered and resolved at an earlier point in time. Accordingly, auditors discovered only isolated problems with information technology providers.

In the health sector, a particular point of focus for healthcare service providers as of this writing is the implementation of technical IT security measures. In contrast, the implementation of organisational IT security measures still has plenty of room for improvement. At the management level, there is often a lack of awareness of the importance of IT security. As a result, many operating companies have yet to draft the policies needed for an ISMS or obtain corresponding approval from company management or the management board. In the health sector, other operating companies have not yet migrated their IT risk management, medical device risk management and IT incident management systems into their respective hospitals' main risk management/ business continuity management systems. With pharmaceutical companies, one particular set of challenges lies in assuring the provision of centralised protection for multiple sites and safeguarding the industrial control systems utilised for manufacturing medicinal products.

The food trade and production industries in the agri-food sector present a comparable situation. Operating companies have a strong technical basis here, as well. They point to the recent introduction of management systems to explain the organisational deficiencies identified - such as failings in processes, policies or responsibilities. One particular challenge is providing protection for industrial IT components. The industry also needs models for handling contingency planning without major difficulties, even in round-the-clock production.

The transport and traffic sector is very diverse, with industries including aviation, maritime/inland shipping, rail transport, road transport, public transport and logistics. Common to all of these sectors is the fact that many companies have not yet incorporated the technical and organisational measures they have decided upon into an integrated management process such as an ISMS. Particular weaknesses here include fire prevention, as well as logical and physical access controls. Industry employees often exhibit a lack of awareness and training, as well.

In the energy and water sectors, the deficiencies identified are typically found in the categories of network segregation, business continuity management and physical security. To mount an effective defence against attacks, appropriate network segregation is important. This approach blocks unauthorised access from the internet or office networks to production networks (which control plant systems, for example), and therefore to critical services. In addition, unauthorised activities at any network gateways are also detected. Business continuity management requires effective rules and processes, and its importance has been thrown into sharp relief by the recent COVID-19 pandemic. BCM can also have an indirect effect on IT security. This is particularly true of cases where prevailing security rules need to be changed or even relaxed for the purposes of crisis management, even as fewer IT specialists are available within organisations. While deficiencies in physical security are not to be considered less important, they typically not only require longer-term planning for the measures to be implemented, but can also be compensated for in the interim by introducing organisational measures. From companies' approval processes to construction permits and project implementation, long periods of time may pass before deficiencies are finally resolved. To bridge

this period of time until measures are completed, operating companies must initiate other protective measures in order to counter extant risks.

Across all categories of deficiencies, the BSI works closely with operating companies to ensure that flaws can be resolved promptly. After all, improving the level of IT security for critical infrastructures operations is a common goal of both CI operators and the BSI itself. The BSI therefore remains in constant dialogue with operating companies to promote and support the resolution of deficiencies.

2.2.1.2 Reactive Measures (BSI Act section 8b): Insights Gained from CI Operator Notifications

In 2015, the new German IT Security Act introduced a notification requirement for operators of critical infrastructures (BSI Act section 8b(4)). During the reporting period, the BSI received 419 such notifications; table 1 provides a sector-by-sector breakdown.

Energy	Food	Finance and insurers	Health	ITC[8]	Nuclear plants	Transport & traffic	Water	Total
73	9	65	134	75	0	56	7	419

Table 1 Total notifications by CI sector in the reporting period

While the threat landscape in relation to critical infrastructures remains serious, no threats were observed in the reporting period that targeted critical infrastructures exclusively.

In the case of the electricity segment, the notifications and types of notification received in the reporting period clearly illustrate the significance of this industry for attackers and how they attempt to access internal IT systems. Utility companies have observed an increase in active scanning, which aims to discover - and then potentially exploit - any existing vulnerabilities in systems connected directly to the internet. Attempts to glean login or contact details through covert attacks on third parties associated with the electricity industry have also been observed.

During the reporting period, the energy and water sectors reported several incidents that could be traced back to malfunctions in the control components necessary for the operation of their critical infrastructures. The effort required to resolve these disruptions was considerable and lasted over a month in some cases. Thanks to precautions taken and the redundant design of operators' systems, no supply disruptions occurred in any of the incidents. Since disruptions to component functionality can only be resolved with the help of manufacturers and service providers, however, these incidents clearly indicate the importance of stakeholders acting in concert to ensure an optimum level of protection.

In the health sector, most notifications concerned technical failures, followed by cyber attacks, external service outages, and errors in applications or configuration settings. In the transport and traffic sector, the notifications received did not involve IT security incidents, but concerned reports of disruptions in technical IT systems. Similarly, most of the IT faults reported regarding critical infrastructures in the agri-food sector could be ascribed to technical failures, with electricity outages often identified as the problem.

In the finance and insurance sector, *DDoS attacks* on IT infrastructure and online banking services caused disruptions in payment transactions in the first quarter of 2020. There were several days on which targeted incursions used advanced attack patterns and changed strategies as they progressed. Initially, *DDoS* mitigation measures achieved only limited success. By introducing other measures (including at the network and application layers), a successful defence was mounted, and no further attacks occurred.

In terms of the overall picture for the sector, most of the incidents reported were caused by the failure of IT infrastructure. In 2019, technical failure was responsible for almost 75 percent of finance and insurance sector notifications. Just over ten percent of the notifications stemmed from organisational issues, and slightly less than ten percent were due to the failure of the infrastructure in use. Only 1 in 20 of the notifications submitted was the result of a technical attack. Most of these attacks experienced by the sector involved DDoS attacks and ransomware incidents.

Crisis management support for operators of critical infrastructures

The COVID-19 pandemic represents a significant challenge for operators of critical infrastructures: even in a peri-

[8] Information and communications technology

od of crisis, critical services must nonetheless continue to be provided to the public. Many organisations therefore requested documentation from the BSI to confirm their status as CI operators. The BSI issued the corresponding confirmation documents to all registered CI operators.

Events in relation to the pandemic have created novel circumstances that also constitute a cyber security challenge. Many people have relocated their workplace to their own four walls and the government has offered many types of worker's emergency assistance, which requires an online application. The BSI has published a range of warning notices, backgrounder documents and management bulletins on subjects as varied as the strategic effects of the pandemic on the IT security situation in Germany, secure mobile working or advice on the potential threats involved in using the COVID-19 emergency assistance application websites.

This crisis situation is also impacting the implementation of the BSI Act by operators of critical infrastructures. As one example, restrictions on travel and personal contact have meant that on-site audits are no longer possible for operators. In response to this, the BSI suspended the warning procedures for operators with evidence submission deadlines from March to July 2020 and has postponed these procedures by five months. This will allow operators of critical infrastructures to concentrate their resources on managing the crisis and ensuring the provision of their critical services.

2.2.2 CI Implementation Plan (UP KRITIS)

UP KRITIS, an initiative for cooperation between the industry and the state in order to protect critical infrastructures in Germany (cf. *Bibliography*[26]: https://www.upkritis.de), is a public-private cooperation between CI operators, their associations and the competent government agencies. In May 2020, there were 700 member organisations in *UP KRITIS*.

UP KRITIS has the objective of maintaining the provision of critical infrastructures services in Germany. Moreover, since critical infrastructures is increasingly dependent on information and communications technology (ICT), this area forms a core part of its work. *UP KRITIS* also addresses topics beyond this explicit focus on ICT, however. To ensure the provision of comprehensive protection to critical infrastructures, strategies must integrate both physical safeguards and IT security - as has been shown by the COVID-19 pandemic.

In terms of content, *UP KRITIS* focuses on topics from the fields of risk and crisis management, among others. Important forums for this kind of work include the topic- and industry-oriented working groups of *UP KRITIS*, which publish things like position papers and industry-specific security standards. As two examples of this work, the working group for the topic of 'Supplier and Manufacturer Requirements' published an updated version of its paper 'Best Practice Recommendations for Supplier Requirements to Safeguard Information Security in Critical Infrastructures', while the 'Media' industry working group produced a security level agreement that provides CI operators with a template for agreeing the required levels of quality and IT security involved in working processes between suppliers and operating companies.

Organisations participating in *UP KRITIS* have agreed to share information about the current threat landscape with one another through the *UP KRITIS* industry working groups. To ensure that the results of this process remain comparable among sectors and can be recorded on a continuous basis, a risk matrix has been developed by members of the 'Operational Information Transfer' working group. This risk matrix helps to ensure the structured collection of risk data, as well as its presentation and evaluation and the documentation of trends over time (cf. table 2, page 56).

Initial feedback from nine industries concerning the risks identified have now been analysed, which has resulted in the definition of two key areas of focus:

1. Vulnerabilities/lack of security *patches*
2. *Advanced persistent threats* (APTs)

Among the conclusions drawn from these results, *UP KRITIS* has resolved to redouble its efforts in relation to requirements for suppliers and manufacturers. *UP KRITIS* has already set up a working group to address this topic. APTs are another area already being addressed by *UP KRITIS*. A related working group for the topic of 'Detection' is now being set up to focus on the early detection of APT attacks.

Risk matrix: BAK example, dated 02/04/2020	Gross observations (without safeguards)					With Safeguards	
Threat	Risk in prev. month	Risk trend	Probability of occurrence	Potential scale of damage	Risk	Assessment of vulnerability	**Notes**
	(without safe-guards)	(without safe-guards)	(low / unlikely / probably / most likely)	(low / medium / critical / existential)	(without safe-guards)	(Vulnerability with active safeguards)	
Cross-sector threats (acc. to B3S orientation guidance A1)	Copy from previous month		to fill out	to fill out		to fill out	
‚Cyberattack' category							
Hacking and manipulation	critical		low	critical	medium	unlikely	Focus: external attackers
Malware	existential		most likely	existential	existen-tial	most likely	Focus: malware infection successful (any source)
Advanced persistent threat (APT)	existential		probably	existential	existen-tial	probably	Focus: targeted, attacks over time on specific companies (often economic espionage, competitors)
‚phishing' category							
Identity theft (phishing, skimming, forging of certificates)	critical		probably	medium	medium	unlikely	Focus: technical attacks aiming to steal third-party identities
Misuse (attacks by insiders)	critical		unlikely	existential	critical	probably	Focus: intentional actions by (dissatisfied) employees
Social engineering (Phishing, Vishing (Voice-Phishing))	medium		unlikely	medium	medium	unlikely	Focus: attacks on people with the intention to gather information about third parties and organisational units
‚Process vulnerabilities' category							
Dependencies on service providers and manufacturers (failure of external service providers)	medium		probably	medium	medium	unlikely	Focus: dedicated suppliers (e.g. production IT, NLT), partners, cloud service providers, etc.
Unauthorised access	existential		probably	existential	existen-tial	probably	Focus: Vulnerabilities in access control management (including org. processes)
Vulnerabilities/lack of security patches	critical		most likely	medium	critical	probably	Focus: system and application security including patch mgmt process
‚Attacks on availability' category							
Manipulation, theft, loss, destruction of IT oder IT-relevant systems and system parts	critical		unlikely	critical	medium	unlikely	Focus: OT, SCADA, remote control technology, routers, modems in facilities and IT in data centres and end devices
Targeted destruction / denial of service (DDoS, targeted system crashes,...)	medium		unlikely	medium	medium	low	Focus: external (overload) attacks on IT systems / applications
Damage or destruction of procedural components, equipment and systems	low		probably	low	low	unlikely	Focus: sabotage (physical) of facilities „in the field" (switchgears, transformer stations, pumps, etc.)
‚Force Majeure' category							
Natural hazards	low		unlikely	medium	medium	unlikely	Focus: threats specifically to systems, facilities, locations necessary for running the business (e.g. locations of data centres, power lines, wastewater treatment plants, etc.)
Further overall treats (e.g. from current events, if these cannot be assigned above)							
Lack of staff (e.g. illness, fluctuation, restructuring, provision of resources)	critical		probably	critical	critical	probably	Focus: Operating and security processes cannot be maintained, events / incidents cannot be responded to appropriately.
Industry-specific threats (electricity, water, gas, communication technology etc.)							
Firmware attacks on production and broadcasting systems	low		unlikely	critical	medium	unlikely	
Manipulation of production systems	critical		probably	critical	critical	unlikely	
Manipulation of incoming data streams	medium		low	existential	medium	probably	

Table 2 Risk matrix (figures are illustrative only).
Source: UP KRITIS

2.2.3 Certification of Intelligent Metering Systems in the Energy Sector

The BSI has determined the technical feasibility of installing intelligent metering systems and thus approved the rollout of such systems in an announcement published on 24 February 2020. This marks a key milestone for the digitalisation of the energy transition in Germany.

Following the publication of the BSI's second market analysis on 31 January 2020, the requirements for installing intelligent metering systems have now been fulfilled, with three smart metering gateway manufacturers successfully completing the BSI's product certification procedure.

As a next step, meter operators must equip some four million electricity customers with an annual electricity consumption between 6,000 and 100,000 kWh with an intelligent metering system. Following the BSI's determination of technical feasibility, meter operators have a total of eight years to do so - i.e. until 2028. At least ten percent of these mandatory installations must be equipped with an intelligent metering system within the first three years, however. Where annual electricity consumption is less than 6,000 kWh, installation is optional: in such cases, the decision to install a meter is at the discretion of the meter operator with 'basic responsibility' (by default, this is the grid operator in question). Decentralised power generation plants (as defined by the German Renewable Energies Act/ Combined Heat and Power Generation Act) and 'flexible consumers' ('controllable consumption points' according to section 14a of the German Energy Act) do not need to be equipped in this first phase because the German Federal Ministry for Economic Affairs and Energy has announced modifications to the legislative framework for 2020.

In the future, this use of intelligent metering systems, combined with the resulting deployment of certified smart meter gateways, will ensure that critical systems in the energy grid are interconnected by a secure communications infrastructure. At the same time, this provides an effective countermeasure to cyber attacks. The use of smart meter gateways allows the collection of grid status data and thereby ensures transparency regarding power flows in the distribution network. Moreover, flexible consumption points (heat pumps, electric vehicles, etc.) and decentralised power generation plants can then be controlled by the smart meter gateway, and therefore deployed to the advantage of the grid and market. Controlling decentralised power generation and consumption systems via the smart meter gateway is essential to further increasing the proportion of renewables in power grids and, for example, integrating the charging infrastructure needed for widespread electric vehicle (EV) use without extensive and cost-intensive grid expansion.

The installation of intelligent metering systems will therefore make a key contribution to achieving climate and energy transition objectives. In 2019, the BSI and the Federal Ministry for Economic Affairs and Energy prepared and published a joint standardisation strategy for the sector-wide digitalisation of the energy transition. This strategy now forms the common basis for working with industry associations and companies to specify the key technical criteria and the resulting BSI standards for establishing the secure energy grid of the future. As a result, it will be possible to document current trends and innovations in a goal-oriented manner and ensure that the gateway technology is continuously improved for deployment in other areas.

2.2.4 Modern Telecommunications Infrastructure (5G)

Digitalisation brings high speeds, efficiency and effectiveness to processes in both business and government while offering greater comfort and ease of use for private citizens. One technological basis for these developments is the 5G mobile network standard, which is designed to offer faster connections, less latency and higher data rates. The new 5G technology is commonly considered to be a decisive factor in Germany's positive development in the years to come. The BSI has been tasked with creating the environment needed to ensure that 5G networks achieve the highest possible level of confidentiality, integrity and authenticity. The current basis for the development of secure 5G networks is the security requirements specification that the Federal Network Agency, the BSI and the Federal Commissioner for Data Protection and Freedom of Information (BfDI) have revised in line with section 109 of the Telecommunications Act. This specification will be applied to the new 5G networks being set up. Alongside revisions to the Security Criteria for network operators and service providers, initial specifications for the certification of network components have also been prepared and discussed at the European and international level.

Security Criteria

The German Telecommunications Act (TKG) sets out the legal framework for operators of telecommunications networks. In terms of IT security, section 109(6) of the Act is most relevant because it stipulates national security requirements for telecommunications infrastructure in the form of the 'Security Criteria'. These criteria, which have been prepared by the Federal Network Agency in consultation with the BSI and the Federal Commissioner for Data Protection and Freedom of Information, are updated regularly to reflect applicable technical and regulatory frameworks. These ongoing

revisions and updates to the Security Criteria have been careful to accommodate the new 5G mobile network standard: the criteria are now supplemented by a second annex containing additional security requirements for public telecommunications networks and services that are considered to be exposed to a greater potential risk.

This new annex to the Security Criteria focuses on topics such as safeguarding the integrity of components throughout their entire lifecycle, as well as requirements for ensuring that the secure operation of networks is maintained by means of security monitoring and key management. In addition, operators are required to obtain security certification for their critical network components.

Certification strategy

The BSI is currently preparing a certification strategy for 5G that is intended to enable the use of discrete, yet interrelated certification schemes in the various areas of networks - including for both products and systems. In this work, the BSI references internationally recognised and established standards to minimise effort for manufacturers and operators.

The starting point for product certification is the Network Equipment Security Assurance Scheme (NESAS), a testing/auditing scheme developed by the GSMA (Global System for Mobile Communications Association). The BSI is currently working together with the GSMA to extend the NESAS scheme with the aim of establishing it as a European certification scheme as part of the German Cybersecurity Act and integrating other testing requirements into the standard, such as a secure product lifecycle that also accounts for the supply chain. In accordance with the further development of technology and the market, product certification will be extended to include the Accelerated Security Certification (BSZ) and Common Criteria[9] (CC) schemes at a later date. The aim is to ensure the creation of CC-based protection profiles for selected critical network functions and to have these standardised and harmonised at the European level.

In the field of system certification, the BSI is preparing network operator specifications as part of its own IT-Grundschutz and ISO 27001. These specifications include criteria for maintaining secure network operations and handling critical components throughout their lifecycle.

The schemes for product and system certification selected in the course of the 5G certification strategy will also be summarised in a Technical Guideline from the BSI, which will act as an authoritative reference for the Security Criteria. The Technical Guideline will be published by the BSI by the end of 2020 and will be updated on a continuing basis.

European harmonisation

At the European level, the rollout of fifth-generation networking technology is viewed as an important precondition for future digital services in the Digital Single Market. The EU Commission also recommends a concerted approach to the security of 5G telecommunications networks: in its Recommendation 'Cybersecurity of 5G networks' ((EU) 2019/534 of 26 March 2019), the Commission has published a roadmap for developing a common, EU-wide toolbox of measures to increase security in such networks. In particular, these measures include the creation of a Cooperation Group, the establishment of coordinated European risk assessment and the development of a common toolbox of measures to mitigate the identified cybersecurity risks.

The Cooperation Group was set up in April 2019 as a 5G working group (also referred to as the 'NIS 5G Workstream') under the auspices of the NIS Cooperation Group. The BSI has been involved in the workstream since its inception. Here, it is making a particular effort to introduce appropriate certification schemes (e.g. the NESAS scheme mentioned above) as EU certification schemes. To date, the workstream has published its results in two separate documents: 'CG Publication 02/2019 - Risk Assessment of 5G Networks' (9 October 2019) and 'CG Publication 01/2020 - Cybersecurity of 5G Networks: EU Toolbox of Risk Mitigating Measures' (29 January 2020).

2.2.5 IT security in Intelligent Traffic Systems (C-ITS)

Advanced driver-assistance systems

Driver assistance systems are now present in virtually all the vehicles found on Germany's roads. From ABS to automated emergency brake assistant systems, modern vehicles transfer an increasing number of driving tasks from the driver to the vehicle itself and permit the vehicle to execute such procedures independently. Driver assistance systems are a step on the road to fully autonomous vehicles. The BSI conducts spoofing attacks (i.e. attempts intended to deceive) on vision-based driver assistance systems to investigate the robustness of current systems against practical attacks and highlight areas with potential for improvement.

Methods from the field of artificial intelligence (AI) are often used to enable driver assistance systems to extract

[9] An international standard for auditing and evaluating the security attributes of IT products.

relevant information about the state of the vehicle and its surroundings based on a wealth of internal and external sensor data and render corresponding decisions. One example of this use is in the detection of road traffic signs, where a deep neural network is used to identify the location and type of traffic signs currently within the vehicle's 'field of view'. These kinds of systems are often extremely complex, however, which makes them extremely difficult to interpret and exposes them to novel attacks. If a specially prepared, yet innocuous-looking sticker is affixed to a traffic sign, for example, this can fundamentally alter the AI system's decision-making. The BSI is supervising several research students who are working on these kinds of problems and is also engaged in preparing potential criteria and methods for auditing such systems in the 'AI' working group together with the Association of Technical Inspection Agencies (VdTÜV).

Vehicle-to-X communication

Vehicle-to-vehicle and vehicle-to-infrastructure communication for cooperative intelligent transport systems will start being brought to market in 2020. To ensure interoperable and secure communication across Europe, the EU Commission is currently setting up the central bodies for the *public key* infrastructure that will support such systems. A European Certificate Trust List provided by the EU Commission Trust List Manager is being used to register the trusted root certification authorities for roadside facility operators in the individual member states, as well as for the automotive manufacturers. The BSI was involved in drawing up the process and protocol specifications for these central authorities in a working group at the EU Commission.

At the national level, the envisaged public key infrastructure authorities (PKI authorities) for roadside units will also be provided from 2020 on for a pilot operational phase. The BSI is providing support to the Federal Ministry of Transport and Digital Infrastructure (BMVI) and the roadside facility operators for the preparation of the organisational and technical specifications for these systems.

Last year, an initial protection profile was certified by the BSI on the basis of the Common Criteria in the context of cooperative intelligent traffic systems. This 'protection profile for a roadworks warning gateway' specifies IT security requirements for an electronic component of mobile traffic warning signs on motorways, which send warning messages to approaching vehicles as part of vehicle-to-infrastructure communication and can also receive status information from individual vehicles. This information is to be used to create situation reports for local traffic.

2.2.6 Technical Security Device for Electronic Recording Systems

As part of the digital transformation, business transactions are increasingly documented using electronic systems. In the retail trade, the cash register market is characterised by the use of a very wide variety of cash registers. From traditional tills to tablets, smartphones and even server farms, every conceivable type is represented. As a result, the technical challenges for tax inspections have changed radically, especially since later manipulation of electronic records can be practically undetectable if appropriate safeguards are not used.

To counter this kind of tampering, the Fiscal Code of Germany and Cash Register Security Ordinance have stipulated the protection of electronic recording systems in Germany with a certified technical security device from 2020 onwards. This device is contacted by the electronic recording system, proceeds to handle the protection of the data to be secured and files the secure records using a uniform format. Therefore, the technical security device is also equipped with a security module that ensures that records cannot be altered, erased or created anew at a later point in time without those changes going unnoticed.

The new piece of legislation explicitly promotes the usage of various technologies to design and create technical security devices. A standardised digital interface simplifies integration with existing and future electronic cash register systems while also guaranteeing the necessary interoperability in the context of tax inspections. Special requirements for the physical interface are not enforced to ensure that typical standard interfaces such as USB, Ethernet and (micro) SD cards can all be used. To complement purely local security devices, scalable solutions have also been accounted for from the outset by an optional client/server architecture for the security model. These solutions can be deployed in branches or designed as an online service, for example.

The technical requirements and testing standards for the components used in the technical security device are derived from the German Fiscal Code; they have been specified by the BSI in technical guidelines and protection profiles on behalf of the Federal Ministry of Finance (BMF). All of this is set out in the Fiscal Code of Germany (the law underlying all German tax legislation), and the criteria are therefore prepared on behalf of the BMF. The technical guidelines and protection profiles were finalised and published in agreement with the relevant associations and manufacturers as scheduled in 2018.

By introducing a transitional arrangement for 2019, the BSI has also enabled manufacturers to substitute a part of the time-consuming security certification process with an

expert approval from the BSI. This approach was intended to ensure that technical security devices were available on the market as quickly as possible. According to the terms of this transitional agreement, technical security devices may be deployed in the field for one year following the issue of an expert approval.

Four technical security devices have now successfully completed certification utilising the transitional agreement and are now available on the market.

2.2.7 Certification

The BSI service portfolio includes a variety of certification procedures. One of the established procedures in the field of product certification is the certification according to Common Criteria (ISO/IEC 15408). Products can also be certified according to the BSI's technical guidelines. In the field of management systems, the long-established Grundschutz (baseline security) standard also permits the certification of an information security management system (ISMS).

Common Criteria certification (ISO/IEC 15408)

Certification of the IT security of a product by the BSI means that it has been evaluated by an independent party in a fully documented process on the basis of public evaluation criteria (cf. *Bibliography*[27]: www.bsi.bund.de).

For procurement agents, a BSI certificate provides the following:

- A comprehensive documentation of the effectiveness of security functionality
- A decision-making aid for product usability
- Comparability of security functionality
- Conformity with national or international standards

The Common Criteria evaluation criteria, which were initially drawn up and maintained by the nations participating in the Common Criteria Recognition Agreement (CCRA, cf. *Bibliography*[28]: https://www.commoncriteriaportal.org), have now been adopted by the International Organisation for Standardisation (ISO). The standard is currently being updated and extended. BSI collaborates on this programme with experts from IT security evaluation facilities and manufacturers via the German Institute for Standardisation (DIN). The aim is to extend both the conceptual basis for specifying security requirements and the evaluation methodology to improve the applicability of the standard to new technologies.

The EU Commission has taken up the issue of certification as part of its efforts to promote cyber security in Europe. The legislative package for cyber security - the Cybersecurity Act, which also includes an EU-wide IT security certification scheme - entered into force on 27 June 2019. In SOGIS-MRA, the EU member states have a strong, well-established certification model in operation that is currently being integrated into the new EU umbrella legislation.

The demand for certified products has also been enshrined in numerous laws and regulations in recent years. The German Government's digitalisation projects offer a number of examples in this regard, including the deployment of digital technologies in healthcare (eHealth), public sector documents, intelligent metering systems (Smart Metering), digital signatures, and most recently in the field of cash registers to ensure that essential digital recordings are protected against manipulation.

Product certification is supported by protection profiles (PPs), which define a set of security requirements for a particular product type. Examples of new protection profiles are:

- PP Cryptographic Service *Provider* Light (CSPL), e.g. as deployed in electronic cash register systems
- PP Roadworks Warning Unit, deployed to warn approaching vehicles about local roadworks

Certification in line with technical guidelines

Functionality and interoperability as product features are described as a standard in terms of functional requirements within the BSI's technical guidelines (Technische Richtlinie, TR) 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 IT security evaluation facility on the basis of the test specifications defined in the TR. The test is monitored by the responsible certification body within the BSI and confirmed on completion with a notice of conformity and a certificate. For some TRs, the certification body is accredited by the German National Accreditation Body (DAkkS).

ISMS certification according to BSI Grundschutz

In addition to product certification, certification of management systems is also offered based on the commonly used certification according to ISO/IEC 27001 and carried out on the basis of IT-Grundschutz (which is developed within the BSI). The IT-Grundschutz proce-

dure and the recommendations on standard security measures, that IT-Grundschutz offers, represent a de facto standard for IT security by now.

Certification in figures

As part of Common Criteria certification, BSI issued certificates for a total of 63 products, 25 sites and nine protection profiles.

In addition, 77 certificates were issued according to technical guidelines in 12 testing categories; of these, 47 were initial or re-certifications, 23 were maintenance procedures and seven were surveillance audits.

In the context of IT-Grundschutz, a total of 112 procedures were completed successfully in the reporting period. They involved 43 ISO 27001 certificates based on IT-Grundschutz and 69 surveillance audits.

In terms of international rankings, BSI has been among the top five CCIA certification nations with the largest number issued of certificates for years.

2.2.8 IT-Grundschutz and Attestations

For over 25 years, IT-Grundschutz has been a trusted set of BSI services that companies and government agencies can use to increase information security within their organisations. This comprehensive portfolio of baseline measures includes recommendations and requirements for all issues related to information security. These services aim not only at users tackling the concepts of IT-Grundschutz for the first time, but also at advanced users working in government agencies and the world of business. The BSI Standards provide basic knowledge of methods and approaches. The modules of the IT-Grundschutz Compendium can then be used in a target-oriented manner in order to improve the status of information security within an organisation.

IT-Grundschutz Profiles – templates for information security

Since 2018, the sample security models offered as 'IT-Grundschutz Profiles' have made it easier to get started with IT-Grundschutz. These profiles help users take their first steps towards setting up an ISMS and a security policy. An IT-Grundschutz Profile is a template that represents a reference architecture for a specific use case.

On its website, the BSI website publishes IT-Grundschutz Profiles for a very wide range of application scenarios and industries that can be used for conducting individual security assessments. Profiles are available (in German only) e.g. for independent tradespersons, chambers of trades, HEIs, local authorities, state-level authorities, paper factories and shipping companies (both shore and ship operations, also available in English).

IT-Grundschutz Profiles are subject to cyclical revision and are regularly amended and revised - on account of new insights, for example, or on the basis of the annual updates made to the IT-Grundschutz Compendium.

IT-Grundschutz Profiles are currently being created for other industries. The BSI's IT-Grundschutz Unit hosts joint workshops together with the Alliance for Cyber Security to provide support to users interested in creating a new IT-Grundschutz profile. In the long run, the aim is to publish IT-Grundschutz Profiles on as many topics and for as many industries as possible so that users can make use of these proven and practice-focused guidance documents.

IT-Grundschutz attestation for Basic Protection

The 'Basic Protection' approach defined by IT-Grundschutz can be used by an institution as an entry-level methodology for setting up an ISMS. The security assessments it prescribes focus on the 'Basic Requirements' from the IT-Grundschutz Compendium, which offer a basic and initial level of protection across all business processes and tasks. They can be implemented with comparatively few resources in terms of time, money and personnel. As a result, Basic Protection is especially suitable for small and medium-sized enterprises (SMEs) or smaller municipal authorities that want to pursue an integrated approach to setting up an ISMS.

After completing Basic Protection, companies and government agencies can use an attestation to prove that they have implemented IT-Grundschutz at this level of protection. With this attestation, an institution can prove that it has safeguarded all of its business processes, activities, data and components within its information domain assessed to a minimum level of information security while considering aspects relating to systems, infrastructure, organisation and human resources.

The 'Standard Protection' and 'Core Protection' from IT-Grundschutz encompass those approaches that should be pursued to protect an institution appropriately and comprehensively according to the technical state of the art. To provide evidence of this level of security to third parties, an ISO 27001 certificate on the basis of IT-Grundschutz can be acquired.

2.2.9 Support for the Secure Transition to Working from Home

By March 2020, the devastating effects of the COVID-19 pandemic were having a significant impact on society in Germany, as well. Many organisations promptly decided to let their employees work from home to at least maintain their business operations to a limited extent. This fundamental change in working practices created many challenges: IT infrastructure had to be significantly modified, and many organisations faced the novel proposition of a home-based workforce.

The BSI responded quickly to these needs by publishing a press release on 18 March 2020 that offered some initial recommendations on secure mobile working and the further expansion of existing working-from-home infrastructure while accounting for the most important security measures (cf. *Bibliography*[29]: www.bsi.bund.de). Moreover, BSI also offered a range of other services to various government departments to secure home working of their staff. These services were tailored to reflect the departments' various levels of experience and degrees of implementation. Thus, authorities were provided with a wide range of information to help them secure existing remote working environments and to set up new ones. The increased need for security of data processing was also considered.

In a joint initiative with the Alliance for Cyber Security, an online checklist was published that was primarily directed at businesses lacking prior experience in the field of remote working. 'Working from Home? – Stay Safe!' includes a list of pragmatic solutions that can be implemented on short notice to ensure that organisations stay fit for purpose while also maintaining a proper level of confidentiality, availability and integrity (cf. *Bibliography*[30]: www.bsi.bund.de). At the same time, companies with home worker experience can use the included information to review the measures they have already put into place.

Meanwhile, virtually every organisation developed a greater need for videoconferencing solutions. A task force was set up for this topic in order to provide prompt and relevant recommendations. The BSI also published its 'Compendium of Videoconferencing Systems' on 14 April 2020, which provides planners, procurement agents, operators, administrators, auditors and users with information that helps ensure the secure management of videoconferencing systems throughout their lifecycle (cf. *Bibliography*[31]: www.bsi.bund.de).

The various recommendations on working securely in a home environment were accompanied by warnings published on a case-by-case basis for certain target groups with regard to relevant risks in the context of the COVID-19 pandemic (cf. chapter *Threats to Cyber Security due to the COVID-19 Pandemic*, page 33).

It can be assumed that the pandemic will have a lasting impact on the way institutions work. In this context, the COVID-19 pandemic is therefore also an opportunity for the digitalisation of the world of work. Thanks to the wealth of material offered by the BSI, many organisations have now been provided with operational and strategic guidance. Awareness around the importance of information security in a home working environment has been improved, and tailored assistance has also been provided to various organisations.

2.2.10 Alliance for Cyber Security

Membership in the Alliance for Cyber Security is becoming increasingly popular in light of the steadily growing set of challenges arising from the rapid pace of digitalisation. In cooperation with more than 130 business partners, the BSI has used this platform since 2012 to promote the transfer and development of IT security expertise in a number of different formats, such as Cyber Security Days, workshops and recommendations.

During the last 12 months, over 900 organisations have joined the initiative to gain access to numerous offers, as well as to the mailing list for BSI warning notifications. With over 4,400 members, the Alliance for Cyber Security is now one of Germany's biggest business communities in the field of cyber security.

To ensure its members receive appropriate and relevant guidance, it regularly introduces new formats - particularly in cooperation with the umbrella organisations represented on the Alliance's Advisory Council. One of these new formats was the Cyber Security Day organised with the support of the German Chamber of Industry and Commerce in Berlin on 26 September 2019. This event was attended by over 300 members and received live coverage from the media. A video of the event is available on the Alliance for Cyber Security website (cf. *Bibliography*[32]: www.allianz-fuer-cybersicherheit.de).

2.2.11 Dialogue Among Various Cyber Security Initiatives in Germany

Since 2017, the BSI has invited German cyber security initiatives to engage in dialogue under the auspices of the Alliance for Cyber Security. One particular goal here is to work on common projects with the aim of creating new resources for the promotion of cyber security, and to make

these available to as many interested parties as possible through coordinated communication activities.

The current reporting period once again witnessed a wide range of such campaigns. Two of their key points of focus were raising IT security awareness among employees and increasing companies' cyber *resilience*. One result of these working groups was the service package 'Introducing IT Business Continuity Management', which sketches out key steps towards establishing an internal BCM system. The 'IT Emergerncy Card', for example, drew particular interest as a way to display instructions in the workplace on actions to take in the event of an IT security incident (much like an 'in case of fire' sign). Further details can be found by visiting the Alliance for Cyber Security website (cf. *Bibliography*[32]: www.allianz-fuer-cybersicherheit.de).

Once again, this partnership was characterised by the interdisciplinary makeup of the working groups: By bringing together individuals with different skills and backgrounds, projects could be developed and successfully advanced by drawing on widely varying experiences and perspectives. With the support of such wide-ranging expertise, it was possible to make the IT Emergency Card (which had originally been intended only for German SMEs) into a universally deployable response measure. The commitment of those involved has now resulted in an instrument that can be used in organisations of any size - from SMEs to large corporations. The IT Emergency Card has also been translated into many languages, which means it can also be used in an international context.

2.2.12 Other Solutions/ Services for Business

Criteria Catalogue for Cloud Service Security

The Cloud Computing Compliance Criteria Catalogue (C5) defines a list of criteria for the security of *cloud* services. While providers use the C5 to substantiate the level of security offered by their *cloud* services, the ensuing audit report can be used by customers to control their *cloud* usage risks.

The C5 was published by the BSI in 2016 and has since been adopted worldwide. In 2019, it was revised with the help of providers, consumers, associations and auditors, which contributed their experience and concerns in feedback workshops to supplement the BSI's own expertise. The overall intention here was to maintain or increase the already impressive security levels achieved while making sure that these were both attainable and clearly communicable to customers. New legislation such as the EU Cybersecurity Act (EUCSA) also needed to be accounted for. The draft of the new C5:2020 catalogue was then published as a consultation document at the IT security trade fair it-sa 2019. After incorporating all of the comments made, C5:2020 was presented to the public before an audience of 90 specialists in Frankfurt am Main on 21 January 2020.

The revisions to C5:2020 include the following:

- Product security as a new regulatory area in which security objectives for *cloud* services are designed based on article 51 of the EUCSA

- A new regulatory area for handling government requests for user information; the *cloud* provider must be able to prove to the customer that such requests follow an orderly procedure subject to legal scrutiny, and that data is released only in cases where this legal scrutiny has verified the legitimacy of the request in question

- Criteria for corresponding user controls; all C5 reports include details of the customer's responsibility to contribute to the security of *cloud* service (this is an expression of the principle of shared responsibility). In C5:2020, this aspect is addressed by corresponding criteria. For each criterion applicable to the *cloud* provider, these state whether the customer can also make a contribution and what form this contribution should generally take. However, further details of the measures specific to each use case must be provided.

A C5 audit report provides all customers with a meaningful basis for their own risk management work and acts as a catalyst for security questions that may arise in contract negotiations between the provider and the customer. The improvements made to the new C5:2020 further define (and thus advance) the level of security of *cloud computing*, which is now an integral part of information security for contemporary digitalisation projects in government, business and society.

Investment Monitoring

The BMI involves the BSI as part of its duties in procedures for auditing investments made 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 Ordinance (AWV).

The benchmark for these audits is whether material security interests, public order or the 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 systems certified for classified information, operates critical infrastructures, or 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 potential risk situations with regard to IT security. This risk assessment influences the BMI's verdict from a security policy perspective.

At the EU level, the EU Screening Regulation (2019/452) establishes a framework for screening foreign direct investments more effectively. Germany has also begun work on aligning its Foreign Trade and Payments Act (AWG) and Foreign Trade Ordinance (AWW) with the EU Regulation.

The number of individual audits handled by the BSI in connection with investment control procedures virtually doubles from year to year. The figure rose from four procedures in 2015 to 71 procedures in 2019. The number of procedures received since January 2020 has confirmed this trend, which is why the BSI expects to work on more than 100 audit procedures in 2020.

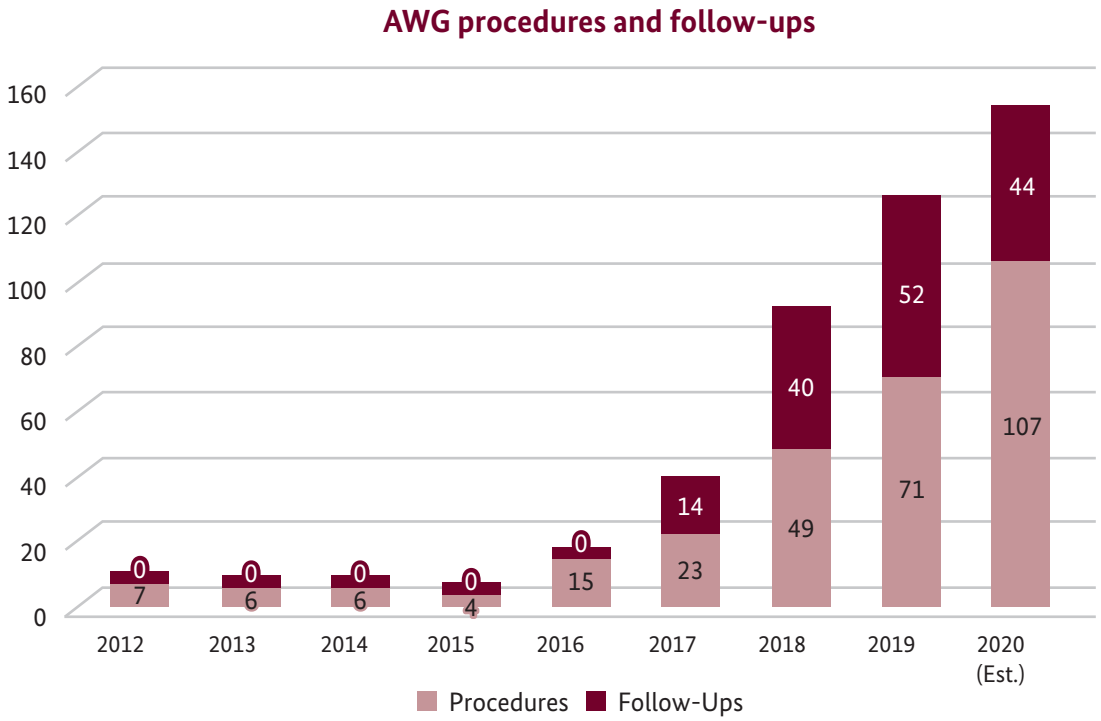


Figure 9 Trend in individual audits in conjunction with individual audit procedures.
Source: BSI

2.3 Federal Government/ Administration

Protecting government networks from attack is one of the BSI's core tasks and also one of its most significant challenges. As part of the National Cyber Response Centre and as operator of the Federal Security Operations Centre (BSOC) and CERT-Bund, the BSI has a key role to play here. It thus analyses cyber attacks and malware and develops measures to close any security gaps discovered. Prevention is also an extremely important area in which

state and local governments are provided with information security advice on setting up and operating information technology. The BSI also draws on its expertise in a wide range of projects focusing on the implementation and improvement of IT infrastructure and the deployment of new security technologies.

2.3.1 Threat Landscape in the Federal Administration

Government networks are exposed to cyber threats from the internet on a daily basis. These include not only the kinds of non-targeted, scattergun attacks to which all internet users are exposed, but also coordinated campaigns directed specifically against government networks.

Spam filters, web filters and virus scanners are deployed to repulse non-targeted attacks. As in other areas, the primary *attack vectors* of non-targeted attacks in the Federal Administration include malicious email attachments and links propagated through emails, social media accounts or websites. In both cases, social engineering methods are used to trick users into clicking and thereby installing malware onto their system.

During the reporting period, the Federal Administration experienced an increasing number of attacks with links in emails and on social media or websites. Such links lead the end user to servers on the internet where attackers have prepared malware as downloads. The BSI uses web filters to protect government networks from such attacks. Malware containing websites are blocked by those filters, so that they cannot be accessed from within the Federal Administration. In the current reporting period, an additional 52,000 websites had to be blocked. This marks an increase of around 46 percent compared to the previous reporting period. An abnormally large number of new blockings were necessary at the start of the fourth quarter of 2019, and especially at the end of the same year. In December 2019, the index of website blockings reached a peak of 230 points - a value more than twice as high as the average figure for 2018.

At the turn of the year, a wave was also observed in email-based malware attacks. Compared to similar surges seen at this time of year, however, this wave was noticeably smaller and had ended by early February. By an automated antivirus protection, an average of 35,000 harmful emails of this kind were intercepted in real time every month before they managed to reach the recipients' mailboxes. Of these, an average of around 9,200 malicious emails were detected each month using internally created antivirus signatures alone. One reason for the development of these indicators compared to the previous year's report was the change in tactics observed in malware attacks. In this context, there was a further increase in the trend towards sending malware more often as a link in emails than as a file attachment.

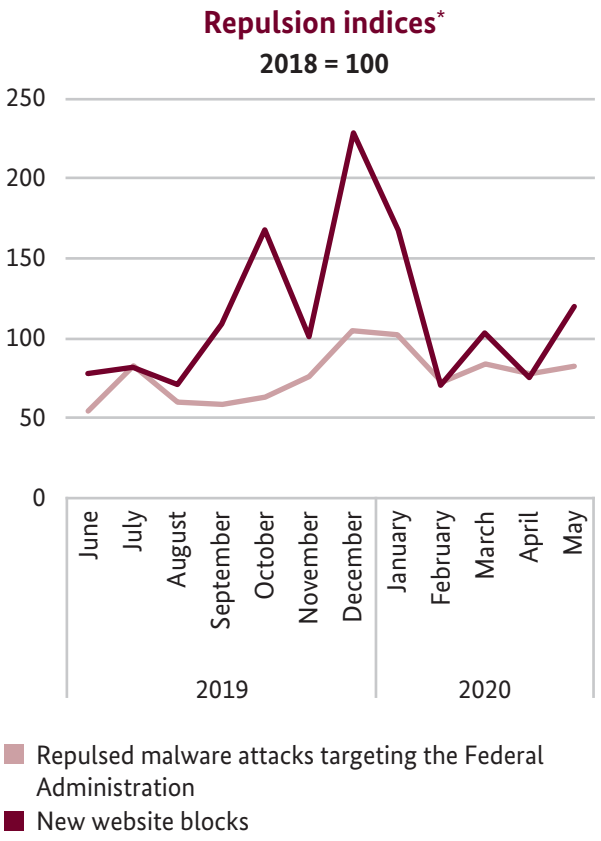


Figure 10 Repulsion indices, Source: BSI analysis of its own sources

*Not including attacks on agencies that do not participate in the central protective measures of the BSI.

In addition to these automated antivirus measures, the BSI operates another system for detecting malware in government network data traffic. This system combines automated testing processes with manual analysis and is particularly suitable for detecting targeted attacks and new malware variants. In this way, BSI analysts were able to detect another 4,900 attacks per month on average that had not been recognised or blocked by the commercial protection products in use.

In addition to the virus scanners and web filters mentioned, the federal networks have a centralised protection system against unwanted *spam* email. This protects against not only unsolicited advertising mail, but also cyber attacks such as *phishing* emails, *malware spam* or

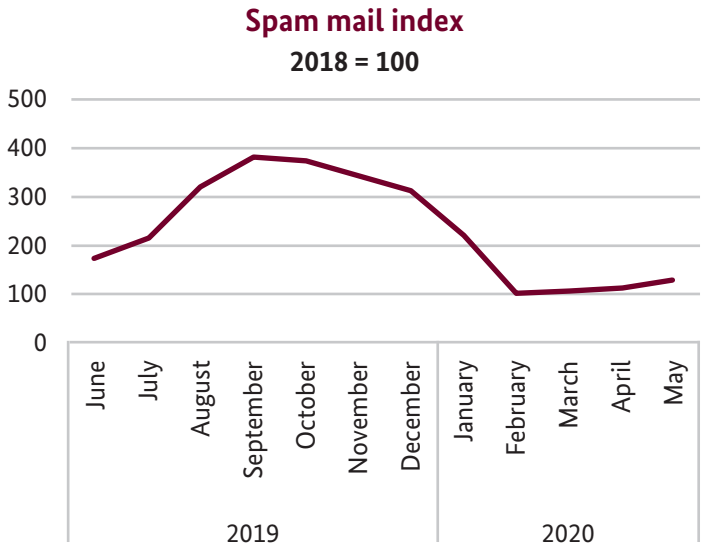


Figure 11 Spam mail index, Source: BSI analysis of its own sources

bulk virus mailings. The proportion of unwanted *spam* mail in all of the email received by federal networks was 76 percent on average during the reporting period. This figure is seven percentage points higher than in the previous reporting period (69%).

Amounts and trends pertaining to *spam* email in federal networks are measured using the *spam* mail index. The sharp rise in this indicator is primarily ascribable to the pronounced *spam* waves witnessed in the third quarter of 2019. In September 2019, this indicator reached 382 points - a value nearly four times higher than the average figure for 2018. The *spam* wave ended abruptly at the beginning of February, and things have stabilised at a lower level since then.

2.3.2 National Cyber Response Centre

The National Cyber Response Centre (CRC) is a platform for collaboration and the exchange of operational information among federal agencies with varying competencies in the field of cyber security. The core agencies working at the CRC are: the Federal Office of Civil Protection and Disaster Assistance (BBK), the Federal Office for the Military Counterintelligence Service (BAMAD), the BSI, the Federal Office for the Protection of the Constitution (BfV), the Federal Criminal Police Office (BKA), the Federal Intelligence Service (BND), the Federal Police Presidium (BPOLP) and the Cyber and Information Space Command (KdoCIR) at the Federal Armed Forces. Other government bodies participate as associated units. Partners from other levels of the administration are involved on a case-by-case basis; at the state level, for example, this includes *CERTs*, the State Criminal Police Offices and the State Offices for the Protection of the Constitution. As part of its continued development, it was agreed last year that the coordination of the CRC should be handled by the core agencies on a rotating basis. At the end of 2019 the role was transferred tot the BKA for the next term. As the host agency, the BSI continues to supply core personnel for the operative arm of the CRC, as well as its premises and their shared IT infrastructure.

Within the CRC, the participating organisations exchange information relevant to cyber security and the details of any ongoing and planned measures. In the process, the CRC pursues an integrated approach that monitors a wide range of threats both inside and outside cyberspace, including espionage, sabotage, terrorism and other crimes.

Apart from situation monitoring, another key area of activity within the CRC is the coordination of the day-to-day processing of actual incidents among government agencies. The actual processing of these incidents is carried out by the specialist units in the participating agencies within their respective remits. Insights and results are continuously consolidated within the CRC before being evaluated and reported to the appropriate bodies.

As a result of the increased relocation of many activities online during the COVID-19 pandemic, two key points of focus in the reporting period were the joint evaluation of developments in relation to cyber security and the coordination of measures to protect at-risk facilities.

2.3.3 Federal Security Operations Centre

The BSI operates the Federal Security Operations Centre (BSOC) to protect government networks and IT systems from cyber attacks. By achieving the greatest possible degree of automation through the deployment of modern, standardised products; code developed in-house; and methods supported by artificial intelligence (AI), the aim here is to give the BSI‘s experts the space they need to conduct indispensable manual analyses of attacks and malware. Such analyses have proven essential to the BSI‘s ability to detect attacks on the Federal Administration with a high degree of success.

The tasks assigned to the BSOC include services for the collection and analysis of log and sensor data, as well as for the detection and repulsion of malware in emails and web traffic. To manage this remit, the BSI has developed a range of systems that are continuously modified (by in-

corporating in-house antivirus signatures, detectors and technical platforms, for example) to match the current threat landscape. Meanwhile, detection does not merely take place at network boundaries; end-user systems are also accounted for in the protected facilities.

To further improve the Federal Administration's overall analysis and response capabilities with regard to cyber attacks while ensuring that the administration's available resources are deployed appropriately, the BSI works closely with other federal agencies on detecting and countering such attacks. In one particular instance, the BSI works with the government's IT service providers to set up the BSOC Association. This combines the core services provided by the BSI with the local security measures of participating federal agencies - especially in the area of operational cyber security.

2.3.4 Computer Emergency Response Team for Federal Agencies

The BSI operates the Computer Emergency Response Team for Federal Agencies (CERT-Bund) in order to conduct preventive and responsive measures in relation to vulnerabilities and IT security incidents. CERT-Bund prepares and publishes preventive recommendations on avoiding losses or damage, warnings about vulnerabilities in hardware and software products and responsive measures designed to limit or repair damage that does occur. It also provides support for responses to IT security incidents on a case-by-case basis and issues daily updates to German network operators about various internet servers or accounts that are publicly accessible or vulnerable. These *providers* are asked to inform their affected customers accordingly.

The services offered by CERT-Bund are provided first and foremost to government agencies. In the process, CERT-Bund works together with the BSI's National IT Situation Centre to provide a 24/7 on-call service, analyses incoming incident reports, operates a warning and information service, and offers active support by coordinating and analysing corresponding IT security incidents. CERT-Bund makes use of CVDs to respond to vulnerabilities. This process for the publication of vulnerabilities coordinates and optimises the necessary exchange of information between finders, manufacturers and any other affected parties (such as industry suppliers). The primary aim here is to keep end-user exposure to the risk created by these vulnerabilities as low as possible. To do so, end-users and those who discover vulnerabilities must be confident that manufacturers will abide by their responsibilities and correct the reported errors according to security-by-design principles and the rules of the CVD process, as well as any deadlines set within it.

A commitment to communications and reliable response processes is an elementary part of ensuring a viable working relationship in an external reporting process. The involvement of the BSI as a coordinator can also be requested by manufacturers and finders. CERT-Bund provides support for vulnerability reports and any liaison activities that may be required, as well as the notification of potentially affected parties.

In the reporting period, support was provided for over 20 CVD cases, and vulnerabilities detected during security studies conducted by the BSI were also reported to manufacturers. These included vulnerabilities in energy metering systems, industrial control systems, applications and apps in the healthcare and finance sectors, microcontrollers, hardware tokens, blockchain applications and software products.

A total of six 'data troves' were also submitted to CERT-Bund during the reporting period. Such data troves are collections of identity data that is publicly available online and has been discovered by IT security researchers, for example, or by other specialists as part of their research. CERT-Bund analyses these data troves in close consultation with their finders and on the basis of a questionnaire that was developed in-house. An analysis revealed that the six data troves contained outdated data such as passwords which have since been changed. While this data can no longer be used for a direct attack on the affected accounts, it could nonetheless still be used for the creation of highly authentic-looking *phishing* emails.

To ensure the continuous improvement of its analysis and response capabilities, CERT-Bund cooperates nationally and internationally with *CERTs* based in many other countries, companies and other organisations. One benefit of this networking is the ability to respond on short notice to changing situations that cross territorial boundaries and to reach the parties affected by these changes. CERT-Bund is also the central point of contact for incidents relating to IT security in Germany.

Together with the other duties assumed by the BSI in its role as the BSOC and the German Government's centralised situation centre for cyber security incidents, this ensures that attacks are detected and a rapid response can be mounted - even locally (MIRT) when necessary.

2.3.5 National Liaison Office

In the digital era, information security requires a common approach by the Federal Government and states in order to be successful. For this reason, the BSI promotes collaboration between federal and state administrations at various levels. The goal of this enhanced cooperation is to improve the level of cyber security in Germany as a whole.

Following a successful pilot run by National Liaison Office in the Rhine-Main region in 2017, other liaison offices were inaugurated in 2018 and 2019. As of this writing, the National Liaison Office now includes offices in Berlin, Bonn, Dresden, Hamburg, Stuttgart and Wiesbaden and thus has created points of contacts with direct, designated contacts for all 16 states in Germany. The products and services offered by the BSI for target groups in government, industry and society are made available via these offices and therefore information security for the country as a whole.

Collaborative efforts between the BSI and the German states are currently being expanded. In order to do so, the BSI has developed specific areas of cooperation within the field of cyber security. Within these areas, the states can select the kind of cooperation they need - depending on respective requirements - in order to promote their information security together with the BSI. As the cyber security agency on a federal level, the BSI considers cyber security to be a nationwide undertaking and will therefore continue to develop this collaborative approach.

2.3.6 Realization of the Federal Implementation Plan (UP Bund)

The primary goal of UP Bund is the continued improvement of information security in the Federal Administration by means of a monitoring process and a targeted, interdepartmental control system. Progress made in achieving the Federal Implementation Plan (UP Bund) is therefore evaluated on an annual basis. Following the entry into force of the new UP Bund 2017, data collection based on a process-oriented approach was redesigned and completed in the prior reporting period for the first time in this new shape and form.

With the aid of the maturity level methodology selected, concrete measures were first identified and presented on a prioritised basis, so as to effectively and efficiently improve information security in facilities and departments. This partitioning into two areas - the maturity level methodology and the flexible collection of individual (e.g. quantitative) data outside this maturity model - has proven its worth and will be pursued for the 2020 surveys. The reuse of maturity level questions reduces both costs and time requirements while ensuring compatibility between reporting periods. In the flexible model, questions have been adjusted to novel developments and topics in information security (such as Emotet), and the wording has also been optimised as envisaged by the redesign process. Overall, the new execution methodology reduces the time required for information security officers during the survey process. This is aided by a more targeted approach to user support while improving the quality of data collection.

The second UP Bund status quo survey has fully realised the advantages of the redesigned methodology. For the current reporting period, the implementation status for the recommended measures from last year's survey (2019) can now be documented specifically. This also marks the first occasion when different test periods can be compared with one another on the basis of quantitative key figures (maturity/capability levels), so as to fully document successes and unused potential during the implementation. The annual completion of the status quo survey therefore exposes information security trends common to all facilities and departments, which promote the effective and efficient prioritisation, planning and implementation of measures as well as offering long-term support to the goals of UP Bund.

2.3.7 Information Security Consulting

The unauthorised publication of personal data on the internet, which became public in early 2019, was also a point of focus in the second half of 2019 in terms of providing advice to affected parties. The guidance and strategies developed at short notice were and will be continuously amended, expanded and updated, to enable the broadest possible use of these documents. A second point of focus was the provision of advice to the Federal Administration in the context of the new threats posed by *Emotet*.

The information security unit also provided support for major digitalisation projects run by public administrators, including work on implementing the Online Access Act (OZG) and the hardening of electronic legal correspondence. Support was provided to administrative officials in the context of state parliament elections. Providing advice to government agencies and federal administrative departments on ISMS setup, maintenance and improvement continues to be a topic of great importance. One facet of this worth noting is the support provided in the context of larger-scale projects in the Federal Administration and the creation of security concepts. Another

element is the support provided for issues of topical importance - such as the increased incidence of staff working from home during the COVID-19 pandemic.

Steps were also taken to strengthen ties with the Federal Academy of Public Administration (BAköV). Achievements here include a major revision to the manual used for training IT security officers working in public administration: this up-to-date and state-of-the-art edition has now been used for training since the beginning of 2020.

Information security consulting for state/local government

Since about a year the BSI's information security consulting unit for state/local government has provided tailor-made advice to customers at a state and local government level on general questions of information security, with a focus on information security management, security models and IT-Grundschutz.

On the basis of the memorandum of understanding agreed with the German states, an initial set of support projects with various state administrations were successfully conducted and completed. From participation in committees including the Information Security Working Group (AG InfoSic), the IT Planning Council and the ICT Security Commission (part of the Conference of the Ministers of the Interior), an awareness of the local information security situation is maintained on a continuous basis.

Collaboration with local government was also further strengthened by cooperation with municipal umbrella organisations, and further expanded by participation in the ongoing development of shared solution strategies for multi-level procedures, for example.

2.3.8 Smart Borders and Public Sector Identity Management

The goal of the European Smart Borders programme and EU-wide regulations on the interoperability of European IT systems in terms of security, migration and borders is the secure identification and verification of third-country nationals within the Schengen Area. To achieve this, the European Entry/Exit System (EES) and the European Travel Information and Authorisation System (ETIAS) are integrated on a technical level with the Schengen Information System (SIS) for law enforcement, the Visa Information System (VIS) as well as other IT systems at a European level. As a result, identity management for third country nationals is centralised, standardised and uniform throughout the EU.

Alongside digitalisation in the border control process with the introduction of the Entra/Exit System and preliminary checks of submissions to ETIAS - a process every visitor not needing a Schengen visa must complete - it will now be possible to securely identify duplicate or alias identities via facial images and fingerprints from third-country visitors. The possibility of cross-checking with all relevant EU information systems therefore represents the closure of the last loopholes for the misuse of identity. This forms the basis for detecting irregular migration as well as terrorist activities.

Here, the BSI is part of the national Smart Borders project group involving all agencies and spearheaded by the BMI, which provides support to this project with technical specifications and rules for the implementation of a secure identity management process at all levels. Alongside the operative law enforcement agencies at a federal level, Smart Borders will also address the asylum and migration agencies of individual states.

Alongside the technical guidelines for the *authentication* of electronic travel documents in public sector applications, in 2019 the BSI also submitted the first version of TR BSI TR-03156, 'Public sector identity management in conjunction with European registers' for biometric border control procedures. This guideline covers the identity management processes within the Smart Borders project in relation to the new border control systems to be created. This marks the first definition of secure border control procedures while using the new technical facilities at a European level.

In 2019, other points of focus in relation to this work were the drafting of technical criteria for the new EU regulations on interoperability and the revision of the Visa Information System, which is currently ongoing.

2.3.9 Technology Verification in Security Labs

Source code analysis serves to investigate security-critical technologies that are deployed at a federal level or within other sensitive infrastructure in Germany. This analysis aims to provide insights about specific technologies relevant for certain target groups as recommendations for action in the sense of solutions to ensure 'cyber-secure' operations (e.g. in critical infrastructures) and thereby enhance security in general. To do so, the BSI maintains contact with many manufacturers of information and communications technology and deepens the technical level of this dialogue with 'security labs'. These labs serve firstly as a dialogue platform for holding meetings and video conferences with development departments around the globe, and can also be

used to pursue more in-depth technical discussions and achieve insights that extend to perusal of products at the source code level. In this work, BSI employees may also be supported by experts from accredited testing laboratories who specialise in the performance of code audits, for example. Thanks to this close collaboration with development units at manufacturers, trends and risks can be identified at an early stage.

Basis for source code analysis

Source code analysis takes a closer look at sections of code and modules that are relevant for security. An important precondition for any analysis is first to ensure that the code to be analysed is actually deployed in a product. One very reliable method is to compile the code independently, a process that is also known colloquially as 'building' the software. The process is rather like the construction of a house: the source code corresponds to the blueprints for the new property and the 'compilation' is the completed building. While architects can draw certain conclusions about a building from its plans, they will obtain a far better understanding by participating in or supervising the construction product personally. When building a house, external factors such as the tools being used or even the ambient temperature will all have an influence on the final result. The same principles apply to source code analysis: the final compilation is highly dependent on environmental factors such as the time of day, for example, or the software environment used when compiling. To ensure that compilations can be properly classified, however, the BSI works to normalise these factors. The technical jargon for this process is known as a 'reproducible build'. For source code analysis, this method enables a definitive relationship to be constructed between the source text investigated and the code version running on the product. This is ensured using 'checksums', which are generated following a successful compilation process. Typically, this task is reserved for completion by BSI employees, who carry out the build process locally on the manufacturer's premises. Once these checksums have been stored in a database, the operator (e.g. a mobile phone network operator) can later run automated tests to confirm that the software tested is the same software installed on the operator's devices. The procedure used to achieve this is also known as 'remote attestation'.

2.3.10 App Testing for Mobile Solutions

Applications on mobile devices extend the functionality provided by the base system and also play a key role in the success of mobile solutions. However, the deployment of apps does present security risks, both for the security of the processed data and for the security of the overall solution. These security risks must be evaluated in order to be able to make a general statement about the security of a mobile solution.

The app testing service provided by the BSI to federal agencies, which is supplied as part of a partnership with T-Systems, offers an important set of decision-making criteria for those in management positions needing to decide whether to deploy an app and under which conditions. This offers the greatest possible flexibility when deploying additional apps that are popular or required individually. The app tests that are performed take into account issues relating both to security and to data protection. The test reports also include tips and recommendations for end users about the settings or general conditions that should be considered to ensure the app in question can be used as securely as possible.

If necessary in individual cases, the BSI also recommends against the use of an app if the test results justify such a decision.

Government agency app testing users can also access a more wide-ranging repository of historical results for apps already tested, while also being able to initiate new tests as required. Another option is to have apps tested on a continuous basis, so as to ensure that results for any apps previously approved are always up-to-date.

As of this writing (May 2020), the app testing service is now being used by registered users from over 50 government agencies and organisations; test results are available for more than 300 previously tested apps.

2.3.11 Emission Security

When considering threats to the confidentiality of governmental classified information, the manifold security risks and attack methods dominating the public discourse need to be reconsidered with regard to the formidable resources of foreign intelligence agencies. IT hardware used to process classified information has to pass an assessment to verify that no compromising emanations are emitted from these devices. Compromising emanations summarize all electromagnetic effects which are a by-product of IT equipment during operation that, given the proper methods and resources, can be diverted to reconstruct the information being processed. As there are no active defence mechanisms available to fend off this kind of clandestine espionage method, the most effective mitigation is realized by means of prevention.

To ensure emission security of IT hardware used by the Federal Administration and associated authorities BSI has acknowledged a couple of companies with specific expertise who produce equipment enhanced with technical countermeasures against compromising emanations. The effectiveness of these countermeasures is verified by BSI, while in addition public agencies are supported with consulting services and technical on-site inspections for systems with particularly high security requirements. During the reporting period, 653 prototypes for series manufacturing were TEMPEST-approved according to the National Zone Model of BSI and an additional 11 prototypes were approved for the highest emission security class Level A.

2.3.12 Countersurveillance

Alongside the primary function of the BSI's countersurveillance unit - the auditing of departments in federal and state agencies or businesses working with classified information at risk of eavesdropping - the unit also provided technical support to the Federal Network Agency for its auction of 5G spectrum in 2019. The assignment here was to ensure that the bids submitted by network operators remained confidential. Although a major undertaking, this was nonetheless completed successfully without any anomalous incidents.

Conferences were also held at which classified information was discussed. As in previous years, these meetings were supported with consulting and auditing services.

2.3.13 Classified Information Product Approval and Manufacturer Qualification

The BSI issues approvals for IT security products on the basis of sections 51 and 52 of the Classified Information Directive (Verschlusssachenanweisung, VSA). This approval confirms that the products can be used to provide an adequate level of security when protecting classified information in IT systems.

In the current reporting period, the BSI issued or renewed 66 such approvals. Accordingly, the number of approved IT security products or updated product versions increased again to a total of 216. A list of BSI approved products can be found by consulting BSI publication 7164, which is updated on a daily basis.

Apart from processing approval procedures, the BSI approvals unit also organised and hosted a wide range of seminars and information events in order to provide details about the content of the amended VSA, which had been published in August 2018.

For further details about approval and BSI Bulletin 7164, please visit www.bsi.bund.de (cf. *Bibliography*[33]: www.bsi.bund.de).

Developer Qualification

In order to be able to participate in the "Qualified Approval Procedure" for VS-NfD (German classification level similar to RESTRICTED) a developer of IT security products has to undergo a Developer Qualification process successfully. By assessing the suitability of developer processes the BSI confirms that a developer is in general able to manufacture IT security products suitable for approval. Thus, a qualified developer can complete a BSI approval procedure much faster than possible in a conventional approval process. The efficiency of this approach has been confirmed by a large number of cases in which product approval was obtained within four to eight weeks.

Until now, three manufacturers have successfully completed Developer Qualification, while four are currently in the process of doing so.

Classified Information Requirements Profiles

Classified Information Requirements Profiles (VS-Anforderungsprofile, VS-AP) define IT security requirements for IT security products that are subject to approval. These requirements are defined as part of a cooperative process involving governmental users, operators and the BSI. This approach ensures that security requirements are defined by means of an approach that is harmonised, efficient and tailored to clients' needs. A total of 13 finalised VS-APs for various product types and the corresponding range of IT security products that conform to these requirements has now been published. A detailed description and listing of completed and pending VS-APs is available from www.bsi.bund.de (cf. *Bibliography*[34]: www.bsi.bund.de).

Procedure for integrating Common Criteria certification with the BSI approval scheme

Since threat scenarios are constantly changing and product development cycles are steadily becoming shorter it is now a major challenge to provide the consumer with approved IT security products. To address these difficult circumstances, the existing approval scheme must be improved on a continuous basis and enhanced by incorporating innovative methods and instruments.

Supplementing the "Qualified Approval Procedure" (cf. *Bibliography*[35]: www.bsi.bund.de), which has already been integrated into the BSI approval scheme with great success, the BSI is now working on the efficient integration of Common Criteria certification results.

Currently this approach is subject to a validation period, that aims to find synergy effects for products previously certified by the BSI according to the Common Criteria and that shall now be approved. This means that the evaluation results obtained as part of the successful common criteria certification can be reused as much as possible during approval. This is possible because of the fact that the evaluation approach in both schemes (Common Criteria Certification and Classified Information Product Approval) is based on very similar concepts. As a result, only the aspects that go beyond the scope of a Common Criteria (CC) certification need to be evaluated. Compared to the process of completing a conventional approval procedure the integration procedure guarantees the same level of assurance while saving a significant amount of resources for all parties involved.

A number of promising initial trials of the procedure have now been completed and the procedure is likely to be incorporated into the BSI approval scheme before the end of the year.

Objective: CI strategy

To be considered a success, a forward-looking innovation strategy for the CI product market must ensure the faster provision of more approved CI solutions that meet clients' needs. To achieve this, clearly defined action areas are used to decide about prioritising CI requirements and corresponding product developments, all while leveraging synergies by focusing on the shared use of resources across organisations.

The effective and efficient achievement of these goals is assured by the regular bi- and multi-lateral consultations held among key stakeholders in the approval scheme. In particular, these stakeholders include operators and governmental customers, manufacturers and integrators of CI products, testing laboratories, the BMI and the BSI. These parties deploy their resources together to ensure that the main focus of their activities is shifted from what is at least partially a reactive position to a largely proactive shaping of the CI product market.

These bi- and multi-lateral consultations among the stakeholders are conducted on a variety of platforms known as 'innovation forums'. The annual Omnisecure Congress in Berlin also plays a central role in this future CI strategy. Since 2018, the BSI has increasingly promoted issues relating to CI as a main point of focus of this congress, and it has thus evolved into 'the' meeting-point and flagship event for CI and CI product approvals.

As a result, the congress now gives interested delegates the opportunity to learn more about the current state of play and the initiatives and projects planned in the field of classified information and CI product approvals. The BSI also invites interested parties to participate actively in shaping the future orientation of the CI strategy as part of workshops focused on specific topics, presentations by and for stakeholders, multi-lateral discussion and information panels, as well as bi-lateral talks.

Alongside the considerable interest shown in these CI forums, the success of the CI strategy adopted, and the format used can also be seen in the growing number of stakeholders who now participate in the approval scheme. This applies to both the ever-increasing number of presentations related to CI and the growth in exhibitors focusing on CI topics.

2.3.14 Implementation of the Online Access Act: Components for the Secure Digitalisation of Administrative Processes

Following its entry into force in 2017, the German legislation to improve online access to administrative services (Online Access Act, OZG) requires federal and state administrations to extend their service provision to digital administration portals and link these together into a portal network by 2022. To be able to make use of these services, it is essential that end users - such as private citizens and businesses - be able to securely identify and authenticate themselves online by means of the user accounts prescribed at the federal and state level by the OZG.

Criteria for the secure integration of identification and authentication procedures with these user accounts are set out in BSI Technical Guideline TR-03160, 'Service Accounts'. This guarantees the identity of users at the respective level of assurance for the administrative procedures connected to these user accounts without requiring the procedures to know the exact details of this identification and *authentication*. In addition, TR-03160 defines criteria for ensuring the interoperability of federal and state solutions to ensure that users only need to complete the identification procedure in one state before being able to utilise the services of a different state or services provided at a federal level.

The service accounts provide mailboxes for the electronic delivery of the official documents created by the administrative procedures. The corresponding criteria that need to be developed will be incorporated into TR-03160 to ensure the interoperability of the various mailbox solutions.

Cryptographically secure barcodes can be attached to official documents so that checks to confirm their integrity can be made even if they are submitted as printouts or displayed on mobile devices. These kinds of digital seals conforming to BSI TR-03137 are already being used on public-sector documents such as proofs of arrival to verify that the printed data is indeed genuine. An amendment to TR-03137 already in preparation will then permit the same process to be applied to deeds, notifications and other official documents.

2.4 International Affairs

Neither IT security nor current threats in cyberspace are issues that heed national borders. To address them effectively, it is necessary to concentrate efforts at the international level. This is why the BSI works with various partners both bi-laterally and in committees. In Europe and elsewhere around the world, the BSI's experts are sought after for their expertise and advice. One reason for this is the BSI's conviction that cyber security in Germany is significantly strengthened by international collaboration and the global marketplace of ideas.

2.4.1 International Activities of the BSI

Since its formation nearly 30 years ago, the BSI has viewed international collaboration as an essential instrument for the improvement of cyber security. Complementing its national role as the cyber security agency for the German Government, the BSI also aims at shaping international developments in the field while strengthening its own competencies in technological assessment. To properly account for its responsibilities in this context, the BSI intensifies and expands its relationships with international agencies, organisations, companies and key actors in research and civil society on a continuous basis. Participation in various expert committees addressing information and cyber security in the context of the EU, NATO and other international areas therefore forms an important part of the BSI's international engagement.

A key milestone in its European collaboration was the Cyber Security Directors' Meeting initiated, organised and hosted by the BSI at the beginning of the year. For the first time, this meeting provided the heads of Europe's cyber security agencies with the opportunity for an exclusive exchange in the run-up to the Munich Security Conference.

Beyond this, the BSI is especially engaged in strengthening and expanding its bi- and multi-lateral partnerships with cyber security agencies, whereby special focus is currently being placed on the topic of security of 5G networks. As cyber security agency for the German Government, the BSI also has an important role to play both within and vis-à-vis NATO. In pursuing its vision of helping to ensure a high level of cyber security worldwide, the BSI is also supporting an EU project to establish cyber security capacity in the EU Eastern Partnership countries.

2.4.2 EU-wide Recognition of the German eID

As part of the continuing digital transformation, electronic identities (eIDs) and the associated electronic identification of both people and things are rapidly gaining in importance. Secure electronic identities are the only way to achieve sustainable success in preventing identity theft. In order to expand the reach of secure national eIDs and with regard to the digitisation of the European Single Market, the eIDAS regulation established a uniform framework for the mutual recognition of electronic identification means and trust services at the EU level already in 2014.

With strong involvement of the BSI, Germany has successfully completed the notification procedure of the Germen eID already in 2017 and is the first member state to have a notified eID that must be recognised within the EU/EEA. The notification of the German eID at the highest level of assurance according to the eIDAS Regulation was published in the Official Journal of the EU in September 2017. On this basis, the mutual recognition obligation has been in effect since September 2018. Since this time, all EU/EEA Member States that operate corresponding online services must recognise and integrate the German eID in their public-sector applications - and therefore in the e-government in particular.

As a result, 18 countries (Austria, Belgium, Denmark, the Czech Republic, Estonia, Finland, Greece, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Slovakia, Slovenia, Spain, Sweden and the United Kingdom) and the European Commission had already successfully integrated the German eID into their own eID schemes by April 2020, with technical support provided by the BSI. Consequently, it is already possible to use the German eID (just as it is the case in Germany) for online services in over half of all the other EEA member states. While not all remaining member states operate corresponding online services and are therefore exempted from the recognition obligation, eight other countries (as of May 2020) are now running systems or are preparing to run pilot systems. Thus, further growth in coverage is to be expected in the near future.

Other countries are also making efforts to have eID schemes notified. By the end of April 2020, a total of 13 other countries had done so (Belgium, Croatia, the Czech Republic, Denmark, Estonia, Italy, Latvia, Luxembourg, the Netherlands, Portugal, Slovakia, Spain and the United Kingdom). Other notification procedures are currently ongoing or nearly finished. The BSI is also contributing its technical expertise to these procedures.

The eID schemes in the various countries differ in parts widely from one another. While many of the eID systems assessed do in fact use national chipcard-based ID documents, others are based on the use of certified SIM cards or other hardware- or software-based security features of devices. Some of these solutions are also based on the use of 'identity providers' that are partly organised as private sector companies and offer multiple types of identification means (based on the use of a mobile app, SMS-OTP, etc.).

These various approaches naturally lead to a range of different assessments in the context of the peer reviews conducted during the notification procedure. While the chip card-based eID schemes are generally assessed with the highest level of assurance, systems based on the use of video identification or SMS-OTP are assigned with only a substatial level of assurance. App-based solutions represent a special case as their assessment depends heavily on the security features offered by the mobile device itself.

The notified electronic identities will be integrated into the German e-government and thereby recognised by citizen portals as part of the implementation of the Online Access Act (Onlinezugangsgesetz). As part of this work, the Federal Citizens' Portal (Bundesportal) is planned for launch in mid-2020.

2.5 Other Developments in IT Security

With each and every technological advance, new security questions arise that require adequate answers. For this reason, the BSI engages in many different ways with universities and other research establishments. One important topic is artificial intelligence - not least because it gives rise to security-relevant questions from a number of different angles. Cryptography is another important subject area. The pace of development in quantum computing is raising serious questions about the security of our digital infrastructure, which is currently dependent on the use of cryptographic procedures. Nevertheless, what does quantum cryptography truly have to offer, and what is the current state of play in quantum computing? The BSI is working with its partners on answers to all of these questions.

2.5.1 Artificial Intelligence

Methods of artificial intelligence (AI) show amazing performance in many application areas, such as object recognition on images. They are increasingly used in areas that affect our everyday lives. The topic is becoming ever more important for our society, the industry and the state. Accordingly, the topic of AI is a key point of focus for the BSI.

Security of AI systems

Despite significant progress in research, important aspects of AI-based systems, such as their robustness and reliability, their transparency, the ability to explain their decision-making as well as non-discrimination, are still not sufficiently understood. The BSI sees a need for action, especially with regard to establishing reliable security features. In the Federal Government's AI strategy, these are also considered essential for acceptance in industry and society. In comparison to conventional IT systems, new types of *attack vectors* exist in AI systems: by manipulating training or input data, systems can often be fooled into making incorrect decisions. Even slight changes that are hard to detect, and possibly not even directly recognisable as such by humans, can have serious consequences. Another example is that under certain circumstances the output from AI systems may allow conclusions to be drawn about potentially confidential training data.

During the reporting period, the BSI supervised the work of a number of research students and interns looking at attacks on AI systems and potential countermeasures. On top of that, the BSI published a systematic overview (cf. *Bibliography*[36]: http://arxiv.org) of selected AI models regarding their vulnerability and options for hardening.

Alongside the analysis of security properties, the ability to prove that these properties are in fact present is a crucial part of any kind of verification process. During the reporting period, BSI worked with various partners on the development of audit criteria and methods for AI applications in a number of domains, with a particular focus on automotive and *cloud* services.

These activities will be expanded in the future and brought together in a larger framework: The German Institute for Standardisation (DIN) is working on a roadmap for standards in the field of AI on behalf of several federal ministries, with BSI playing a major role with regard to security aspects. In particular, BSI makes decisive contributions to shaping a rollout plan for this roadmap. Over

the next few years, the plan aims to establish a broadly based national programme with the involvement of relevant stakeholders in order to develop, test and introduce audit standards for a large number of AI application domains.

Accompanying this, BSI was represented in a number of other relevant working groups during the reporting period, including the Platform for Learning Systems (cf. *Bibliography*[37]: www.plattform-lernende-systeme.de) and the ETSI Industry Specification Group Securing Artificial Intelligence (cf. *Bibliography*[38]: www.etsi.org). It also participated in the preparation of publications (cf. *Bibliography*[39]: www.plattform-lernende-systeme.de) as part of this work.

Manipulating media with AI

AI-assisted methods are now increasingly used for media manipulation. While counterfeiting media without the use of AI is typically restricted to static content (images and text) and requires considerable time and money, the use of AI makes it possible to carry out forgery attacks on dynamic media content - including faces and voices in video and audio streams - that can produce deceptively realistic results under certain circumstances. The various techniques are commonly and collectively referred to as 'deep fakes'. Attackers can use these methods to fake false identities, for example, in biometric authentication procedures in video conferences or in media files shared via social media. During the reporting period, the BSI supervised a number of master's theses in this subject area, which dealt with the detecting of these kinds of manipulations.

Use of AI in cryptography

In the reporting period, the BSI continued to deal with the use of AI methods in cryptography: The focus of the investigations conducted throughout this time was on mathematical cryptanalysis (cf. *Bibliography*[40]: www.link.springer.com) and side-channel attacks (cf. *Bibliography*[41]: https://eprint.iacr.org). A key aspect of these investigations was the comparison of AI-assisted attacks with conventional attacks, which revealed a slight superiority of the AI-based methods in the scenarios considered. The results obtained will be applied to evaluation procedures for product certification and admission in order to assess cryptographic algorithms and their implementations.

2.5.2 Cryptography

The security of our digital infrastructure is fundamentally dependent on cryptographic methods. Specifically, modern digital communication involves encrypting messages with a cryptographic key that has typically been agreed on beforehand using a *public key* system. The security of this key agreement process is based on the assumed difficulty of solving certain mathematical problems. As one example, the security of the widespread RSA algorithm, which is used to both encrypt and sign messages, is based on the fact that finding the prime factors of very large integers is a virtually impossible task.

With the tools available today, the common *public key* systems cannot be broken. However, this will no longer apply once quantum computers with sufficient capabilities are available. In recent years, huge progress has been made in the development of quantum technologies (cf. *Quantum Computers: The State of Play*, page 76), which means that point in time is now virtually upon us.

As an alternative to traditional *public key* systems such as RSA, methods are now being developed and standardised that will presumably be unbreakable even for an attacker using a quantum computer (post-quantum cryptography). These quantum-resistant methods are based on mathematical problems for which neither conventional nor quantum algorithms are known to provide an efficient solution.

Some initial quantum-resistant methods for key transport are already recommended in BSI Technical Guideline TR-02102. It should be noted, however, that these methods are still undergoing standardisation and are primarily intended as initial recommendations for protecting data with long-term protection needs. The BSI has also published some initial recommendations on migrating to post-quantum cryptography, which can now be implemented to counter the threat presented by quantum computing.

An alternative approach to post-quantum cryptography is quantum cryptography itself, and quantum key distribution (QKD) in particular. The promise of quantum cryptography lies in how it offers security based on the fundamental laws of nature. BSI will prepare a protection profile to evaluate QKD products according to Common Criteria, and will further investigate the theoretical and practical security offered by QKD.

Developments in quantum cryptography are being funded by the QuNET project run by the Federal Ministry of Education and Research (BMBF). An initial prototype of a link for quantum-resistant key exchange between the BMBF and the BSI is scheduled to be presented to the public in a demonstration planned for autumn 2020. The

QuNET Consortium, BMBF and BSI are now working hard on preparations for this demo. The BSI is also a participant in Q.Link.X, a joint project run by a cluster of research institutions and businesses in Germany that aims to lay the groundwork for quantum repeaters (and therefore quantum networks).

Building on the BSI's previous blockchain technology position paper, this provided developers and potential users of blockchain solutions with tools to fully assess the opportunities and risks and take IT security into account from the outset. Examples were also included to illustrate various aspects, such as long-term security.

Quantum Computers: The State of Play

To obtain a sound assessment of the current state of development and the potential future availability of quantum computers, the BSI commissioned a study entitled 'The State of Quantum Computing' from researchers at Saarland University (Germany) and Florida Atlantic University (USA). The study examines current technological approaches and quantum algorithmic innovations in detail and discusses their implications in the context of cryptography currently in use. In 2019, a first revision to the study has suggested that recent algorithmic and technological advances (in error correction, for example) have the potential to reduce the number of physical quantum bits (qubits) required for a specific task. A second revision will be published in 2020. The study, together with an executive summary, can be downloaded from the BSI website at https://www.bsi.bund.de/qcstudie (cf. *Bibliography*[42]: www.bsi.bund.de).

Organisations in the realms of research and industry are also working on quantum random-number generators. Here, the BSI is cooperating with the Fraunhofer Institute for Applied Optics and Precision Engineering (Fraunhofer IOF) in work-shops and in-depth consultations to establish a starting point for the security evaluations of such generators.

2.5.3 Blockchain

Blockchain remains a hotly debated topic in the field of information security. As with all new technologies, security should be considered from the outset with *blockchain*, and a security-by-design approach should also be pursued. This prompted the BSI to publish a position paper on *blockchain* security in early 2018, thus initiating a public discussion.

In spring 2019, the BSI then published a comprehensive document entitled 'Designing Secure Blockchains: Concepts, Requirements and Assessments'; an English version of this document was also published in December 2019.

Due to the particular significance of data protection in the context of blockchain technology, the BSI is also working on this subject with the Federal Commissioner for Data Protection and Freedom of Information. This work has involved discussions of the rights of data subjects as formulated in the EU GDPR - to rectification, erasure and data portability, for example - in the context of blockchain technology.

At the same time, the BSI also commissioned a market surveillance report on blockchain applications before having select products from various product classes evaluated as examples of this technology. The main findings of this study were published in May 2020 (cf. *Bibliography*[43]: www.bsi.bund.de)

All of the materials published by the BSI about blockchain as a technology are available as downloads from the BSI website (cf. *Bibliography*[44]: www.bsi.bund.de).

3 Summary

3 Summary

A tailwind for digitalisation - a long-term strategy for information security

SARS-CoV-2, COVID-19 or just 'the coronavirus': these terms have been on everyone's lips over the last few months. The pandemic was the defining event for the first six months of 2020, with no end in sight at the time this report went to press. Its many and varied effects continue to have a considerable impact on government, industry, civil society and each and every one of us in Germany, Europe and the world. Apart from all of the related medical and epidemiological issues, however, the coronavirus crisis has given a considerable boost to digitalisation in Germany and provided a striking example of how well-functioning and secure information technology is the very lifeblood of our contemporary society. Without online collaboration, videoconferences and chats, digital business processes, online shopping, video streaming and the opportunity to work from home, the effects of the pandemic on the industry and civil society, while indubitably serious, would likely have been even worse.

Many people - and many businesses, as well, including SMEs in particular - had to reorganise their established processes in a very short time and adjust them to entirely novel conditions. In private life, people often used video chat services to remain in regular contact with family and friends. Many companies took innovative and creative approaches to exploiting the options offered by information and communications technology by opting to digitalise their processes and offer their products and services in a digital format. It is also refreshing to see that these efforts did not include information security merely as an afterthought. Not least because of the long-standing efforts in education and awareness on the part of the BSI, many private and professional users alike were keen to use innovative solutions that are practical, usable and secure. The public debate about the German 'Corona Warn App' offers a good example of how data security is now seen to be both important and relevant - and a necessary precondition for ensuring effective privacy. This tailwind for digitalisation must now be exploited in order to accelerate developments in this area in the post-COVID era.

Functional and secure IT enables concentration on core business

Over the last few years, the digital transition has been particularly important within the healthcare sector. Healthcare processes were becoming increasingly digitalised even before the coronavirus struck. Many hospitals and medical doctor's practices are digitalised and utilise the options provided by modern IT medical devices in order to make both diagnosis and treatment more effective, more efficient and more tolerable for patients. For both doctors and nursing staff, the primary objective is to save lives, cure the sick and provide the best care possible to their patients. Accordingly, they should not have to worry about whether the ward PCs are working or whether security updates need to be installed on a medical device or the computer used to control a heart-lung machine. Secure, available and well-functioning information technology creates an environment in which medical personnel can carry out their various duties. This naturally applies in the same way to any other profession. Yet the (partially) successful cyber attacks targeting hospitals and the regular reports of vulnerabilities found in medical devices indicate that work still has to be done in some areas to achieve comprehensive protection for these technologies. The importance of information security in ensuring the success of digitalisation becomes very clear when human lives are at stake. One can easily imagine the consequences of a successful cyber attack on a hospital that is already stretched to its limit by the enormous stresses of the coronavirus pandemic. Even before COVID-19, the BSI had thus launched a number of initiatives and specific, practice-oriented support measures intended to further improve the safeguards in place in the healthcare sector (cf. chapter *Civil Society*, page 39).

The essential contribution made by information security to the success of digitalisation projects applies not only to healthcare, but also to other areas of the industry, as well as critical infrastructures. In the 2015 German IT Security Act and a wealth of recommendations and implementation guidance from the BSI, the Federal Administration has created the legislation and conditions needed to ensure the secure operation of critical infrastructures. CI operators must implement appropriate security measures to provide state-of-the-art protection to their IT systems, components and processes, and provide proof of this to the BSI every two years. An analysis of the evidence submitted to the BSI reveals a mixed picture: while some CI segments are well positioned, there is still room for improvement in others (cf. chapter *Threat Landscape for the Industry – with a Focus on Critical Infrastructures*, page 51). Overall, however, the IT Security Act has clearly been successful in improving information security within the critical infrastructures that is so important for the wellbeing of our society.

Flexible responses to a dynamic threat landscape

The coronavirus crisis provides a good example of the importance of flexibility and pragmatic problem-solving in the field of cyber security. COVID-19 has certainly demonstrated how adaptable cyber criminals are and how the threat landscape changes to match. The BSI observed an increase in cyber attacks including references to the coronavirus against both companies and private citizens. One example were the broad-based waves of spam offering fake advice about the coronavirus. These mails encouraged company employees to disclose personal or company-related details on replicas of official websites. The cyber criminals designed these to resemble the (government) institutions handling applications for emergency assistance funds. Other criminal activities included setting up fake online shops to exploit the rise in demand for protective clothing or face masks.

The underlying methods and tactics have been observed before. Even before the current pandemic, these types of attacks were used with other 'hot topics' to hook prospective victims. In the context of the coronavirus, however, these attacks demonstrate how important it is to keep users aware of the tactics used and give them the tools they need to shield themselves better as part of digital consumer protection. Even so, this only gets us halfway: at the same time, the digital industry must take care to ensure that new technologies, products and services are designed to be secure as part of their development and that they remain secure when placed on the market. At the moment, consumers have no means of recognising how 'cyber-secure' a product actually is. To enable them to do so in the future, the BSI is working with other federal agencies and business partners to develop the IT Security Mark (cf. chapter *The IT 'Security Mark' – Reassurance for Consumers*, page 41).

The BSI is therefore helping on both sides of the equation: while consumers benefit from the information services and practical recommendations it offers, the BSI is also providing companies with an appropriate package of support by defining minimum requirements, publishing technical guidelines and offering opportunities for certification. In relation to Common Criteria certification alone, the BSI completed just under 100 product and site certifications in the current reporting period.

The BSI adapts to the dynamic threat landscape and helps users in government, the industry and civil society to mount rapid and effective responses. In the context of COVID-19, for example, the BSI worked quickly to publish a comprehensive set of advice and recommendations tailored to various groups, which helped internet users and companies alike to protect themselves effectively against cyber attacks and attempted fraud.

The BSI will continue to make such recommendations 'post-COVID'. New kinds of attacks will again be attempted and again require a flexible and effective response. Cyber attacks featuring *ransomware* have continued unabated during COVID-19 and will continue to be a threat for businesses and government agencies in particular once the pandemic is over. Multi-staged attacks (using the Emotet malware, for example) were a particular source of problems - some very serious - for government and businesses up until the end of 2019. At the beginning of 2020, other types of malware were then also deployed, with comparably harrowing consequences for their victims. This threat situation will persist as long as this criminal business model remains lucrative for perpetrators. For its part, the BSI will continue to take appropriate steps in prevention, detection and response while providing support to those affected.

Digitalisation 'Made in Germany'

Other topics in information security will also return to the public eye or remain the focus of public debate 'post-COVID', such as artificial intelligence, 5G, networked and autonomous driving or secure smart homes.

As digitalisation maintains its rapid tempo, the challenge here is to keep pace with this dynamic process and help to shape it - especially in the context of information security. The BSI is pursuing a cooperative approach and making its expertise and experience available to all actors within government, the industry and civil society - regionally, nationally and internationally. However, this approach must indeed be collaborative and not a one-way street. Wherever insights are gained, in whatever institution or organisation that may be, they must be shared responsibly in order to strengthen cyber defences and raise awareness within society about the persistent threats from cyberspace. This makes information security a defining quality of digitalisation 'Made in Germany', which Germany can utilise to strengthen and develop its position within international markets both during and after the coronavirus crisis.

The work of the BSI makes an important contribution to securing the path each of us takes to enjoying the benefits of a digitalised society. Thanks to the BSI's wide range of targeted operational activities, supportive partnerships, forward-looking guidelines and guidance aimed at raising awareness, Germany has become much more cyber-secure over the last few months. This is not to say that we should rest on our laurels. With new vulnerabilities, new types of vectors and the growing complexity of infrastructure, the threat landscape remains both dynamic and perilous, with the potential for harrowing consequences for companies, government agencies and individuals. Dynamic

situations require a dynamic response, and Germany is not helpless in the face of these challenges. In a modern high-performance PC, efficient multi-core processors, fast SSD storage and purpose-built software come together to produce a powerful and capable tool. In the same way, the BSI's experts are drawn from a wide variety of disciplines to work together on the most important digital topics of our time. Together, we at the BSI are guiding Germany towards a secure digital transition.

4 Glossary

Advanced Persistent Threats
An advanced persistent threat (APT) is a targeted cyber attack on select institutions and organisations in which the attacker gains persistent (long-term) access to a network and then propagates the attack to other systems. These attacks are characterised by a high level of resource deployment and considerable technical skill on the part of the attackers. The attacks are generally difficult to detect.

Adversarial Attack
A scenario in which an input image is deliberately modified by a potential attacker in order to fool a neural network. Adversarial images are pictures and objects intentionally designed to fool the computer's perception. They contain certain structures and patterns placed over the actual image or object that work to trick the system. These patterns are not visible to the human eye, however. An image that looks like a tortoise to a human might be classified as a house to an AI system, for example.

Attack Vector
An attack vector is a combination of attack practices and techniques used by a perpetrator to gain access to IT systems.

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

Authentification
An authentification process is a procedure to verify the identity of a person or a computer system by means of a particular attribute. It may be based on password entry, a chip card or biometrics, for example.

Authentication
Authentication refers to the process of proving authenticity. Amongst other means, an identity can be authenticated based on a password, a chip card or biometrics. The authentication of data can be carried out using cryptographic signatures, for example.

Backdoor
A backdoor is a program typically installed by a virus, worm or Trojan that grants third parties unauthorised access to a computer but remains concealed and bypasses typical security defences.

Backup
A backup involves the copying of files or databases to physical or virtual systems at a different storage location. These resources are kept in this separate location in order to restore the system in the event of a device failure or some other catastrophic incident.

Bitcoin
Bitcoin (abbreviation: BTC) is a digital currency, or ‚cryptocurrency'. Payments are made between pseudonymous addresses, which makes identifying the parties to a transaction considerably more difficult.

Blockchain
Blockchain describes a distributed, synchronised, decentralised and consensual storage of data in a peer-to-peer network. A hash-chained list of data blocks is maintained in all network nodes redundantly and updated by means of a consensus mechanism. Blockchain is the technological basis for cryptocurrencies such as Bitcoin.

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

CEO Fraud
The term 'CEO fraud' refers to social engineering attacks that target corporate employees. In such attacks, perpetrators use identity data acquired previously (phone numbers, passwords, email addresses, etc.) to impersonate a CEO, company president or similar individual and trick employees into paying out large sums of money.

CERT/Computer Emergency Response Team
A CERT team is a team of IT specialists. CERTs have been established in many companies and institutions to handle defence against cyber attacks, respond to IT security incidents and implement preventive measures.

CERT-Bund
CERT-Bund (Computer Emergency Response Team for Federal Agencies) is located within the BSI, where it functions as the central coordinating body for federal agencies for both preventive and responsive measures regarding security-related incidents that affect computer systems.

Cloud/Cloud Computing
Cloud computing denotes the on-demand provision, use and billing of IT services via a network. These services are offered and used solely by means of defined technical interfaces and protocols. The range of services offered within cloud computing covers the entire spectrum of information technology, including infrastructure (such as computing power and memory), platforms and software.

Digital Nudging

The term 'digital nudging' refers to the subtle and casual exertion of influence on human behaviour with the intention of encouraging consumers to act in both their own interests and the interests of society as a whole. The idea is that consumers should be influenced to make better decisions without taking away their freedom to choose or decide for themselves and without dictating a particular path they should follow. The ultimate goal is to help consumers take better and more conscious decisions - in choosing products with better information security features, for example.

DoS/DDoS Attacks

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

Drive-by Download/Drive-by Exploit

The term 'drive-by exploit' refers to the automated exploitation of vulnerabilities on a PC. The act of viewing a website, without any further user interaction, is sufficient to exploit vulnerabilities in a web browser, additional browser programs (*plug-ins*) or an operating system and thereby covertly install malware on the PC.

Exploit

An exploit refers to a method or a piece of program code that can be used to execute unintended commands or functions via a vulnerability in hardware or software components. Depending on the type of vulnerability, an exploit can be used to crash a program, elevate privileges for an account or execute arbitrary program code, for example.

Firmware

Firmware is software that is embedded in electronic devices. Depending on the device, firmware can offer operating system or application software functionality. Firmware is specifically adapted to the respective hardware and is not interchangeable.

Internet of Things/IoT

The Internet of Things (IoT) is a term used to describe objects equipped with information and sensors that are capable of collecting, processing and storing data from the physical and virtual worlds, and which are networked with one another.

Malware

Malicious functions, malicious programs and malicious software are all synonymous with 'malware'. An abbreviation of the phrase 'malicious software', malware refers to software designed specifically with the goal of executing unwanted and typically harmful functions. Examples of malware include computer viruses, worms and Trojans. Malware is usually designed for a specific operating system version and is therefore most often written for widely used systems and applications.

Morphing

Morphing is a digital image processing technique used to merge several images into a single picture. This technique can be exploited by attackers to combine facial images from several people into a new facial image (the 'morph') that represents a mixture of the facial features of all of the people merged into the morph image. These morphed images can be used by attackers as a reference image when applying for an ID document (such as a passport), for example. Typically, ID documents that contain a morphed image as a reference image can then be used for authentication by all of the individuals that were included in the morph.

Patch/Patch Management

A patch is a software package that software manufacturers use to resolve security vulnerabilities in their programs or implement other improvements. Many programs offer an automated update function to make the installation of these patches 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 phishing attacker attempts to access the personal data of an internet user via bogus websites, emails or messages and to misuse this data for their private purposes, usually at the victim's expense.

Phishing Radar (NRW Consumer Advice Centre)

Since 2010, the Consumer Advice Centre for North Rhine-Westphalia has analysed fraudulent email that consumers forward to the Phishing Radar (phishing@verbraucherzentrale.nrw). On the basis of its daily haul of 200–300 emails - which include phishing, advertising and other types of cyber crime - the centre posts warnings about the latest scams on its website, Twitter and Facebook. In autumn 2017, it began a partnership with the BSI, with one particular aim being the advanced statistical (anonymised) analysis of this data.

Plug-in

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

Potentially Unwanted Application (PUA)

Application software (often distributed as bundled software) that cannot be classified definitively as malware. While PUAs will typically have been installed by the user, they then exhibit unexpected behaviour or covertly execute certain functions that could be construed as undesirable. These include collecting and sharing information on user behaviour or displaying advertising banners.

Provider
A service provider that can act in a number of roles. One role is as a network provider that makes infrastructure available for data and voice traffic as a mobile network provider, internet service provider or carrier. Alternatively, a service provider may offer services that go beyond network provision, such as in the operation of networks within an organisation or the provision of social media.

Public Key Cryptography
Public key cryptography, also known as asymmetric encryption, always involves the use of two complementary keys. The public key is used to encrypt the message, while the other - the private key - is used for decryption. Together, the two keys form a key pair.

Ransomware
Ransomware refers to malware that restricts or prevents access to data and systems and only releases (unlocks) these resources upon payment of a ransom fee. Ransomware is an attack on the availability of a security target and is therefore a form of digital extortion.

Resilience
In the context of this report, 'resilience' refers to the capability of IT systems to resist security incidents or attacks. The resilience of systems results from the complex interplay of organisational and technical preventive measures, such as the deployment of qualified personnel, the IT security budget in question and the available technical infrastructure.

Responsible Disclosure
The term 'responsible disclosure' refers to a procedure in which the manufacturer of a product is first provided with a detailed report after the discovery of a product vulnerability. This gives the manufacturer the opportunity to develop countermeasures - in the form of product updates, for example - before the information that is required to exploit the vulnerability is released into the public domain. Typically, the manufacturer is given a fixed time frame (usually a few months), after which details of the vulnerability will then be disclosed.

Security by Default
A product delivered according to the principles of security by default is already secure in its out-of-the-box state and needs no further configuration in this respect.

Security by Design
The principles of security by design mean that information security requirements have already been met during product development.

Side-channel Attack
An attack on a cryptographic system that exploits the results of physical measurements made on the system (such as energy consumption, electromagnetic radiation or operation runtime) in order to derive insights into sensitive data. Side-channel attacks are highly relevant for the practical security of information processing systems.

Sinkhole
A sinkhole is a computer system to which queries from botnet-infected systems are redirected. Sinkhole systems are typically operated by security researchers in order to detect botnet infections and inform 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 personal systems. In terms of both cybercrime and espionage, the attackers are skilful at exploiting perceived human weaknesses such as curiosity or fear in order to gain access to sensitive data and information.

Spam
Spam refers to unsolicited messages sent by email or other communication services to a large number of people in a non-targeted way. Harmless spam messages generally contain unsolicited advertising. Often, however, spam is also sent with attachments containing malware or links to infected websites, or is utilised to conduct phishing attacks.

Two-Factor or Multi-Factor Authentication
In two- or multi-factor authentication, an identity is authenticated by means of various authentication factors that are taken from separate categories (knowledge, possession or biometric attributes).

UP KRITIS
The CI Implementation Plan (www.upkritis.de) is a public-private partnership between critical infrastructures (CI) operators, their associations and government agencies such as the BSI.

VPN
A virtual private network (VPN) is a network physically operated within another network (often the internet), but 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. While the term 'VPN' is often used to refer to encrypted connections, other methods can also be used to secure the transport channel, such as special functions that are available in the transport protocol used.

5 Bibliography

1 https://www.bsi.bund.de/EN/Publications/SecuritySituation/SecuritySituation_node.html
2 https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/BotNetze/Avalanche/BotNets/FAQs/botnets_faq_node.html
3 https://www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar
4 http://www.heise.de/newsticker/meldung/Microsoft-leakt-250-Millionen-Eintraege-aus-Kundendatenbank-4644161.html
5 https://www.greenbone.net/wp-content/uploads/CyberResilienceReport_EN.pdf
6 https://www.trustedsec.com/blog/netscaler-honeypot/
7 https://deyda.net/index.php/en/2020/01/15/checklist-for-citrix-adc-cve-2019-19781/
8 https://dcso.de/2020/01/16/a-curious-case-of-cve-2019-19781-palware-remove_bds/
9 https://www.fireeye.com/blog/threat-research/2020/01/vigilante-deploying-mitigation-for-citrix-netscaler-vulnerability-while-maintaining-backdoor.html
10 https://msrc-blog.microsoft.com/2019/08/13/patch-new-wormable-vulnerabilities-in-remote-desktop-services-cve-2019-1181-1182/
11 https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2019/DejaBlue-Schwachstelle_140819.html
12 https://www.link11.com/en/blog/threat-landscape/link11s-2019-ddos-report-reveals-complexity-and-volume-of-attacks-continues-to-grow/
13 https://www.cl.cam.ac.uk/~sp849/files/RAID_2018.pdf
14 https://www.datensicherheit.de/aktuelles/netscout-cybersicherheitsreport-herausforderungen-unternehmen-30345
15 https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Dienstleistungen/Qualifizierte_Dienstleister/QDL_node.html
16 https://shattered.io
17 https://sha-mbles.github.io
18 https://minerva.crocs.fi.muni.cz
19 https://tpm.fail
20 https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Checklisten/checklisten_node.html
21 https://www.bundesregierung.de/breg-en/issues/wirksam-regieren-with-citizens-for-citizens/protection-of-online-accounts-1736000
22 https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/Digitale_Gesellschaft/IdgD/IdgD_node.html
23 www.bsi-fuer-buerger.de
24 https://www.bsi.bund.de/DE/Themen/KRITIS/Allgemeines/Stand_der_Technik/Uebersicht/Uebersicht_node.html
25 https://www.bsi.bund.de/DE/Themen/KRITIS/Allgemeines/Stand_der_Technik/Orientierungshilfe/Orientierungshilfe_node.html
26 https://www.kritis.bund.de/SubSites/Kritis/EN/activities/national/cipimplementationplan/cipimplementationplan_node.html
27 https://www.bsi.bund.de/EN/Topics/Certification/certification_node.html
28 https://www.commoncriteriaportal.org
29 https://www.bsi.bund.de/DE/Presse/Kurzmeldungen/Meldungen/Empfehlungen_mobiles_Arbeiten_180320.html
30 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/empfehlung_home_office.pdf
31 https://www.bsi.bund.de/DE/Presse/Kurzmeldungen/Meldungen/KoViKo_140420.html
32 https://www.allianz-fuer-cybersicherheit.de/ACS/29CST
33 https://www.bsi.bund.de/DE/Themen/Sicherheitsberatung/ZugelasseneProdukte/Zulassung_node.html
34 https://www.bsi.bund.de/DE/Themen/Sicherheitsberatung/ZugelasseneProdukte/VS-Anforderungsprofile/VS-Anforderungsprofile_node.html
35 https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2019.pdf
36 https://arxiv.org/pdf/2003.08837.pdf
37 https://www.plattform-lernende-systeme.de/home-en.html
38 https://www.etsi.org/committee/1640-sai
39 https://www.plattform-lernende-systeme.de/files/Downloads/Publikationen/AG3_6_Whitepaper_07042020.pdf
40 https://link.springer.com/chapter/10.1007/978-3-030-26951-7_6
41 https://eprint.iacr.org/2020/165.pdf
42 https://www.bsi.bund.de/EN/Topics/Crypto/Cryptography/QuantumComputing/quantum_computing_node.html
43 https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2019/Blockchain-Sicherheit-230519.html
44 https://www.bsi.bund.de/EN/Topics/Crypto/Cryptography/Blockchain/blockchain_node.html

Imprint

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

Phone
+49 (0) 22899 9582-0

Last updated
September 2020

Printed by
Appel & Klingler Druck und Medien GmbH,
Schneckenlohe, Germany

Concept, editing and design
Faktor 3 AG

Content and editing
Federal Office for Information Security (BSI)

Image credits
Title: GettyImages ©perihelio; p. 3: BMI; p. 4: BSI; p. 8, 38, 78: GettyImages ©perihelio; p. 36: GettyImages ©mattjeacock; p. 51: GettyImages ©Morsa Images

Graphics
Federal Office for Information Security (BSI)

Item number
BSI-LB20/509e

www.bsi.bund.de