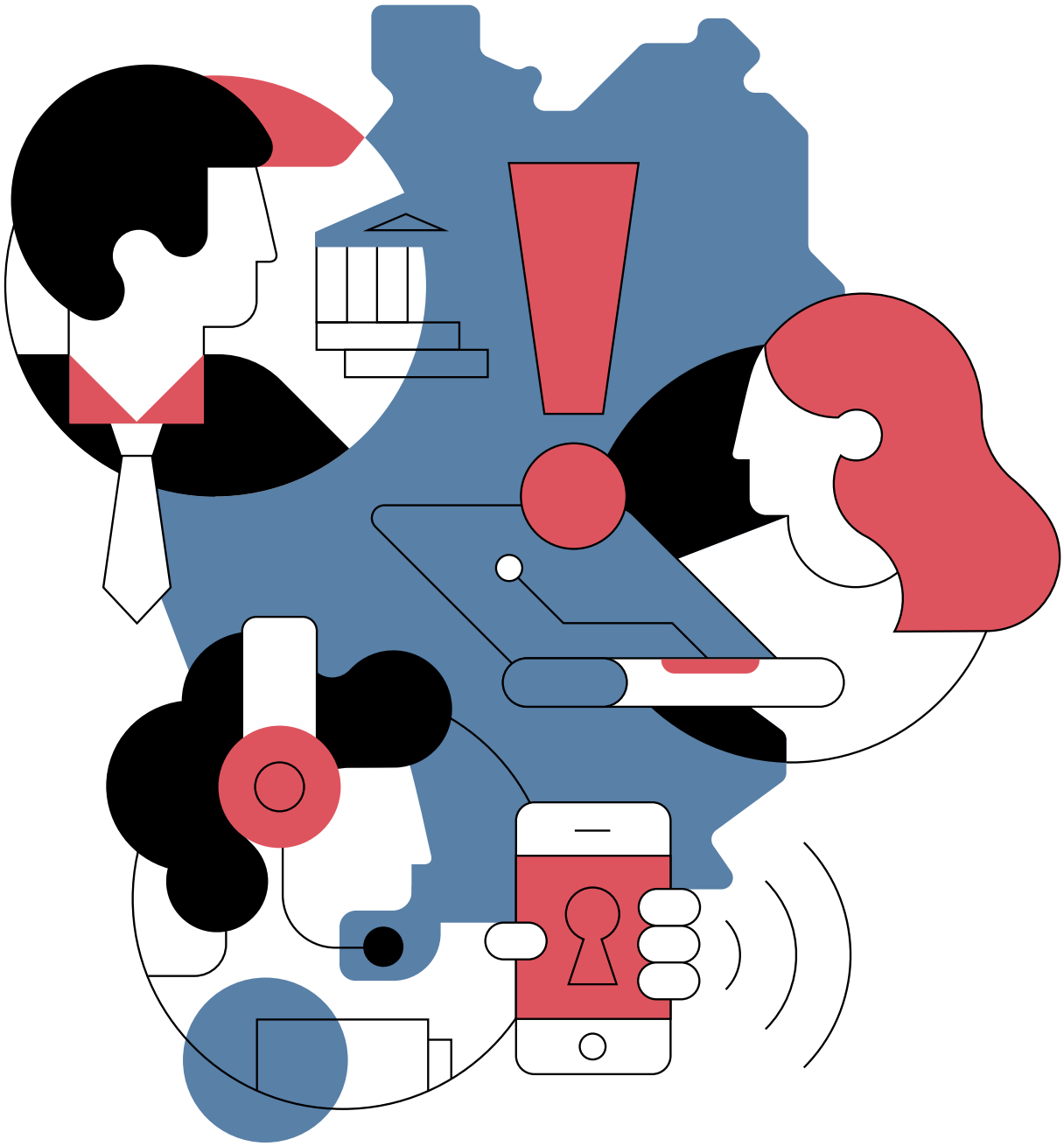
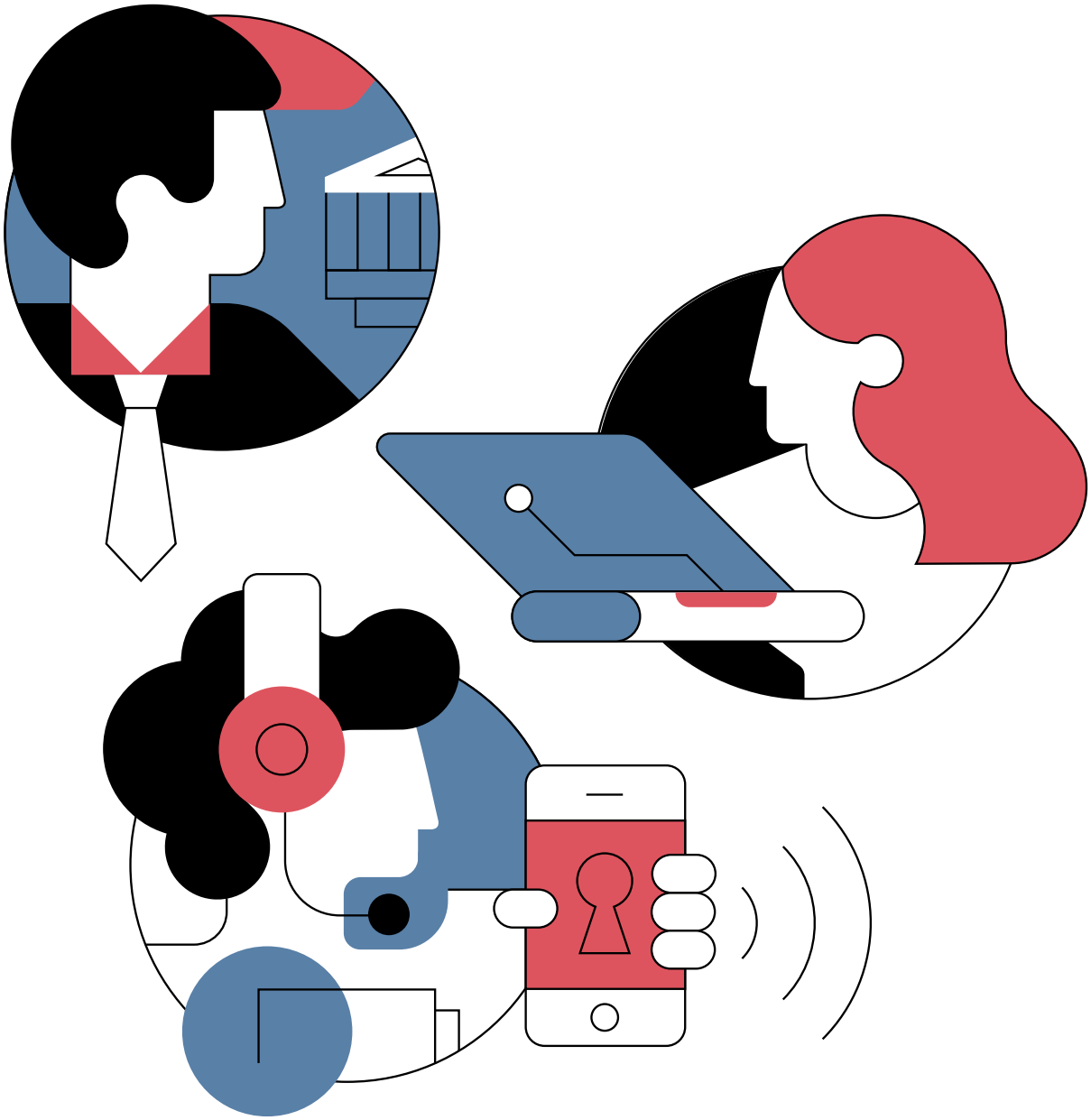
The State of IT Security in Germany in 2022



Federal Office
for Information Security

Table of Contents



Register of Selected Incidents in the Reporting Period:

Register of Figures:

Foreword

Nancy Faeser, Federal Minister of the Interior and Community

In the face of Russia's war of aggression against Ukraine, it has become clear how closely linked external and internal security are. This is particularly true for cyber security. There are no borders in cyberspace.

I consider cyber and information security to be key aspects of digital transformation. We can see how important secure digital systems, processes and structures are for a vigilant democracy. The turning point we are experiencing with the threat to peace in Europe requires significant investment in our cyber and information security.

The BSI's report on the state of IT security in Germany in 2022 is clear: The threat level in cyberspace is higher than ever. Cybercriminals are using state-of-the-art technologies to attack individuals, businesses and government institutions. We must take decisive action to confront these attacks. Citizens rightly expect their government to be proactive and protect society from digital threats.

The cyber security agenda of the Federal Ministry of the Interior and Community addresses this challenge. Among other things, we are striving to provide a strong security architectures and the highest possible level of protection in cyber security.

I am very pleased to have the BSI and our other security agencies as strong and reliable partners by our side, doing their utmost every day to protect us – citizens, businesses and administrations – from the dangers of cyberspace.

Foreword

Dr. Gerhard Schabhüser, Vicepresident of the Federal Office for Information Security (BSI)

Germany · Digital · Secure · BSI

This report on the state of IT security in Germany covers a period that was marked not only by the continuing effects of the COVID-19 pandemic, but also by the consequences of the Russian war of aggression against Ukraine.

In light of the experiences of the past few months, risk assessment has to be continuously developed. This is because there has also been collateral damage and individual cyber attacks in Germany within the context of the Russian war of aggression against Ukraine. More than ever, these developments have demonstrated that cyber security has become a central element for the state, for companies, institutions and, last but not least, for consumers in an increasingly digitally connected world.

However, the threat situation had remained very high even before the start of the war. For example, ransomware attacks on IT service providers, districts and municipalities as well as on large companies, traffic overload attacks (DDoS) on online shops on busy sales days – all of these IT security incidents clearly illustrate how important information security is for our secure digitalisation. More and more, uninvolved third parties are affected by cyber attacks. For example, when citizens are no longer able to use municipal services because administrations are affected by ransomware, or when consumers are unable to pay for their purchases because providers are incapacitated by cyber attacks. The manufacturers and providers of digital services in particular have a duty: They have to live up to their responsibility and ensure that the data entrusted to them cannot be lost or misused. Moreover, they must ensure that their digital services are secure and their products are fully available.

These incidents demonstrate that ensuring cyber and information security is a key element for the well-being and protection of our society. However, this report also shows that we in Germany are not defenceless against these threats. As the Federal Cyber Security Authority, the BSI has continued to strengthen and expand its prevention, detection and response activities for all target groups from the state, industry and society. This was made possible by the creation of important prerequisites by lawmakers in April 2021 with the IT Security Act 2.0.

Nevertheless, the continuing professionalisation of cyber extortion methods, the ongoing serious consequences of ransomware attacks, the ever-increasing variety of malware variants and critical vulnerabilities in widely used software products such as Log4j all reveal that we must continue to strengthen cyber security.

The challenges posed in cyberspace remain high and will continue to grow rapidly. In order to not only keep pace with this development, but also to strengthen protection against cyber attacks in Germany and thus its future viability, information security must be a top priority in the state, the economy and society. For this reason, I warmly welcome the Federal Government's planned continuing modernisation of cyber security architecture and the expansion of the BSI to become the central agency for information security in the relationship between the federal government and the states. During the reporting period, the BSI once again proved that it has the capability to react competently and quickly to new challenges. I am certain, in view of the commitment and highly respected expertise of the BSI's staff, that this will also apply to future tasks.

State

1. Threats to Cyber Security in Germany

As the Federal Cyber Security Authority, the Federal Office for Information Security (BSI) continuously monitors the level of IT security threats in Germany. The BSI focuses on cyber attacks on companies, state and public institutions and private individuals, as well as on measures to prevent and combat these situations. This report takes stock of the period from 1 June 2021 to 31 May 2022 (reporting period). Therefore, the report addresses current and possibly ongoing cyber threats. It also assesses the state of IT security in the context of Russia's war of aggression against Ukraine.

Using numerous concrete examples across many different sectors, the report traces the path and typical methods used by attackers, while at the same time showing how people and organisations can protect themselves. The overview begins with a summary of the general level of danger and current cyber threats. Not only do attacks have a direct impact on the people and organisations affected, but they also affect the lives of everyone in a digitised society. This makes it all the more important to shed light on each individual area with its specific threats and, subsequently, to present the countermeasures specifically for the target group.

1.1 — Summary and Assessment

Overall, the ongoing tense situation continued to worsen in the reporting period. The threat in cyberspace is thus higher than ever. A high threat of cybercrime was observed during the reporting period – the same as in the previous year. Ransomware remained the main threat (see. chapter *Ransomware,* page 13), especially for companies. In addition, there were various threats related to the Russian war of aggression against Ukraine, e.g. through hacktivism, especially by means of Distributed Denial-of-Service (DDoS) attacks, and collateral damage in cyber sabotage attacks in the context of the war. There were also disruptions to IT supply chains during the reporting period due to both cybercrime and cyber-activities in the context of the war in Ukraine. Increasing resilience to cyber attacks and technical disruptions is therefore a major task for all involved actors in the state, economy and society.

Russian War of Aggression against Ukraine:

Up to now, there has been an accumulation of smaller incidents and hacktivism campaigns in Germany in connection with Russia's war of aggression against Ukraine (see for example incident *Collateral Damage after Attack on a Satellite Communications Company,* page 49, and incident *Cyber Attack on German Petroleum Trader,* page 50). There was no evident overarching attack campaign against German targets. The situation in the cyberspace of NATO partners, on the other hand, was tense in some cases and critical in Ukraine, in some cases threatening the very existence of the country.

Extortion Methods in Cyberspace:

The expansion of methods of extortion in cyberspace observed in the previous reporting period has continued in the current reporting period. In particular, so-called big game hunting, meaning the extortion of high-revenue companies with encrypted and exfiltrated data has continued to increase. Both the ransom and hush money payments reported by IT security service providers and the number of victims whose data was published on leak sites, due to non-payment, for instance, have continued to rise. In addition, there were also repeated cases of blackmail with stolen identity data in the current reporting period.

There were also several observed sextortion campaigns, some of which were unusually pronounced. In these spam emails, attackers claim to have compromising, intimate secrets of the victim and threaten to publish them. In order to prevent the publication of the allegedly compromising information, the victim is supposed to transfer a certain amount in a cryptocurrency (e.g. Bitcoin.)

Vulnerabilities:

in the previous year. More than half of them had high or critical scores according to the Common Vulnerability Scoring System (CVSS). The vulnerability in Log4j was particularly critical, as it was found in many freely available software components. Besides, IT security officers usually found it difficult to assess whether the software they were using had the vulnerability. Due to the high distribution of Log4j, it was to be assumed that there was a large attack surface for cyber attacks.

Advanced Persistent Threats (APT):

In the current reporting period, there were more attacks on perimeter systems such as firewalls or routers. While targeted APT attacks using malware in emails usually require a high level of effort, perimeter systems are directly accessible from the internet, comparatively poorly protected and therefore easier to attack. More and more, APT groups are scanning the internet for known vulnerabilities in perimeter systems for which no patches are yet available in order to target them.

Distributed Denial of Service (DDoS):

According to reports from various mitigation service providers, the number of DDoS attacks has continued to increase. For example, the German mitigation service provider Link11 recorded an increase in DDoS attacks of around 41 percent in 2021 compared to the previous year. Around the annual online shopping event Cyber Week and in the run-up to Christmas, in particular, there were noticeably more attacks. In the period around Cyber Week 2021, the number of DDoS attacks doubled compared to Cyber Week 2020.

1.2 — Malware

The term malware includes any computer program that can perform harmful operations or enable other programs to do so. Malware can enter a computer in attachments or via links in emails. If the user clicks on a malicious attachment or on a link that leads to a malicious website, the malware can install itself. In addition to emails as gateways, typical attack vectors include forged links in websites and the misuse of legitimate programmes. Malware usually uses vulnerabilities to infect an attacked IT system. These occur in software or hardware products and at network transitions. Moreover, as in the case of social engineering, the "human" factor is becoming increasingly significant for cyber attacks.

The individual malware programmes differ in terms of their functionality, but a malware programme can also have several functionalities. Ransomware is, for example, malware that restricts access to data or systems by encrypting them so that the attacker can then extort a ransom (for more details, see chapter *Ransomware*, page 13). Malware that disguises itself as benign software or hides in legitimate data is called a Trojan, and malware that can be controlled remotely, for example with the help of command-and-control-servers, is called a bot (see chapter *Botnets,* page 24).

In addition to regular security updates, antivirus programmes offer protection against malware attacks by detecting them, preventing them from running successfully and removing them from the system. However, some attacks also make profound changes to the infected system that cannot easily be undone.

1.2.1 — New Malware Variants

A new variant of a malicious programme is created when changes are made to the programme code. Any variant with unique checksum (hash value) is therefore considered as new. While detection methods exist for known malware variants, new variants may not yet be recognisable as malware immediately after their appearance, making them particularly threatening.

The number of new malware variants has increased by around 116.6 million in the current reporting period (see Figure 1; this source and the following data: BSI malware statistics based on raw data from the AV-Test GmbH institute).

On average, the number of new malware variants increased by almost 319,000 daily. This was 19 percent less than in the previous reporting period (see Figure 2), which stood out with exceptionally high values. The indicator has thus normalised again. Nevertheless, there were considerable fluctuations. While in the summer of 2021, there were still around 300,000 new variants per day, in the autumn of the same year, there were up to 436,000 new malware variants (see Figure 2) per day.

1.2.2 — Ransomware

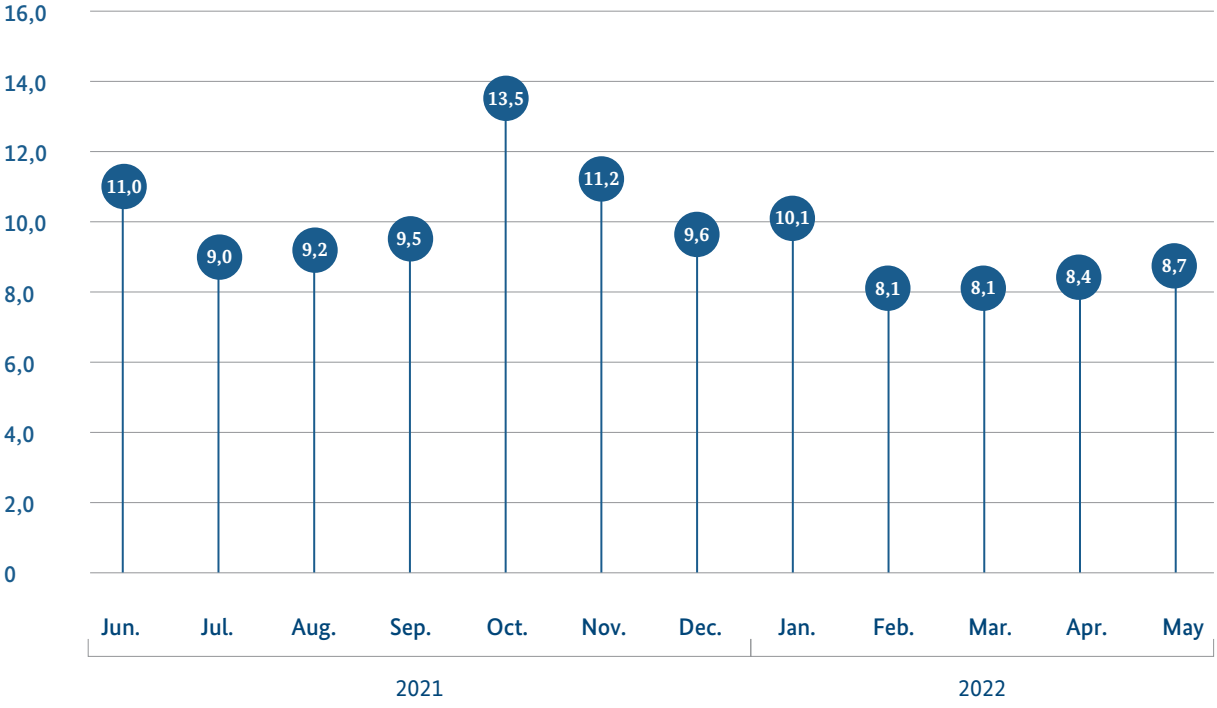
Ransomware attacks represent one of the greatest cyber threats to the state, economy and society.

Ransomware is malware that blocks access to local or networked data and systems. It often encrypts user data such as office, image and video files or entire data infrastructures such as databases or server systems. The attackers then leave a ransom message. The data can then only be decrypted with a tool specific to the ransomware used. During extortion, the attackers threaten to destroy this key material. Additionally, they steal sensitive data before encrypting it and threaten to publish it to increase the pressure of their demands (double extortion). The combination of these two methods (ransom and hush money) has become the norm in ransomware attacks during the reporting period. The ransom payment is usually demanded in digital currencies. This makes prosecution more difficult, as such payments cannot always be attributed to an individual.

Ransomware attacks are overwhelmingly perpetrated by cybercriminal attackers. However, APT attackers could also use them to disguise or distract from other attacks, or use them purely for sabotage. In the case of sabotage, the attackers may only feign an interest in the ransom or may never technically plan to decrypt the data again later. If this is the case, the ransomware acts as a wiper and the encrypted data cannot be technically restored (see the use of wipers in the context of the Russian war of aggression against Ukraine, see chapter *Cyber Security Situation in the Context of the Russian War of Aggression against Ukraine,* page 45).

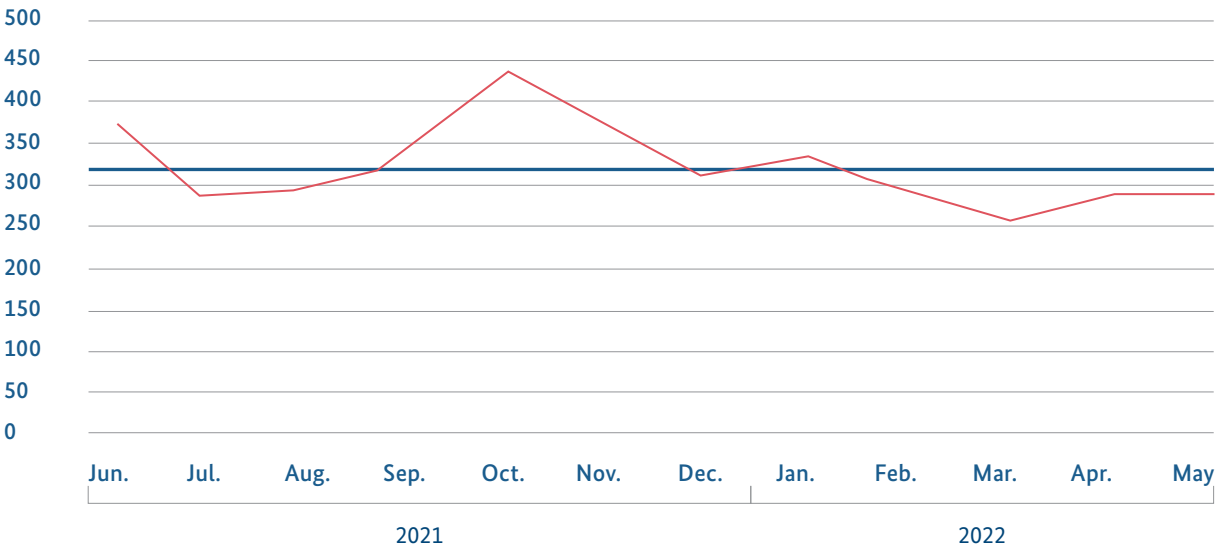
New Malware Variants from June 2021 to May 2022
Number in millions

Figure 1:
Source: BSI malwares statistics based on raw data from the AV-Text GmbH institute



Average Daily Growth of new Malware Variants from June 2021 to May 2022
Number in thousand

Figure 2:
Source: BSI malware statistics based on raw data fro the AV-Test GmbH institute



Cybercriminals are grouped together based on the malware they use and their modus operandi. The Conti ransomware, for example, is used by a different grouping than the LockBit 2.0 ransomware.

Within the cybercriminal space, a kind of division of labour has developed over the past few years: Components of a cyber attack are outsourced to specialised attacker groups. This phenomenon can be compared to the outsourcing of services in the private sector. It is referred to as Cybercrime-as-a-Service (CCaaS). CCaaS allows an attacker to source almost every step of an attack as a service, or at least the malware needed to do so, from other cybercriminals. The BSI suspects that this is a driving factor behind the increase in the threat.

1.2.2.1 – Example Attack Sequence

A ransomware attack often begins with a malicious spam or phishing email, compromising remote access such as Remote Desktop Protocol (RDP), or exploiting vulnerabilities. This initial infection is the starting point for subsequent action by the attacker.

In the next step, an attacker tries to spread laterally in the IT network of the affected party. There are various means at their disposal for this purpose: Additional malware can be downloaded, access data can be stolen and vulnerabilities can be exploited. Sometimes legitimate software is misused that is actually meant for the

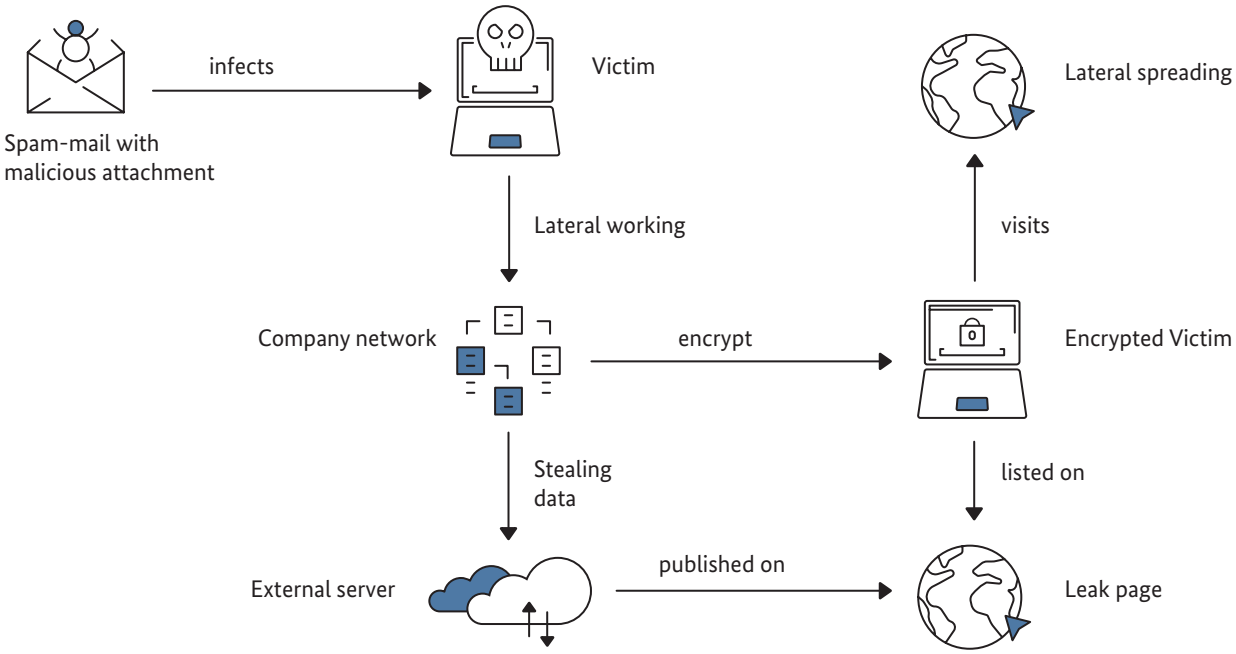
administration of the IT system. The attacker's activities thus appear like those of an administrator, for example, and can remain undetected for longer.

Once an attacker has spread sufficiently throughout the IT network, they usually steal sensitive data. Various tools are available to them for this purpose as well: from malware designed for this purpose to software that can work together with cloud services. After completing the data theft, the attacker distributes the ransomware in the IT network. All compromised systems will be encrypted.

Lastly, the attacker leaves a ransom note on the encrypted systems (see Figure 3). In the ransom note, the victim is informed about their situation and is often asked to visit one or more of the attacker's websites in order to make a payment. Attackers sometimes operate separate websites for individual victims, through which ransom payments are negotiated and processed (see section *Ransom Extortion*, page 16). In addition, attacker groups operate leak sites, on which the data of those affected are published. In some cases, information such as the number of employees, turnover or industry is provided for the companies concerned. Attackers publish data by adding links to these entries, which can be used to retrieve the stolen data (see section *Hush Money Extortion,* page 16).

Example attack sequence

Figure 3:
Sample sequence of a ransomware attack with ransomware and hush money extortion (schematic representation)
Source: BSI



Example of a blackmail message

Figure 4:
Example of a blackmail message
Source: BSI

```
Your network has been breached and all data were encrypted.
Personal data, financial reports and important documents are ready to disclose.
To decrypt all the data and to prevent exfiltrated files to be disclosed at

http://hiveleakxxx.onion/

you will need to purchase our decryption software.

Please contact our sales department at:
   http://hivecustxxx.onion/
      Login:    Jxxx
      Password: gxxx

To get an access to .onion websites download and install Tor Browser at:
   https://www.torproject.org/ (Tor Browser is not related to us)

Follow the guidelines below to avoid losing your data:
 - Do not modify, rename or delete *.key.cggbt files. Your data will be
   undecryptable.
 - Do not modify or rename encrypted files. You will lose them.
 - Do not report to the Police, FBI, etc. They don't care about your business.
   They simply won't allow you to pay. As a result you will lose everything.
 - Do not hire a recovery company. They can't decrypt without the key.
   They also don't care about your business. They believe that they are
   good negotiators, but it is not. They usually fail. So speak for yourself.
 - Do not reject to purchase. Exfiltrated files will be publicly disclosed.
```

1.2.2.2 — Evolution of the Threat Situation

Hush Money Extortion

The number of victims of ransomware attacks followed by hush money extortion is steadily increasing. Nevertheless, often only those cases become known in which the victims paid neither hush money nor ransom. A statistic from the news site "The Record" counts the victims whose data was published on leak sites on the internet[1] . According to the statistic, the first ransomware attackers began using leak pages and hush money extortion as leverage in late 2019 and early 2020. In the second half of 2020, this developed into a trend that more and more cybercriminals followed. This is also reflected in the steady increase in data leaks over the same period (see Figure 5).

Several successful internationally coordinated prosecutions were revealed in early 2021. This involved shutting down the Emotet malware infrastructure and the Ransomware-as-a-Service (RaaS) offerings of Netwalker and Egregor. It is likely that these measures were partly responsible for the decline in data leaks. RaaS is a form of CCaaS in which the attacker acquires the ransomware and often its associated infrastructure from the RaaS operator. The operators of the ransomware receive a share of the extorted money as a form of "commission". An attacker who obtains this service is also called an "affiliate".

The decrease in data leaks after May 2021 has been remarkable (see Figure 5). This was due to the fact that a number of RaaS offers were discontinued. However, as early as the summer of 2021, several RaaS, some of them new, attempted to fill the gap in the market that had previously emerged. Most notably, the RaaS LockBit 2.0 emerged stronger than before; rising to the top three ransomware families in the second half of 2021 (see Figure 6). Others are the RaaS Conti and the ransomware Pysa.

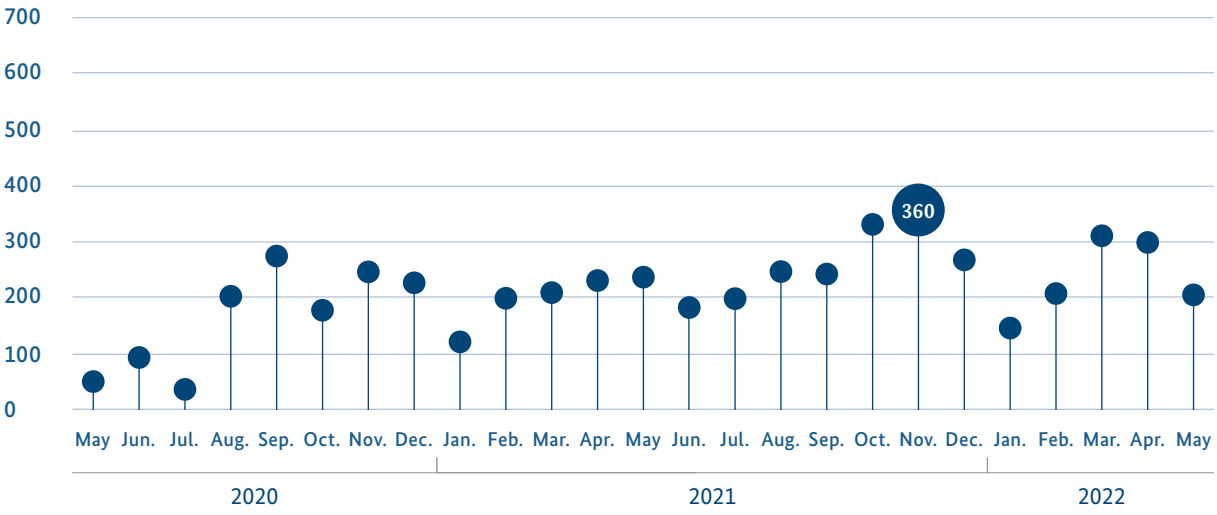
Ransom Extortion

The ransomware attacks reported to the BSI are accompanied by a presumably high number of unreported incidents that remain undisclosed. Statistics from IT security service providers are usually limited to their respective clientele, so absolute figures on ransomware incidents tend to be under-reported and should always be interpreted with caution. Regardless, however, most sources show a clear trend: The sum of extorted ransoms is increasing. The exact amount differs from source to source, as there is no comprehensive data basis and ransomware statistics only pertain to the clientele of individual IT security service providers.

One statistic from the IT security service provider Coveware, for example, shows the ransoms paid within a quarter for incidents that Coveware assisted with (see Figure 7). According to the report, average ransom

Development of the Threat Situation
Victim Data Released on Ransomware Extortion Site

Figure 5:
Victims of data leaks from January 2020 to November 2021
Source: The Record



payments increased from $84,116 in the fourth quarter of 2019 to $154,108 in the fourth quarter of 2020 - an increase of approximately 183 percent. Coveware noted the highest average payment in the fourth quarter of 2021 at $322,168, while lower ransom payments were previously observed in the second and third quarters. This temporary drop is probably mainly due to increased action by law enforcement following several major ransomware incidents in 2021 (see also section *Hush Money Extortion,* page 16).

Extortion with Captured Identity Data

For the hush money extortion described above (see section *Hush Money Extortion,* page 16), attackers usually leak large amounts of data, often including identity data as well as sensitive personal data, which are also published on corresponding leak sites together with the other leaked data. Moreover, during the negotiation phase, attackers may threaten victims already affected by a ransomware attack with DDoS attacks, for example, in order to add further pressure to their demands for ransom or hush money.

Captured identity data enables the attackers to exert additional extortion pressure and to force the victim of the attack to act even more. Attackers use the data for the following additional extortion methods in particular:

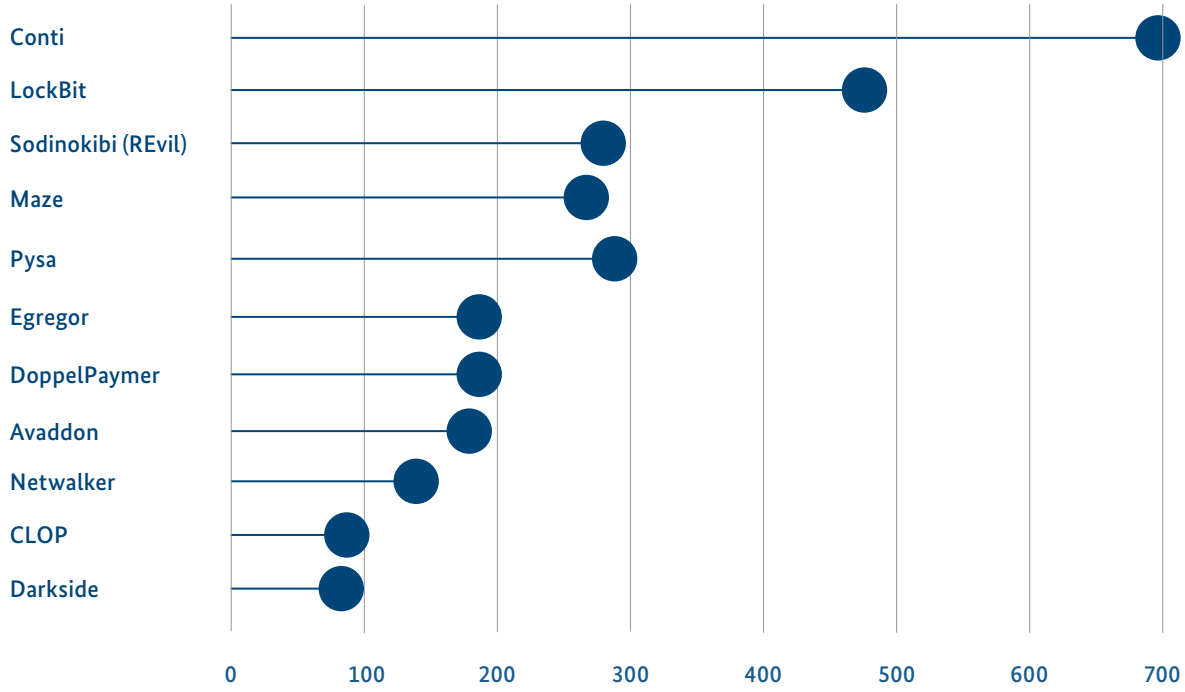
1. Attraction of public attention:
Some attackers actively approach the victim's customers or the public to exert additional pressure. This goes beyond publishing the information of victims on leak pages set up for this purpose. For example, attackers might contact a victim's clients or employees by email and inform them that sensitive data about them has become public due to unpaid hush money. This can damage the victim's reputation in the long term, especially if the victim is not transparent in its dealings with those potentially affected by the data leak. Dutiful notification of competent data protection or regulatory authorities can limit the negative impact.

2. The sale of sensitive data:
If the victim is not willing to pay, some attackers may sell or auction off captured data to third parties. In addition, the buyers of the captured data can use it for extortion against the victim themselves. This is especially true when it involves valuable trade secrets or compromising information about individuals. It is usually no longer possible to determine to whom such data is ultimately auctioned off to. Once data has been stolen, it is considered permanently compromised even in the event of a hush money or ransom payment.

Victims of Data Leaks according to Attacker Group

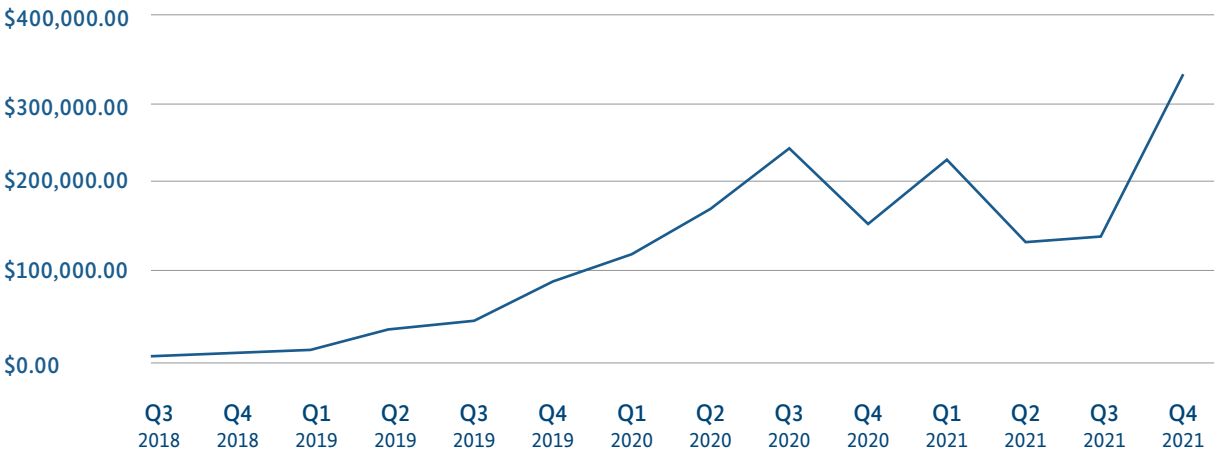
Victims Posted to Extortion Sites

Figure 6: Data leak victims by attacker group
Source: The Record



Ransom Payments By Quarter

Figure 7:
Ransom payments 2018 to 2021
Source: Coveware



3. Threatening to report to the relevant data protection or regulatory authority:
In the event of a cyber attack, victims may be in breach of the General Data Protection Regulation or other regulations if, for example, they fail to comply with their reporting obligations or it can be proven that sensitive data was stored on poorly secured web servers, for example. Such due diligence or reporting violations on the part of victims are used by some attackers as further leverage to threaten to notify regulators of the breach. Since both the attack and compromised data can also become public through other channels, victims should avoid breaches of the law by reporting them dutifully and at an early stage.

In many cases, however, ransomware attacks are not the only cause of data leaks. The involuntary publication of sensitive data by one's own service providers due to a lack of adequate protective measures is still not uncommon and was observed in increasing numbers during the current reporting period. This repeatedly results in sensitive (often personal) data being made public without the involvement and in many cases without the knowledge of those affected. In 2021, for example, a misconfigured lottery portal of a large German media group enabled third parties to access the user data of participants.

Moreover, attackers specifically and often automatically look for misconfigured systems as well as vulnerabilities that allow identity data to be leaked. They use special scanning and scraping methods for this. During the reporting period, incidents were observed in which vulnerabilities at several German Covid testing centres allowed access to the home and email addresses, telephone numbers, dates of birth and the particularly sensitive test results of those tested (see chapter *Vulnerabilities in Software Products*, page 31).

Initial observations also indicate that cybercriminal groups are emerging that primarily rely on data leaks as a means of extortion. Such groups no longer use ransomware, but start their extortion directly after the data theft, allowing them to move more quickly from initial infection to extortion.

1.2.2.3 — Recommendations

The most important prerequisite for restoring operational capability after a ransomware attack is a clear backup strategy. This includes the availability of functioning and up-to-date backups. The functionality of these backups must be checked regularly. It is now common in malware infections for attackers with previously obtained administration rights to specifically search for all backups and encrypt them, as well as production systems. For this reason, at least one copy of each should be backed up offline. These copies are separated from the other systems of the institution after backup and are therefore protected from remote attacks.

In order to effectively counter the increasing leakage of data and the threat of publication, systematic, rule-based monitoring of data transfer is necessary. For example, it is possible to detect and prevent the outflow of unusually large amounts of data.

Updates of the operating systems as well as the server and application software should be carried out regularly and promptly. To minimise the attack surface, the number of externally accessible systems should also be kept low and their use by unauthorised persons should be made more difficult (for example, by means of multi-factor authentication, use of a virtual private network (VPN), strict password requirements). Proper internal segmentation of IT networks and restrictive administration rights help to limit the extent of damage in the event of successful attacks. For all institutions, comprehensive and continuous training of all employees on the topic of information security (raising awareness) and limiting administrative access to the systems to as few people as possible should be a given. These and similar measures serve to make IT-supported business-critical processes as resilient as possible, meaning that they are more resistant to cyber attacks.

The effects of a short-term failure of IT-supported processes can also be countered by establishing alternative or redundant digital services (e.g. Content Delivery Networks (CDN) for websites, email services provided by a service provider). The ability to restore such processes in a timely manner serves to minimise any damage that may result from a failure. It is crucial here to consider appropriate measures in the event that an IT-supported process cannot be regularly restored in the long term, for example due to ransomware.

In order to be prepared in the event of an attack, response scenarios must be documented in writing that include all of the described aspects of an attack, for example damage to production facilities, the deployment of personnel and security companies, alternative business processes or loss of reputation, as part of emergency management.

The BSI generally advises against complying with a ransom demand, especially since there is usually no guarantee that the attackers will actually hand over the key.

Further information can be found here :[a]

Disaster Alert after Ransomware Attack on District Administration

Situation
A district administration in Saxony-Anhalt was the target of a ransomware attack on 5 July 2021. All IT systems at all locations of the district administration were affected. As a result of the attack, no services could be provided to citizens. On 9 July 2021, the county declared a local emergency. The declaration was not lifted until 2 February 2022. Not all damage had been repaired at this point, but functionality of the affected software had been restored.

The ransomware Grief was identified as responsible for the incident. The district administration did not pay the ransom. The attackers then published some data previously stolen as part of the attack on the ransomware's leak page.

Assessment
The failure or significant impairment of municipal administrative processes can lead to a variety of burdens within the population. This is especially true for groups of people who may be directly affected by the loss of critical services due to non-payment, for example of social benefits or parental allowance.

The ransomware Grief was identified as the successor to the ransomware DoppelPaymer. In the cybercriminal landscape, attackers frequently change their brand names that have been in use for a longer period of time. In this case, the attackers stopped using their ransomware DoppelPaymer and switched to the partially newly developed ransomware Grief. This process, known as rebranding, makes it difficult to attribute attacks to individual attackers or attacker groups. If an attack can be assigned to a known group, this makes it easier to respond to an incident in a targeted manner.

Response
The State Office of Criminal Investigation of Saxony-Anhalt and the public prosecutor's office in charge took up the investigation.

The BSI was already on site on 8 July 2021 with a Mobile Incident Response Team (MIRT, see chapter Computer Emergency Response Team for Federal Authorities, page 84) at the request of the district administration. The BSI also supported the affected district in the continued coordination of crisis management from Bonn. Additionally, the BSI analysed the malware used in the incident and advised the affected parties on essential security requirements for rebuilding the IT infrastructure. BSI's measures were carried out in close coordination with the support of the Bundeswehr, which was also requested by the district.

Ransomware Attack on a Retailer

Situation
In November 2021, a consumer electronics retailer became the victim of a ransomware attack. The company owns two electronics store chains.

According to media reports, the merchandise management systems and some of the cash registers in the shops were apparently affected. While the sale of inventory in the shops continued to function, it was not possible to order, return or collect goods. All 1,000 stores of both chains in 13 European countries were affected, including more than 400 in Germany alone.

Originally, the attackers had demanded a ransom of 240 million US dollars. The demand was later reduced to 50 million US dollars.

The RaaS Hive was used for the attack. The group behind the ransomware has the company listed as a victim on its data leak page. Possibly leaked data has not yet been published.

Assessment
The attack took place just before "Black Friday" and the annual pre-Christmas shopping season – a traditionally high-turnover time when the potential for damage to retailers is particularly high. This creates critical pressure to act on the attackers' ransom demands.

The RaaS Hive first hit the headlines in the summer of 2021. The FBI warned about Hive after Ohio's Memorial Health System was a victim of this ransomware. The incident described here fits the pattern of big game hunting, where larger organisations are attacked because higher sums can be extorted from them.

Response
Both the appropriate law enforcement and data protection authorities were informed by the company concerned. The BSI supported the affected party with a MIRT team, forensic investigations and by sharing Indicators of Compromise (IoCs). These are artefacts on a compromised system.

Ransomware Attack on Medical Technology Company

Situation

A Japanese medical technology company, which also has several locations in Germany, fell victim to a ransomware attack in September 2021. According to media reports, its locations in Africa, Europe and the Middle East were affected by the incident. According to a company press release, its sales and manufacturing sectors were affected by the attack in the meantime. However, so far there are no indications that company data was leaked. The company concerned said that after the incident was initially detected, a response team was mobilised to investigate the attack. As a result, the systems were shut down and taken off the grid. Although no further information was shared, several sources assume that the malware used was the ransomware BlackMatter. The suspicion is based on several demands for ransom that have been found on the infected systems.

Assessment

The BlackMatter ransomware is offered as RaaS and can thus also be purchased by affiliates, i.e. other cybercriminals, and used for attacks. BlackMatter has been attributed to the same group that previously developed and operated the RaaS Darkside. Darkside was active as a RaaS from November 2020 to May 2021 and was most recently used in the incident against the US pipeline operator Colonial Pipeline (see The State of IT Security in Germany in 2021[2]). BlackMatter attacks are usually accompanied by double extortion demands, i.e. extortion of protection money and hush money.

Response

The BSI assessed BlackMatter to be a serious threat. The RaaS ceased service in November 2021 for unknown reasons.

1.2.3 — Botnets

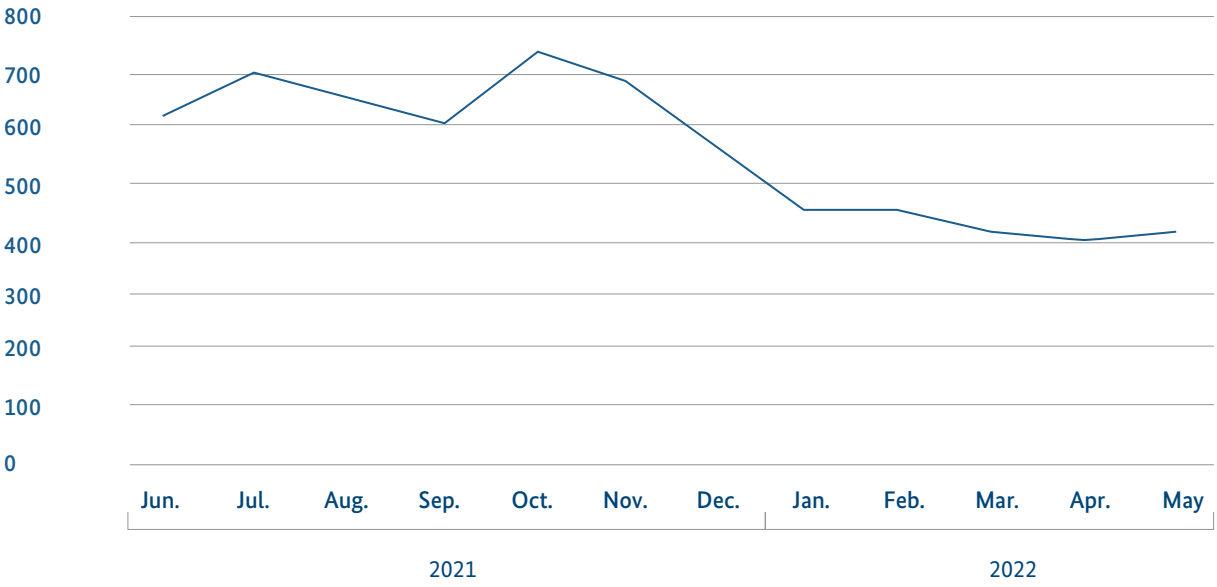
A botnet is a group of systems (bots) infected with a malicious programme that can be controlled by a bot master via a command and control server. Bot software exists today for almost all internet-enabled devices, so in addition to classic computer systems, mobile devices such as smartphones or tablets, as well as IoT devices such as routers, webcams or smart TVs can be compromised and taken over by attackers.

The modular structure of current bot software enables bot masters to use the adopted systems specifically for their own purposes by retrofitting required functions with updates. On the one hand, this includes direct damage to the infected systems, for example through the interception of personal data, online banking fraud, cryptomining or even encryption of device data. On the other hand, the devices can also cause damage to third party systems, for example by sending spam emails or carrying out DDoS attacks.

The BSI observed botnets in Germany during the reporting period through sinkholing. The Unique IP Index, which measures the emergence and development of infected systems in the botnets observed by the BSI, averaged 562 points during the reporting period. The number of observed infected systems that were active in botnets on a daily basis was thus 5.62 times greater than the annual average for 2019 (see Figure 8). As in the previous reporting period, bots were primarily used to spy on personal information as well as to spread other malware. In mass attacks, mobile operating systems based on Android and IoT devices were the main focus. FluBot, for example, remained the most commonly observed infection in both Android and bots in general, accounting for 37 percent of bots, despite attackers taking measures against ongoing sinkholing to keep new infections undetected. ArrkiiSDK was ranked second in the observed botnets with around 13 percent of the bots. This malware tracks user behaviour and installs additional applications on the mobile phone unnoticed. The third most frequently reported infections were related to QSnatch, at around ten percent.

Unique IP Index[1] for Germany in the reporting period
2019 = 100

Figure 8:
Unique IP Index for Germany in the reporting period
Source: BSI



[1] Excluding infected IP addresses that were not captured in the sinkholding.

Bots (unique IPs) per observed botnet in Germany on average over the reporting periodShare in % in all unique IPs

Share in % in all unique IPs

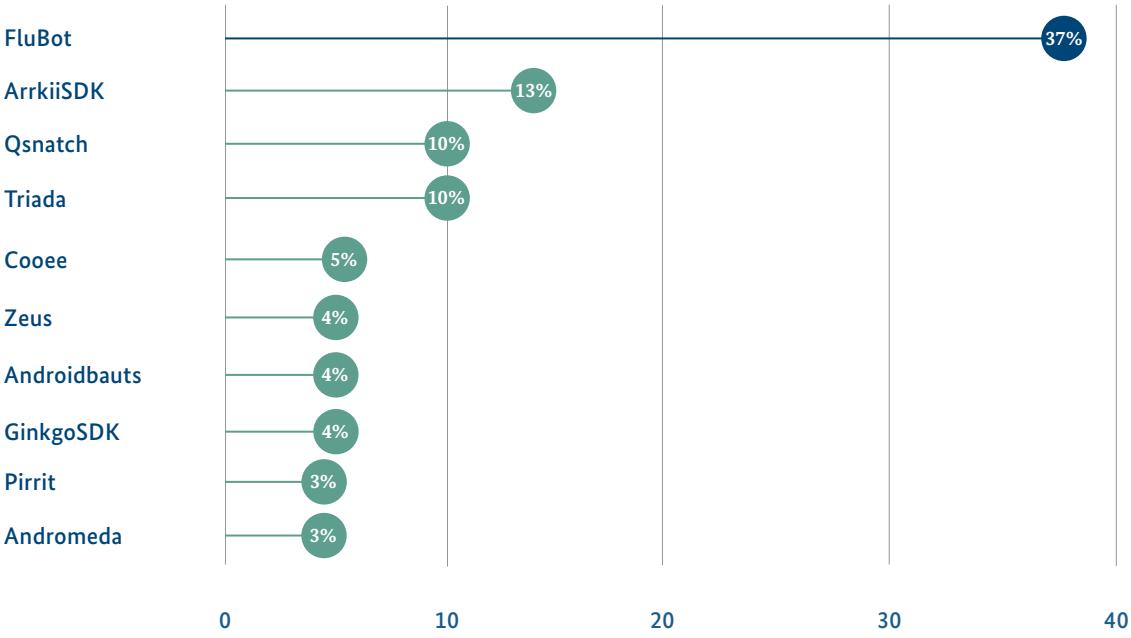


Figure 9:
Bots per observed botnet in Germany during the reporting period
Source: BSI

This malware infects network storage devices from the manufacturer QNAP. New botnet variants observed during the reporting period mostly targeted the Android platform.

In the case of the more targeted attacks on financially strong victims, the focus was primarily on popular server and desktop operating systems such as Microsoft Windows and Linux (see chapter *Ransomware*, page 13). In this area, the spread of ransomware was at the top of the list. In Germany, the botnet *Emotet* played a special role (see incident *Emotet Botnet Active Again,* page 26).

During the reporting period, the BSI sent an average of 41,100 reports about potentially infected systems in Germany to the German network operators and internet providers, who in turn identified and notified affected customers. Due to multiple infections, a significantly higher number of total infections is to be assumed. The infection data mainly comes from the BSI's own and external sinkhole systems, which receive and log the contact requests of bots instead of the regular Command-and-Control servers. A description of the sinkholing procedure and profiles of the most frequently reported malware families can be found on the website of the BSI[3].

As in previous years, the threat from botnets remains high. The increasing professionalisation of cybercriminals as well as the strong growth of potential victim systems leads us to expect that the number and size of botnets will also increase in the future. The infection numbers determined from sinkholing always represent a lower limit, as only a portion of the currently known botnets can be actively monitored. For example, current botnet families such as Emotet, FluBot or Glupteba take measures to avoid classic domain name-based sinkholing by using IP addresses, tunnelled DNS connections (DNS over HTTPS, DoH) or blockchain techniques to communicate between control servers and bot.

Emotet Botnet Active Again

Situation
Signs of the Emotet botnet being rebuilt have been observed since mid-November 2021. In a coordinated takedown by various international law enforcement agencies, including the Federal Criminal Police Office (BKA), the Emotet botnet was taken offline in January 2021 (see The State of IT Security in Germany in 2021[4]). The BSI had previously reported on Emotet several times and issued cyber security warnings about it. The Emotet malware is characterised by its mass use of attack techniques previously known only from elaborate APT attacks on selected targets. Emotet has therefore also been called the most dangerous malware in the world. The takedown resulted in a month-long halt to the sending of Emotet spam. However, since mid-November 2021, regular spam has again been sent to spread the Emotet malware using the attackers' new infrastructure.

Assessment
So far, the spread of Emotet in Germany and Europe has not yet reached the level it had before the takedown. The attackers seem to be focusing more on the Asian region at the moment.

One possible reason for this is that ransomware attack groups have resorted to other "door openers" to access potential victims' IT networks after the takedown of Emotet. One example is Qakbot, which, like Emotet, spreads via spam mails with fake supposed replies to spied emails.

However, it is possible that the Emotet Group will turn its focus back towards Europe at any time. Isolated waves of spam have been observed in this regard. With increased spam waves, there could be a renewed increase in infections and associated damage.

Response
The BSI issued a cyber security warning in November 2021, warning of a possible resumption of spam sending by the Emotet botnet[5]. IT security managers were asked to check the effectiveness of their Emotet protection measures and update them if necessary.

1.2.4 — Spam and Phishing

In general, unsolicited emails are referred to as spam. Spam is sent, for example, via compromised or commercially rented servers, via legitimate email accounts stolen by attackers whose access data has previously been exposed (see section *Extortion with Captured Identity Data,* page 17), or via infected systems that are added to botnets and then made available for spam services (see chapter *Botnets,* page 24).

Spam emails can be unsolicited, but essentially harmless advertising spam, as well as messages with an attack motive, such as extortion or fraud emails. During the reporting period, advertising spam accounted for around 16 percent of spam emails. The largest share of spam was cyber attacks such as email extortion with 36 percent and email fraud with 33 percent. Other spam accounted for 15 percent. This included dangerous malware spam, i.e. spam containing malware distributed en masse (see Figure 10).

The waves of spam from the range of attempted cyber extortion already observed in the previous reporting period have continued in the current reporting period. A pronounced extortion campaign drove the spam ratio for business in Germany to 4.5 in February 2022, the

Spam during the reporting period by time
Shares in %

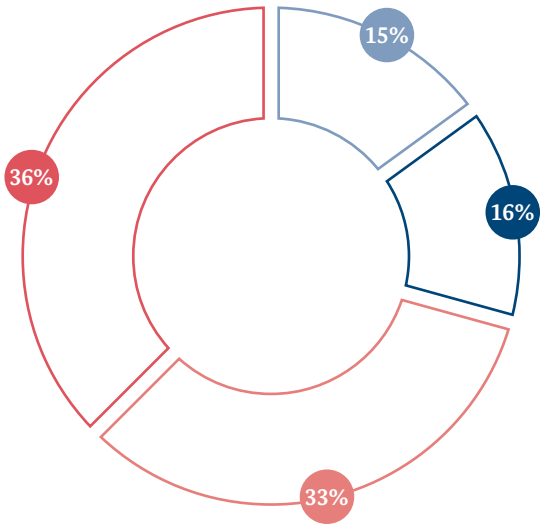


Figure 10:
Spam during the reporting period by time
Source: Email traffic statistics

- Others
- Advertising
- Scam
- Blackmail

highest monthly average since the statistics began. The spam ratio indicates how many spam emails per legitimate email were received on average in a reporting period. For example, an email inbox that received 100 legitimate, wanted emails in February 2022 was also statistically addressed with an average of 450 spam emails.

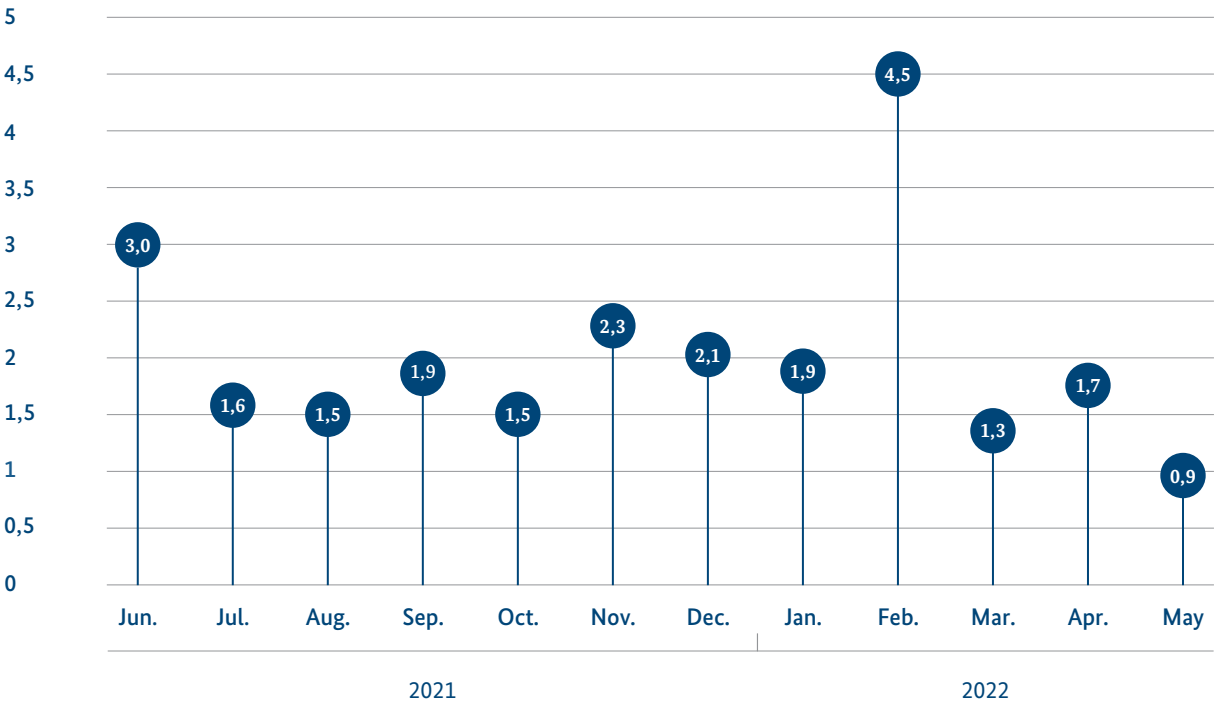
The reason for the noticeable increase in spam emails in February 2022 was a pronounced sextortion campaign that lasted several days. The attackers claimed to have compromising video footage showing the victim visiting pornographic websites. They threatened to release the alleged material to the public (see Figure 12) if a low four-digit US dollar amount in Bitcoin was not paid within 48 hours. The sextortion wave not only made itself felt in business in Germany and in the federal administration, but also targeted consumers. Modern spam filters with high-quality state-of-the-art detectors were able to catch most of the sextortion emails.

At 76 percent, sextortion emails accounted for the largest share of extortion emails in the reporting period. Another 12 percent of the extortion emails were in the health category. In the remaining emails, attackers used various topics to extort hush money. What all extortion emails have in common is that the attackers pretend to have intimate secrets about the victim's state of health or sexual preferences, for example. They build up additional extortion pressure by suggesting that they can monitor the victim day and night in all activities on all their devices.

In the area of fraud emails, phishing emails take the largest share with around 90 percent. Phishing emails aim to persuade the victim to divulge identity or authentication data using social engineering methods. A distinction must be made between phishing and spear phishing methods. While attackers use spear phishing to target individuals, such as important personalities in government or business, in an elaborate and targeted manner in order to capture their identity data (see for example incident *Spear Phishing by APT Group GhostWriter,* page 40), phishing emails distributed en masse and in an untargeted manner are directed against the general population. Attackers used finance phishing especially frequently in the current reporting period. These emails are now usually written in very good German and designed to match the corporate design of large banks in Germany. Designs are often used that are modelled on those of savings banks, Volksbanks or the Postbank. In this way, the attackers suggest to the victims that they have to carry out a supposedly necessary verification, in which they elicit the access data for their online banking. Since banks in Germany do not ask their customers to enter access data by email, users should always consider such emails as phishing

Spam ratio in the business sector in Germany
Number of spam mail per legitimate, wanted e-mail

Figure 11:
Spam ratio in the business sector in Germany
Source: Email traffic statistics



attempts, never enter access data or click on links contained in them and inform their email provider or financial institution so that they can take countermeasures.

In addition, the BSI again observed so-called advance fee scams by email in the current reporting period. Such spam emails are used to trick victims into transferring money. The attackers pretend to be a rich person who needs to move their assets abroad to safety and needs help to do so. The victim is supposed to transfer a certain amount in order to be able to open an account, for example. In return, they are promised a high reward as soon as the supposed assets of the rich person are safely abroad. Scam emails such as these accounted for around ten percent of fraudulent spam emails in the current reporting period.

Charity scams were again observed in connection with the flood disaster in North Rhine-Westphalia and Rhineland-Palatinate and the Russian war of aggression against Ukraine. Attackers spread fraudulent "appeals for donations" via spam emails and social media channels and tried to exploit the willingness to help and donate (see chapter *Cyber Security Situation in the Context of the Russian War of Aggression Against Ukraine*, page 45).

Example of Sextortion Email

Figure 12:
Example of sextortion email
Source: BSI

From: [redacted]
To: [redacted]
Subject: Vergessen Sie nicht, innerhalb von 2 Tagen die Steuer zu zahlen!
Date: 18 Feb 2022 03:03:06 +1000

Hallo, wie geht es Ihnen?
Ich weiß, es ist unangenehm, das Gespräch mit schlechten Nachrichten zu beginnen, aber ich habe keine andere Wahl.
Vor ein paar Monaten habe ich mir Zugang zu Ihren Geräten verschafft, die Sie zum Surfen im Internet benutzen. Danach konnte ich alle Ihre Internetaktivitäten aufspüren.

Hier ist die Vorgeschichte, wie es dazu kommen konnte:
Zunächst habe ich mir von Hackern den Zugang zu mehreren E-Mail-Konten erkauft (heutzutage ist das online sehr einfach zu bewerkstelligen). So konnte ich mich problemlos in Ihr E-Mail-Konto einloggen ([redacted]).
Eine Woche später habe ich in den Betriebssystemen aller Ihrer Geräte, die Sie zum Öffnen von E-Mails verwenden, einen Trojaner installiert. Ehrlich gesagt, war das ziemlich einfach (da Sie die Links aus Ihren E-Mails im Posteingang geöffnet haben). Das Geniale ist ganz einfach.
Meine Software ermöglicht mir den Zugriff auf alle Steuerungen in Ihren Geräten, wie Mikrofon, Tastatur und Videokamera. Ich kann ganz einfach alle Ihre privaten Daten auf meine Server herunterladen, einschließlich des Verlaufs Ihres Internet-Browsings und Ihrer Fotos. Ich kann mühelos auf alle Ihre Messenger, Konten bei sozialen Netzwerken, E-Mails, Kontaktlisten und Chatverläufe zugreifen. Mein Virus aktualisiert ständig seine Signaturen (weil er treiberbasiert ist) und bleibt daher von Ihrem Antivirusprogramm unbemerkt. Sie können sich also schon denken, warum ich die ganze Zeit unentdeckt geblieben bin.

Als ich Informationen über Sie sammelte, konnte ich nicht umhin festzustellen, dass Sie auch ein echter Fan von Webseiten mit Inhalten für Erwachsene sind. Sie lieben es Pornoseiten zu besuchen und perverse Videos anzuschauen, während Sie sich selbst befriedigen. Ich konnte ein paar schmutzige Aufnahmen mit Ihnen als Hauptdarsteller machen und mehrere Videos montieren, die zeigen, wie Sie beim lustvollen Masturbieren zum Orgasmus kommen. Wenn Sie immer noch unsicher sind, ob meine Absichten ernst gemeint sind, kann ich Ihre Videos mit wenigen Mausklicks an alle Ihre Verwandten, Freunde und Kollegen weiterleiten. Ich kann diese Videos auch für die Öffentlichkeit zugänglich machen. Ich glaube ehrlich gesagt nicht, dass Sie das wirklich wollen, denn in Anbetracht der Besonderheit der Videos, die Sie sich gerne ansehen (Sie wissen natürlich, was ich meine), können all diese perversen Inhalte zu einem Grund für ernsthafte Probleme für Sie werden.

Wir können diese Situation jedoch auf die folgende Weise lösen: Alles, was Sie tun müssen, ist eine einmalige Überweisung von 1850 $ auf mein Konto (oder den entsprechenden Betrag in Bitcoin
je nach Wechselkurs zum Zeitpunkt der Überweisung) und sobald die Transaktion abgeschlossen ist, werde ich alle schmutzigen Inhalte, die Sie entblößen, sofort entfernen. Danach können Sie sogar vergessen, dass Sie mir begegnet sind.
Außerdem schwöre ich Ihnen, dass alle schädlichen Programme auch von allen Ihren Geräten entfernt werden. Zweifeln Sie nicht daran, dass ich meinen Teil erfüllen werde. Das ist wirklich ein großartiges Angebot zu einem vernünftigen Preis, bedenkt man, dass ich ziemlich viel Energie darauf verwendet habe, Ihr Profil und Ihren Datenverkehr über einen längeren Zeitraum zu überprüfen.
Wenn Sie keine Ahnung vom Bitcoin-Kaufprozess haben, können Sie ihn ganz einfach online durchführen, indem Sie sich alle notwendigen Informationen beschaffen.
Hier finden Sie meine Bitcoin-Wallet: [redacted]

Sie sollten die oben genannte Überweisung innerhalb von 48 Stunden
(2 Tagen) nach dem Öffnen dieser E-Mail abschließen. Die folgende Liste enthält Aktionen, die Sie vermeiden sollten:
....

Lassen Sie uns dieses Geschäft auf faire Weise abschließen!
Ach ja, noch etwas... in Zukunft sollten Sie sich besser nicht mehr in ähnliche Situationen verwickeln lassen!
Ein letzter Rat von mir: Ändern Sie regelmäßig alle Ihre Passwörter für alle Konten.

Example of a Finance Phishing Mail

Figure 13:
Example of a finance phishing mail
Source: BSI

Von: Sparkasse Mitteilung <SparkasseMitteilung@[redacted]>
Gesendet: 5. März 2022 09:31
An: [redacted]
Betreff: Mittteilung Ihrer Sparkasse

[redacted]

Verifizierung benötigt

Sehr geehrte*r Kunde*in,

Durch die neuen Änderungen des Bundes sind wir die Kreditinstitute dazu verpflichtet in regelmäßigen Abständen Informationen unserer Sparkassen-Kunden zu überprüfen.

Wir als Ihr Kreditinstitut haben die neuen Gesetze umgesetzt.

Mit dem Verfahren können unsere Kunden Ihre Informationen für die Legitimation ganz einfach durchführen.

Anschließend werden die von Ihnen eingetragenen Informationen an einen unserer Kundenberater übermittelt und vervollständigt.

Die Überprüfung muss bis zum 31.03.2022 abgeschlossen werden. Wir bitten Sie daher diese Legitimation schnellstmöglich zu vervollständigen. Andernfalls werden wichtige Funktionen Ihres Giro-Kontos für eine bestimmte Zeit eingeschränkt.

Zur Bestätigung

Wir bedanken uns für Ihre Aufmerksamkeit.

Viele Grüße, Ihre Sparkasse

1.2.5 — Social Bots

Social bots are computer programmes that can be used to simulate and automate communication in social networks. This automation is used as a tool to distribute content. As a result, social bots can be used as a harmful tool to systematically spread false news and propaganda, as well as malicious content (for example phishing postings in social networks).

In cooperation with the University of Münster, the BSI conducted an analysis on the topic of "Detection, Spread and Technological Development of Social Bots" in 2021. The aim of the analysis was not only to examine current technologies for the detection of social bots, but also to analyse the current situation against the background of the 2021 Bundestag elections. The analysis built on and extended the findings of a 2017 study. The focus of the investigation was, among other things, on the dissemination of malicious content (for example phishing links) in social networks. The analysis of the two studies has shown that social bots have become common tools in social networks. However, fully automated and reliable proof that a specific account is a bot is only possible in a few cases. This is because the technical development of automated detection mechanisms for social bots is still prototypical and at the same time not very reliable.

The most promising methods are therefore those that consist of upstream automatic detection of conspicuous account behaviour and downstream investigation of suspicious accounts by human analysts. Therefore, as part of the 2021 situation analysis, this new methodology was used to detect suspected automation against the backdrop of the 2021 federal election. The social network Twitter was chosen for this purpose because it provides a suitable interface for data analysis. The entire Twitter stream was analysed, restricted to German-language content on the federal election.

However, no recognisable spread of malware or infected links was found in the Twitter stream examined during the election campaign.

It could also be generally observed that various interest groups did use social bots in the election campaign. However, these were unable to achieve any demonstrable influence on political opinion-forming due to low coverage. No attribution to parties and/or organisations was made, as the BSI has no mandate to evaluate the content of social media accounts. While in 2017 mainly post multipliers were used for the automated distribution of content, i.e. the multiple posting of tweets, in 2021 it was reply multipliers. They aim to spread content in discussions as subtly as possible. Post multipliers are easily identified by human users and are also quickly recognised and removed by Twitter. Reply multipliers, on the other hand, react to individual posts by users with similar or identical content. The latter perceive this as normal communication. It is also more difficult for Twitter to detect spam or social bots in this case.

In the meantime, it is technically possible to automatically generate realistic tweets with the help of language models. Especially when it comes to texts as short as those on Twitter, this content can hardly be distinguished from other natural-language texts written by humans. This makes it possible to circumvent a previous weakness in social bots, namely generating texts that are similar to texts written by humans (see chapter *Artificial Intelligence,* page 94). The methods used to date to detect social bots are not capable of reliably identifying them.

1.3 — Vulnerabilities

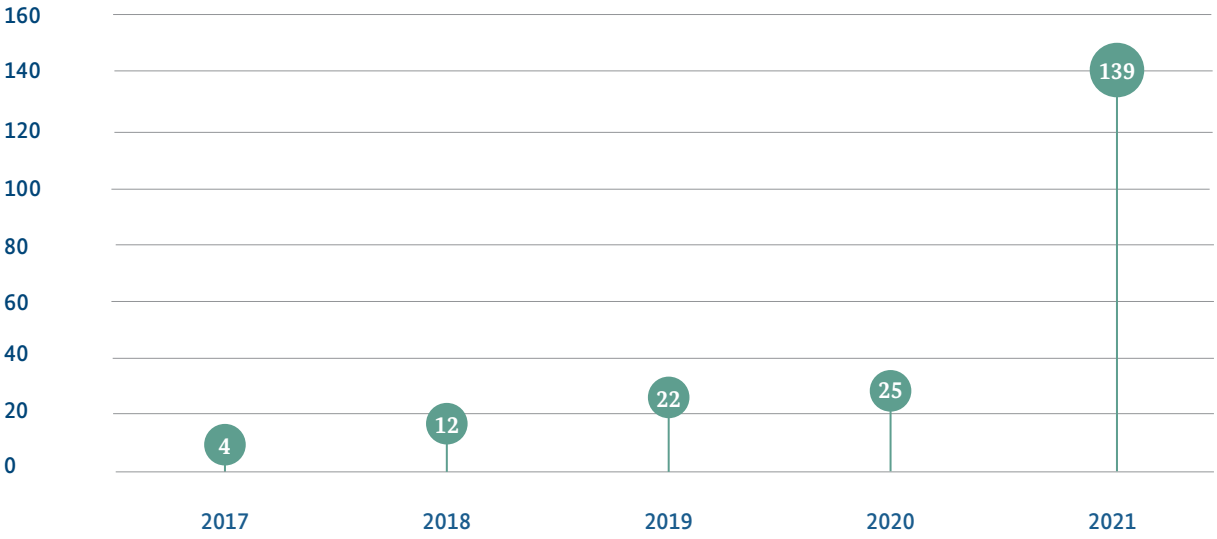
The number of known vulnerabilities has increased recently. Cybercriminals can use the gaps in software and hardware products to cause widespread damage or to tap into valuable information. Detecting, reporting and closing the corresponding vulnerabilities as quickly as possible is therefore particularly important.

1.3.1 — Vulnerabilities in Software Products

The principle of Coordinated Vulnerability Disclosure (CVD) involves the coordinated publication of information regarding a vulnerability and the provision of patches or mitigation measures for affected software products in a transparent, systematic time sequence. For several years, CERT-Bund at the BSI has supported security researchers in reporting vulnerabilities to manufacturers and in coordinating the publication process. To facilitate the evaluation and comprehension of vulnerability reports, the BSI put a vulnerability report form online during the reporting period[6].

Coordinated Vulnerability Disclosure cases from 2017 to 2021
Numbers

Figure 14: Coordinated Vulnerability Disclosure-cases from 2017 to 2021
Source: BSI



The form enables security researchers to report vulnerabilities found in software to the BSI in a structured way. The information provided in it serves to ensure the traceability of vulnerability reports, the determination of the criticality of the vulnerability found and the assessment of possible effects on IT security for the BSI's target groups. As part of a CVD process, the BSI subsequently supports security researchers in communicating with the manufacturer of the vulnerable product and in the coordinated disclosure of the vulnerability and, for example, the creation of security advisories. These are recommendations from the manufacturers to IT security managers in companies and other organisations on how to deal with vulnerabilities that have been found.

Furthermore, many software manufacturers have not yet created the prerequisites for carrying out a CVD process independently. As a first step, they should generally offer an IT security contact to whom security researchers can turn. The BSI supports researchers and manufacturers in carrying out the CVD process and participates as a neutral coordinating body.

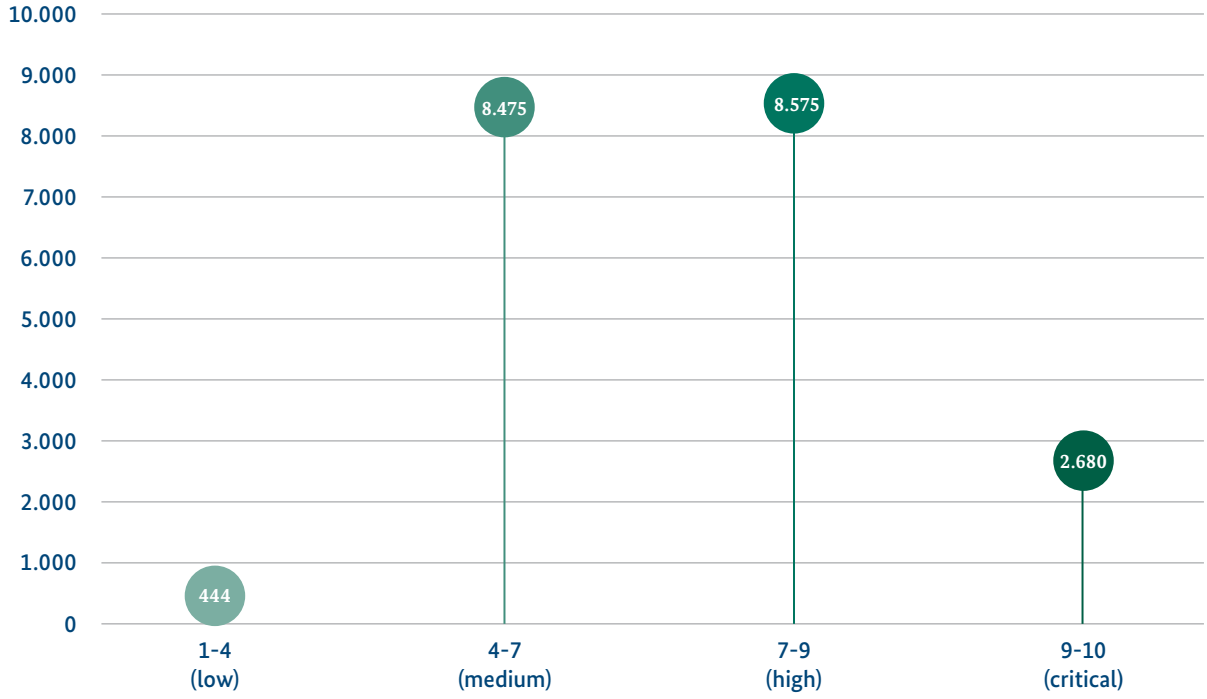
The BSI received a total of 139 CVD notifications in 2021 (see Figure 14). The increase compared to the previous year is probably mainly due to the introduction of the above-mentioned vulnerability reporting form. The community of IT security researchers was consulted in advance. This meant that the reporting form was not only already known there when it was activated on the BSI website, but also fulfilled the requirements that security researchers place on such a reporting option.

As in the previous reporting period, the vulnerabilities reported to the BSI in the current reporting period were often in the software of Covid testing centres. One reason for this is probably that the security research community is aware of the sensitivity of the data stored there and has therefore focused on the relevant data-

Known Vulnerabilities in 2021 according to the CVSS Criticality Score[1]
Numbers

Figure 15:
Known Vulnerabilities in 2021 according to the CVSS Criticality Score
Source: Vulnerability Statistics

[1] Risikobewertung nach CVSS-Version 3.1



bases and applications accordingly (see section *Digital Pandemic Response,* page 61, in addition see section *Extortion with Captured Identity Data,* page 17, on the problem of sensitive data in IT systems).

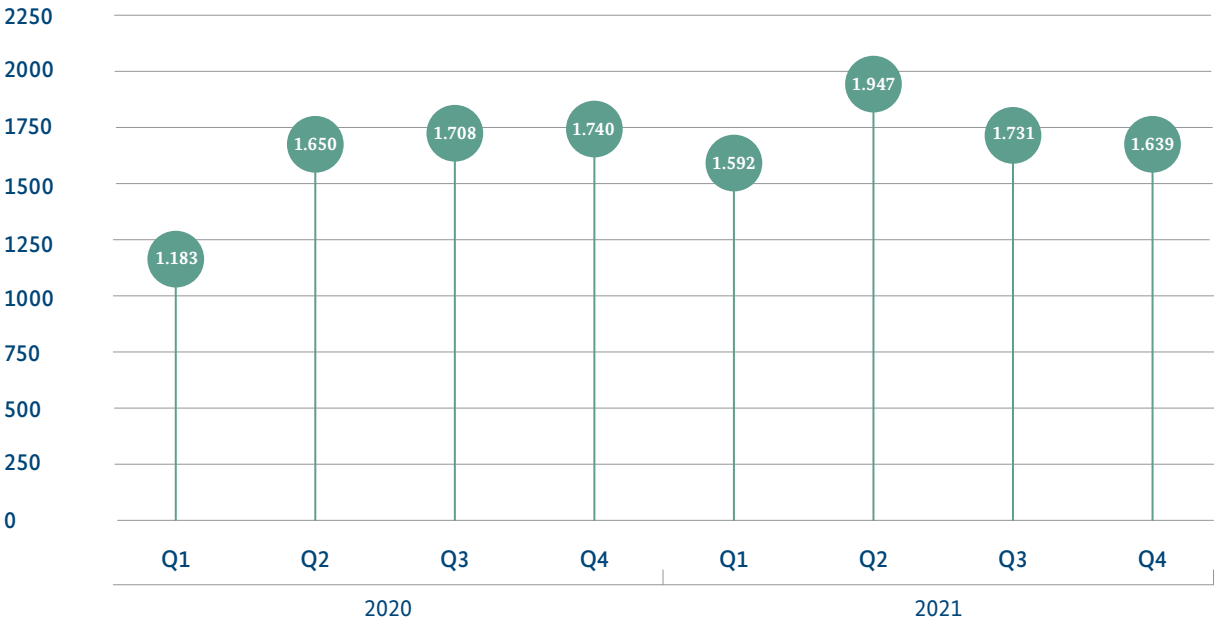
To assess the IT security situation, the BSI also checks public sources daily for new information on vulnerabilities. Based on this, the situation in the reporting period was more threatening than average. On the one hand, with security vulnerabilities in Microsoft Exchange and Log4j, there were again particularly critical vulnerabilities in widely used products (see incident *Log4j: Vulnerability in Open Source Library,* page 37). On the other hand, the number of vulnerabilities that have become known has also increased across all criticality levels. In 2021, the CVSS scoring system, an industry standard used to assess the criticality of vulnerabilities in an internationally comparable way, recorded 20,174 vulnerabilities in software products – around ten percent more than the year before.

The criticality of the vulnerabilities that became known was mixed. About two percent (444) had low scores and 42 percent (8,475) had medium scores on the ten-point scale (see Figure 15). A total of 11,255 – more than half – had high (7-9) or critical (9-10) CVSS scores, with 2,680 of them receiving critical scores. The proportion of critical vulnerabilities in 2021 was around 13 percent.

These and other findings are incorporated into the BSI's Warning and Information Service (WID), which monitors the 150 most common software products on the German market and assesses the vulnerabilities that have become known in them. This makes the WID an essential tool for informing users. Information on vulnerabilities is collected, processed and published on www.cert-bund.de. All interested parties have the opportunity to register for the WID and subscribe to information on the IT products relevant to them as an email. Issues that are assumed to be of particular relevance to private individuals – for example vulnera-

WID Reports 2020 to 2021
Numbers

Figure 16:
WID Reports 2020 to 2021
Source: BSI



bilities affecting common operating systems or Office applications – are also published as technical warnings/ Bürger-CERT warnings.

You can find more information here:

The added value of the WID for users consists, on the one hand, of the fact that up-to-date content from various sources is collected, evaluated and offered centrally in one place. On the other hand, the allocation of issues into different risk groups supports IT security managers in prioritising security updates to be rolled out.

In 2021, WID published a total of 6,910 vulnerability reports in the 150 most popular products – around ten percent more than in the previous year.

In addition, there were 2,412 advisories for IT security officers in federal agencies (up 13 percent from the previous year) and 265 technical warnings (up 17 percent from the previous year).

If information is available on vulnerabilities with an exceptional threat potential, the BSI also publishes cyber security information, which is divided into three categories:

1.) **Cyber security warnings (information on vulnerabilities with technical depth)**

2.) **Management information (information on current threats at the decision-making level)**

3.) **Incident warnings (attack indicators and protective measures observed in incidents that have occurred)**

The Federal Office used this tool a total of 68 times in 2021 (including 49 cyber security warnings, nine management information and ten incident warnings). Particular focus was placed on the Java vulnerability Log4Shell (see incident *Log4j: Vulnerability in Open Source Library,* page 37).

The appearance of Log4shell illustrates a threat that has already been pointed out in the past: the increasing modularisation of software production, i.e. the use of third-party software in own applications (see *The State of IT Security in Germany in 2021,* page 27 f). Often, certain functionalities of a programme or software are implemented using external components that are obtained from third-party providers, but whose security risk for software development is difficult to keep track of. For economic reasons, some manufacturers even stipulate to their software development that, before in-house development, it must be checked whether or not it is possible to obtain the required functions externally. Often such components are then used without knowing exactly their full scope of functions and implementation. In addition, new risks arise due to the way they are integrated into applications if the usage scenarios of the component do not match those of the application. In many cases, components also contain functional parts that are not required for the intended purpose of an application. This not only increases the attack surface of the application, but also creates new dependencies. In addition to availability, vulnerabilities and attacks can also affect the integrity and confidentiality of applications.

To make matters worse, it is very difficult to assess the security of a software component or its integration by developers on the basis of its documentation. Independent security analyses are often required to investigate the security of such components. However, these may only relate to general security risks, which may also only apply to a specific usage scenario. In particular, specific risks inherent in the design (and also the function) of the component or its specific use can be difficult to assess by external parties. Third-party components often try to cover a wide range of usage scenarios in their standard configuration. Components that are delivered with a broad, pre-configured active range of functions are therefore in conflict with the principle of Security by Default.[7]

1.3.2 — Vulnerabilities in Hardware Products

SVulnerabilities in hardware products have in common that they are usually very deeply rooted in the respective architecture or manufacturing process. Attacks start, for example, with the physics of transistors in highly integrated circuits, the microarchitecture of a processor or even the "production" and "supply chain" steps of an IT product. The effort and costs for exploiting hardware vulnerabilities are initially higher than for software vulnerabilities. However, the potential benefit from an attacker's perspective is also higher, as hardware vulnerabilities often cannot be fixed by simple software patches.

As in previous years, two attack classes dominated vulnerabilities in hardware products during the current reporting period. These are, on the one hand, attacks that exploit characteristics of the transient execution of instructions in processors. Since the Meltdown and Spectre attacks were published in 2017, more than 25 vulnerabilities and variations of these attacks now exist. In 2021, for example, the new vulnerabilities "I see dead Micro-Ops", Blindside and CIPHERLEAKS were discovered. Transient executions in modern processors are essential for high performance. At the same time, however, such a microarchitecture poses a fundamental challenge for a vulnerability-free design. Therefore, vulnerabilities from this attack class can be expected to continue as long as fundamental redesigns of the architecture are not carried out.

On the other hand, attacks that exploit side effects in the operation of random-access memory continue to dominate. Here, data values in neighbouring memory cells can be changed by targeted high-frequency accesses to memory cells. Although this phenomenon has been known since 2014, no widely available countermeasures exist as yet. Even error-correcting memory (ECC memory) does not remedy this. In 2021, the BlackSmith attack method demonstrated that modern DDR4 memory is also susceptible to such side effects.

Due to numerous software-based attacks and increased awareness of the threat of cyber attacks, hardware-based solutions are increasingly being used to secure IT systems, for example in the IoT sector, in two-factor authentication (2FA) (see chapter *Two-Factor Authentication,* page 63) or in crypto wallets. Often, commercial off-the-shelf microcontrollers in place of dedicated security controllers are used. However, such microcontrollers usually have hardware vulnerabilities that can be exploited with relatively moderate effort. At the beginning of 2021, for example, vulnerabilities were discovered in several commercially available micro-

Supply Chain Attack on Widespread Virtual System Administrator (VSA)

Situation

On 2 July 2021, supply chain attacks became known via the Virtual System Administrator (VSA) software of an American software manufacturer, which is also widely used in Germany. VSAs are used by Managed Service Providers (MSPs) and IT system houses, for example, for remote maintenance, monitoring and management of their customers' IT systems. MSP's clientele also includes many small and medium-sized enterprises (SMEs). Independent of MSPs, VSAs are also operated by the software manufacturer itself as a Software-as-a-Service. VSA play a sensitive role for an organisation's IT network, because any managed client can be accessed and software can also be distributed via the VSA's management server. In the software supply chain attack, attackers used the REvil ransomware (also known as Sodinokibi) to exploit the VSA's management functionality. Using the zero-day vulnerability CVE-2021-30116, the attackers distributed the ransomware REvil en masse to clients managed by the VSA within a few days. The VSA used by MSPs were affected. In contrast, the systems managed by the VSA software manufacturer's Software-as-a-Service (SaaS) solution were spared from the attack. Nevertheless, the SaaS was shut down as a precaution to prevent the attack from spreading until appropriate patches for the zero-day vulnerabilities were available. Therefore, the VSA was not available for a period of nine days.

Between 800 and 1,500 end customers may have been directly affected by the attack, as well as probably others for whom the SaaS was temporarily unavailable. On 11 July 2021, the VSA's software vendor provided patches for the exploited zero-day vulnerabilities.

On 22 July 2021, the software manufacturer received the key material for the attack campaign from a trusted third-party source. In this way, the data of the end customers affected by the encryption could be restored.

Assessment

Software supply chain attacks are characterised by the fact that the malicious code is already incorporated into legitimate software during the manufacturing process. Supply chain attacks on products such as the VSA (like here via the IT network) can be extraordinarily "successful". Such managing software often has exceptions to access restrictions or extended access rights to clients because they are also used to play out software in regular administration. In this case, the attackers exploited this ability of the software.

MSPs often provide software services to numerous companies, both large and small and medium-sized. Attacks of this kind against MSPs may therefore scale quickly and can result in widespread outages beyond the attacked company in the short term. Even if attackers do not succeed in transferring the network from the attacked MSP network to the customer networks, the repair work that follows the attack often results in outages or restrictions for the end customers of the MSPs.

The infrastructure of the REvil ransomware, including the payment portal and leak site, went offline completely on the morning of 13 July 2021. According to media reports, the shutdown is due to measures taken by US authorities as well as unspecified partner countries and IT security service providers.

After a brief return in September 2021, the RaaS REvil infrastructure went offline again in October 2021.

Response

The BSI issued a cyber security warning on 4 July 2021, which was then regularly updated. The BSI intensively monitored how German organisations were affected, advised those affected on IT forensic measures and provided first aid documents.

Log4j: Vulnerability in Open Source Library

Situation

At the beginning of December 2021, a vulnerability in "Log4j" became known, which was first widely publicised in the IT security community and shortly afterwards in the media. Log4j is a free and open source library that is included in numerous applications to log events for later analysis. This library is very common in Java applications. The vulnerability made it possible to execute arbitrary malware on systems with vulnerable applications.

Assessment

The high criticality of the vulnerability resulted from the comparatively easy exploitability in some exposed applications. At the same time, especially with commercial software, there is often no "content specification", meaning that many IT managers were often unable to know which subcomponents the programmes they used consisted of and whether they were affected by the vulnerability in Log4j. Since it was already known from past incidents that attacker groups usually exploit known vulnerabilities on a large scale and thus lay the foundation for further malicious activities such as installing encryption Trojans or stealing confidential information, the vulnerability was assessed as particularly critical.

Response

Because of the risk of a possible broad exploitation of the vulnerability for cyber attacks, a so-called "special organisational structure (Besondere Aufbauorganisation, BAO)" was created in the BSI's National IT Crisis Response Centre. The impact of the vulnerability on cyber security in Germany was analysed, as well as the level of concern among the target groups of the BSI.

Furthermore, a red-level cyber security warning (highest warning level) was published and a guideline for implementing reactive and preventive measures was distributed to the public as well as to the target groups of the BSI. Active media work by the BSI drew the attention of those responsible for IT in Germany to the problem in order to bring about a short-term solution to the problem.

controllers in which the readout protection could be bypassed by deliberately changing the power supply. This allows secrets stored on the controller, such as secret keys, to be read out.

Another trend is the integration of security functionality in dedicated areas of the processor, a so-called Trusted Execution Environment (TEE). However, integrating such security functions into a complex design is challenging; and almost all implementations available on the market have revealed vulnerabilities over time. In 2021, the SmashEX vulnerability was discovered, which exploits incorrect behaviour in many TEEs when programmes enter an error state. This behaviour allows access to protected sections of data.

Exploiting vulnerabilities in hardware products, especially those based on transient execution in processors, is costly in practice. Since simpler attack vectors exist due to numerous software vulnerabilities, attacks on the aforementioned hardware vulnerabilities are currently not widely exploited. To avoid exploitable hardware attacks, critical data and operations should be stored and processed in dedicated security elements or in logically completely separated processor areas. Confidence in the implemented security functionality can only be created by an independent security certification, for example according to the ISO standard 15408: Common Criteria for IT Security Evaluation.

Further information can be found here:[c]

1.4 — Advanced Persistent Threats

Advanced Persistent Threats (APT) differ from other cyber security threats in the motivation and modus operandi of the attackers. For example, while malware is usually distributed en masse by criminal, opportunistically motivated attackers (see chapter *Ransomware,* page 13), APTs are often attacks planned over the long term and with great effort on individually selected, singled-out targets. APT attacks are not for criminal gain, but for obtaining information about the target and, if necessary, for sabotage.

In the current reporting period, there were a number of new developments that shaped the APT threat landscape.

Perimeter Attacks:

APT groups continue to expand their portfolio of attack types. While in the past years mainly emails with malicious attachments or malicious links were sent, an increase in attacks on perimeter systems has been observed for around two years. This includes servers, firewalls, VPN gateways and routers that are directly accessible from the Internet. In the majority of cases, the attackers look for known vulnerabilities which have not yet been updated.

In addition to exploits against vulnerabilities, password spraying and well-known, simple techniques such as brute forcing are being increasingly used. This trend can be observed with a diverse set of attacker groups, for example APT28, APT25/Ke3chang and APT31.

In these attacks, the attackers typically install webshells on compromised servers. These are a few lines of code that allow attackers to connect to the servers from the outside and execute commands.

This development has implications for the work of IT security teams. Perimeter systems are usually less well monitored, and there are fewer security products than for end devices or office computers. Webshell activity often cannot be detected in network traffic, but must be specifically detected on the systems (i.e. host-based). The widespread sharing of Indicators of Compromise (IoCs)

in the security community is becoming less effective, as a much-used type of IoC relies on the use of control servers. However, the attack methods in question often work without a control server and access is made directly through anonymisation services to the webshells.

For the foreseeable future, the "perimeter" attack vector will remain relevant and should be considered with appropriate priority in all IT security considerations (network architectures, incident handling, forensics, logging, consulting.

Compromised Home Routers for Anonymisation:

One consequence of the attacks on perimeters is that attackers now need fewer control servers and can instead actively establish connections themselves from anonymising networks. They use these connections to execute exploits and, after a successful compromise, control the further spread in the victim's IT network via webshell (lateral movement). This is done using commercial VPN services. Alternatively, a new trend is to compromise home routers in order to set up attacker-operated anonymisation networks via these devices.

Examples of groups that compromise routers are APT31, BlackTech and APT32/OceanLotus.

The BSI assesses that other groups will attack routers in the future. One reason is that due to the trend towards perimeter attacks, there is a corresponding need for infrastructure to disguise internet connections; additionally, routers are widely available, tend to be poorly maintained by users and are typically not equipped with security and monitoring products. It is also more difficult for security companies to obtain telemetry about routers and thus detect attacks, which is likely to be another incentive for attackers.

***The Cloud as an Entry Point*:**

Another trend is the use of cloud services as an attack vector. Until now, the main risk of using the cloud was that the data processed or stored in the cloud could be stolen by attackers. In the current reporting period, however, reports on the APT29/Nobelium group showed that the cloud can also be misused as an entry point into customers' internal IT networks. For example, the attackers first try to guess or steal passwords for cloud access. Once they have gained such access, they use trust relationships between the cloud and the customer network to access computers on internal customer networks. It is likely that other groups will build on this trend and possibly develop new techniques.

Sabotage in the Middle East:

In the Middle East, actors are beginning to use cyber sabotage in interstate conflicts. One of the parties in the conflict relies on the disguise of such attacks by means of ransomware. Other actors with opposing goals carry out sabotage attacks under the flag or guise of hacktivism, which also have an impact on the population, for example by disrupting train logistics or petrol supplies. The possibility that these strategies could spread outside the Middle East in interstate conflicts that still remain below the threshold of military escalation cannot be ruled out. Cyber sabotage was also used in Russia's war of aggression against Ukraine (see chapter *Cyber Security Situation in the Context of the Russian War of Aggression Against Ukraine,* page 45).

Hackers-for-Hire:

During the reporting period, special media reports highlighted so-called hackers-for-hire, who sell products or services for offensive cyber operations. There are a number of companies, such as NSO Group Technologies and its product Pegasus, that offer services and products for this purpose. Internationally, strategic measures have already been discussed and partially implemented, including sanctions and new rules on export restrictions. The existence of specialised companies for the development of exploits, malware services and the execution of cyber operations also makes it possible for actors who previously had few offensive capabilities to carry out attacks. In addition, companies that operate internationally make it more difficult to distinguish groups of attackers (or customers) from one another. The threat situation is thus becoming more critical and at the same time more difficult to analyse due to the increasing number of attackers and the high availability of qualitatively mature exploits and malware.

Spear Phishing by APT Group GhostWriter

Situation

In the reporting period, in a campaign phishing emails were sent in several waves to German politicians and activists. The phishing waves lasted for several months. The campaign was attributed to an attack group called GhostWriter. The group is known to collect access to email inboxes and websites and use them to distribute content for disinformation campaigns.

A particular feature of the attacks was that they were not directed against the official inboxes of parliamentarians and their staff. Instead, the phishing emails were sent to their personal GMX and T-Online inboxes. The aim was to trick the recipients into entering their private email credentials on the attackers' servers.
In March 2022, the Federal Office for the Protection of the Constitution warned in a letter to potentially affected persons that the GhostWriter group was again sending phishing emails against German citizens. The authority assumed a connection with the war of aggression against Ukraine and the resulting German support for Ukraine[8].

Assessment

What was striking in 2021 was that the group, which is normally active against Eastern European targets, became active in Germany precisely in the "super election year" of 2021. It could therefore not be ruled out that there was a connection with the upcoming federal and state elections at the time. However, it was not possible to identify the motivation or goal of the campaign beyond doubt. No disinformation content that could be clearly linked to this campaign was observed. In particular, members of state parliaments were also attacked in federal states where elections were not held in 2021 (and in some cases not even in 2022).

A BSI analysis of the 2021 campaign showed that the attackers sometimes addressed inboxes that did not belong to politicians but to people with the same name. Many of the email addresses could be found via web searches or in large password leaks. The BSI assesses that this is likely how the attackers collected the email addresses and that they did not verify whom the inboxes belonged to.

Response

The matter was handled at the National Cyber Defence Centre. The authorities undertook awareness-raising measures and IT security consultations with parliamentary groups and other potentially affected parties.
At the beginning of September 2021, before the federal election, the Federal Government expressed its assessment in a press conference that the group could be attributed to the Russian military intelligence service GRU.

1.5 — Distributed Denial of Service

Denial-of-Service attacks (DoS attacks) are overload attacks on Internet services. If such an attack is carried out by several systems in parallel, it is called a distributed denial-of-service (DDoS). DDoS attacks have been around for over twenty years now. DDoS continues to be one of the main threats to cyber security. This is also confirmed, among other things, by a representative study by Bitkom e.V., in which more than 1,000 companies from all sectors were surveyed on how they were affected by cyber attacks in 2020 and 2021. Around 27 percent said that DDoS attacks had caused damage to the company within the last twelve months. This was 2nd place among attack types behind malware at 31 percent and corresponded to an increase in DDoS attacks causing damage of around eight percentage points compared to the previous reporting period[9].

During the reporting period, the BSI observed the development of DDoS attacks in the network of a major German internet provider. The average bandwidth in the reporting period was around 684 Mbps (megabits per second). However, individual attacks repeatedly reached maximum bandwidths of over 200,000 Mbits. The maximum measured bandwidth of a DDoS attack in this data was over 290,000 Mbits in the reporting period. The attack took place on 2 December 2021 and lasted 228 minutes. The average bandwidth of this attack was 50,000 Mbits.

Averaged across all attacks, the mean bandwidth of observed DDoS attacks tended to decrease during the reporting period (see Figure 17).

One of the reasons for this is probably that a structural change within the DDoS attack types that has been observable for years is continuing: The attackers no longer rely so much on high bandwidths, but attack more at the network and transport level, which goes hand in hand with lower bandwidths. In these attacks, the attackers proceed precisely in order to trigger overloads in the attack target with an efficient use of resources.

Technical Situation

Internationally, security provider Radware Inc. recorded 75 percent more DDoS attacks in 2021 within the first nine months than in the first nine months of the previous year[10]. In Germany, the German mitigation service provider Link11 recorded a 41 percent increase in attacks for the full year 2021 compared to the previous year[11].

Despite the trend towards network and protocol level attacks, record levels of volumetric DDoS attacks were broken on three continents in Q3 2021. Both the bandwidths and the demand rates reached previously unobserved levels. Microsoft reported a thwarted DDoS attack with a bandwidth of 2.4 Tbps (terabits per second) that targeted an Azure customer in Europe in the last week of August 2021[12]. This is well above the maximum bandwidth observed by the BSI in the German provider network (see above). According to Microsoft, the attack traffic originated from about 70,000 sources and several countries in the Asia-Pacific region as well as in the United States. The attack vector was UDP reflection, which lasted for more than ten minutes with short bursts, each increasing to terabit volumes within seconds. Due to its high attack bandwidth, the attack had a very high technical potential. As the connection bandwidth in the target was higher than the attack bandwidth, the incident had no significant impact.

In mid-August, Cloudflare reported a DDoS attack that reached a record request rate of 17.2 Mrps (million requests per second). The attack was carried out using the Mirai botnet, involving more than 20,000 infected devices from 125 countries. The target of the attack was a company in the financial sector[13].

Only a little later, the Russian DDoS mitigation service provider Qrator reported a DDoS record value of 21.8 Mrps for the DDoS parameter request rates[14]. This figure was reached using the newly discovered Meris botnet, with approx. 250,000 infected devices worldwide, most of which come from a single manufacturer. The target of the attack was the infrastructure of a Russian bank hosted on Yandex servers. According to unofficial sources, the botnet can be rented for around 80 US dollars per hour.

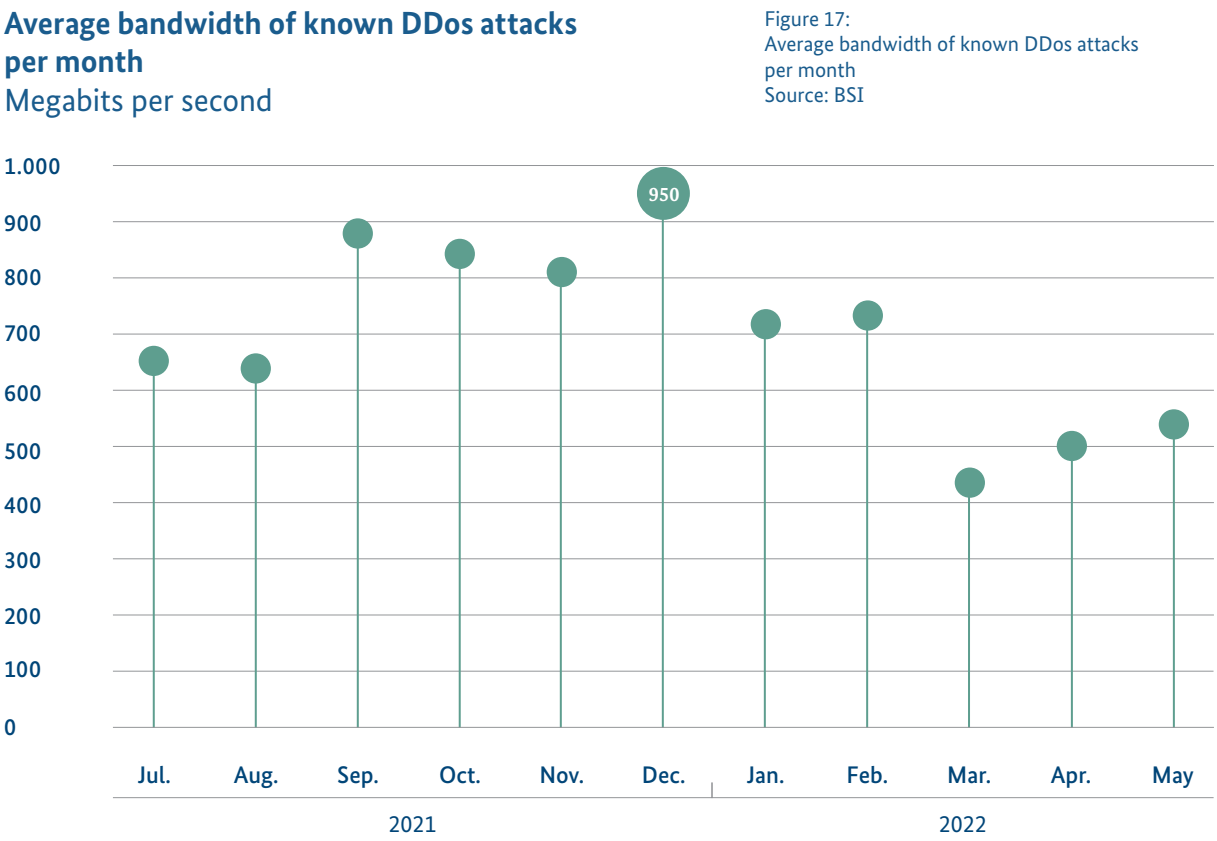


Figure 17:
Average bandwidth of known DDos attacks per month
Source: BSI

During attacks against voice over internet protocol (VoIP) attacks on different OSI layers were combined. While application level attacks targeted HTTP websites and APIs, network and transport level attacks targeted VoIP server infrastructures. TCP and UDP flooding were used for this. VoIP services are particularly vulnerable to UDP-based attacks.

DDoS Protection Rackets as a Modus Operandi of DDoS Attacks

As in the previous reporting period, large-scale DDoS extortion was again observed at the beginning of June 2021. At that time, several countries in Europe had already been affected. Extortion attempts were confirmed in Ireland, Belgium, Portugal, Finland, Austria, Denmark and Switzerland, among others. The wave of extortion hit many companies at a time when a large part of the workforce was still working remotely and relied on unrestricted access to the company network. The approach of the cybercriminals, which call themselves "Fancy Lazarus", was similar in each of the attacks: In an extortion email sent to a company, they announce a demo attack and demand payment of bitcoins. The announced demo attack is mostly carried out with peak bandwidths of approximately 30 to 250 Gbps using the DNS reflection attack vector. If the company fails to pay on time, it is threatened with a high-bandwidth DDoS attack of more than two Tbps.

There are different reports about the actual initiation of these attacks in case the deadline has passed. The FBI has reported many affected companies that did not observe any further activity after the deadline or were able to successfully mitigate the attacks[15]. Link11 also reported on companies that experienced significant disruption. However, the peak bandwidths achieved were regularly far below the threatened attack bandwidth of two Tbps[16].

The extortion campaigns also targeted several VoIP providers in North America and Europe between August and October 2021.

The BSI also observed an increase in DDoS activities in 2021 ahead of the high-turnover events in the e-commerce sector (Black Friday, Cyber Monday, pre-Christmas

sales, Christmas sales). The setting of record-breaking peaks for attack bandwidth (DDoS against MS Azure) and for request rates (DDoS against Yandex with Meris botnet) by newly developed DDoS attack technologies are evidence.

The BSI has issued a public warning in the forefront of the pre-Christmas shopping season based on various observations of technical DDoS developments and developments in DDoS extortion attacks. Organisations were advised to evaluate their DDoS protection measures in order to be able to counter the current threat situation. Special attention should be paid to UDP reflection attacks and attacks with high request rates.

In fact, DDoS activity increased by 100 percent compared to the previous year[17]. At 1.1 Tbps, the highest volume attack measured in Germany to date was detected, which was twice as high as the previous record value from May 2021 with 550 Mbps.

In addition to the criminally motivated DDoS extortion attacks described above, the BSI has also observed cases of politically motivated DDoS activities.

For example, there were several cases of DDoS incidents around the 2021 federal election in Germany. Situations where websites were overloaded due to legitimate requests were also observed, for example, around party conventions.

In the context of the Russian war of aggression against Ukraine, politically motivated DDoS attacks were also carried out internationally, which were predominantly attributed to the phenomenon of hacktivism (see chapter *Cyber Security Situation in the Context of the Russian War of Aggression against Ukraine,* page 45).

1.6 – Attacks in the Context of Cryptography

Cryptographic mechanisms are important building blocks for the implementation of security functions in IT products. State-of-the-art cryptographic algorithms provide excellent security guarantees for this. In Technical Guideline TR-02102, the BSI recommends a number of cryptographic procedures and protocols that are generally considered secure based on in-depth mathematical cryptanalysis.

In contrast, the following factors can lead to a reduction of the theoretical security level in practice:

- Weaknesses in cryptographic mechanisms or protocols
- Implementation errors
- Inadequately secured side channels
- Weaknesses in key generation

Selecting unsuitable algorithms or faulty implementations can, in the worst case, completely nullify the effectiveness (for an example, *see box Weak RSA Key Generation – Wrong Methods and Bad Randomness,* page 44.)

When securing cryptographic systems that are intended to withstand even attackers in close proximity, additional side channels (e.g. power consumption or electromagnetic radiation of the devices) must be taken into account, via which data can also flow out. Side-channel analysis, that is, analysis for vulnerability to side-channel attacks, is an emerging branch of research that has produced new countermeasures and new attack vectors. A current trend in side channel analysis and mathematical cryptanalysis is the use of artificial intelligence methods (see chapter *Artificial Intelligence in Cryptography,* page 95).

An essential prerequisite for the secure use of cryptography is the generation of true random numbers, which must fulfil certain criteria of quality. Random numbers are needed, among other things, for key generation. For cryptographic applications, random numbers must not be predictable and must not have exploitable statistical defects. In order to prevent attacks by weak random numbers, the BSI defines functionality classes of random number generators for different purposes in AIS 20 and AIS 31 (application notes and interpretations on the scheme). On a positive note, many products now have a physical random number generator certified under the German Common Criteria scheme.

However, the security guarantees of many cryptographic algorithms used today no longer apply as soon as a sufficiently powerful quantum computer is available. Chapters *2.5.2 Cryptography* (page 96) and *2.5.3 Quantum Key Distribution* (page 96) show ways to counter this threat and present the BSI's activities in this field.

Weak RSA Key Generation – Wrong Methods and Bad Randomness

The security of RSA-based cryptographic procedures is based in particular on the difficulty of factorising RSA modulus n. This is part of the public RSA key and the product of two non-public prime numbers p and q. If p and q are known to an attacker, the cryptographic procedure can be easily broken. In the Technical Guideline TR-02102, the BSI specifies the length of the RSA module and its generation. If these conditions are observed when generating n, it is practically impossible, according to the current state of knowledge, to determine the two prime factors p and q from the knowledge of n only. RSA-based methods will no longer be secure as soon as a sufficiently strong quantum computer is available (see chapter Cryptography, page 96).

In February 2022, an attack was published (CVE-2022-26320)[18] in which Fermat's factorisation method was applied to a large number of published RSA moduli and thus the prime factors could be determined for a small number of these moduli. The RSA moduli in question belonged to the public keys of TLS certificates of various printer models, all of which used a specific cryptographic module. Fermat's algorithm, which is more than 300 years old, can always be applied efficiently when the two primes p and q are relatively close to each other. This can happen, for example, if the key generation algorithm first chooses p at random and then counts up from p until the next prime number q is found. In essence, Fermat's algorithm searches for candidates for the prime factors p and q in a relatively small neighbourhood of the root of n. If p and q are sufficiently close, the search is quickly successful – and n is factorised. For example, in the extreme case where p and q coincide, the prime factor p is already given by the square root of n.

Another vulnerability published in September 2021 concerns the generation of identical RSA keys by the Javascript library Keypair (CVE-2021-41117)[19]. Keypair was used by the GitHub client GitKraken and possibly other clients to generate keys for the SSH protocol. An analysis of the source code of Keypair identified a number of critical vulnerabilities in the implementation of random number generation: Keypair uses its own deterministic random number generator. This must initially be given a seed, which should ideally consist of real randomness. Once this has been done, any further processing is completely deterministic: Identical seeds always lead to the output of identical random numbers. An error in the source code of Keypair prevents the execution of an RNG of the Javascript library that should actually be used to calculate the seed. The only remaining alternative seed source is an RNG that is unsuitable for cryptographic purposes. An additional implementation error ultimately results in this RNG outputting almost only zeros. The values output by the Keypair RNG thus repeat regularly and result in the generation of identical RSA keys.

1.7 — Hybrid Threats

Unlawful foreign influence operations, so-called hybrid threats, pose a threat to the state, economy and society and are intended to destabilise the respective target country. Hybrid threats can include different measures that are deployed in an orchestrated manner, with the aim of disguising authorship as much as possible. The measures and attack vectors usually remain deliberately subtle – compared to an open military conflict – and often have an ambivalent effect that makes it difficult for the target country to respond to this type of threat. Potential methods include inter alia cyber attacks in particular, as well as economic measures, the targeting of immigration or disinformation. Measures can also increase in intensity and can lead to open armed conflict with hybrid warfare, as illustrated by Russia's war of

aggression against Ukraine (see chapter *Cyber Security Situation in the Context of the Russian War of Aggression against Ukraine,* page 45).

DThe "cyber" dimension plays a prominent role in terms of hybrid threats. Cyber attacks are an attractive attack vector for hybrid attackers, especially due to their speed, greater difficulty of attribution, lack of location and borders, and low cost, which can also be used as a multiplier to support other methods.

Attacks in the "cyber" dimension can also have an effect in other dimensions, such as information or media. One example of this is so-called hack-and-act operations, in which data is first captured by means of cyber attacks and then published by an attacker at a later, favourable time.

The BSI's tasks in the defence against hybrid threats in the "cyber" dimension include, among other things, the establishment and coordination of measures to ensure the security of elections, dialogue with operators of social media, raising the awareness of the state, the economy and society for IT security issues, as well as the support of operators of critical infrastructure (see incident *Cyber Attack on German Petroleum Trader,* page 50).

The reporting period was marked by the "super election year 2021" and potential threat scenarios for the federal election. In the run-up to the election, there were waves of phishing emails against German elected officials in the federal and state governments, which can be interpreted as preparatory acts for further attacks, perhaps also in the context of spreading disinformation. The Bundesamt für Verfassungsschutz (BfV) and the BSI therefore issued a joint warning and took appropriate measures to protect selected officials.

1.8 – Cyber Security Situation in the Context of the Russian War of Aggression against Ukraine

The Russian war of aggression against Ukraine has been accompanied by ongoing operations in cyberspace. This requires permanent monitoring and assessment of the situation. To this end, the BSI is in constant close contact with national and international authorities and reports regularly to the Federal Government and the federal administration. Cooperation with national authorities takes place in particular in the National Cyber Defence Centre.

There have been many different types of cyber activities surrounding the war. During the first days, so-called wipers were used in particular against Ukrainian agencies. Wipers are programmes that are used to irretrievably delete data. They were used against Ukrainian banks, for example. Since the beginning of the war, increased activity by certain APT groups has also been observed, for example spear phishing emails directed at Western political, administrative or military agencies.

At the beginning of the war, troll activity was observed on social media in Germany. In the process, a large number of pro-Russian comments were left on social media sites of Western media.

In the course of the war, hacktivist groups appeared. These were activists who took sides with one of the two sides and attracted attention through high-profile actions. A prominent example is the pro-Russian group Killnet, which carried out DDoS attacks on targets in European countries, among other things. The BSI assessed the threat for Germany from DDoS attacks by Killnet as rather low. There were several waves of attacks against German targets that were attributed to Killnet. However, the attack bandwidths used here were comparatively low and, according to the BSI's findings, the attacks had little impact on availability of services. They could be effectively mitigated with the activation of DDoS protection mechanisms at the latest.

Prominent examples of pro-Ukrainian hacktivist groups here, in turn, are the Anonymous and IT-Army collectives. There have also been attacks against companies outside Russia that either have business relations with Russia or belong to a Russian group. One example is an attack by Anonymous against a German CI operator that is part of a Russian oil company. The attack resulted in the limitation of a critical service.

The cyber attacks observed in Ukraine showed mostly no substantial technical innovations. The exception is a new variant of Industroyer. The malware specifically targets process control systems and was used in 2016 to cause power outages in Ukraine. Industroyer2 was found again in Ukrainian substations in April 2022, but was able to be deactivated before it could sabotage anything.

The sanctions against Russian companies also led to restrictions on IT services for Russian companies. For example, an IT security incident against a Russian company in Germany showed that rapid recovery by IT

service providers was only possible to a limited extent. The availability of software updates may also be limited for sanctioned companies.

The attackers behind the RaaS Conti positioned themselves as pro-Russian at the beginning of the Ukraine war and threatened Western states with retaliatory strikes if they attacked Russian facilities or critical infrastructure. As a result of this positioning, a large amount of the group' internal data was leaked, showing that the pro-Russian positioning of the hacker group must have been quite controversial internally. Then, in April 2022, several Conti incidents were reported in Costa Rica, which the attackers described as a demonstration of a cyber attack against an entire country. As a result, on 8 May 2022, the day he took office, the President of Costa Rica had to declare a state of emergency. At least 27 state institutions were affected, nine of them severely. For the first time ever, an entire state was affected by a cyber attack. In addition to the attackers' claim that it was a targeted attack for demonstration purposes, the BSI cannot rule out a financially motivated, opportunistic attack that the attackers only reinterpreted afterwards. According to IT security service provider AdvIntel, the attackers behind RaaS Conti shut down their servers on 19 May 2022. The BSI can neither confirm nor deny this. In the event that the RaaS Conti is terminated, the BSI assumes that the affiliates will migrate to other active RaaS groups.

As part of its analytical expertise, the BSI warned of collateral damage in Germany at the beginning of the war. One such case occurred during the war when an attack on a satellite service provider led to the failure of modems in German wind turbines. This case is the first known cyber collateral damage that the BSI has observed in the course of the conflict (see incident *Collateral Damage after Attack on a Satellite Communications Company,* page 49).

The Russian war of aggression against Ukraine has further increased the overall threat situation in Germany. Numerous cyber-activities against various Western states could be observed, some of which also affected critical infrastructure in Germany (see incident *Collateral Damage after Attack on a Satellite Communications Company,* page 49, and incident *Cyber Attack on German Petroleum Trader,* page 50). However, a centrally controlled campaign against Germany with a broad impact was not discernible by the time of going to press. At the same time, there is still a major threat from attacks that are not related to the war against Ukraine, especially from ransomware. Furthermore, the BSI has observed that the war against Ukraine has also been used as a scam in the context of spam. The first spam emails targeting the broad mass of the population appeared shortly after the start of the war. Charity scams, which had already been observed in connection with the flood disaster in the summer of 2021, also exploited the war against Ukraine to supposedly raise funds (see Figure 18).

To appear trustworthy, the attackers also forge the corporate design of reputable aid organisations. The victim is thus tricked into clicking and then revealing supposed donations and personal data (see Figure 19). In advance fee scams related to the war, for example, attackers posed as Ukrainian refugees and promised spam victims a handsome reward for their financial help in a supposed escape.

The effects of the war were also evident in the category of finance phishing. Attackers forged the corporate design of widespread banks and savings banks for this purpose and sent spam emails to allegedly check compliance with sanctions. However, the aim of these phishing emails is merely to trick the victim into clicking and to grab personal data such as access data for online banking.

Example of Charitiy Scam Mail

Figure 18:
Charitiy Scam Email
Source: Phishing radar of the BSI in cooperation with NRW Consumer Advice Center

Von: Ukraine Crisis Relief Fund <ukrarelief@unations.com>
Gesendet: Dienstag, 1. März 2022 11:39
An: [redacted]
Betreff: [redacted], Donate To Ukraine and save a life, Please read

Hello,

We are urging you to please donate to Ukrainians as many people have fled their homes to seek refuge. Help us provide a safe solution for Ukrainian families who have already suffered too much, Shelter, water for those who need it the most in this time of crisis.

You can give any amount, since the banks are not working, kindly save a life, and donate to us through our UCRF (Ukraine Crisis Relief Fund) wallet.

Bitcoin Wallet: [redacted]

We Sincerely appreciate your help.

Thank You,
Amin Awad
Ukraine Crisis Relief Fund

Example of Charity Scam Mail

Figure 19:
Charity Scam Mail
Source: Phishing radar of the BSI in cooperation with the NRW Consumer Advice Centre

Von: Für Menschen mit Herz <mail@world-of-shopping-mail.de>
Gesendet: 27. Februar 2022 14:37
An: [redacted]
Betreff: +++ Ukraine: Hilfe dringend benötigt +++

Sollte der Newsletter nicht richtig dargestellt werden, klicken Sie bitte hier

Malteser International
Order of Malta Worldwide Relief

Malteser
...weil Nähe zählt.

Eskalation im Ukraine-Konflikt

Erste Hilfslieferung unterwegs

Bild: Malteser Ukraine

♡ Jetzt spenden!

Liebe Leserin, lieber Leser,

wir alle hatten die Hoffnung, dass die Ukraine und Russland ihren Konflikt ohne weitere kriegerische Handlungen lösen. Heute kamen dann die unfassbaren Nachrichten: Russland hat die Ukraine angegriffen.

Collateral Damage after Attack on a Satellite Communications Company

Situation

On 24 February 2022, a satellite service failed in European space at around 3 a.m. Universal Time. Among other things, processes for the interference suppression of wind turbines in the electricity sector are maintained via satellite communication solutions. As a result of the disruption, around 5,800 wind turbines could no longer be maintained via remote maintenance[20]. Furthermore, German customers also experienced disruptions in the implementation of satellite communication solutions and, in addition, devices of the emergency services of a district were also affected.

The operator admitted to malfunctions due to a firmware update and suspected tampering (i.e. a cyber attack). A service provider has been appointed to investigate the incident. The affected modems had to be factory reset to restore their functionality[21].
Other countries were also affected by the disruption, including France and Ireland[22].

Assessment

On 30 March 2022, the operator published more information and confirmed that it had been an attack on 24 February 2022. However, no attribution was made. The aim of the attack was to make the service unavailable. The attack is said to have targeted only one area of the satellite network used by private users. According to the report, the company first discovered a targeted Denial-of-Service attack with a very high volume of data traffic that caused many modems to go offline. The analysis showed that the data traffic was sent from several modems and other associated devices belonging to customers from Ukraine. However, according to the operator, no access to customer data or unlawful access to personal customer devices could be detected. The forensic analysis revealed that the attackers had gained access to a management network through a misconfigured VPN connection. The attackers presumably used this to execute commands on tens of thousands of modems at the same time. This overwrote the flash memory and rendered the modems unusable. The service provider responsible reportedly installed new modems in several tens of thousands of customers and the modems were patched via an over-the-air update[23].

The IT security incident with its disruption of the availability of satellite communication in the conflict area subsequently also had an impact on the maintainability of wind turbines in Germany, among other things. Nevertheless, no effects on the security of supply in the indirectly affected sectors of German critical infrastructures, such as energy, were observed. Power supply and grid stability were likely not affected by the incident. The wind turbines could operate self-sufficiently during regular operation without any external intervention.

Response

The BSI received various fault and incident reports in connection with the incident. The operator carried out a forensic analysis and confirmed the attack. All affected modems have been replaced by the responsible service provider.

Cyber Attack on German Petroleum Trader

Situation
On 11 March 2022, several virtualised server systems failed at a German petroleum distribution and trading company with a Russian parent. In response, the operator immediately informed its IT service provider and reported the incident to the BSI in accordance with the CI reporting obligations under §8b para. 4 BSIG.

The group Anonymous Germany claimed responsibility for the attack. It had succeeded in penetrating deep into the company's systems and extracting data on a large scale from various storage systems, mail servers and hard disk images. However, the data has not been published. Nevertheless, the operator had to consider all its systems compromised and shut them down. Service providers were required in order to restore the systems to emergency operation, but initially refused support due to legal ambiguities regarding the interpretation of the EU sanctions list. After clarifying the situation with the help of various authorities, the required systems could be put into emergency operation. There were no noticeable supply bottlenecks.

At the time of going to press, the company was still in emergency operation in a closed environment. In addition, efforts were made to set up a new, secure system environment, taking security-by-design into account. However, this also required service providers who refused to cooperate with the German subsidiary of a Russian parent company, citing the sanctions. By the time of going to press, no solution had yet been found.

Assessment
The Petroleum Stockholding Association is required to hold crude oil and petroleum products at all times in the amount of the net imported quantities in Germany over a period of 90 days. Stocks of petroleum products are distributed throughout Germany in order to be able to meet demand quickly and across the country, as well as to respond effectively to regional supply disruptions. The petroleum trade in Germany is handled by a network of distribution points spread over a large area.
If the disruption had continued, economic damage and supply shortages (with high oil prices) would have been unavoidable.

Response
The BSI accompanied the incident analysis and clean-up together with an external BSI-qualified APT service provider and was in regular contact with the operator, the APT service provider and other authorities.

Industroyer2 Attack on the Ukrainian Energy Sector

Situation

On 12 April 2022, Ukraine's CERT reported an attack on a Ukrainian organisation in the energy sector. The attack group Sandworm allegedly prepared a blackout for 8 April 2022. However, the preparations were discovered and the blackout was prevented[24]. A new malware variant called Industroyer2 was allegedly used in the incident. This appears to be a new version of the Industroyer malware – also known as Crashoverride – that has been known since 2016. Both versions have implemented control commands of a standard communication protocol of the IEC (International Electrotechnical Commission) and thus target Industrial Control Systems (ICS). The code of the new variant strongly resembles a module from the Industroyer variant available at the time. Therefore, IT security researchers assume that it is the same code base. The aim of the attack is said to have been to use Industroyer2 to cause damage to substations, thereby interfering with or preventing the transmission of electricity.

In addition to Industroyer2, the following malware is also alleged to have been used:

- *CaddyWiper was designed to slow down the recovery of Windows-based systems and prevent the energy company's operators from regaining control of the ICS systems. The CaddyWiper malware had previously been used against a Ukrainian bank and a Ukrainian government organisation.*
- *Linux servers were to be damaged by using the wipers Orcshred, Soloshred and Awfulshred.*

At the time of going to press, neither the initial attack vector nor how the attackers were able to get into the ICS network was known.

The group Sandworm is often attributed to a Russian intelligence service and was allegedly responsible for a cyber attack on the Ukrainian power grid as early as 2015.

Assessment

The Ukrainian electricity grid has been connected to the European synchronous grid since mid-March 2022. This means that a large-scale power blackout in Ukraine could also cause a small part of the balancing power held in reserve by the European synchronous grid to be used to stabilise the Ukrainian power grid. In 2016, Industroyer caused a large-scale power blackout in Ukraine. It can therefore be assumed that the potential damage from Industroyer2 would be comparable.

In contrast to Industroyer – Industroyer2 features a hard-coded configuration. This requires the attackers to modify the malware for each use or target. Thus, the use of this version of Industroyer2 against other targets is rather unlikely. At the same time, this change makes detection more difficult, as hashes for Industroyer2 as Indicators of Compromise (IoCs) will each be specific to a particular target.

A similar incident could also affect critical infrastructure in Germany. The possibility of energy network components being affected as a result of a successful attack with an appropriately modified version of Industroyer2 cannot be ruled out.

Response

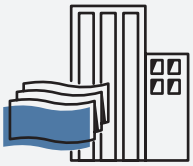
The BSI sent out a cyber security warning to the relevant target groups on 12 April 2022.

Top 3 Threats per Target Group

Civil Society

Theft of identity data
Sextortion
Fake shops on the internet

Industry



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

Government / Administration

Ransomware
APT
Vulnerabilities, unprotected or poorly secured online servers

First digital disaster emergency in Germany

207 days of digital emergency

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

The number of malware programmes is constantly increasing.

The number of new malware variants has increased by

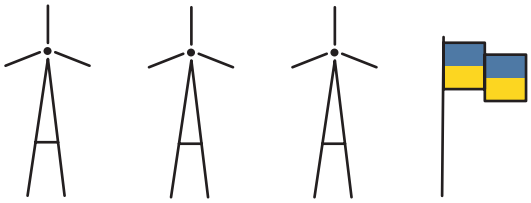
116,6 million in the current reporting periode.

Hacktivism in the context of the Russian war:

Mineral oil company in Germany must restrict critical services.

Collateral damage

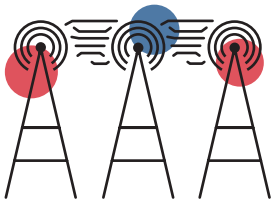
after attack on a Satellite Communications Company.



20.174

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

15 million reports on malware infections in Germany were sent by the BSI to German network operators in the reporting period.



34.000

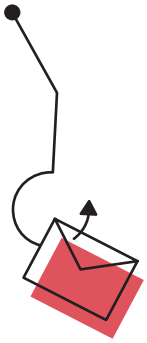
mails with malware were intercepted on average every month in German government networks.

78.000

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

69%

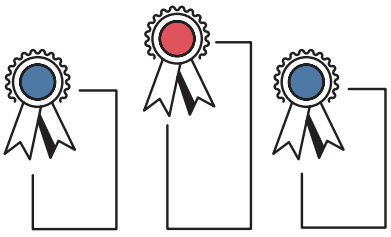
of all spam emails in the reporting period were cyber attacks such as phishing emails and mail extortion.



90%

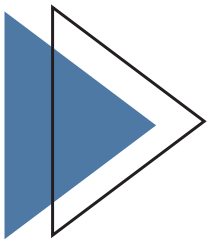
of the mail fraud in the reporting period was finance phishing, i.e. the fraudulent mails gave the impression of having been sent by the banks.

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



5.100 2021

4.400 2020



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

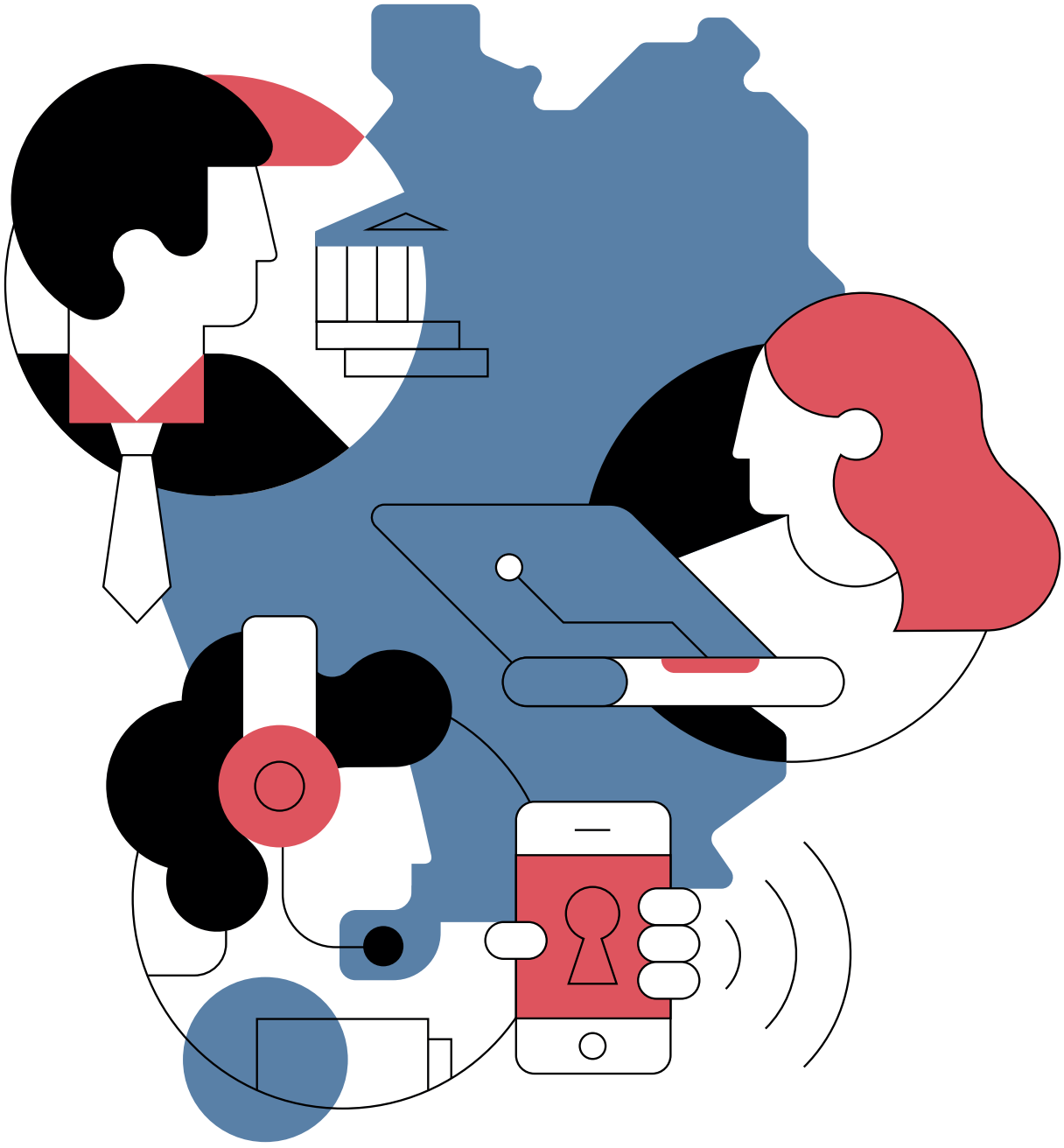
6.220

PARTICIPANTS.

12 Months of Cyber Security at a Glance


December
21
• Critical vulnerability in widely used software product Log4Shell
• Warning of increased risk from ransomware attacks at Christmas
• BSI publishes guideline on the current state of quantum-safe cryptography
• BSI launches application process for the IT security mark
February
22
• Collateral damage after attack on a satellite communications company
• Publication of an attack in which Fermat's factorisation method was applied to a large number of published RSA moduli
• BSI publishes IT-Grundschutz Compendium
• 18th German IT Security Congress with presentation of the first IT Security Label
Spear phishing by APT group GhostWriter
April
22
• Thwarted attack on Ukrainian energy sector
• BSI updates the minimum standard for the use of Transport Layer Security
• Digital personal certification made possible as part of the implementation of the Online Access Act
January
22
• BSI publishes "Smart Cities/Smart Regions Information Security for IoT Infrastructures"
• BSI publishes technical guideline for cooperative intelligent transport systems
• BSI and ZF launch project with TÜViT on the topic of AI security in cars
March
22
• Warning against the use of anti-virus products
• Cyber attack on German mineral oil trader
• Bundesamt für Verfassungsschutz warns potential victims of spear phishing emails
• BSI and Saarland sign cooperation agreement to strengthen cyber security
May
22
• Assessment of the cyber security situation in Germany after the Russian attack on Ukraine
• BSI issues first IT Security Labels for broadband routers
• Publication of white paper on the inventory of the auditability of AI systems

Insights & Services



Insights and Services for Specific Client Groups

As the Federal Cyber Security Authority, the BSI is shaping secure digitalisation in Germany – together with citizens, the business community, as well as with the state and administration and international bodies. With the entry into force of the IT Security Act 2.0, the BSI's mandate has been expanded to meet the challenges of advancing digitalisation, among other things by enshrining digital consumer protection as a mandate of the BSI. This enables the BSI to support consumers in the risk assessment of technologies, products, services and media offerings.

2.1 — Civil Society

Nowadays, digitalisation plays a role across a number of areas in our society – from the use of a wide range of online services and healthcare to voting and elections. Information security is necessary for all of this. The BSI is continuously working on improving information security in all areas of our lives so that citizens can be confident that their personal data is in good hands, that they can use IT safely and that they can move confidently in our networked world. To achieve this, the BSI combines its extensive know-how in the areas of prevention, detection and response and derives specific information services for social groups, as well as for individual citizens. During the reporting period, the BSI addressed issues such as the security of connected medical products, electronic identity procedures and the possibilities of virtual meetings and voting.

2.1.1 — Insights from the Threat Landscape in Civil Society

The BSI and the Police Crime Prevention of the Federal States and the Federal Government (ProPK) are cooperating in order to provide consumers with comprehensive information about protection options and the risks on the Internet. The cornerstone of this work is the Digitalbarometer, a joint, representative online survey that has been conducted annually since 2019. The survey investigates the importance of security on the Internet for consumers, the extent to which they protect themselves from the dangers of the digital world and how they inform themselves about vulnerabilities, risks and protective measures.

Internet Crime Increases Slightly – More than One in Four is a Victim

Consumers' general level of concern has recently risen slightly compared to the past three years: 29 percent of the respondents stated that they had already been victims of crime on the internet. In previous years, the figure was 25 percent. In each case, a quarter of the respondents had experienced fraud when shopping online (25%), third-party access to an online account (25%) and/or infection with malware (24%). In contrast to online shopping fraud (2021: 19%), the figures for being affected by third-party access to an online account (2021: 31%) or infection with malware (2021: 29%) have decreased compared to the previous year. Only 19 percent of respondents were affected by phishing – in the previous year, this applied to one quarter (25%).

The use of protective measures among consumers leaves space for further actions. The use of anti-virus programmes (53%), secure passwords (52%) and an up-to-date firewall (44%) is common among the population. Only about one third (34%) of respondents said they update their systems automatically. Only 38 percent of respondents had activated 2FA.

Handling Security Recommendations

Over two out of five respondents are aware of security recommendations for protection against crime on the internet (45%). Of these, again more than half (58%) said they partially implemented these recommendations. 22 percent implement them fully, only 4 percent not at all. More than half of the respondents (51%) inform themselves about internet security, while just over a fifth (23%) never do. Security is particularly important to respondents when banking online (83%), installing software (70%) and shopping online (62%).

Wishes Concerning Emergency Guidance

The victims of crime on the internet mostly stated that they approached the situation on their own. When asked, what kind of help they would wish for, most would like an emergency checklist to help them, followed by a website with informational videos and a police advisor. Overall, more than half wanted more information on topics related to security on the internet, especially tips on how to recognise crime on the internet and information on how to protect online accounts.

2.1.2 — Digital Consumer Protection

Phishing and data leaks are two terms that unfortunately play a major role in the everyday lives of consumers (see chapter *Spam and Phishing*, page 26, and section *Extortion with Captured Identity Data*, page 17). The BSI therefore recommends that consumers secure online services using 2FA. It is the responsibility of online service providers to offer secure and easy-to-use 2FA and recovery procedures[25]. According to a market survey by the Federation of German Consumer Organisations (vzbv), only a few providers meet this responsibility. Supported by a consumer survey conducted by the vzbv, it is also clear that consumers have little knowledge about the strengths and weaknesses of individual 2FA procedures and their secure use.

The BSI has compiled a comparison of common 2FA procedures for digital consumer protection, including evaluation tables, which explain certain procedure characteristics to experienced and technically minded consumers. The comparison considers aspects of IT security, usability (usable security) and data confidentiality. When assessing IT security – and assuming a secure usage environment - attack scenarios that could pose a threat are considered. These scenarios relate to phishing attacks, data leaks and attacks from a distance on the second factor. The comparison concludes that the hardware-based Chip TAN and ID card procedures are resistant to these attack scenarios. In the future, the Smart eID procedure will be available for identification, which will bring additional advantages in terms of usable security compared to the aforementioned use of the ID card.

Further information can be found here:[d]

Corporate Digital Responsibility – Taking Responsibility for Better Security

What do consumers worry about most when shopping online? Data theft and financial damage due to fraud are the top responses, according to a representative survey by the Federal Ministry of Justice (BMJ). Providers are seen as having a responsibility to ensure data protection and cyber security. According to the vast majority of respondents, however, companies are not currently meeting this demand[26] . Corporate Digital Responsibility (CDR) is therefore intended to create a framework for guidance and requirements for the responsible use of digital technologies.

In line with Corporate Social Responsibility (CSR), the concept first described in 2015 is based on a voluntary and holistic approach. Considering the implications of digital technologies from the start focuses on building and maintaining trust[27]. This also means that measures can have a direct positive impact on products and services for consumers. The level of awareness of CDR so far is still low and CDR has been taken up only by a select few. Frameworks of reference, fields of action and measures are currently being discussed in detail. The CDR Code was the first time an overarching approach was developed together with companies. In terms of content, the commitment includes the consistent further development of information security and its consideration as early as the product development stage[28]. For companies, this offers an opportunity to implement and communicate information security in a positive way as an added value and competitive advantage. The BSI supports the common goal of achieving a higher level of security for consumers through its many services.

2.1.3 — IT Security Label

In December 2021, the BSI opened the application procedure for an IT Security Label and thus success-

fully implemented an important new task from the amended BSI Act (BSIG). Since then, the BSI has received applications for a variety of products and services from the areas of broadband routers and email services.

On 1 February 2022, the first four IT Security Labels were issued and handed over to an email provider by BSI President Arne Schönbohm at the 18th German IT Security Congress.

In order to raise awareness of the added value of the new IT Security Label, the BSI is conducting an ongoing dialogue with stakeholders from the fields of consumer protection and industry. A comprehensive range of information on the BSI website explains to consumers and interested companies how the IT Security Label works, providing a broad overview of the topic.

BSI President Arne Schönbohm and Fabian Bock, Managing Director of mail.de GmbH, at the presentation of the first IT Security Label. Source: BSI

The BSI is working to expand the scope of the IT Security Label by continuously developing and publishing new product categories, for example for consumer IoT products. The basis for these new product category is the European standard ETSI EN 303 645, which specifies baseline security requirements for consumer IoT devices.

With this new label, the BSI is making the security of products and services on the German consumer market more transparent. Manufacturers and service providers can make the security promise of their products particularly visible and easily recognisable to customers.

Further information can be found here:[e]

2.1.4 — Consumer Information and Raising Awareness

One of the BSI's goals in digital consumer protection is to increase consumers' risk awareness. The aim is to raise the awareness for the risks of a cyber incident. In addition, the BSI wants to increase consumers' problem-solving skills and teach them how to respond to an IT emergency. That is why the BSI regularly provides information on current developments, gives recommendations on what basic digital protection looks like, and points out dangers and common attack methods. The BSI wants to provide these services to help consumers move around the Internet safely and independently.

The Website as a Central Point of Contact

On the website of the BSI, interested parties can find concrete recommendations for action on questions of everyday digital life and background information from the field of cyber security.

In addition, the BSI specifically addressed new target groups during the reporting period: for example, the gaming community with an extensive virtual presence at Gamescom in August 2021. The BSI reached a different target group for German Senior Citizens' Day in November 2021. In four virtual lectures, hundreds of private users and volunteers learned how to safely navigate their digital lives.

Growing Community

The BSI gained many new subscribers on its social media channels, which are primarily aimed at consumers. Explanations about technology and internet phenomena as well as warnings about current security incidents are particularly popular. Storytelling formats also ensured increased attention. Additionally, the newsletter "Sicher • Informiert" (Informed safely) has grown and now keeps more than 121,000 subscribers

up to date on current developments in the digital world. Last but not least, after more than a year, the podcast "Update verfügbar" (Update available) is one of the top 10 percent of the most streamed podcasts on the German market. The monthly active community amounts to 4,500 to 7,000 listeners with more than 3,000 subscriptions.

Online Shopping as the Focus of the #einfachaBSIchern Campaign

Online shopping has become an integral part of shopping behaviour in private everyday life. For this reason, the focus of the information and awareness campaign on IT security by the BSI and the Federal Ministry of the Interior and Community (BMI) between July and the beginning of September 2021 was on secure online shopping on the Internet. Interested parties received tips and information on three central aspects: secure online shops, secure user accounts and secure payment. The tips were also specifically publicised again at the end of the year during Cyber Week and the Christmas shopping season.

Further information can be found here:[f]

2.1.5 — "Dialogue on Cyber Security" Project

The BSI is pursuing the goal of shaping cyber security for, with and in the whole of society. Since spring 2021, it has been continuing dialogue in the field of cyber security with all societal groups in the project "Dialogue for Cyber Security" based on a participatory multi-stakeholder approach. In a pilot process, a dialogue model is being implemented that was developed by the dialogue participants[28] in the predecessor project "Institutionalisation of Social Dialogue" (see *The State of IT Security in Germany in 2020*).

With this dialogue, the BSI wants to open itself up in the sense of an open government approach, and build trust, expand bidirectional communication, enable participation and create a platform for a lasting dialogue on cyber security with all societal groups.

Following the think tank workshop 2021, at which the dialogue partners elected a dialogue committee and topics for further work, the joint work in five workstreams started in July 2021. Four of these were implemented by March 2022, one could not be completed. Products have been created on the following topics, which are available on the project website:

1. Digital best-before date
2. Dos and don'ts for sustainably secure products
3. Effective IT security awareness
4. Update4Schule - Data collection on digital education

The first project cycle ended with the presentation of the workstream results. The dialogue project will run until the end of 2024.

Further information can be found here:[g]

2.1.6 — Security on the Internet of Things, Smart Homes and Smart Cities

Connected devices on the Internet of Things offer a wide attack surface for cyber attacks. In particular, hijacked IoT-devices integrated into botnets pose potential for damage. Thus, compromised devices become a tool for further attacks – on the one hand against the affected consumers, on the other against third party targets if attackers use the computing capacity for DDoS attacks (see chapter *Botnets*, page 24).

The European standard ETSI EN 303 645 defines basic requirements for the IT security of consumer IoT devices, e.g. in smart homes. Including, for example, security mechanisms (e.g. passwords) that protect the product from access by unauthorised persons. The associated test specification ETSI TS 103 701, published in August 2021, was developed with significant participation by the BSI. Hence, it is possible to check whether a connected device meets the requirements of the European standard. Since May 2022, both documents are the underlying standards for issuing the IT Security Label to a wide range of product categories, such as smart cameras or smart speakers.

The first two product categories of the German IT Security Label, introduced in December 2021, rely on the existing BSI standards for email services (BSI TR-03108) and broadband routers (BSI TR-03148). Since the demand from manufacturers and service providers is high, a number of IT Security Labels have already been issued.

For the third season of the corresponding BMI funding programme 28 further “Smart Cities Model Projects” have been selected As a result, the digitalisation of regions, districts, cities and municipalities is also gaining further momentum in the context of public services of general interest. Consequently, a total of 73 projects have now been in funding since 2019. For this purpose, the BSI has published target group-oriented recommended actions.

Further information can be found here:[g]

2.1.7 — Security in Healthcare

Digital healthcare can make people's lives easier, minimise long journeys and waiting times, and help quickly in the event of illness or emergency. But all the benefits of eHealth are impossible without information security. This is because digitalisation also increases the risk of IT security incidents and cyber attacks in the healthcare sector (see for example incident *Ransomware Attack on Medical Technology Company,* page 23).

Security of Medical Devices

Since the last reporting period, there have been two events that have had a particular impact on the IT security of connected medical devices: The "BadAlloc" collection of critical vulnerabilities, published in August 2021, also poses a threat to many components in the medical field due to the use of the Blackberry QNX real-time operating system and, depending on its use, may allow remote code execution. In addition, the "Access:7" vulnerabilities in Axeda-branded remote management products became known in March 2022. These products are used especially for remote maintenance of connected medical systems in hospitals and laboratories and can allow unauthorised access. The published patches and measures for both vulnerability collections continue to ensure security in the medical sector; according to the current status, there are no known impairments to patient safety.

Security of Telematics Infrastructure

During the reporting period, digitalisation in the health sector, including in the area of telematics infrastructure (TI), again increased significantly. After the introduction of the first specialised applications for emergency data management (Notfalldatenmanagement, NFDM), the eMedication Plan within the framework of drug therapy safety (Arzneimitteltherapiesicherheit, AMTS) and the electronic patient file (elektronische Patientenakte, ePA), which allows all statutorily insured persons to store their medical findings and information from previous examinations centrally and securely and, if necessary, to make them available to other treating physicians even across practices and hospitals, further expansion stages of the TI were concretised and tested with regard to their specifications. They are now on the verge of being implemented. One example of this is the e-prescription (eRezept), which has been undergoing a test phase since the end of 2021 coordinated by gematik (Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH) and represents a milestone in the digitalisation of the healthcare system.

In particular, under the current conditions of the COVID-19 pandemic, the health system has been severely challenged. Tests planned in advance for the functional expansion of the telematics infrastructure (TI) ran under more difficult conditions due to the now partly scarce or otherwise tied up personnel resources.

Digital Pandemic Response

Since the beginning of work on the Corona-Warn-App, the BSI has been conducting security analyses to complement the development process. The BSI supports the continued development of the app through seven-day penetration tests and code reviews at two-week intervals. The development of the Corona-Warn-App takes place transparently in a publicly accessible source code management system (GitHub). There, the BSI reports the identified vulnerabilities to the developers (see also the chapter *Vulnerabilities in Software Products,* page 31). Since the release of the Corona-Warn-App, various extensions have been developed in close cooper-

ation between the BSI, the Robert Koch Institute (RKI), Deutsche Telekom AG and SAP.

In 2021, the Corona-Warn-App was expanded to include, among other things, an event registration function and a connection to the COVID digital certificate and Covid testing centres. The BSI's IT security analyses as part of the enhancements have identified a total of nine vulnerabilities in the Corona-Warn-App since June 2021. These were able to be remedied within the framework of the close cooperation between the BSI and the consortium. Among other things, the tests proved that the consortium responded quickly and appropriately to the vulnerability known as "Log4Shell", so that the Corona-Warn-App is not vulnerable to this vulnerability.

Digital Proof of Vaccination

Since the beginning of the development of a digital proof of vaccination, the BSI has supported the Federal Ministry of Health (BMG) and the RKI both in the evaluation of security concepts and through penetration tests and code reviews. All further developments of the apps and the background systems were supported by the BSI. Technical vulnerabilities could thus be communicated to the developers in a timely manner. This cooperation made it possible to create a complete system consisting of background systems, the CovPass app and the CovPass Check app, which has demonstrated a high level of IT security since its release. In total, about 40 vulnerabilities have been identified and fixed since the app's development began.

2.1.8 — Making Virtual Meetings and Voting Secure

During the reporting period, many companies and public institutions continued to be forced to enable their employees to work from home and therefore had to further digitise business processes. This results in an increased need for digitising administrative processes, such as elections of works councils, equal opportunities commissioners or boards of directors. Many companies are therefore currently entering the market for online elections with new products. In the project "Market and Vulnerability Analysis of Online Choice Products" (Markt- und Schwachstellenanalyse von Online-Wahlprodukten), the BSI is preparing a comprehensive market and security analysis of a selection of currently available products. The aim of this analysis is to create a detailed situation report on the state of IT security in this area. The results will feed into the Technical Guidelines and Protection Profiles for non-political elections and voting.

The topic of online elections also found its way into the Bundestag in 2022. On 6 April, the Committee on Education, Research and Technology Assessment (Ausschuss für Bildung, Forschung und Technikfolgenabschätzung, ABFT) held a public expert discussion on the topic of e-voting. The Office of Technology Assessment is currently conducting a short study on this topic; the interim results were presented at the expert meeting in the form of a thesis paper and discussed with experts, including from the BSI. The key questions included: "To what extent does e-voting comply with the principles of electoral law?" and "Can online elections be implemented securely?" The question was also discussed: "Should e-voting be used in federal elections in Germany?" The consensus among the experts was: "E-voting will not become an option in federal or state elections in the next few years." The experts were unanimously in favour of testing the possibility of online voting for the time being in elections to self-governing bodies – social insurance elections or committee elections – and to scientifically evaluate the knowledge gained from this with an interdisciplinary approach.

Further information can be found here:[i]

2.1.9 — Security of Payment Methods

In the smsTAN procedure (also called mTAN), the bank sends the customer a transaction number (TAN) by SMS to the mobile phone number stored in the banking portal. This TAN is required for the authorisation of the transaction initiated by the customer, for example the authorisation of a bank transfer. In addition to the TAN, the SMS contains details of the transaction to be carried out, such as the recipient and the amount of a transfer, so that it can be verified.

The problem: SMS are transmitted unencrypted, making it possible to intercept data. In addition, the bank account is not linked to a specific device of the user, but

is usually only linked to a mobile phone number. This poses the risk of SIM swapping. Here, another SIM card is ordered in the name of the user for the mobile phone number so that mTANs are sent to several devices. Similarly, if the mobile device is stolen or lost, there is a risk of fraud if criminals are in possession of the login data for online banking. In the past, fraudulent use of the smsTAN procedure alone caused damage amounting to several million euros per year.

The BSI has been pointing out this problem for a long time, with the result that more and more banks have now abandoned the mTAN procedure. Due to the spread of smartphones, credit institutions use i PushTAN or PhotoTAN. Cryptographic procedures are first used to create a device link between the smartphone and the customer's online banking access. Once the smartphone is uniquely linked to the bank account, the TAN is only sent to the registered device. The TAN is transmitted via a push message to the smartphone or by reading a 2D barcode with the smartphone camera. For the ChipTAN procedure, your own bank card is used together with a separate TAN generator that is not connected to the internet. A graphical code is created from the transaction data, which is read out with the ChipTAN generator. This makes this procedure particularly secure, as features stored on the card are required to generate the TAN.

Current surveys suggest that the incidence of losses due to TAN fraud is decreasing on the basis of the use of the new procedures.

Further information can be found here:[j]

2.1.10 — Two-Factor Authentication

In the meantime, many online service providers have introduced procedures with which users can identify themselves in addition to or as an alternative to entering a password when logging into an account. This two-factor authentication, or 2FA for short, is available in numerous variants. Hardware-based procedures in particular offer a high level of security.

The usual method of authentication is still based on entering a password. A single factor – the "knowledge" of the password – is requested by the service to authenticate the user. Passwords as an authentication mechanism are easy to implement, but have several disadvantages:
For example, knowledge of the one factor "knowledge" is sufficient to overcome the authentication mechanism.

More and more services are therefore requesting a second factor in addition to the password in order to authenticate the user more securely, for example with a further request for "knowledge" in the form of an authentication code that is sent to a smartphone to counteract identity theft, for example. However, a higher level of security is only achieved here if there is a real separation of the devices and the factors can thus not be collected through an attack. For orientation purposes, the BSI has developed the Technical Guideline TR-03168 Authentication Procedures and Systems to provide a more detailed overview and recommendations on the sensible combination of different factors. A consideration of various factors from the consumer's point of view was presented in the framework of an evaluation table (see chapter *Digital Consumer Protection,* page 58).

One way to feature multiple factors follows the standards of the Fast IDentity Online Alliance, founded in 2013 with many different representatives from government and industry to develop open and licence-free industry standards for global authentication on the internet. Proof of the security of the FIDO authenticator used is necessary to ensure secure implementation of the protocols in products. As a member of the FIDO Alliance, the BSI is involved in defining verifiably secure authenticators.

The BSI examined two commercially available, non-externally certified FIDO tokens with the question of whether they fulfil a "substantial" trust level according to BSI TR-03107-1. Example attack scenarios were considered in which the attackers had physical access to a FIDO token for a limited time. Here, both tokens were found to have significant possibilities for manipulation, which means that they were unsuitable for the trust level "substantial".

Further information can be found here:[k]

2.1.11 — Evaluation of Electronic Identification Procedures

In the case of electronic identification procedures, the BSI examines both basic technologies and concrete procedures in order to assess and minimise the risks for the state, the economy and society.

The BSI evaluates specific private-sector procedures in the context of the Online Access Act. These technical assessments form the basis for the BMI to decide within the IT Planning Council on the use of the respective procedure in eGovernment, specifically for user accounts of the federal government and the states. During the reporting period, the BSI successfully completed the evaluation of one additional procedure. The BSI continues to cooperate with the BKA to investigate the possibilities and risks of photo- and video-based checks of identity documents.

2.1.12 — Secure Electronic Identities on Smartphones

Unsecured, open or incorrectly configured online servers and services represent a broad attack surface for cyber attacks (see for example chapter *Ransomware*, page 13 and specifically chapter *Example Attack Sequence*, page 14). Captured identity data can be misused for a variety of other attacks (see for example the section *Extortion with Captured Identity Data*, page 16). Improving cyber security is a joint task of both manufacturers and providers of products and online services as well as users.

A basic prerequisite for the successful implementation of digitalisation projects is the broad availability of eID procedures that enable identification at a suitable level of trust. The current major project Digital Identities of the Federal Government provides for the introduction of a mobile identity solution for this purpose, which will be implemented through the Smart-eID. This is based on the technology of the identity card and enables identity data to be stored securely and data-sensitive services to be used via smartphones.

Since smartphones, like any connected device, are constantly exposed to the risk of a cyber attack, special requirements must be met to ensure the secure storage of an eID on smartphones. The basis for the Smart eID is therefore an eID applet that may only be executed within a security element of the mobile device. Either a Secure Element ("SE") or an eUICC ("eSIM") can be used for this purpose. The applet itself is based on the established cryptographic protocols of the identity card. This has the advantage that the Smart eID is compatible with existing services that have already integrated the online ID function.

During the implementation of the Smart eID, the BSI is acting as technical project manager for the companies commissioned with the implementation and is drawing up technical concepts, security specifications and interfaces with the aim of providing a highly secure and, at the same time, user-friendly solution for citizens. In parallel, the BSI is holding talks with manufacturers of mobile end devices and contributing corresponding expertise to international standardisation committees.

2.1.13 — Multimedia Identities

A multimedia identity describes the representation of an individual in digital media such as videos or audio recordings. Through methods from the field of artificial intelligence, it is becoming increasingly easy to manipulate such an identity, even without special expert knowledge. These methods are known colloquially as "deepfakes" because of the use of deep neural networks.

The threat situation due to the manipulation of multimedia identities increased during the reporting period. Until now, manipulated multimedia identities have often been considered for entertainment purposes or merely in theory as an abstract danger. However, high media attention was given to a so-called CEO fraud in October 2021, in which a Hong Kong bank director was tricked into authorising wire transfers totalling 35 million US dollars to cybercriminals via a fake voice call. Likewise, the use of deepfakes for propaganda purposes, for example in conflict situations, became a realistic threat. In March 2022, a supposed surrender speech by Ukrainian President Zelenskyy appeared on social media and on infiltrated Ukrainian news portals. However, this video, in which the artificially generated head of the president was placed on an actor and the voice was artificially manipulated, was of low quality, which is why the fake was recognised as such relatively quickly and was thus unable to cause any major damage.

It is becoming increasingly apparent that manipulated multimedia identities are being used in a wide variety

of threat scenarios against the state, the economy and society. Furthermore, it was observed during the reporting period that the real-time capability of manipulation methods is increasing in both audio and video with increasing quality. This was also demonstrated by the BSI (see Figure 21). Similarly, a growing public availability of tools to create fakes has been observed, making it easier for forgers to carry out high quality manipulations.

Since one key preventive countermeasure against the dangers of deepfakes is education about this technology, the BSI published a topic page on deepfake technology at the beginning of 2022.

Figure 21: Result of a face swap (right) from Arne Schönbohm (centre) as the target to a BSI employee (left) as the attacker.

Further information can be found here:[l]

2.1.14 — Modern Messengers for Secure Communication

Alongside telephone and email, modern messengers have long been part of everyday life and are among the most widely used means of communication. In 2021, 83 percent of Germans used a messenger service at least once a week, and among those under 30, the figure is as high as 99 percent. 73 percent of users practise multi-homing, meaning they use at least two different messenger services in parallel. Messaging solutions are also becoming increasingly popular in the federal administration and are used by many authorities[29]. Their use has continued to increase, not least because of the ongoing COVID-19 pandemic and the associated increase in home office working.

To ensure the confidentiality of communication, most messengers today make use of some form of encryption. Which contents are encrypted – i. e., whether only text messages or also pictures, files and audio/video calls, whether only in individual or also in group conversations – and how these are encrypted – that is, whether it is an end-to-end or a transport encryption – varies greatly and is sometimes also a matter of the settings chosen. In addition to the actual communication content, a number of other data, so-called metadata, are generated when using a messenger. Some of these metadata cannot be avoided from a technical point of view, while others (including profile information) are deliberately collected by some operators and used, for example, for advertising purposes or reselling.

The BSI is therefore working intensively on the topic of messaging and monitors important developments in this area. At the end of 2021, for example, the BSI published several publications on the technical foundations of modern messengers[30] and the topic of "interoperability"[31] and recently published an expert video[32]. In addition, the BSI supports other authorities and members of the Bundestag by providing technical expertise in this area. One of the messaging projects supported by the BSI in the federal administration is the proof-of-concept operation of the messenger Wire, known as "Wire Bund". In the middle of the year, an important milestone was reached: a cryptographically secured federation of different Wire instances, which enables end-to-end encrypted, communication across backends.

Unlike telephone and email, where it does not matter which provider one uses, with a messenger one can only communicate with users of the same messenger service. One technical hurdle for this lack of interoperability is due to the fact that most messengers nowadays are encrypted and until now there has been no standardised cryptographic protocol that could have been used for this purpose. Although many messengers' encryption is based on the Double Ratchet Protocol, most messenger providers have implemented their own variant of the protocol. In practice, the resulting changes - even of just minor details - mean that the different messengers are not interoperable with each other, i.e. they cannot encrypt or decrypt messages for each other, for example. In this regard, the IETF standard "Messaging Layer Security" (MLS)[33], the development of which the BSI closely follows, is another important topic. MLS is a further development of the Double Ratchet Protocol, which in particular enables efficient key management

even in large groups. In addition to Wire, a number of well-known companies (including Mozilla, Twitter, Cisco, Google, Facebook) as well as research institutions (INRIA) and universities (MIT, University of Oxford) are involved in the development of the standard. Wire Bund, along with Wire, is one of the first messengers implementing the new MLS protocol, and it is expected that many of the other messengers on the market will follow this example.

2.2 — Industry

The success of digitalisation will determine the future of Germany as a business location to a large extent. A functioning and secure IT infrastructure creates the essential prerequisites for this – be it for the operation of critical infrastructure (CI) or the successful transformation of the business models of SMEs. This is why the BSI supports the robustness of Germany as a cyber location with numerous offers as well as CI operators in the implementation of preventive measures against cyber attacks. SMEs benefit from professional dialogue and practice-oriented IT security recommendations. With the Alliance for Cyber Security, in turn, the BSI has been strengthening the robustness of Germany as a business location. For higher information security in new technologies, the BSI designs, among other things, practice-oriented security requirements, standards and recommendations for action. The BSI also acts as a central certification and standardisation body and makes a significant contribution to the success of large-scale digitalisation projects.

2.2.1 — Findings on the Threat Landscape in the Industry

The business sector was again exposed to a large number of cyber attacks in this reporting period, the majority of which were again characterised by ransomware (see chapter *Ransomware*, page 13).

The central challenge for companies in Germany is to increase cyber resilience, i.e. to combine effective preventative measures with the ability to respond to cyber attacks with the aim of maintaining and securing the company's operations. The BSI has observed a strong increase in demand for its support services – from cyber security standards to sharing and support formats such as the Alliance for Cyber Security. The state of IT security in the business sector is essential for the cyber security situation in Germany, so intensifying the efforts of companies in this area is of great importance for improving cyber security.

2.2.2 — Threat Landscape of Critical Infrastructure

Critical infrastructures (CI) are organisations with important significance for the public. They provide critical services such as medical care or the supply of food, water or electricity. Critical services, however, also include the processing and storage of data in data centres or the supply of cash to the population.

All critical services are particularly dependent on trouble-free IT. A disruption, impairment or even failure of these central services can lead to lasting supply bottlenecks, significant disruptions to public security or other dramatic consequences. Therefore, the BSIG provides CI operators with measures for the prevention (§ 8a BSIG) and management (§ 8b BSIG) of IT security incidents or IT disruptions.

Russian War of Aggression against Ukraine Shifts Focus to Vulnerability of Critical Infrastructure

Even in the previous reporting period, the public's attention to incidents in the health system due to the COVID-19 pandemic increased. As a result of the Russian war of aggression against Ukraine, the security of critical infrastructure in Germany has now become an even greater focus of public attention. Even before the Russian attack on Ukraine began, the BSI had activated the National IT Crisis Response Centre and called on operators of critical infrastructure, among others, to increase their vigilance and readiness to respond.

The Threat of Attacks on the Software Supply Chains of IT Service Providers

For years, the BSI has been observing an increasing trend towards elaborately prepared APT attacks, which also threaten operators of critical infrastructure worldwide. In addition, the attacks on the software supply chains of IT service providers to their customers observed in recent years constitute a new, particularly worrying threat.

The spread of malicious code via the regular update mechanisms of the (security) software of globally operating IT service providers allows established security mechanisms to be circumvented. The manipulation of (security) updates that are installed on customers' systems makes it possible to carry out attacks on very well-protected IT systems. Such attacks are also extremely difficult to detect, as the source code cannot usually be viewed or evaluated by clients.

Only by analysing supply relationships in detail, the threat of attacks on the supply chain can be countered. With this in mind, a careful selection of suppliers is of crucial importance for CI operators.

Updating of Industry-Specific Security Standards in the Reporting Period

CI operators must take appropriate organisational and technical precautions to prevent disruptions in order to implement § 8a (1) BSIG. They are expected to comply with the state of the art in this respect. In order to define and substantiate the state of the art, the various sectors may develop industry-specific security standards (B3S), which the BSI will determine upon request whether they are suitable for fulfilling the legal requirements. More than twenty CI sectors have already created or are developing B3S. Due to the dynamic technical development, the suitability of each B3S must be reassessed by the BSI after two years.

During the reporting period, the BSI determined suitability of B3S from the following industries:

- B3S food trade V2.2
- B3S for traffic control and guidance systems in municipal road traffic
- B3S water/wastewater

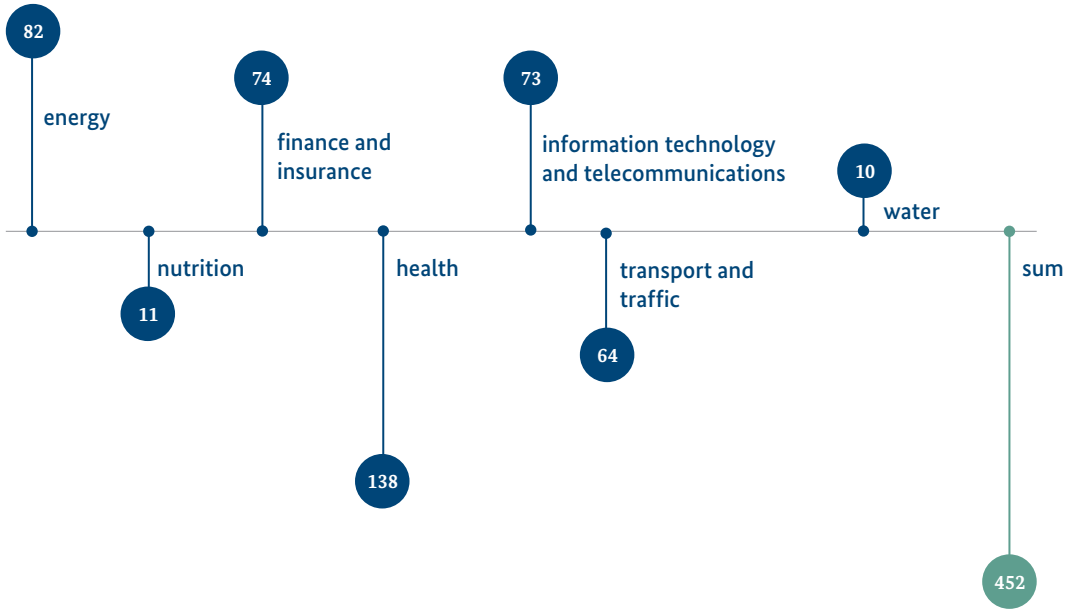
The current list of B3Ss that have received a positive assessment from the BSI is available on the BSI website:[m]

Reporting Figures by CI Sectors in the Reporting Period

In 2015, the IT Security Act introduced a reporting obligation for operators of critical infrastructure in § 8b (4) BSIG. The reporting obligation applies to disruptions that have led or may lead to the failure or significant impairment of the functionality of the critical infrastructure they operate.

Reporting figures by CI sector in the reporting period (June 2021 to May 2022)

Figure 22:
Notification figures by KRITIS sector in the reporting period (June 2021 to May 2022)
Source: BSI



In the reporting period, the BSI received 452 corresponding reports.

Security Deficiencies in Selected CI Sectors

Pursuant to § 8a (3) BSIG, CI operators must provide documentation of compliance to the BSI every two years that their IT security is state of the art. The following statistics therefore refer to this two-year period and not to the reporting period of the annual report. The compliance documentation contains information on security deficiencies and implemented security measures.

For years, the BSI has systematically analysed the deficiencies uncovered as part of the periodically submitted documents of all CI operators. By classifying the deficiencies, aggregating them into overarching deficiency categories and then analysing the time series over several detection cycles, trends can be derived for all CI sectors. This analysis enables the BSI to identify specific focus areas for individual sectors and to develop appropriate measures in close cooperation with the operators. The insights gained from the CI compliance documentation is also important information for the industry working groups of UP KRITIS.

During the two-year period from 1 April 2020 to 31 March 2022, a total of 2,941 security deficiencies were found in the energy, food, finance and insurance, health (medical care only), information technology and telecommunications, and water sectors during the audit of the periodic verifications.

The frequency of security deficiencies for the aforementioned CI sectors is presented below. For this purpose, the deficiencies were assigned to the deficiency categories of the BSI's "Orientation guide to documentation of compliance according to Section 8a (3) of the BSI-Act", which were combined into overarching categories in the following diagrams.

Further information can be found here:[n]

Deficiencies in the CI Sector of Energy

In the CI sector of energy, the proportion of deficiencies in the ISMS category has increased compared to the previous report. Deficiencies in the category of structural/physical security account for the second largest proportion, which is partly a result of the low proportion of on-site inspections during the pandemic. Deficiencies in the asset management category form the third largest area.

Deficiencies in the CI Sector of Food

In the CI sector of food, a large proportion of the identified deficiencies fall into the ISMS category. Deficiencies in the area of technical information security also play a major role with over 20 percent.

Deficiencies in the CI Sector of Finance and Insurance

In the CI sector of finance and insurance, deficiencies were most frequently identified in the categories ISMS, technical information security and incident identification and processing. Compared to the previous evaluation period, detected deficiencies fell more frequently into the ISMS category, whereas in the previous year's report, almost a quarter of all deficiencies were still attributed to technical information security. The deficiency categories of review during live operation and asset management played a lesser role in the current evaluation period.

Deficiencies in the CI Sector of Health (Focus Solely on Medical Care)

In the CI sector of health (focus solely on medical care), no deficiency category is above average. The largest shares of the identified deficiencies are in the areas of ISMS, business continuity management for the essential service and asset management.

Deficiencies in the CI Sector of Information Technology and Telecommunications

In the CI sector of information technology and telecommunications, deficiencies were most frequently identified in the areas of ISMS, technical information security and personnel and organisational security. Compared to the previous evaluation period, the proportion of deficiencies in the ISMS area in particular has increased significantly. Deficiencies in the areas of technical information security and personnel and organisational security also continue to account for a large proportion.

Deficiencies in the CI Sector of Water

IIn the CI sector of water, most of the deficiencies were again attributed to the area of ISMS. Deficiencies in this category already accounted for about one third of all deficiencies in the previous year, and in the current evaluation period, the share rose to over 50 percent. The categories of structural/physical security and technical information security together account for 20 percent of the identified deficiencies. The cooperation of the operators in the water sector with the BSI on corrective action has intensified in recent years.

2.2.3 — UP KRITIS

UP KRITIS is a voluntary cooperation between CI operators, their professional associations and the competent authorities with a total of 840 participating organisations. In *UP KRITIS*, there are thematic and industry working groups in which members exchange ideas and work together on specific topics. The plenum is the assembly of the speakers from the working groups and the responsible authorities. The Council works at the political level, it consists of high-ranking persons from the CI sectors as well as from the authorities of the BMI, the Federal Office of Civil Protection and Disaster Assistance (BBK) and the BSI. The BSI is represented in numerous working groups, the plenum, staff and council of the *UP KRITIS*.

New Industry Working Groups

With the *IT Security Act 2.0,* the Federal Government has added another sector to the nine CI sectors: The "municipal waste disposal" sector is a new addition. This means that the most important waste management companies are also classified as critical infrastructure operators. The companies and infrastructures that are specifically affected will be described in detail in the BSI Kritis Regulation (BSI-KritisV), which has yet to be adapted. This is expected to happen towards the end of the year. Due to this development, *UP KRITIS* founded the associated industry working group for "municipal waste management" in summer 2021.

For some time now, *UP KRITIS* has had an industry working group for all insurance companies. Due to the very different structures and processes in private insurance companies and the statutory health insurance sector, the plenum of *UP KRITIS* founded a separate industry working group for the statutory health insurance sector in autumn 2021.

The BSI supports the activities of *UP KRITIS* in many of its working groups. Numerous publications were issued by the working groups during the reporting period.

QR code to guidelines on the use of systems for attack detection:[o]

Further information to UP KRITIS can be found here:[p]

Operational cooperation

At the operational level, the members of *UP KRITIS* cooperate on current affairs. The Russian war of aggression against Ukraine led to operational challenges for many CI operators. In spring 2022, this led to an intensive exchange of information, which resulted in the establishment of a separate working group.

The topic "Dealing with the COVID-19 pandemic" covers the entire reporting period. CI operators shared their experience with crisis management during the pandemic in the working group "scenario-based crisis preparedness".

2.2.4 — Companies in the Focus of European and German Cyber Security Regulation

The IT Security Act (IT-SiG 2.0) came into force on 28 May 2021. IT-SiG 2.0 represents the further development of the first IT Security Act from 2015, which legally obliged CI operators in Germany to register and report relevant IT security incidents to the BSI.

IT-SiG 2.0 expands the powers of the BSI as the central reporting office for information security of the state and the economy, contains new requirements for the IT security of CI operators and provides for higher fines for violations of the law.

Obligation to Utilize Intrusion Detection Systems

IT-SiG 2.0 explicitly adds the use intrusion detection systems to the requirement of "adequate security". By using technical tools and implementing organisational processes, attacks on information technology systems of CI operators should be detected at an early stage, thus minimising the impact of disruptions. The BSI, together with the detection working group of UP KRITIS, has created and published guidelines on the use of intrusion detection systems to support implementation.

Companies of Particular Public Interest (UBI)

The IT-SiG 2.0 also introduced rights and obligations for other companies that are of outstanding importance to society. In the law, these companies are referred to as Companies of Particular Public Interest (Unternehmen im besonderen öffentlichen Interesse, UBI).

UBIs include:

- Manufacturers/developers of goods within the meaning of § 60 of the Außenwirtschaftsverordnung (Foreign Trade and Payments Ordinance, “AWV”), i.e. companies active in the field of weapons, ammunition and armament material or in the field of products with IT security functions for the processing of classified government information or components essential for the IT security function of such products (UBI 1),

- Germany's largest companies in terms of domestic value added and major suppliers to these companies (UBI 2) and

- Operators of top tier facilities within the meaning of the Hazardous Incident Ordinance or operators who are equivalent to such pursuant to § 1 paragraph 2 of the Hazardous Incident Ordinance (UBI 3).

The IT-SiG 2.0 provides for reporting obligations for UBI, as they already apply to CI operators. In addition, UBI 1 and UBI 2 are each subject to an obligation to register with the BSI and to submit a self-declaration on IT security. For UBI 3, registration is voluntary; a self-declaration does not have to be submitted.

UBIs registered with the BSI benefit from a range of BSI services. For example, they receive alerts, situational awareness products and cyber security recommendations. In addition, they can access special support services offered by the BSI.

For UBI 3, the new obligations will apply from 1 November 2021, for UBI 1 from 1 May 2023 and for UBI 2 at the earliest two years after the entry into force of the UBI Regulation, which defines which companies are subject to the new regulations for UBI.

Further information can be found here:[q]

Network Code on Cyber Security

With the latest EU internal energy market package[34], the regulation on network access conditions for the cross-border exchange of electricity was revised. One of the amendments included the authorisation basis for the European Network of Transmission System Operators for Electricity (ENTSO-E) and for the European Distribution System Operators Association (EU DSO entity) to develop a network code on cyber security.

Network codes in the electricity sector are primarily developed by ENTSO-E and translated into a European regulation by the Agency for the Cooperation of Energy Regulators (ACER) and the European Commission. The Network Code on Cyber Security contains requirements for the European electricity interconnection system with the aim of aligning and continuously increasing the security level of the member states.

State of Current Development

The development of a network code was started by ENTSO-E and the EU DSO entity after the entry into force of the internal electricity market package and the associated amendment, stipulating that a network code must also be drawn up on the subject of cyber security. The proposal prepared by ENTSO-E and the EU DSO entity was submitted to ACER in January 2022. It can be assumed that the network code will probably enter into force as a European regulation at the beginning of 2023 at the latest.

Content of the Network Code

The network code aims in particular to achieve a uniform level of cyber security as well as a uniform handling of cyber security incidents by actors in the European electricity interconnected system. In particular, transmission system operators, large distribution system operators, providers of critical services and various authorities are addressed. The core requirement is to carry out regular risk assessments with regard to cyber security in the power supply. This is done by identifying companies that make a critical or high contribution to Europe's electricity supply.

For these companies, uniform guidelines for carrying out risk analyses, risk assessments and risk treatments are to be developed within the company, nationally, across regions and at the European level. In addition, uniform risk management measures are being developed, including the definition of minimum and advanced cyber security requirements based on existing standards. The handling of cyber security incidents that have a cross-border element will also be further developed through the development of uniform information and response processes and the introduction of a European crisis management system.

The Significance of the Network Code with Regard to Existing National Legislation

The Network Code will supplement already existing cyber security requirements in the energy sector with requirements that primarily affect the cross-border aspect of electricity supply. The Network Code will thus contribute to increasing the level of cyber security throughout the European electricity interconnected system.

2.2.5 — The Special Situation of SMEs in Germanyd

2.6 million small and medium-sized enterprises in Germany are facing the challenges of digitalisation and the associated cyber security. This sub-sector of companies, which proportionately accounts for 99.4 percent of German business enterprises, breaks down as follows:

Companies in Germany by size
Data in %

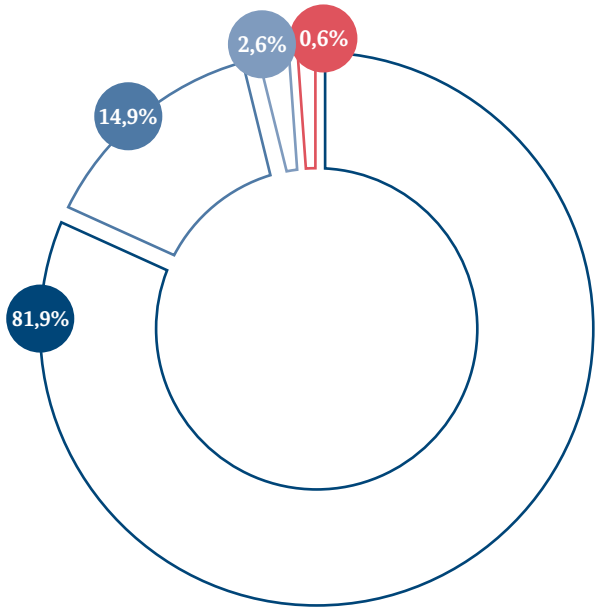


Figure 23:
Source: Federal Statistical Office, as of July 2021

In particular, micro (less than ten employees) and small (less than 50 employees) enterprises often do not have the necessary staff to take care of operating and securing the company's information technology systems.

According to findings by the BSI and a study by the Federal Ministry for Economic Affairs and Energy (BMWi)[35], many companies will continue to have neither knowledge of the general cyber threat situation nor of their own risk profile in 2022. They therefore

lack the awareness to invest more in their security. On the other hand, those who have already developed an awareness of the problem and want to recruit IT staff often experience that they cannot compete in a competitive market as a potential employer against the salaries at large companies or IT service providers. And those who want to outsource IT/IT security to a service provider often find that there are either too few qualified service providers in their region or only those that do not fit their own company size. All of this leads to some SMEs falling victim to cybercriminals on the one hand and not being able to react appropriately to an incident on the other.

A study published on behalf of the BMWi in 2021[36] came to the following conclusion: "In the event of an incident, SMEs often don't know where to turn for expert help. In contrast to burglaries in the analogue world, digital damage is not always and not immediately apparent to many SMEs. The reluctance to report incidents and attacks to the police, the state criminal investigation offices or other authorities is high.

For this reason, the BKA has published a short handout for affected companies in the event of an emergency[37].

In order to provide SMEs with customised support in this regard, the BSI has compiled the most important information for this target group in a separate section on the BSI website.

In order to provide SMEs with customised support in this regard, the BSI has compiled the most important information for this target group in a separate section on the BSI website:[r]

Information on the preventive protection of IT systems and further offers of the Alliance for Cyber Security are supplemented, among other things, by a directory of qualified IT service providers who can help in an emergency. In addition, SMEs that are affected by a cyber attack can report it to the BSI via the website. Companies that want to be better prepared for cyber threats can find helpful guidance and recommendations in different IT-Grundschutz profiles. The BSI has published an IT-Grundschutz profile for trades enterprises, among others. Detailed assistance is also provided by a route planner, which can be used to implement an operational process for increasing information security step by step. In terms of prevention, cyber insurance – as a relatively new product in the insurance industry – can be attractive to companies, as a cyber security-related incident can quickly affect a company financially as well.

2.2.6 — Cyber Security in the Automotive Sector

The topic of cyber security will continue to be a focus of the automotive industry in 2022. After international regulations for the cyber security of motor vehicles were adopted at the level of the United Nations Economic Commission for Europe (UNECE) in 2020 (UNECE Regulation 155), they will now become mandatory for vehicle manufacturers under EU law (EU Regulation 2019/2144) from July 2022. The regulation requires car manufacturers to address potential IT-related threats through a Cyber Security Management System (CSMS) that provides for appropriate development and response processes, e.g. for IT incident management and vulnerability resolution.

Some manufacturers have already implemented a CSMS and had it audited by IT Technical Services, which is a prerequisite for subsequent approval of vehicle types under the aforementioned regulation. The BSI has accompanied selected auditing procedures in support of the Federal Motor Transport Authority (KBA). In December 2021, the KBA granted the world's first type approval in the field of automated driving for an Automated Lane Keeping System (ALKS) for a model from the manufacturer Mercedes-Benz. This system complies with automation level 3 according to the SAE J3016 standard, in which the driver does not have to constantly monitor the automatic control. A prerequisite for approval was compliance with the cyber security requirements under UNECE Regulation 155.

In addition to accompanying CSMS audits and type approvals as part of witnessing the designation of technical services, the KBA and the BSI have also deepened their cooperation on the basis of the administrative agreement concluded in 2020 for the area of market surveillance and the exchange of information on IT-related incidents and vulnerabilities.

In July 2021, the Act Amending the Road Traffic Act and the Compulsory Insurance Act – Autonomous Driving Act came into force. Among other things, it enables the

use of motor vehicles with autonomous driving functions in defined operating areas of public road traffic. This creates the legal basis for the first time for the operation of automated vehicles at level 4 (according to the previously mentioned standard) in regular operation. Application scenarios are, for example, driverless buses that travel at low speed on defined routes (shuttle transport and people movers), or automated parking in specially equipped car parks (Automated Valet Parking). The law and the ordinance implementing the law on autonomous driving define, among other things, requirements for the technical condition and equipment as well as obligations for those involved in the operation of such motor vehicles. IT security and the involvement of the BSI in the evaluation of such vehicle systems for test approvals are explicitly required here. With regard to IT security, according to §1i StVG, the KBA is to involve the BSI in the creation, implementation and in the further development and evaluation of corresponding technical requirements.

In January 2022, the BSI published the Technical Guideline BSI-TR-03164 "Guidance for Cooperative Intelligent Transport Systems (C-ITS)". In Cooperative Intelligent Transport Systems, connected road users and transport infrastructure communicate with each other. The aim is to make road traffic safer, more comfortable and more efficient using the information exchanged. A Certificate Policy (CP) and other standards have been developed at European level for this purpose. The Technical Guideline is to be seen as a supplement to the CP and the relevant standards and serves as a guideline for the operation of public key infrastructures and C-ITS stations within the context of European applications. The aim of the Technical Guideline BSI TR-03164 is to close gaps in the specifications and to define specifications in concrete terms in order to enable a consistently high level of security for all instances and to ensure the interoperability of the C-ITS participants.

The BSI published the State of the Automotive Industry in 2021 for the first time. In addition to IT in the vehicle, this also looks at cyber security in the company context and the supply chain in the manufacturing process. For example, insufficiently tested or manipulated hardware or software can limit the security of the vehicle if this is not detected in time during the production process. Attackers not only target manufacturers around the world, but also their suppliers. This can lead to significant disruptions in the supply chain. In 2021, several automotive suppliers were affected by ransomware incidents (see also chapter *Ransomware,* page 13). This caused massive interruptions in production.

2.2.7 — Cyber Security in Aviation

Together with the BMI and the Aviation Security Authorities of the states in Germany, the BSI has drawn up the principles for the implementation of the Implementing Regulation (EU) 2019/1583, which were published by the BMI at the end of 2021. These principles serve to implement Implementing Regulation 2019/1583, which came into force on 31 December 2021, and provide companies regulated under §§ 5 and 8 of the Aviation Security Act (LuftSiG) with the framework for implementing information security. In the process, the principles were laid down in the National Aviation Security Programme (NLSP). This means that these requirements must be checked as part of the regular re-certification process and demonstrated to the State Aviation Safety Authority. The requirements for auditing compliance with the legal provisions were also laid down in the principles.

In Germany, the BSI is currently responsible for organising and managing information security measures for companies regulated under §§ 5 and 8 LuftSiG. This includes the 28 German airport operators as well as the fields of passenger and baggage controls. The Federal Ministry for Digital and Transport (BMDV) is responsible for §§ 9 and 9a LuftSiG, which cover air carriers and those involved in the secure supply chain. In the meantime, a departmental agreement has been signed between the BMDV and the BMI with the aim that the BSI will be responsible for §§ 9 and 9a LuftSiG in the future.

After the Russian attack on Ukraine, the warning and reporting system for information technology in aviation security has already been put to the test. Within the context of daily special reporting and intensified situation monitoring in the aviation sector, the theoretical processes and procedures were tested for their practicability and optimised.

2.2.8 — Digitalisation of the Energy Sector

Cyber attacks on companies, state institutions and critical infrastructure in Ukraine have shown that critical infrastructure is increasingly coming into focus. Through the use of smart metering systems and the associated use of certified Smart Meter Gateways,

important systems of the energy grid are connected via a secure communication infrastructure to effectively counter cyber attacks.

In addition to ensuring IT security, Smart Meter Gateways can provide grid status data and feed-in values, among other things, so that electricity grid operators can obtain important information about the current load on their grid with the help of smart metering systems. This allows potential bottlenecks to be recognised in time and prevented. In addition, the information helps to make the expansion of the electricity grid efficient and cost-effective. Flexible consumption devices (heat pumps, electric vehicles, etc.) and decentralised generation plants can also be controlled via the Smart Meter Gateway in the future making them useful for the grid and the market. The secure and standardised remote control of consumption and generation plants via the Smart Meter Gateway is fundamental for a future-proof *smart grid*.

The development and application of BSI standards to ensure cyber security is necessary to successfully digitise the energy transition and create a secure smart grid. Currently, four manufacturers of Smart Meter Gateways have successfully completed the BSI's product certification procedure according to CC. Together with the Federal Ministry for Economic Affairs and Climate Action (BMWK), technical cornerstones for the further development of the standards were developed with associations and companies in the energy industry in 2021. The BSI standards were also further developed in the form of the update of the Technical Guideline TR-03109-1. As of 31 January 2022, a total of three independent manufacturers have already successfully completed certification in accordance with TR-03109-1. In addition, TR-03109-5 will be published in 2022 as a minimum requirement for products that can be securely connected to the HAN (Home Area Network) of the Smart Meter Gateway in the future.

Due to the massive expansion of renewable energies planned and the increasing networking, the efforts of the BSI in cooperation with the BMWK, partner authorities and the industry to promote the gradual rollout of secure and certified Smart Meter Gateways must continue to be intensified, while at the same time continuing the joint dialogue on the target scenarios for secure digitalisation.

2.2.9 — Cyber Security in the Industrial Supply Chain

Digitalisation is becoming more and more widespread along the industrial supply chain between manufacturer, supplier, shipper and many more. IT security is of great importance here, among other things because an attack on the digital processes can lead to a disruption of the industrial, physical supply chain.

For many of these digital processes, individual products, their characteristics and the events that affect them must be traceable and readable. This is made possible by digital twins (i.e. digital representations of physical objects), which must also fulfil IT security requirements such as forgery protection and confidentiality. For this reason, the BSI has been involved in the standardisation of a digital twin. The project is underway in the DKE/AK 931.0.16 committee as IEC 63278 "Asset Administration Shell for Industrial Applications".

Another threat to industrial supply chains is posed by compromised hardware and software that can enter the production environment as supplier products (see chapter *Vulnerabilities in Software Products,* page 31). Under today's conditions, it is not possible to subject every single supplier product to a security check. A Software Bill of Materials (SBOM), which is supposed to certify the installed software of a product, can be easily forged. Therefore, security researchers' efforts are aimed at making SBOM counterfeit-proof and tying it to individual products[38].

The digital business relationships that emerge along the industrial supply chain rely on a variety of credentials and corporate identities that can be issued by different authorities. Together with the Industrie 4.0 platform, the BSI is looking into the question of how proof can be tied to company identities in a legally secure manner and how this can be verified with digital processes. The BSI sees the eIDAS Regulation as an important building block towards this, and has been involved in its design and practical implementation.

2.2.10 — Modern Telecommunications Infrastructure (5G/6G)

With the introduction and integration of modern mobile communication standards as well as technologies in the area of 5G, new threats to public and private mobile networks are emerging. Old mobile phone generations continue to operate in parallel as highly complex networks are being created. The BSI has the legal mandate to create a comprehensive overview for the security of these networks in order to accompany the implementation of security requirements in cooperation with the authorities, network operators and all other stakeholders involved.

By implementing the legal obligation to certify critical components in the 5G network, the BSI has made an important contribution to the overall concept of information security in the mobile communications sector. The BSI also designates permissible certification programmes (link to TR-03163) and helps to shape them.

Further Information (on this topic) can be found here:[s]

The BSI, for example, developed a new 5G sector-specific certification programme based on a cross-industry framework for security in the mobile industry. During the reporting period, two certifications have already been carried out through the programme (see chapter *Transition of Product Certification into the European Cyber Security Legislative Act,* page 77 *and NESAS-CCS-GI for more information).*

Further information can be found here:[t]

In addition to the work on the secure expansion of mobile networks, analysing cyber attacks and vulnerabilities is also essential to ensure the *resilience* of mobile networks. At the national level, severe impairments and major outages in the reporting period were limited to local or regional areas and were mainly caused by the flood disaster in the summer of 2021.

BSI Support Programme "Cyber Security and Digital Sovereignty in 5G/6G Communication Technologies"

The BSI has been funding research and development projects to strengthen digital sovereignty and cyber security for 5G/6G communication technologies since June 2022. The selected projects will help ensure that Germany takes a leading role as a technology provider in 5G/6G and that the new communication technologies are established. The projects will develop and test modern network technologies that reduce the risk for the deployment of 5G/6G technologies and close security gaps.

Further information can be found here:[u]

2.2.11 — Security of Cloud Services

Cloud Computing offers great benefits thanks to high scalability, computing power and availability. Just as with classic information technology, use of cloud services involves not only opportunities, but also specific risks. In 2021, there were some major security incidents at cloud providers, the analysis of which can help make the complex cloud technology more secure to use.

Early last year, a fire incident at a cloud service provider led to the loss of entire data centres and customer data was lost. This shows the importance of a precise analysis of the security requirements related to the processed data before procuring cloud services. When using a cloud service, all options necessary to meet these requirements should then be included in the contract.

In another case, a hardware defect caused alarm signals to be sent that falsely indicated a drop in ambient temperature in part of the cloud data centre. The endangered systems were then shut down. It was only many hours later that the data could be accessed again after the cause had been identified. This was an extremely rare incident. However, carrying out a risk analysis before using the cloud services can show whether such a cloud service failure would have serious consequences. If it would, this risk could be reduced or even completely mitigated, for example, through a multi or hybrid cloud strategy.

At another large cloud service provider, security researchers were able to obtain access keys for other cloud service customers twice in quick succession using different cloud services, which could have been used to access their data. The causes were an insufficiently secured use of third-party software and a faulty configuration by the cloud service provider. In both cases, the vulnerabilities were fixed by the cloud provider within a short period of time or customers were informed about how to fix the vulnerabilities. The likelihood that such an incident will come to light very quickly is very high, since cloud services operate extensive monitoring of activities, if only to be able to bill the costs incurred to the second. Nevertheless, cloud service customers should be fundamentally aware of the risks associated with shared platforms and, depending on the sensitivity of the data processed, consider additional protective measures, such as encrypting the data when planning to use the platforms. It is also important to pay attention during the deployment phase if any vulnerabilities are reported for the cloud service being used and if it is necessary to apply a security patch on the customer's side in order to close any vulnerabilities.

In another major incident last year, a cloud service provider was the direct target of an attack. The attackers managed to manipulate a cloud service within the cloud environment so that when it was used, *ransomware* was installed on customer systems. Such attacks represent a very serious threat to cloud services. Cloud service customers can make sure that the cloud service provider proves the security of the deployment environment with proofs of security. Furthermore, it is important that the customer environment connected to the cloud service is also protected with state-of-the-art security.

This overview of some of the incidents that have occurred in the past year highlights potential risks associated with the use of cloud services, as well as some suggested advices for safeguarding against them. The BSI also offers various publications that help companies and institutions systematically protect themselves against these and other comparable incidents.

The IT-Grundschutz compendium[39] contains tools for securing the customer environment and for the secure use of cloud services. The BSI guideline "Secure Use of Cloud Services"[40] describes information and explanations on user rights and obligations during all phases of cloud use in detail. The "Cloud Computing Criteria Catalogue C5"[41] specifies, among other things, a set of security criteria that the cloud service provider must meet to secure the cloud services it offers. There is also guidance for cloud service customers on what needs to be taken into account so that the security functions provided can be used in the best possible way. For federal authorities, the "Minimum Standard of the BSI for the Use of External Cloud Services" is binding and sets out defined steps for the secure use of cloud services. Companies and other institutions can also use these best practices.

Further information can be found here:

2.2.12 — Technical Security Systems for Electronic Record-Keeping Systems

As part of the digital transformation, business transactions are now increasingly recorded electronically. The use of various types of cash registers is a clear feature of the retail trade. From classic cash registers, tablets and smartphones to cash registers in server farms, every conceivable type can be found. This has greatly changed the technical challenges for tax auditing, as any subsequent manipulation of electronic records is almost impossible to detect without appropriate safeguards.

In order to counteract such manipulations, in accordance with the Fiscal Code of Germany and the Cash Register Anti-Tampering Ordinance electronic record-keeping systems are required to be protected with a certified Technical Security System since 2020. The Technical Security System is accessed by the electronic record-keeping system, secures the data to be recorded and saves the secured records in a standardised format. For this, the Technical Security System contains a security module that ensures that recordings cannot be subsequently changed, deleted or created without being detected.

The legal regulation explicitly promotes a technologically open design approach for the Technical Security System. In addition to the purely local security devices, scalable client-server architecture solutions suitable for online services have also been taken into account from the beginning.

The technical requirements and test specifications for the components of the Technical Security System are defined by the BSI in Technical Guidelines and protection profiles.

To date, nine different Technical Security Systems have successfully passed certification and are available on the market. Four of them can be integrated directly into cash registers and mobile devices as USB sticks and (micro) SD cards. Four other solutions can be integrated into data centres as so-called “cloud” Technical Security Systems. There is a “cloud-based” solution for mobile devices based on Android as well.

2.2.13 — Transition of Product Certification under the EU Regulation Cybersecurity Act

The European Cybersecurity Act (CSA) entered into force on 27 June 2019. One of the objectives of this EU regulation is to develop European Cybersecurity Certifications Schemes. With a certificate, an organisation can provide proof that a product or service meets defined security requirements. The planned Europe-wide mutual recognition of certificates is also intended to strengthen the Digital Single Market. Under the leadership of the European Union Agency for Cybersecurity (ENISA), several Ad Hoc Working Groups (AHWG) have been established for this purpose. In terms of product certification, the AHWG for the development of the European Cybersecurity Certification Scheme based on the Common Criteria (EUCC) is actively working since November 2019 The AHWG for the development of the European scheme for 5G mobile equipment (EU5G) has been active since November 2021.

Reports from the Committees

The SOG-IS MRA agreement on mutual recognition of CC certificates in Europe will be replaced by the EUCC scheme, which will be the first scheme to enter into force under the CSA. During the reporting period, the BSI took a leading role in the development of the EUCC scheme in the EUCC AHWG. Since March 2022, this has included active participation in the strategically important development of the structures and groups for the maintenance of the EUCC scheme.

Through its participation in the working groups, the BSI was able to identify necessary changes at an early stage and initiate processes in order to ensure a smooth transition to the EUCC scheme as soon as the corresponding Implementing Act is adopted by the European Commission. In addition, the BSI was one of the first European cyber security authorities to implement the required internal separation of certification and supervision activities.

The BSI is also the first European cyber security authority to establish a national certification scheme for 5G mobile network equipment, based on the Network

Equipment Security Assurance Scheme (NESAS), which was defined by GSMA in close collaboration with the BSI. The GSMA is the global association representing the worldwide mobile communications industry. The BSI has thus established the first certification scheme of this kind in Europe and is taking a pioneering role in European harmonisation in the EU5G AHWG.

With the Beschleunigte Sicherheitszertifizierung (BSZ), the BSI has created another horizontal cyber security certification scheme at the national level. The BSZ is characterised by plannable evaluation periods and a risk-driven approach to evaluation. The BSI is planning mutual recognition of comparable national certificates in Europe and is developing a corresponding European standard together with other nations. The aim is also to create a European scheme under the CSA.

Certifications in Figures

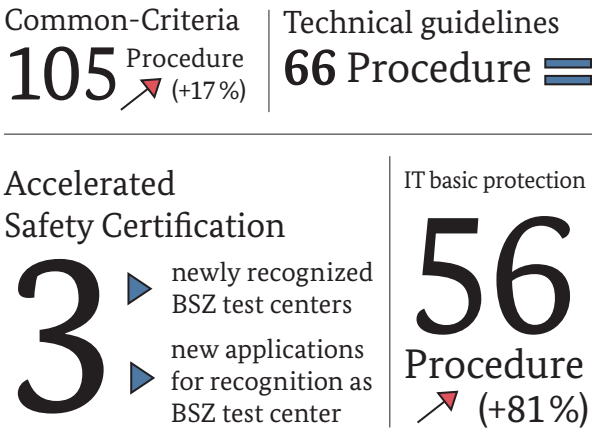


Figure 24: Certification in figures
Source: Schwachstellen-Statistik

2.2.14 — IT-Grundschutz

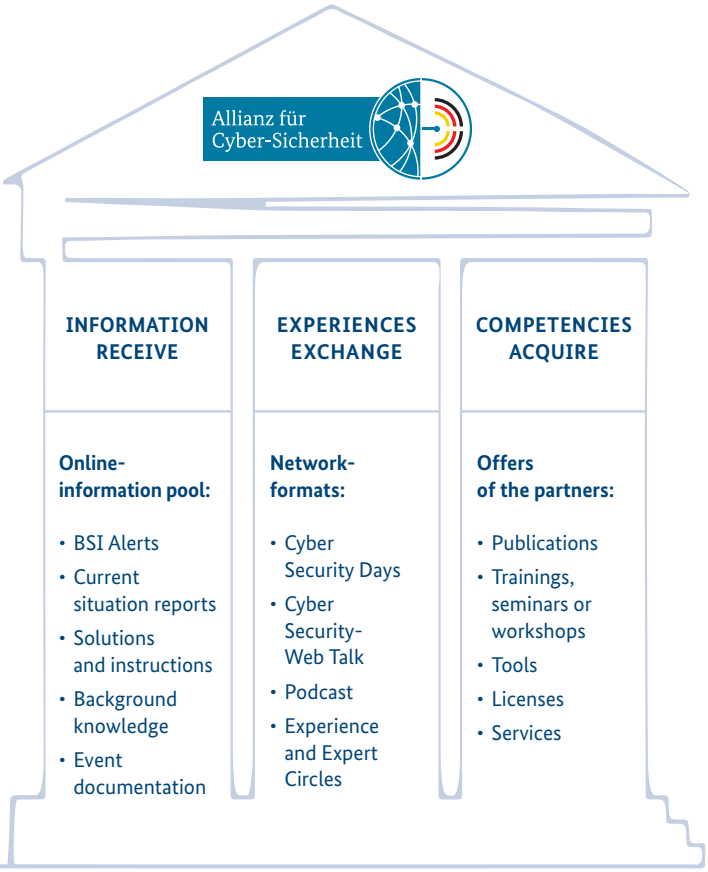
The diverse and dynamic attacks described in Chapter 1 (see chapter *Threats to Cyber Security in Germany*, page 10) illustrate once again the importance of a systematic, comprehensive and pragmatic approach to securing digital information. The BSI's IT-Grundschutz has been providing this for around 30 years. It is based on two core components: the BSI standards, which describe the IT-Grundschutz methodology, and the IT-Grundschutz compendium, which contains the IT-Grundschutz modules. Typical technical, infrastructural, organisational and personnel security requirements are summarised in the IT-Grundschutz modules. Together with the BSI standards, the IT-Grundschutz modules offer institutions an important tool for establishing an Information Security Management System (ISMS) and thus also for protecting business-relevant information.

In the 2022 edition of the IT-Grundschutz, seven new IT-Grundschutz modules have been added, for example in the areas of building automation and remote maintenance in the industrial environment. These newly added topics make it possible to take a more comprehensive look at information security, beyond just "classic" office IT.

If support is needed, institutions can draw on the expertise of the growing number of approximately 150 trained IT-Grundschutz advisors. In 2020, there were 89 IT-Grundschutz advisors and in 2021 there were as many as 140 IT-Grundschutz advisors. BSI-certified advisors can provide support in establishing an ISMS in accordance with IT-Grundschutz. Over 3,000 people have completed the training and examination to become IT-Grundschutz practitioners. The steady increase from 1,504 IT-Grundschutz practitioners in 2020 and 2,644 in 2021 is a testament to the demand. IT-Grundschutz practitioners make an important contribution to the implementation of IT-Grundschutz in their institutions and can define and implement measures based on IT-Grundschutz together with IT-Grundschutz advisors.

Ten Years of ACS – Ten Years of a Strong Network

Figure 25:
The collaborative approach of the Alliance for Cyber Security



2.2.15 — Alliance for Cyber Security

In 2022, the Alliance for Cyber Security (ACS) will celebrate its big anniversary: Ten years ago, Europe's largest private-public partnership in cyber security was launched. The goal: Cooperating and networking to enable companies and organisations to strengthen their prevention capabilities and become resilient in the fight against cyber attacks. The key to success lay in the idea of cooperation and mutual networking: A public-private partnership should pool the expertise and experience of the BSI and companies in Germany and promote prevention with best-practice products as well as information and handouts.

One Convincing Idea – A Lot of Tailwind for a Cooperation Platform

The founding idea of ACS finally born. The Federal Association for Information Technology, Telecommunications and New Media (Bitkom e.V.) proved to be a strong partner from the private sector.

In March 2012, BSI and Bitkom e.V. announced the founding of the ACS at CEBIT in Hanover – which officially followed at it-sa 2012 in Nuremberg after a successful pilot phase in which many companies had already been recruited as members and initial partner contributions had also been initiated. The cooperative approach of the ACS has been based on these three pillars from the beginning: Get information, share experiences, acquire skills. This is the foundation on which the ACS builds its work, its services and today, ten years after its foundation, also its success story.

Because the founding idea has become a strong network. In addition to the experience and expert groups, Germany's cyber security initiatives meet regularly under the umbrella of the ACS. A wide range of programmes, such as 31 Cyber Security Days, nine Cyber Security Web Talks, two hybrid events, 18 podcast episodes and

153 documents in the information pool enable a lively exchange of information and experience. The network can draw on the know-how of more than 6,400 participants, including 106 multipliers, as well as 177 partners and their numerous offers – and is growing continuously.

Entrepreneurs who deal with cyber security now contribute to securing the existence of their own company in the long term. Because now more than ever, it is time to raise our own shields and invest in cyber security.

2.2.16 — Cyber Security Network

The Cyber Security Network (CSN) is a association of qualified voluntary helpers who agree to make their expertise and know-how available for the solution of IT security incidents.

The CSN is intended to provide valuable support in case of an IT security incident, especially for small and medium-sized enterprises, but also for all members of the public. The function of the BSI is to provide the framework for the initiative. The network offers numerous services to prepare for an incident and to be able to act in a worst-case scenario, because some incidents may really threaten the existence of a company.

Short Profile of the CSN

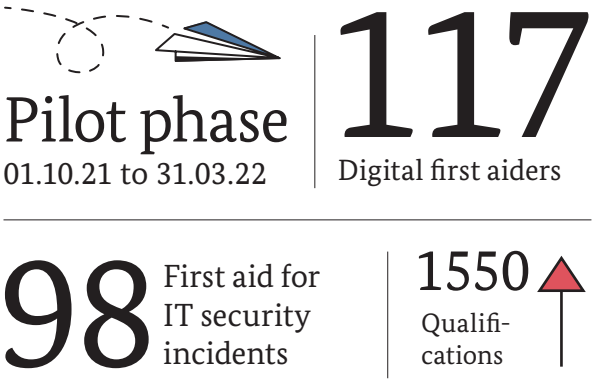


Figure 26:
Short profile of the CSN

The CSN is designed to act as the first point of contact for IT security incidents and to provide efficient support. Depending on the IT security incident, often the first question is: Who can help and how? For this, the CSN has developed the Digital Rescue Chain as a core component. It defines the work of helpers in the CSN in a coordinated manner and it enables a chain of different, reactive help offers, starting with the identification of a suitable helper, going on to first assistance, and finally coming to comprehensive solution support and incident clarification. To begin with a pilot phase, the Digital Rescue Chain will continuously be reviewed and expanded.

High-quality incident handling by helpers is ensured by a standardised and quality-assured qualification programme. The opportunity to exchange experiences in regional forums or to meet in the annual forum of the CSN completes the range of programmes.

Further information to the basic course can be found here:[w]

The regional forums offer both companies and helpers the opportunity to train in a safe environment to deal with incidents. As supplementary material to the forums, the CSN provides a training kit with a free collection of exercises and games.

2.2.17 — Other Solutions for Businesses

Investment Screening

The BSI has been commissioned by the BMI to avert potential threats to investments in domestic companies and production facilities by foreign investors in accordance with §§ 4ff. of the German Foreign Trade and Payments Act (Außenwirtschaftsgesetz, AWG) as well as §§ 55ff. and §§ 60ff. of the German Foreign Trade and Payments Ordinance (Außenwirtschaftsverordnung, AWV). The BMWK is responsible for the investment screening procedures on behalf of the federal gov-

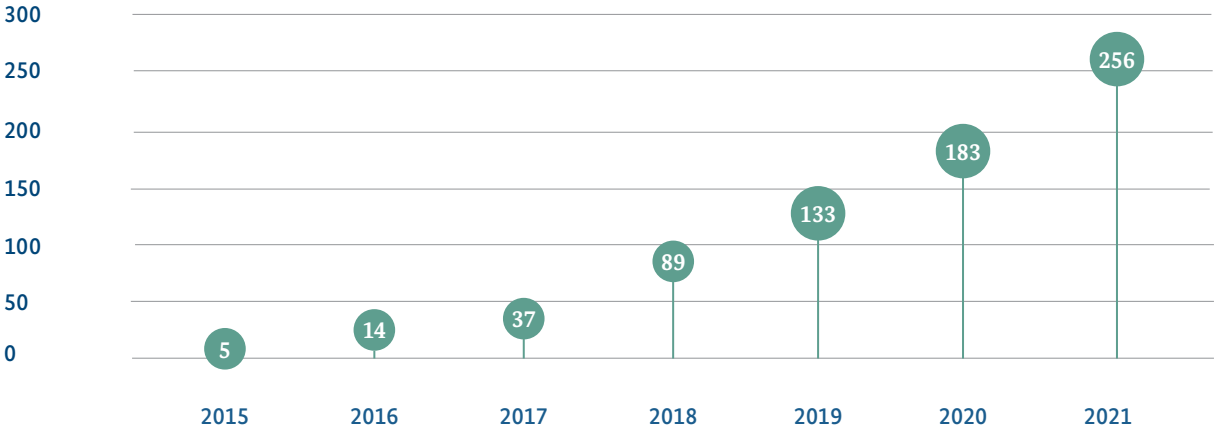


Figure 27:
AWG-Decress 2015-2021
Source: BSI

ernment. The BSI has been commissioned by the BMI to participate in procedures with a possible cyber security connection in order to assess and avert threats and has received corresponding test assignments (decrees). In order not to unnecessarily burden the open movement of capital through the procedures, the BSI carries out the sometimes very complex individual checks very quickly, i.e. usually within a few working days up to a maximum of one or two working weeks.

Taking into account the respective economic, legal and technological situation of the buyer and the target company, the BSI analyses and evaluates possible threat situations and develops position and solution proposals for averting danger. Possible IT security threats may include the leakage of sensitive information to unauthorised third parties, the installation or concealment of vulnerabilities, the endangerment of critical infrastructures or the loss of technology carriers in key technology sectors (e.g. semiconductors or artificial intelligence). In 2021, for example, the BSI was involved in the investment screening procedure of one of the world's leading suppliers to the semiconductor industry, where the BSI contributed its technical expertise.

Since 2015, the number of review requests by the BMI in the context of the investment screening procedures has increased enormously in line with the increase in investment screenings, i.e. 256 decrees were processed by the BSI in 2021, compared to five in 2015. This huge increase in investment screening procedures continued in 2022 and further records are expected during the course of the year. The reason for this lies in the expanded legal basis for auditing, participation in EU investment procedures, as well as increased public sensitivity regarding trade policy effects on the national security situation and technological sovereignty (see *The State of IT Security in Germany in 2021*).

Market Surveillance

In September 2021, the establishment of the Market Surveillance Agency for certified service providers and products began at the BSI. On the basis of § 9c para. 8 BSIG, the Market Surveillance Agency can check the properties assured by the manufacturers of all certified and labelled products and services in the BSI on a random, unsolicited or ad-hoc basis. The aim is to identify and eliminate vulnerabilities as quickly as possible in order to further strengthen IT security in Germany.

With the award of the first IT security labels, the first formal and official acts were already performed in March

2022. In preparation for the implementation the Cyber Security Act (CSA), the Market Surveillance Agency is involved in the establishment of the National Cybersecurity Certification Authority (NCCA). After implementation, supervision will also be taken over for the certificates awarded under the CSA.

2.3 — The State and Administration

One of the BSI's core tasks is to defend against cyber attacks on government networks and the federal administration. The BSI provides a wide range of services for improving information security for federal, state and local authorities: Information security consulting, IT-Grundschutz and minimum standards as well as certification and accreditation provide the basis. In the event of IT security incidents, *CERT-Bund,* Mobile Incident Response Teams (MIRT) and the National Cyber Defence Centre provide support to affected authorities. The central point of contact for the states and municipalities is the BSI's national liaison office. Liaison offices are located in Hamburg, Berlin, Bonn, Wiesbaden and Stuttgart.

2.3.1 — The Threat Landscape in the Federal Administration

Government networks are exposed to attacks from the internet on a daily basis. In addition to predominantly untargeted mass attacks, there are also targeted attacks on the federal administration. The BSI uses various complementary measures to protect government networks from these attacks.

Web filters are a preventive measure that block access to websites or the connection to web servers that are associated with malware. This prevents, for example, access to malware hidden behind download links that is spread via email, social media or websites as part of social engineering attacks. It also prevents malware from communicating with the corresponding web servers, for example to reload further components or commands. In the current reporting period, about 78,000 additional *malicious* websites had to be blocked. While the number of websites blocked each month remained relatively stable from June 2021 to February 2022, the threat assessment changed significantly in March 2022 against the backdrop of the Russian war of aggression against Ukraine, so that noticeably more *malicious* websites had to be blocked from access by the federal administration. The index jumped by 158 percent to 353 points within a month (see Figure 28) - the highest value since records began.

Malware sent directly in email attachments is detected by automated antivirus protection measures, which stops delivery to the recipient. During the reporting period, this affected an average of 34,000 emails per month. After a very strong wave of attacks in the previous reporting period and the shutdown of the Emotet infrastructure at the end of January 2021, the "Index of malware attacks on the federal administration" initially normalised. Then, in March 2022, a significant spike in the indicator marked the sharp rise in Emotet spam (see Figure 29). Activity in the botnet had already been observed since autumn 2021 and had noticeably intensified since March 2022.

Around 5,200 emails per month were identified as malicious solely on the basis of antivirus signatures specially created by the BSI. In order to be able to detect targeted attacks on the federal administration in particular, the BSI operates a system for detecting malware in the data traffic of government networks downstream in addition to the measures already described. Using a combination of automated testing procedures and manual analysis, the BSI analysts were able to identify an average of just under 2,500 more attacks per month that were neither detected by a commercial solution nor by one of the automated solutions mentioned above.

In addition, the security of government networks is increased with central protection against spam emails. This measure is not only effective against unsolicited commercial emails. It also detects cyber attacks such as phishing emails.

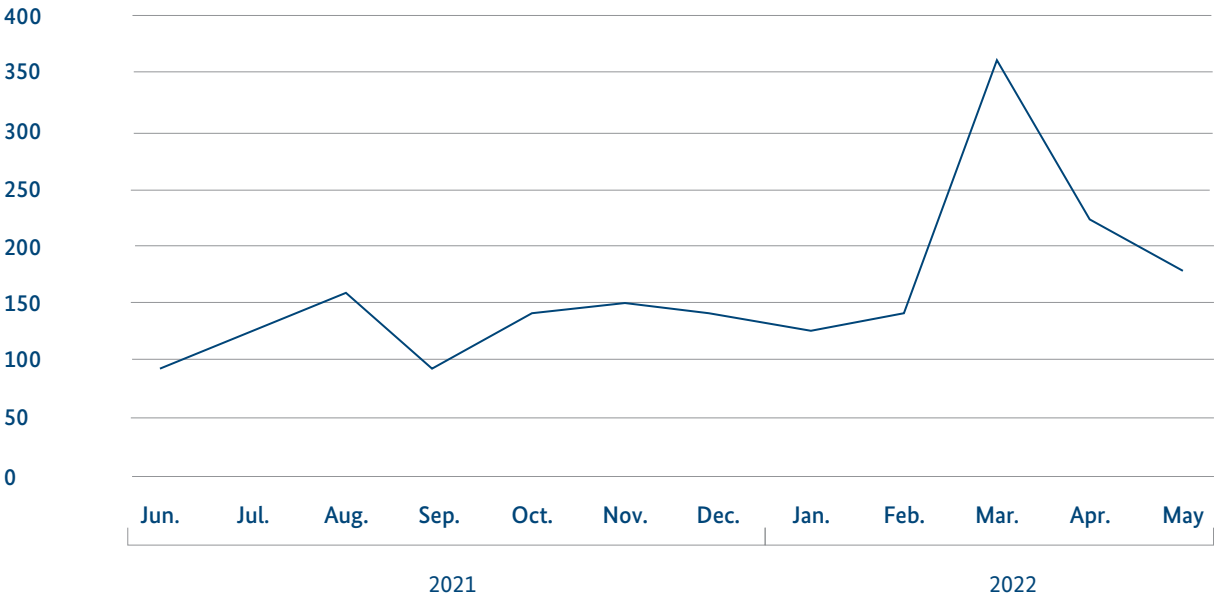
The spam rate, i.e. the share of unsolicited emails in all incoming emails, averaged 58 percent in the reporting period. The volume and development of spam emails in the federal government's networks are measured by the spam mail index. This reached an average of 111 points in the reporting period. In the previous reporting period, the indicator was still at 114 points. There were considerable fluctuations in some cases. While spam levels were below average in late summer and autumn 2021, the index values jumped significantly in December 2021 and especially in February 2022.

In December 2021, a sextortion campaign following the online shopping events Black Friday and Cyber Monday

The Threat Situation in the Federal Administration

2018=100

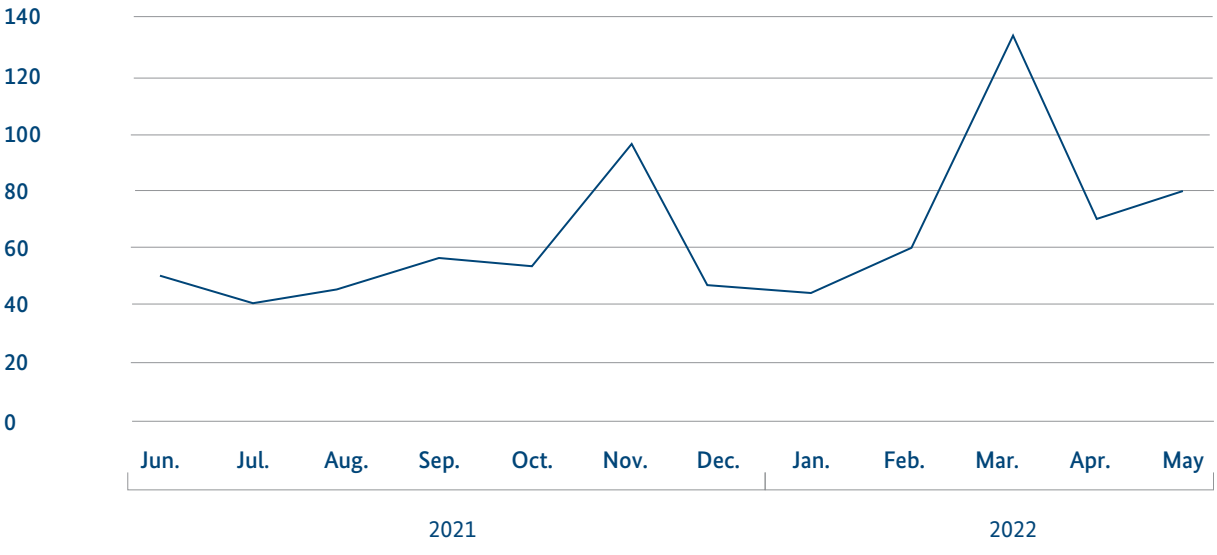
Figure: 28
Index about the new blockings of malicious websites
Source: Web Filter Measurement



Index on Malware Attacks on the Federal Administration[1]

[1]without attacks on authorities that do not participate in the BSI's central protection measures

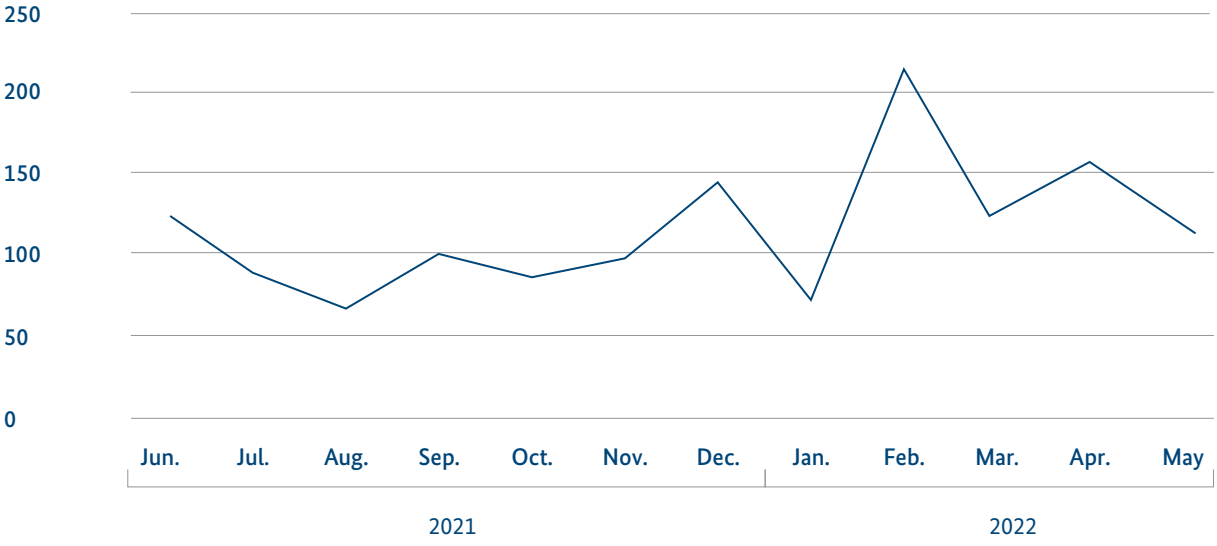
Figure: 29:
Source: Survey on Malware Attacks on the Federal Administration



Spam Mail Index for the Federal Administration[1]
2018=100

Figure 30:
Source: Survey on email traffic within the federal administration

[1]Without spam mails to authorities that do not participate in the BSI's central protection measures



drove the values up (see also chapter *Spam and Phishing,* page 26). The federal administration's spam filters reliably block such spam waves so that they do not reach the addressed users.

2.3.2 — Computer Emergency Response Team for Federal Authorities

With the specialist units of the *Computer Emergency Response Team* of the Government *(CERT-Bund)*, the BSI is the central point of contact for preventive and reactive measures with regard to incidents in computer systems that are relevant to security and availability. In order to fulfil these diverse tasks, in *2021 CERT-Bund* has been expanded into an independent department with five units: Principles and Warning and Information Service (WID), Incident handling and Liaison Office for the National Cyber Defense Center, Mobile Incident Response Team (MIRT), Technical Analysis and Industrial Control and Automation Systems. They deal with a wide range of topics, including cyber security warnings, the coordinated vulnerability disclosure (CVD) process (see chapter *Vulnerabilities in Software Products,* page 31), incident handling and *CERT-Bund* reports. On-site operations are only carried out by the MIRT in exceptional cases according to § 5b BSIG. This is particularly the case if the attacks are of a sophisticated technical quality or if the rapid restoration of the security or functionality of the affected information technology systems is of special public interest.

In addition, *CERT-Bund* continues to be very active in various CERT and cyber security communities.

Under the IT-SiG 2.0, the BSI has been given the authority to check IP addresses of federal institutions, critical infrastructure, digital services and Companies of Particular Public Interest for vulnerabilities on an ad hoc basis pursuant to § 7b BSIG. Accordingly, initial port scans were carried out on 2,298 IP address blocks with more than one million IP addresses of the immediate and secondary federal administration. The results are now being verified together with the authorities concerned. Initial improvements have already been identified and appropriate measures introduced. In addition, as already mentioned, the liaison office to the National Cyber Defence Centre has been established within *CERT-Bund*. This means that the BSI provides the premises and infrastructure for the

National Cyber Defence Centre and is actively contributing to its further development. Due to its integration in *CERT-Bund* it is possible, for example, to quickly cooperate with the other security authorities in the event of incidents.

During the reporting period, there were several high-profile events, such as Log4Shell (see incident *Log4j: Vulnerability in Open Source Library,* page 37) and the Russian war of aggression against Ukraine (see chapter *Cyber Security Situation in the Context of the Russian War of Aggression against Ukraine,* page 45), which significantly increased the workload. This is reflected, for example, in the number of Cyber Security Warnings (CSW) as well as in the number of working days spent on incident handling.

2.3.3 — National Liaison Office

The design of information security in digitalisation can only be successful through joint efforts by the federal government and the federal states (the Länder). For this reason, the BSI has further expanded its support options for the federal states and promotes cooperation at various levels. The overarching goal of the cooperation is to create a uniformly high level of IT security in Germany.

The National Liaison Office, with its liaison offices in Berlin, Bonn, Hamburg, Stuttgart and Wiesbaden, facilitates exchange considerably through its direct contact persons for all 16 federal states and thus contributes significantly to increased cooperation. The liaison offices are responsible for bringing the BSI's products and services to the target groups - federal states, the industry and society - and thus for spreading the topic of information security.

The close cooperation between the federal government and the federal states is reflected in the cooperation agreements that have been successively concluded with the federal states since the end of 2021. This forms the basis for the implementation of specific cooperation projects that significantly increase the level of cyber security at the national and federal state levels.

2.3.4 — Cooperation with the Federal States and Municipalities

In 2021, the first cooperation agreement to expand federal state cooperation was signed with the federal state of Lower Saxony. A total of 17 areas of cooperation were identified, including mutual support in the event of high-profile cyber security incidents. In addition, the BSI cooperates with the federal states on a variety of topics, for example in the federal-state committees, and offers them support in a variety of ways, for example by providing advice. Since cyber threats are not confined to federal state borders, the BSI is continuously expanding its cooperation in this area.

Efficient cooperation with the almost 11,000 municipalities nationwide requires structured approaches that can only be carried out together with multipliers from the municipal umbrella organisations and federal state institutions. The goals are, in particular, to raise awareness at the management level and to support the operational level in the implementation of information security. In addition to the joint creation of IT-Grundschutz profiles, the focus is also on providing scalable guidelines for getting starting and implementing IT-Grundschutz.

Together with the federal states and the municipal umbrella organisations, the BSI regularly participates in congresses and conferences and creates technical papers. The BSI also designs and organises information events.

In 2021, the BSI for example designed and prepared the Roadshow Municipalities (Roadshow Kommunen). This is a virtual event series for the target group of municipalities, which will be carried out together with interested federal states from 2022.

2.3.5 — Cyber Security of State Elections

Elections are very important in democracies because they are the basis of legitimacy for governments and parliamentary action. After the "super election year 2021", four federal state elections were held in 2022. In addition to three other state elections, a nationwide election will follow in 2023 with the Sozialwahl (social insurance election). Election-related cyber attacks in other countries show that state and non-state actors are trying to attack, disrupt or even sabotage democratic processes. Examples in France and the UK, among others, illustrate the vulnerability of elections to cyber attacks: In the so-called Macron Hack, attackers published more than 20,000 stolen emails from the campaign team of one of the candidates one day before the run-off in the 2017 presidential election. In 2019, confi-

dential documents on the free trade agreement between the United States of America and the United Kingdom were leaked through "Hack & Leak" in the run-up to the General Election to influence the vote.

In addition to state-directed attack attempts that specifically target both the electoral landscape and the public opinion-forming process (see chapter *Advanced Persistent Threats,* page 38), cybercrime activities such as ransomware attacks (see chapter *Ransomware,* page 13) and malware spam also threaten the electoral landscape. The interest of the latter attackers is not to disrupt or subvert democratic elections, but to extort ransom or protection money from institutions involved in the electoral process. Such activities can significantly disrupt confidence in the proper conduct of elections. For example, a ransomware attack against a city or district administration could cause delays in holding the election or counting the votes if, for example, email communication is unavailable due to the attack. The loss of trust within the population towards the electoral process is accepted by the attackers or is even considered as a goal.

Even if the actual voting in Germany is analogue – with pen and paper – information technology is used extensively in the electoral process and the electoral and information landscape. Processes are becoming increasingly digitised. This trend was further strengthened by the COVID-19 pandemic: Party congresses are held digitally, citizens increasingly use the internet to inform themselves about electoral options, and election campaigns have already been taking place on social media, among other places, for several years. Institutions and actors deliberately publish public information, such as election programmes or information on the election process, digitally as part of their communication with citizens or voters. At the same time, they also process internal, non-public data that is only intended and released for a restricted group of participants. These data require protection in a wide variety of forms. The availability, confidentiality, integrity and authenticity of information in this area may be threatened.

In accordance with the federal, legal framework conditions, the BSI also supports the safeguarding of state elections through various services.

- The BSI is available as a point of contact for the state electoral administrations to secure the formal electoral process and its IT support. For the numerous parties involved in the elections as well as the candidates, the BSI offers extensive information and recommendations via its web and target group service (public administration, consumers, businesses and critical infrastructures), for example on the further improvement of existing protection measures, networking as a source of up-to-date information and warnings, the use of IT services and much more.

- Added to this is the expansion of supporting measures. This includes, in particular, the expansion of daily 24/7 situation monitoring of various public, non-public and social media.

- The BSI also participates in various federal working groups on threat identification and assessment and is involved in the design of tangible measures. Corresponding reports, advice, information, etc. are made available to the different target groups via the BSI's various channels.

2.3.6 — Information Security Advisory Service

The Information Security Advisory Service for the federal government advises federal agencies on all information security issues. It focuses on the establishment, maintenance and improvement of information security management. In addition, another task of the Security Advisory Service is to deal with policy matters.

A major focus of the work in the reporting period was on safeguarding the electoral process. This included advising parliamentary groups, candidates and parties on information security issues. The Information Security Advisory Service has provided a supportive IT security guide for candidates in federal and state elections. The pandemic created another topic in 2021: The Information Security Advisory Service reviewed the information security concept for the digital proof of vaccination. Intensive cooperation with the Federal Academy of Public Administration (BAköV) also helped to support the training and further education of information security officers.

2.3.7 — Consulting on the Protection of IT used for Processing Classified Information

In accordance with the legal regulations, the BSI participates in the implementation of the General Administrative Provision for the Material Protection of Classified Information (Classified Information Directive (VSA)). The modernisation of the VSA 2018 should take into account the advancing digitalisation in the field of the protection of classified information in particular. Since then, the need for advice and evaluation on technically innovative digitalisation projects involving IT used for processing CI (CI-IT) has increased considerably. Major projects such as currently, the federal IT consolidation, interdepartmental classified communication, cross-level CI-IT projects, etc., as well as other future digitalisation projects, entail a steadily increasing amount of consulting and evaluation, especially in the area of protection of CI-IT. In order to be able to meet these challenges even more efficiently, the reorganisation of the BSI on 13 December 2021 resulted in a division of the previous unit for consulting von protection of classified information into the two central fields of action – CI-IT on the one hand and material security on the other.

Consulting on protection of CI-IT takes place upon request for federal agencies within the scope of the VSA and other public agencies. Consulting on protection of CI-IT mainly takes place for digitalisation projects with particular strategic and political significance. In addition to consulting, the unit for consulting on protection of CI-IT examines the CI-IT in certain cases and prepares release notes for the conception and operation of CI-IT. In the previously mentioned cases these are crucial prerequisites for ensuring comprehensive and uniform protection of classified information.

During the reporting period, key tasks of the unit of consulting on protection for CI-IT included audits in connection with authorisation of CI-IT and the preparation of release notes for the conception and operation of CI-IT for various complex federal IT projects, such as the federal e-file system E-Akte Bund and the federal operating platform "Betriebsplattform Bund". In addition, the IT-Grundschutz module for the protection of information classified VS-NUR FÜR DEN DIENSTGEBRAUCH was finalised and the inclusion into the IT-Grundschutz compendium was initiated. This module will facilitate the implementation of protection requirements for information classified VS-NUR FÜR DEN DIENSTGEBRAUCH within government agencies. Moreover, the collaboration in NATO committees in the area of CI-IT was intensified, and intensive cooperation with the BAköV supported the training and further education of security officers and their staff as well as classified information registrars.

2.3.8 — Smart Borders and Sovereign Identity Management

The aim of the European Smart Borders programme and the overarching regulations on the interoperability of European IT systems in the area of security, immigration and borders is the secure identification and verification of third-country nationals at the border and within the Schengen Area. This involves technically linking the European Entry/Exit System (EES) and the European Travel Information and Authorisation System (ETIAS) with the Schengen Information System (SIS) for the police, the Visa Information System (VIS) and other IT systems at European level. This will allow for centralised, standardised and uniform European identity management for third-country nationals. In addition to increasing security in the Schengen Area, especially in the context of cross-border crime, illegal immigration and epidemics, another goal of this project is, among others, to establish more efficient border control processes.

Initially promoted in the context of the refugee crisis in 2015, the objectives of the European registers have lost none of their relevance today. Being able to know at all times who is crossing the border of the Schengen Area, who has already applied for asylum in an EU state and who may pose a threat to public safety are all needs that have been frequently expressed in the context of the current refugee movement – but they are also core considerations in the revision of the European register landscape. The secure and timely biometric registration of refugees is also a current challenge, which the BSI is helping to address by preparing state-of-the-art Technical Guidelines. As air passenger numbers recover, issues such as combating cross-border crime and illegal immigration, as well as the need for efficient border control, are also gaining renewed importance.

The BSI is actively involved in the implementation of the above-mentioned European projects at both European level and national level. While working on the further legal acts at the European level, the BSI

remained focused on the security of digital identities and pointed out logical vulnerabilities in cross-system processes of European identity management. Nationally, version 5.2 of the Technical Guideline BSI TR-03121 was published in November 2021, which for the first time contains a separate volume for the use cases in Immigration Offices and can serve as a basis for future tenders. Similarly, a guideline for the processes of digital sovereign identity management when dealing with the new European registers was updated in 2022 in cooperation with other federal authorities under the leadership of the BSI. In parallel with the development of this specification, the BSI is developing data analysis for sovereign systems in order to support the correct and efficient implementation of the components at all levels, nationally and internationally.

2.3.9 — Technology Verification in Technology Labs

The BSI investigates specific IT security issues in products from select manufacturers down to the level of the source code. With the in-depth understanding of technology that is gained as a result, solutions can be developed for a wide variety of aspects. During the reporting period, some of the planned on-site inspections could not be carried out due to the Covid situation. All test dates scheduled abroad were suspended. Moreover, travel to the Security Labs in Bonn was difficult. As a result, audits in Bonn took place with a reduced scope. This also meant that more online workshops and conceptual work was carried out.

Cornerstones of the Technology Verfication Programme:

- *Focus on technical (not political) issues*
- *Application of the equal treatment principle for all manufacturers.*
- *Deepening technical know-how in selected key technologies.*
- *Working closely with the manufacturer's research departments to actively participate in shaping the information security of new technologies in order to establish security standards across the industry.*
- *Work takes place in local and international Security Labs to optimise both the flow of information and to enable local source code analysis.*
- *Audits are always carried out by BSI personnel. However, support from 3rd party labs is always possible. BSIG: § 7a para. 1 provides the legal basis for the audits.*
- *The first step is always the evaluation of the key technology. Downstream source code review only serves to verify correct implementation in the particular system.*
- *Gained understanding will be published in Technical Guidelines as needed and used to create a uniform test catalogue.*
- *Establishment of a link between the verified key technology and the operational networks of stakeholders.*
- *Risikobasierter Ansatz: Es geht hauptsächlich darum, Detektionsmöglichkeiten zu verbessern, anstatt Angriffe gänzlich zu verhindern.*
- *Risk-based approach. The main aim is to improve detection capabilities rather than to prevent attacks altogether.*

All of the above goals can only be achieved with the support of the manufacturers. For this reason, investments are only made in long-term cooperations.

2.3.10 — App Testing for Mobile Solutions

Applications on mobile devices extend the functionality of the basic system and play an essential role in the success of mobile solutions. However, the use of apps poses security risks both for the security of the data processed and for the security of the overall solution. These security risks must be assessed in order to make any kind of overall statement about the security of a mobile solution.

The app testing service for federal authorities provided by the BSI in cooperation with Deutsche Telekom Security GmbH offers an essential decision-making tool for those responsible in each case as to whether and under what conditions an app can be used. This provides the greatest possible flexibility in the use of any additionally required apps on official devices, while at the same time guaranteeing basic IT security.

Aspects of both security and data protection are taken into account during the app tests. The test reports also contain, where applicable, information and recommendations to users which settings or constraints should be observed for the safest possible use of the app in question.

If required in individual cases, the use of an app will also be explicitly discouraged if the test results suggest this.

The governmental users can access a larger pool of already existing test results of tested apps as well as initiate new tests if required. It is also possible to have apps checked regularly so that apps that have been approved for use can be kept up to date.

Currently (as of May 2022), the app testing service is used by registered users from 65 government agencies and organisations. More than 1,100 test results are available for the 655 different apps that have already been tested. In around 70 percent of the test results, advice and recommendations were given on what should be taken into account when using the app in question. In fact, every sixth app tested was advised not to be used.

The app testing service contributes to strengthening IT security in the area of mobile applications on official smartphones.

2.3.11 — Online Access Act: The Portal Network IT Security Regulation

The Online Access Act (Onlinezugangsgesetz, OZG) is an "act to improve online access to administrative services" and provides for the digitalisation of all administrative services at local, state and federal level, so that citizens can apply for these services easily and securely online via administrative portals. The digital administrative process is to be designed uniform throughout Germany, so that the administrative portals are additionally interconnected to form an interoperable network, the Portal Network (Portalverbund) In order to ensure the IT security of the Portal Network, the BMI has emphasised the importance of the BSI in the implementation of the OZG, in particular the BSI Basic Protection Standards 200-1, 200-2 and 200-3, as well as some of its Technical Guidelines in its "Regulation to Ensure the IT Security of the IT Components Used in the Portal Network and for Connection to the Portal Network" (IT-Sicherheitsverordnung Portalverbund – ITSiV-PV) of 06/01/2022. The ITSiV-PV states that the aforementioned BSI requirements for IT security reflect state-of-the-art technology and must therefore be complied with by the components of the Portal Network.

Further information can be found here:[x]

The Technical Guideline TR-03160 "Service Accounts"[42] deals with the service accounts that applicants can use for identification. It does this by setting requirements to prevent misuse and identity theft at the level of trust required in each case, while ensuring interoperability between the different service accounts. Currently, it

is being expanded to include a section that deals with the inbox for receiving notices. An additional section is planned which takes into account the special requirements for organisational accounts.

In addition, the ITSiV-PV mentions the Technical Guidelines TR-03107-1 "Electronic Identities and Trust Services in eGovernment Part 1"[43] and TR-03147 "Trust Level Assessment of Procedures for Identity Verification of Natural Persons"[44], which, among other things, define requirements for the technical basis of identification and *authentication* and the associated mechanisms for digital declarations of intent. The Technical Guideline TR-03116-4 "Cryptographic Specifications for Federal Government Projects Part 4"[45] describes security requirements regarding the implementation of communication procedures in federal government applications.

A new Technical Guideline is also being developed for the Portal Network itself, which describes specific measures for securing the entire network and its individual components against attack scenarios, such as the unauthorised leaking of data. As part of this Technical Guideline, the BSI is currently looking specifically at individual aspects of the Portal Network, such as different portal solutions in use. These are examined in coordination with the portal owners for possible vulnerabilities that could be exploited by potential attackers. The knowledge gained from this will be incorporated into the resulting Technical Guideline.

Lastly, the BSI is involved in addressing IT security issues related to the modernisation of the registry landscape. It serves as a necessary foundation for making the Portal Network user-friendly and for implementing the Once-Only Principle, which should eliminate the need to enter data multiple times. The aim of register modernisation is to ensure the exchange of register data and verifications between different authorities without media discontinuity, as well as for administrative services within the Portal Network.

2.4 — Internationally

IT security is more than just a national task, it is a European and international one. In order to effectively counter the internationalisation of cybercrime, it is more important than ever to join forces at the international level. This has been demonstrated not least by the use of cyber attacks in international conflicts (see chapter Cyber *Security Situation in the Context of the Russian War of Aggression against Ukraine,* page 45). For this reason, the BSI has been working with partners around the globe since its foundation: bilaterally, multilaterally or in committees and working groups. The experts from the BSI are in demand as discussion partners and speakers.

In addition to its national task as the Federal Cyber Security Authority, the BSI also aims to shape cyber security internationally and to strengthen its own technological assessment capability. In order to adequately fulfil this responsibility, the BSI is continuously intensifying and expanding its relationships with authorities, organisations and companies as well as actors from science and civil society worldwide. Its work in various expert committees on information and cyber security in the EU, NATO and the wider international context is an essential part of the BSI's international commitment. As part of digitalisation, there is a need in many states and regions to build up their capacity in the area of IT security. The BSI is responding to the associated need for advice and support by actively developing partnerships in Central and South America, Africa and the Middle East. This enables the BSI to pass on its know-how, set international standards and raise the level of cyber security worldwide. Through cooperation with the BMZ and the GIZ, the BSI's expertise can also be used in the context of German development cooperation.

2.4.1 — The BSI's Engagement in the EU

An increasing number of legislative projects with far-reaching significance for the cyber security of Germany and the European Union (EU) are shaping the European regulatory situation. The proposal for a Directive on measures for a high common level of cyber security in the Union, the NIS 2 Directive, and two initiatives to enhance cyber and information security in the EU institutions, bodies, offices and agencies deserve special attention. During the reporting period, these projects went through different stages of negotiation between the EU institutions. The NIS 2 Directive is expected to come into force before the end of 2022. Discussions on the other two initiatives were only initiated by the European Commission in March 2022. As the national expert for cyber security, the BSI has been intensively involved in the negotiations. The main concern was to achieve a substantial increase in IT security for the state, the economy and society in Germany and Europe.

Parallel to this, important concerns were pursued in various EU expert bodies, for example in the areas of certification, operational cyber security or the protection of critical infrastructure. Another positive aspect is that the number of BSI experts delegated to key EU institutions has been increased.

2.4.2 — The BSI's Engagement in NATO

The BSI performs the roles of National CIS Security Authority (NCSA) and National Cyber Defence Authority (NCDA) for the Federal Republic of Germany within NATO. In the context of NATO engagement, these are the fields of Information Assurance and Cyber Defence. The BSI is actively involved in a number of NATO committees and contributes BSI expertise to the Capability Panel 4 (CaP4) and the Capability Teams below it. As part of the implementation of the NATO Cyber Defence Strategy, the BSI is constantly working to strengthen its role as NCDA.

By taking over the leadership of the NATO Cloud Security Technical Directive Writing Team, which consists of Belgium, Germany, France, the United Kingdom, as well as the NATO Office for Security (NOS) and the NATO Communications and Information Agency (NCIA), the BSI played a significant role in the drafting of the NATO "Technical and Implementation Directive for the Protection of NATO Information within Public Cloud-Based Communication and Information Systems for NATO UNCLASSIFIED". The BSI was also able to successfully introduce minimum requirements for secure *cloud computing* as set out in the *Cloud Computing* Compliance Criteria Catalogue (C5).

2.4.3 — Multilateral and Bilateral Engagement of the BSI

Following the Cyber Security Directors' Meeting, which was held for the first time in 2020, the BSI organised a subsequent event in February 2022 as part of the Munich Security Conference. Given the cross-border threat landscape and the challenges of digitalisation, the event once again offered a unique opportunity to discuss strategically important topics that affect all European cyber security authorities equally and pose major challenges, away from the day-to-day business. The event was again a great success in 2022. The BSI is thus further expanding its position as a thought leader in information security and making an important contribution to improving the networking of European cyber security authorities.

The delegation of BSI staff abroad is another element towards better networking and cooperation with international stakeholders. In the reporting period, the BSI sent delegated national experts to ESA/ESTEC, ENISA and the EU Commission. Moreover, the BSI is currently providing the German spokesperson in the NATO Cyber Defence Committee and continues to be present on site with a liaison in Brussels.

In 2021, the BSI, together with its French counterpart, the French Network and Information Security Agency (ANSSI), once again published a Franco-German IT security situation report, this time on the topic of ransomware. The annual publication, which appeared for the fourth time in 2021, is a visible sign of the close Franco-German cooperation in the field of IT security and simultaneously illustrates that threats are not confined to national borders.

2.4.4 — Structure of the National Cybersecurity Certification Authority

As a result of the amendment to the BSIG in May 2021, § 9a was newly introduced, which stipulates that the BSI is the National Cybersecurity Certification Authority *(NCCA)* within the meaning of (EU) Regulation 2019/881 (Cybersecurity Act (CSA), see chapter *IT-Grundschutz,* page 78). As the NCCA, the BSI is the state certification body for the trustworthiness level "high" as defined by the CSA. By promptly establishing the German *NCCA,* the BSI has taken on a pioneering role in Europe and can thus work towards harmonised implementation of the CSA requirements in the member states within the framework of bilateral exchanges of experience. This has already led to bilateral talks with representatives of the European partner authorities, such as the French ANSSI.

European cooperation is the focus of the BSI as the *NCCA*. For this purpose, a network is being established to ensure regular exchange with the *NCCAs* of the European member states as well as with the European Commission and the European Union Agency for Cyber-

security (ENISA). The aim is to develop and implement the European cyber security certification schemes in a timely manner in order to strengthen IT security for the European single market by standardising the requirements. In July 2021, all European member states had the opportunity to comment on the draft Implementing Act of the European Commission's CC-based European Cybersecurity Certification (EUCC) scheme, which will be the first CSA scheme to be launched in summer 2022. In this context, the BSI is actively involved in the respective bodies, including the European Cybersecurity Certification Group (ECCG), its subgroups and the Ad Hoc Working Groups (AHWG) of ENISA, in the design of the Implementing Act and the Guidance Documents, where the management of vulnerabilities and the use of cryptography are also negotiated in order to preventively ward off threats to ICT products, services and processes. The BSI also actively supports ENISA's scheme developments for cloud (EUCS) and 5G mobile equipment (EU5G) and critically examines and strategically evaluates new regulatory initiatives of the European Commission, such as the delegated act of the Radio Equipment Directive (RED), the revision of the Directive on measures to ensure a high common level of security of network and information systems in the Union (NIS2), the draft AI Regulation and the amendments to the Product Safety Regulation and the Machinery Directive with the aim of improving the IT security situation in Europe.

In order to be as well prepared as possible for the coming requirements, the BSI as NCCA is in continuous exchange with the conformity assessment bodies that will carry out cyber security certification in the future under the CSA for the assurance levels of "basic" and "substantial". In addition, the conformity assessment bodies will undergo an ENISA pilot process for accreditation, independent of the assurance levels of the CSA, which they were registered for by the BSI in August 2021 and which started in October 2021. The manufacturing companies that the BSI has been working together with in confidence within the framework of the CC certification up to now were informed about the upcoming innovations in a virtual information event in December 2021 with the promise that this productive exchange will be continued in order to guarantee the implementation of the specifications of the CSA for a harmonised level of security to reduce threats. The BSI also provides information as part of its public relations work in order to generate the greatest possible transparency regarding the legal requirements and their implementation, both via its website and via an article on the topic of NCCA in the 02/2021 issue of the BSI magazine and in various presentations.

Further information can be found here:

2.4.5 — National Coordination Centre for Cyber Security

The EU Regulation 2021/887, which came into force on 28 June 2021, established the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC), based in Bucharest, and a network of National Coordination Centres (NCCs). The ECCC is intended to act as the European Union's main instrument for pooling investments in research, technology and industrial development, especially in the field of cyber security of the two EU funding programmes "Digital Europe" (DEP) and "Horizon Europe" (HEP). Its purpose is to ensure greater coordination of research and innovation and deployment strategies at both European and national levels. The Competence Centre is managed by the member states and the EU Commission. A Governing Board was set up to serve this purpose, in which the BSI represents Germany.

The National Coordination Centres are the focal point for the ECCC at the state level. This creates a network that intensifies the exchange between the member states and within the cyber security community, so that possible international project partnerships can be found and concluded better and faster, thus strengthening digital sovereignty in Europe. Moreover, the Coordination Centres provide expertise and support in fulfilling the strategic tasks of the ECCC. This also allows national interests to be included in the European research programmes.

The German National Coordination Centre for Cyber Security in Industry, Technology and Research (NCC-DE) is a joint virtual institution of the BMI, BMWK, Federal Ministry of Defence (BMVg) and BMBF as well as other organisations (BSI, DLR-PT and FI CODE) and offers the national cyber security community a comprehensive catalogue of services for support. As the Federal Cyber Security Authority, the BSI acts as the head office and single point of contact and was officially designated as such by the BMI on 10 December 2021 through state secretary Dr Richter. Structures already established in the ministries and institutions, for example for the allocation of research

funds, will be used immediately. In its role as the head office of the NCC-DE, the BSI will work closely with the ministries involved and their subordinate departments as well as with the European Competence Centre and the NCCs of other nations.

Further information can be found here:[z]

2.4.6 — eID: Amendment of the eIDAS Regulation

Digital business processes have continued to grow in importance as the Covid pandemic has unfolded. This has led to an increased need for secure electronic identification/electronic identities to ensure the integrity of digital processes and a high level of trust between users and service providers, and to make online fraud and identity theft in particular more difficult.

In addition to many minor changes, the new draft regulation published in 2021 as part of the regular revision of the eIDAS Regulation provides for a European Digital Identity Wallet, which should be usable as an electronic ID (eID) across borders, but can also provide other attributes (e.g. educational qualifications) in a verifiable manner for service providers in addition to classic identity attributes (first name, last name, etc.). The BSI has been closely involved in developing the necessary framework conditions, has introduced the existing German infrastructure and continues to advocate for secure and user-friendly eID solutions that can be used across borders.

Additionally, other states have designated electronic identification systems for cross-border recognition within the framework of the existing eIDAS Regulation, which are subject to a mutual recognition obligation after a one-year transition period. The BSI has also been intensively involved in peer reviews on this. In total, the recognition obligation now concerns 21 electronic identification systems across Europe.

2.4.7 — Minimum Requirements for IT and Cyber Security of Satellites

In a globally connected world, the state, the economy and society demand services that are available at all times for communication, navigation, position and timing as well as climate monitoring or weather forecasting. In many areas, the only way to implement these services is to support satellite-based infrastructure.

As the Federal Cyber Security Authority, the BSI is responsible for the cyber security of IT and communication systems. This is true regardless of whether the systems are terrestrial, airborne or based in space. This is why the BSI is heavily involved in the cyber and IT security of all satellite systems; low earth orbit (LEO), medium earth orbit (MEO) and geostationary earth orbit (GEO).

In the view of the BSI, it is essential to establish binding nationally coordinated objectives and defined fields of action to answer the cyber security questions specific to space. Against the background of the rapidly increasing commercialisation of outer space (New Space), the issue of what national and international regulatory tools may be required also needs to be clarified.

The BSI has already developed minimum requirements in cooperation with the KdoCIR, the German Space Agency of the DLR, and the national space industry and formulated them into an IT-Grundschutz profile.

Further information can be found here:[aa]

Modernisation of Cryptography for the Next Generation of the European Flagship GALILEO

The European navigation system GALILEO is currently the focus of projects concerning the cyber security of

satellites. Together with other member states, a catalogue of requirements was drawn up back in 2018 under the auspices of the BSI in order to future-proof satellite systems and their communication infrastructure in particular. One essential requirement is *resilience* to the threat posed by quantum computing. Together with international partners, the BSI is assisting the ESA and the Commission in implementing these requirements for the second generation GALILEO's. According to the European Commission's plan, the first satellites with modernised cryptography are to be launched as early as 2024. At the same time, the BSI will support the adaptation of the ground infrastructure.

2.5 — Current Trends and Developments in IT Security

The rapid pace of technological development constantly poses new challenges for IT security authorities. However, solutions to these challenges can partly be derived from the new technologies themselves, which provide security experts with new options for recognising and preventing security-related incidents in good time. The BSI works closely with universities, universities of applied sciences and other research institutions in areas such as artificial intelligence (AI), cryptography, quantum computing and blockchain to find answers to current security questions.

2.5.1 — Artificial Intelligence

As a technology of the future, AI represents an opportunity for information security but also a risk and possible toolbox for attacks. AI can already be misused today to manipulate media such as images, audio or texts ("deepfakes"), in order to generate fake news, for example, or to deceive remote identification procedures (see chapter *Multimedia Identities,* page 64). According to the BSI's findings, it is already possible to abuse these technologies in today's frequently used video conferences. Currently, video manipulation is often still recognisable by typical artefacts, but the development of the technology is progressing. This means that reliable technical detection mechanisms and techniques to ensure the integrity of media are necessary to detect such attacks or to make them more difficult.

AI techniques can also be used to improve information security. One possible scenario is, for example, the (semi-)automatic generation of situation reports. In a current project, the BSI is investigating how AI techniques can be used to automatically analyse and extract textual information from the cyber security domain in order to reduce the workload of analysts and find the appropriate text passages for a posed question.

AI can also make a contribution in the area of secure software development. The ML-SAST project, whose interim report has already been published, shows how AI techniques can improve existing static code analysis techniques to achieve a significantly higher level of accuracy.

However, AI approaches such as deep-learning algorithms can themselves become the target of an attack, for example with the aim of manipulating the decision-making process of such an algorithm. To counter this, the BSI is investigating possible attacks on deep learning algorithms in a recently published study of the project "Security of AI systems: Fundamentals" in order to develop suitable countermeasures as a next step.

Deep learning is becoming increasingly important in the field of biometrics. In November 2021, the Biometrics Evaluation Centre (BEZ) was officially opened in Sankt Augustin near Bonn, where the BSI cooperates with the Institute of Safety and Security Research (IFS) of the University of Applied Sciences Bonn-Rhein-Sieg. Based on their research on the reliability of and vulnerabilities in biometric systems and their AI components, BEZ will offer consulting services, develop evaluation methods for certifications, and establish new security technologies.

The BSI aims not only to improve the security of current technologies, but also to develop security standards for AI. An important step towards the security of AI services in the cloud is the AI Cloud Service Compliance Criteria Catalogue (AIC4), which was already used for audits at several companies last year. Currently, the BSI is developing AIC4 further in order to incorporate the new technological developments as well as findings from the audits already carried out. The BSI is also contributing the experience gained from AIC4 to national and international standardisation bodies, such as DIN, the European CEN/CENELEC, ETSI and ENISA and ISO.

In the reporting period, the BSI also investigated further AI topics and published the results on explainability of AI systems and security of quantum machine learning, a

future technology that combines areas of artificial intelligence and quantum computing.

Based on the diverse topics and challenges in the area of IT security and AI, which are subject to constant change and are becoming increasingly important, it is clear that the BSI needs to intensify its activities in this area.

In light of the diverse topics and challenges in the area of IT security and AI, which are subject to constant change and are becoming increasingly important, the BSI is intensifying its activities in this area. Last year, the BSI established a new AI office on the campus of the Saarland University in Saarbrucken. There, the BSI cooperates with the local research centres in the field of AI and IT security. Results of this cooperation are for example, a study on the topic of "Security of Symbolic and Hybrid AI Systems" that is currently being prepared in cooperation with the German Research Centre for Artificial Intelligence (DFKI) and several Master's theses on the subject that are being supervised by the BSI. Due to the geographical location, cooperation with France and Luxembourg in the field of AI and IT security will also be further intensified from Saarbrucken.

2.5.1.1 — Artificial Intelligence in Applications

In recent years, the performance of systems based on AI has risen sharply, which is why they are being used in more and more areas of application. This also includes applications that are critical to safety, such as automated driving. However, AI systems, despite their huge performance gains, also have various risks that need to be adequately addressed. These include the frequent lack of robustness to changes in the processed input data, which occur, for example, in automated driving depending on the time of day and the weather. Another challenge is the vulnerability of AI systems to qualitatively novel attacks that attackers can use to deliberately induce undesirable decisions. Additional risks exist in many applications, such as the possibility of discriminatory decisions by AI systems in the financial or health sectors.

In April 2021, the European Commission presented a draft regulation on AI, which is currently being negotiated and which addresses these challenges of AI systems from a regulatory perspective. The EU's AI Regulation will impose far-reaching requirements on high-risk AI systems in particular, such as in the mobility sector.

Before the planned operationalisation of the regulation within the next two to three years, however, essential technical questions still need to be clarified in order to transfer the general requirements of the regulation to an appropriate technical level and to develop sufficiently precise auditing procedures. The BSI is actively involved in various working groups at DIN, ETSI and ENISA that are contributing to this extensive task.

In the context of the AI Regulation, the workshop "Auditing AI Systems: From Principles to Practice" was also held in October 2021, which, as in the previous year, was organised by the BSI together with the TÜV Association (VdTÜV) and the Fraunhofer Heinrich Hertz Institute. The focus of the workshop was on exchanging experiences gained during the implementation of initial safeguarding and auditing approaches in practical projects, which were also discussed with a representative of the EU Commission. Based on the workshop, the BSI and VdTÜV working group, which has been in existence since 2019, has produced a white paper in which the current auditability of AI systems is presented in a compact matrix form. On the one hand, this forms the basis for carrying out future assessments and, on the other hand, serves to identify existing gaps in the operationalisation of the AI Regulation.

In addition, the BSI launched the AIMobilityAuditPrep project in December 2021, where the first specific criteria and auditing procedures for AI procedures in automated driving are being developed. In the medium term, this preliminary work should enable the BSI to draft a Technical Guideline.

Further information can be found here:[bb]

2.5.1.2 — Artificial Intelligence in Cryptography

AI came into use in various areas of cryptography for many years: Especially in side channel analysis, machine-learning methods are now firmly established. The best results can be achieved when machine learning is combined with expert knowledge about

possible sources of side-channel information, with the use of neural networks being particularly successful. Therefore, the BSI is currently investigating this topic more closely within the framework of two projects: In the project AI Methods in Side-Channel Analysis (KI-Methoden in der Seitenkanalanalyse, KISKA), the aim is to find out how existing approaches from the field of side-channel analysis of symmetric key encryption algorithms can be adapted or generalised to asymmetric key encryption schemes. The BSI is also working on an AI side-channel guideline. One of the aims of which is to provide evaluators and manufacturers with an overview of the current state of research in this field and to point out attack methods that need to be taken into account when evaluating and certifying implementations.

AI techniques also apply in the field of cryptanalysis. As part of two BSI consecutive projects, a team from the Ruhr-University Bochum is investigating ways to use artificial intelligence in the analysis and evaluation of symmetric key encryption schemes. One of the goals of these projects is the development of AI-based tools that can contribute to the security assessment of block ciphers.

2.5.2 — Cryptography

The progressive development of quantum computers threatens the security of widely used public key cryptography such as RSA and ECC. Therefore, the development and standardisation of cryptosystems that are unlikely to be broken even with quantum computers (post-quantum cryptography) is extremely urgent. For national security systems, BSI is operating under the hypothesis that cryptographically significant quantum computers will be available in the early 2030s. It should be emphasised that this statement is not to be understood as a forecast on the availability of quantum computers, but represents a benchmark for risk assessment. First post-quantum schemes for key transport as well as the hash-based signature schemes LMS and XMSS were already recommended in March 2020 in BSI's Technical Guideline TR-02102-1. The BSI guideline "Quantum-safe cryptography" (see box on the right) provides an overview of post-quantum cryptography and related topics.

The standardisation of post-quantum methods is currently mainly taking place in a process initiated by the US National Institute for Standards and Technology (NIST) with international participation. In July 2022, NIST announced its first selection for standardisation of post-quantum algorithms. The drafts of these new standards are expected to be released in 2023. However, post-quantum cryptography remains an active area of research: In 2022, two of the NIST-submissions, which advanced to the third and fourth round, respectively, were broken due to new attacks. However, the security of the algorithms recommended by BSI and of the ones selected by NIST for standardisation rely on a different set of mathematical problems. Therefore, these algorithms are not affected by the recent attacks.

In addition to the standardisation efforts, many concrete activities are currently underway to migrate to post-quantum cryptography. The recently launched SINA Communicator H is the first IT product in Germany approved up to SECRET, which implements a hybrid key agreement combining classical and post-quantum algorithms. BSI has also launched two projects implementing quantum-safe cryptography in the Thunderbird email client and in the open-source cryptography library Botan. Moreover, in cooperation with KPMG, an awareness survey on the topic of PQ migration was launched.

2.5.3 — Quantum Key Distribution

Quantum Key Distribution (QKD) comprises protocols for quantum computer-resistant key agreement whose theoretical security is based on quantum physical principles. The BSI considers QKD as a possible complement to post-quantum key agreement algorithms. However, this applies only to certain use cases, as the technical requirements for QKD are very limiting. In December 2021, the BSI published a guideline [BSI1] on the topic of quantum technologies and cryptography, which also contains more detailed explanations, recommendations and assessments on the use of QKD.

Further information can be found here:[cc]

Currently, there are no QKD products certified according to international standards. However, a first Protection Profile for QKD devices was completed in early 2022. The Protection Profile was created on behalf

of the BSI in cooperation with the ETSI Industry Specification Group QKD. The next step is to certify the Protection Profile. In order to be able to apply the Protection Profile, an ecosystem for QKD products must be established in which criteria and methods of evaluation – for example for *side-channel attacks* – are agreed upon and further developed.

The development of QKD devices in the EU is still at an early stage. However, some German companies and start-ups are now also developing QKD devices. Moreover, numerous projects in the field of QKD are being funded both in Germany and in Europe. The European project EuroQCI, which all EU member states have now joined, aims to establish a European quantum communication network. There are plans for a terrestrial and a satellite-based component. The BSI is part of the project's Security WorkingGroup. In Germany, the QuNET initiative, funded by the Federal Ministry of Education and Research (BMBF), is researching various aspects of quantum communication. The BSI is supporting the research initiative as a member of its advisory board. QuNET aims to provide highly secure inter-agency communication as a use case. In August 2021, a QKD link was set up between the BSI and the BMBF in Bonn as part of the QuNET project and a video conference secured with post-quantum algorithms and QKD was demonstrated.

2.5.4 — Self-Sovereign Identities and Blockchain Technology

In view of the digitalisation projects in business, industry and administration, the public discussion shows an increasing desire to grant the users of online services the greatest possible data sovereignty. Instead of storing user profiles with central login services, users should be able to store their identity data in a local application (wallet) and manage it themselves. This allows them to decide on a case-by-case basis to whom they disclose what information. The draft amendment to the eIDAS Regulation (see chapter *National Coordination Centre for Cyber Security,* page 92) also provides for such a form of selective identity data disclosure for the European Digital Identity Wallet (EUDI Wallet).

This concept is known as Self-Sovereign Identities (SSI). So far, there are no established recommendations on how to implement it in practice. The BSI published a brief guideline on SSI in December 2021 to draw attention to the aspects that are relevant to IT security.

The key issues paper on SSI can be found here:[dd]

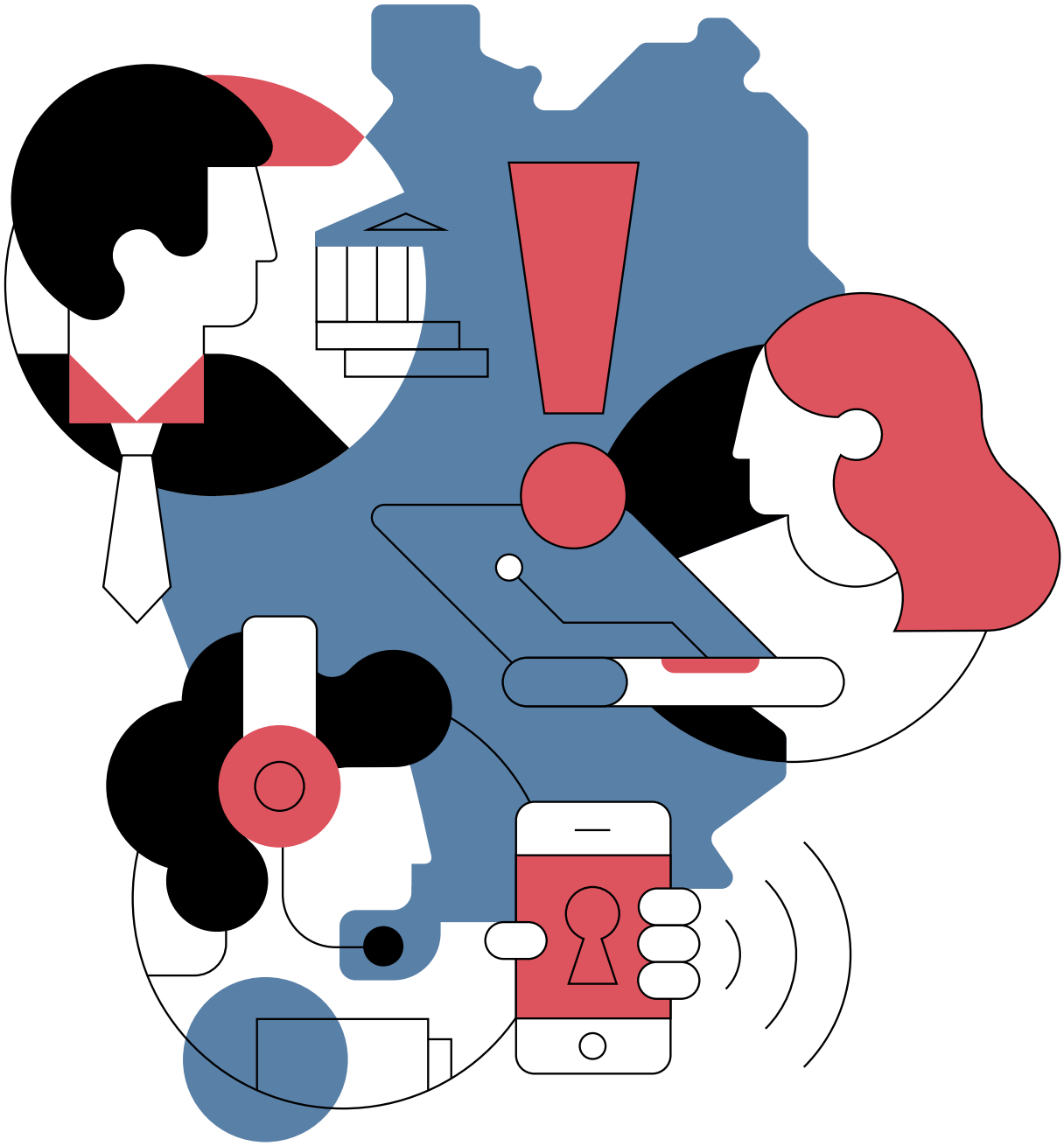
"Quantum-safe cryptography"

The guide "Quantum-safe cryptography - fundamentals, current developments and recommendations" provides an overview of the relevant developments in the field of quantum technologies as well as recommendations to migrate to quantum safe cryptography.

This transition also leads to numerous open questions (e.g. selection of suitable algorithms, necessary adaptations in protocols and standards, etc.), which are discussed in this document.

Further information can be found here:[ee]

Conclusions



Conclusions

The War of Aggression against Ukraine Aggravates the Cyber Security Situation in Germany

This year's report on the state of IT security in Germany was particularly influenced by the Russian war of aggression against Ukraine. This is because it is not just conventional forces and weapons that are being used in this conflict, but also digital methods of attack. For this reason, the BSI has been intensively monitoring the situation since February, strengthening its internal security as well as its crisis response and activating the National IT Crisis Response Centre. Moreover, the BSI also alerted its target groups, including the federal administration, operators of critical infrastructure and other organisations and companies, at an early stage and repeatedly, and called for increased vigilance and readiness to respond.

Since the beginning of Russia's war of aggression against Ukraine, there have been several additional IT security incidents in Germany. For example, the failure of satellite-based communication for the remote maintenance of wind turbines caused collateral damage in parts of Europe. Critical infrastructure operators were also targets of hacktivist attacks. There were also a few additional IT security incidents in Germany up to the deadline for this report, but they rarely had a noticeable impact.

Undeterred, the threat from cybercriminals persists unabated. The focus is once again on cyber attacks with ransomware, which due to their nature have far-reaching consequences for those affected and uninvolved third parties. DDoS attacks (overload attacks) also continue to threaten the information security of online shops and providers of web-based services in particular.

Overall, the ongoing tense situation continued to worsen in the reporting period. The threat in cyberspace is thus higher than ever.

Threat of Cyber Extortion Continues to Rise

The expansion of methods of cyber extortion observed in the previous reporting period has continued in the current reporting period. In particular, the extortion of companies with high turnover has increased further. Both the ransom and hush money payments reported by IT security service providers and the number of victims have continued to rise. The fact that not only companies with high turnover can become the target of ransomware attacks was demonstrated by the effects in several affected municipalities, where administrative processes were disrupted, in some cases massively, for months – with considerable consequences for citizens. The importance of strengthening cyber security at the municipal level in a targeted manner was also demonstrated by the great interest in the webinars offered by the BSI specifically for municipalities during the reporting period and the virtual "Municipalities Roadshow" (Roadshow Kommunen), which was held for the first time.

In addition, there were also repeated cases of blackmail with stolen identity data in the current reporting period. Considering the development in the past reporting period, it must be noted that the amount of identity data in the hands of cybercriminals is constantly increasing. This threat can directly affect every citizen. The BSI therefore recommends that people consider the way they deal with identity data by providing a wide range of information tailored to this target group.

Consumers were also the target of several sextortion campaigns, some of which were unusually pronounced. In these spam emails, attackers claim to have compromising, intimate secrets of the victim and threaten to publish them. In order to prevent the publication of the allegedly compromising information, the victim is supposed to transfer a certain amount in *Bitcoin*.

A New Dimension in Vulnerabilities

The vulnerability situation was more threatening than the average during the reporting period. This was due on the one hand to the fact that particularly critical vulnerabilities occurred in widespread products with vulnerabilities in MS Exchange and Log4j and could only be closed slowly. For Log4Shell in particular, there was prolonged uncertainty about how many IT products were actually affected and how the problem could be comprehensively fixed. On the other hand, the number of vulnerabilities that have become known has continued to increase overall. For example, the CVSS scoring system recorded 20,174 vulnerabilities in software products in 2021, about 10 percent more than the year before. This is also reflected in the reports published in 2021 by the BSI's Warning and Information Service on vulnerabilities in the 150 most common products. At 6,910, the number increased by around ten percent compared to the previous year.

The second half of 2021 also saw outstanding supply chain attacks via the Virtual System Administrator (VSA) software of an American software manufacturer, which is also widely used in Germany and therefore affected numerous customers. The VSA is used, for example, for the remote maintenance and monitoring of IT systems. Vulnerabilities in VSAs are particularly critical because any managed client can be accessed and software distributed via the VSA management server. The BSI therefore issued a cyber security warning on 4 July 2021, which was then regularly updated. The BSI intensively monitored how German organisations were affected, advised those affected on IT forensic measures and provided first aid documents.

A New Era for Cyber Security Made in Germany

Even before the surge in digitalisation that the Corona pandemic amplified, and before the new threat situation in the wake of Russia's war of aggression against Ukraine, cyber security was an essential success factor for an increasingly digitally connected society and economy. However, the accelerated digitalisation in all areas of everyday life – from the supply chains of multinational corporations, the business processes even in small and micro enterprises, the services of public institutions to the digital applications that almost every citizen uses every day – also calls for a new era in cyber security made in Germany.

More than ever before, the well-being of the population depends directly and to a large extent on how successful we are at strengthening the digital resilience of society. And this does not only mean resilience against cybercriminal attacks, against software and hardware failures or configuration errors that can endanger the availability of usual and everyday services. The past year also demonstrated that unforeseen events can raise the threat situation to a new level. That collateral damage from cyber attacks in neighbouring countries can also have a direct impact on Germany and Europe.

All of this makes it clear that preventive IT security measures are the most effective IT security measures. In light of this, the modernisation of the cyber security architecture planned by the Federal Government and the expansion of the BSI into a central office for information security in the federal-state relationship is an important step towards a tightly integrated federal cyber defence. Only intensive, lasting and continued cooperation between the federal and state governments will make it possible to provide an effective response to the dangers in "borderless cyberspace". The BSI will continue to rapidly increase its contribution and drive effective prevention against IT security incidents. Because every computer system that cannot be hacked, every IT-based service that cannot be disrupted, is a fundamental contribution to a functioning digitally connected society.

Glossary

Advanced Persistent Threats
Advanced Persistent Threats (APTs) are targeted cyber attacks on selected institutions and facilities in which an attacker gains persistent (permanent) access to a network and subsequently expands it to other systems. The attacks are characterised by a very high use of resources and considerable technical skills on the part of the attackers and are usually difficult to detect.

Advisories / Security Advisories
Recommendations from the manufacturers to IT security managers in companies and other organisations on how to deal with vulnerabilities that have been found.

Affiliates
In Cybercrime-as-a-Service, cybercriminals who use the service are usually called affiliates. The term comes from affiliate marketing, in which a commercial provider provides its distribution partners (affiliates) with advertising material and offers a commission. In the context of cybercrime, instead of advertising material, ransomware is provided, for example, and the affiliate is promised a share in the ransom.

Attack Vector
An attack vector is the combination of attack paths and techniques that an attacker uses to gain access to IT systems.

Authentication Process
The authentication process describes the process of verifying the identity of a person or a computer system on the basis of a certain characteristic. This can be done by entering a password, chip card or biometrics.

Authentication
Authentication refers to the proof of authenticity. An identity can be authenticated by entering a password, a smart card or biometrics, for example, and data can be authenticated by cryptographic signatures.

Backdoor
Backdoors are programmes, usually installed by viruses, worms or Trojan horses, that give third parties unauthorised access (backdoor) to the computer, but in a hidden way and bypassing the usual security devices.

Backup
Backup is the process of copying files or databases held on physical or virtual systems to a secondary storage location for recovery in the event of equipment failure or disaster, and keeping them safe until then.

Bitcoin
Bitcoin (BTC) is a digital currency, it is also known as a cryptocurrency. Payments between pseudonymous addresses make it much more difficult to identify counterparties.

Blockchain
The term blockchain describes a distributed, synchronised, decentralised and consensus-based data storage in a peer-to-peer network. In this process, a hashed list of data blocks is redundantly maintained in all network nodes, which is updated using a consensus procedure. Blockchain is the technological basis for cryptocurrencies like Bitcoin.

Bot / Botnet
A botnet is a network of computers (systems) that are infected by malware (bot) that can be controlled remotely. The affected systems are controlled and managed by the botnet operator using a Command-and-Control server (C&C server).

Brute Forcing
Attack method based on trial and error. Attackers automatically try out many character combinations to crack passwords, for example, and gain access to password-protected systems.

CEO-Fraud
CEO fraud is the term used to describe targeted social engineering attacks on company employees. The attacker uses previously captured identity data (e.g. telephone numbers, passwords, email addresses, etc.) to impersonate the CEO, management, etc. and induce employees to pay out large sums of money.

CERT / Computer Emergency Response Team
Computer emergency team consisting of IT specialists. CERTs have now been established in many companies and institutions to help defend against cyber attacks, respond to IT security incidents and implement preventive measures.

CERT-Bund
The CERT-Bund (Computer Emergency Response Team of the federal administration) is located in the BSI and acts as a central contact point for federal authorities for preventive and reactive measures regarding computer system security incidents.

Cloud / Cloud Computing
Cloud computing refers to the dynamic provision, use and billing of IT services via a network according to demand. These services are offered and used exclusively through defined technical interfaces and protocols. The services offered within the framework of cloud computing cover the complete spectrum of information technology and include, among other things, infrastructure (computing power, storage space), platforms and software.

Command-and-Control-Server (C&C-Server)
Server infrastructure that attackers use to control infected computer systems (bots) integrated into a botnet. Bots (infected systems) usually report to the attacker's C&C server after infection to accept its commands.

Coordinated Vulnerability Disclosure (CVD)
The principle of Coordinated Vulnerability Disclosure involves the coordinated publication of information regarding a vulnerability and the provision of patches or mitigation measures for affected software products in a transparent, systematic time sequence.

CVSS-Score
An industry standard used to assess the criticality of vulnerabilities in an internationally comparable way.

Cybercrime-as-a-Service (CCaaS)
Cybercrime-as-a-Service (CCaaS) describes a phenomenon in cybercrime where crimes are committed by cybercriminals on demand or services are provided. For example, in the case of Malware-as-a-Service (MaaS), which is a subset of CCaaS, a cybercriminal is provided with the malware for the commission of a crime by an outsider or a specialised attacker group for a fee, and may also be provided with updates and other similar services, much like the legal software industry. One type of MaaS is Ransomware-as-a-Service (RaaS), which often involves providing the malware to encrypt an infected system, updates to that malware, handling ransomware negotiations and payments, and other extortion methods for a fee. The fragmentation of a cyber attack into individual services inherent in CCaaS enables even less IT-savvy attackers to carry out technically sophisticated cyber attacks.

Deepfake
The term "deepfake" is a colloquial term for methods that can be used to specifically manipulate identities in media content using methods from the field of artificial intelligence. An example of this are methods that swap the face of a person in a video with the face of another person, but keep the facial movements unchanged.

DoS / DDoS Attacks
Denial-of-Service (DoS) attacks are directed against the availability of services, websites, individual systems or entire networks. If such an attack is carried out by means of several systems in parallel, it is called a distributed DoS or DDoS (Distributed Denial of Service) attack. DDoS attacks are often carried out by a very large number of computers or servers.

Double Extortion
Attackers not only try to extort ransoms in exchange for encrypted data, but also hush money for exfiltrated data.

Drive-by Download / Drive-by Exploits
Drive-by exploits refer to the automated exploitation of security vulnerabilities on a PC. When viewing a website, vulnerabilities in the web browser, in additional programs of the browser (plug-ins) or in the operating system are exploited without further user interaction in order to install malware on the PC unnoticed.

Exploit
An exploit is a method or programme 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, exploits can be used, for example, to crash a programme, extend user rights or execute arbitrary programme code.

Exploit-Kit
Exploit kits or exploit packs are tools for cyber attacks and are placed on legitimate websites. Using various exploits, automated attempts can be made to find a vulnerability in the web browser or its plug-ins and use it to install malware.

Firmware
Firmware is software that is embedded in electronic devices. Depending on the device, firmware can contain

the functional scope of the operating system or application software, for example. Firmware is designed specifically for the hardware in question and cannot be replaced at will.

Hash Value
A hash value is a string of numbers and letters resulting from the application of a specific hash function. The hash value has a defined length and therefore enables large amounts of data (e.g. malware) to be mapped exactly in comparatively few characters. Hash functions are mathematical functions for the conversion of data. Recalculating the hash value back to the original data is practically impossible, or only possible with extremely high computational effort.

Hybrid Threats
Unlawful influence of foreign states through measures in various spaces. Physical attacks can be accompanied by cyber attacks or disinformation campaigns, for example.

Internet of Things / IoT
The Internet of Things (IoT) refers to objects equipped with information and sensor technology that collect, process and store data from the physical and virtual world and are networked with each other.

IT Security Act 2.0
The "Second Act to Increase the Security of Information Technology Systems" (IT-Sicherheitsgesetz 2.0, IT-SiG 2.0) came into force on 28 May 2021. IT-SiG 2.0 represents the further development of the first IT Security Act from 2015.

Lateral Movement
Lateral Movement refers to the gradual movement of an attacker through an infiltrated network. Attackers usually use this to find data for encryption or destruction.

Legitimate Programmes
Programmes that perform harmless, desired operations.

MaaS
Malware-as-a-Service (see also CCaaS).

Malicious
Bad, harmful. In IT security, programmes or websites that can perform harmful operations on a computer system are called malicious. The term for malicious software, malware, is a portmanteau of mal(icious) and (soft)ware.

Malware
The terms malicious function, malicious programme, malicious software and malware are often used synonymously. Malware is a portmanteau of malicious software and refers to software that has been developed with the aim of executing undesirable and usually harmful functions. Computer viruses, worms and Trojan horses are all examples of it. Malware is usually designed for a specific operating system version and is therefore mostly written for common systems and applications.

NCCA
The BSI is the National Cybersecurity Certification Authority (NCCA) within the meaning of Article 58 para. 1 of (EU) Regulation 2019/881 (Cybersecurity Act, CSA) in conjunction with § 9a BSIG. In accordance with Article 58 para. 4 CSA, the BSI as NCCA performs its supervisory management functions and certification strictly separately and independently of each other.

NESAS
Network Equipment Security Assurance Scheme.

NESAS CCS-GI
NESAS Cybersecurity Certification Scheme – German Implementation.

Password Spraying
Attack method in which the attacker uses popular or typical passwords (e.g. Test1234) to gain access to numerous accounts simultaneously.

Patch / Patch Management
Patches are software packages with which software manufacturers close security gaps in their programmes or integrate other improvements. Many programmes facilitate the installation of these updates through automatic updates. Patch management refers to processes and procedures that help to obtain, manage and apply available patches for the IT environment as quickly as possible.

Payload
In general, the term refers to the payload or the payload data in a data transmission. Within the context of information security, a distinction is made between malicious code that opens a system to further attacks, malicious code that serves as a temporary vehicle, and

malicious code that is ultimately intended to remain on the system. The latter malicious code is called a payload.

Perimeter Systems
Servers, firewalls, VPN gateways and routers that are directly accessible from the Internet.

Phishing
The word is a combination of password and fishing. The attacker tries to obtain the personal data of an Internet user via fake websites, emails or short messages and to misuse them for their own purposes, usually at the expense of the victim.

Phishing Radar of the NRW Consumer Advice Centre
SSince 2010, the NRW consumer advice centre has been evaluating fraudulent emails that consumers forward to the phishing radar (phishing@verbraucherzentrale.nrw). They issue warnings on their homepage, on Twitter and Facebook about current scams based on the 200-300 emails they receive daily - involving phishing, other cybercrime and advertising. Since autumn 2017, they have been cooperating with the BSI to provide, among other things, a more extensive statistical (anonymised) evaluation.

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

Potentially Unwanted Application (PUA)
Application software (often distributed as bundled software) that cannot be clearly classified as malware. A PUA is characterised in particular by the fact that it has usually been installed by users, but may not show the expected behaviour or may covertly perform functions that are considered undesirable, e.g. information collection and possible forwarding of user behaviour, advertising or similar

Proliferation
The term originally comes from the field of military defence and refers to the transfer of weapons of mass destruction, including their technical know-how as well as the material needed to produce them. In the field of IT security, the term is used similarly for the transfer of cyber weapons (software and methods) among attackers. Through proliferation, attack tools and routes can spread very quickly among different attacker groups without each having to build up specific technical competencies.

Provider
A service provider with different focuses, e.g. network provider that provides the infrastructures for data and the transport of voice communications as a mobile network provider, internet service provider or carrier, or service provider that provides services beyond network provision, for example the operation of an organisation's network or the provision of social media.

Public-Key Cryptography
In public-key cryptography, also known as asymmetric encryption, there are always two complementary keys. One of the keys, the public key, is used to encrypt a message, while another – the private key – is used to decrypt it. Both keys together form a key pair.

Source Code
The source code of a computer programme is the human-readable description of the programme's process written in a programming language. The source code is translated by a programme into a sequence of instructions that the computer can execute.

Ransomware
Ransomware refers to malware that restricts or prevents access to data and systems and only unlocks these resources upon payment of a ransom. This constitutes an attack on the security objective of availability and a form of digital extortion.

RaaS
Ransomware-as-a-Service (see also CCaaS).

Resilience
In this context, the term refers to the resilience of IT systems to security incidents or attacks. The resilience of systems results from a complex interplay between organisational and technical preventive measures, such as specialist staff, IT security budget, available technical infrastructures and so on.

Responsible Disclosure
Responsible disclosure is a process in which the manufacturer of the affected product is first informed in detail after a security vulnerability is discovered. This gives the manufacturer the opportunity to develop countermeasures, e.g. in the form of product updates, before the information needed to exploit the vulnerability is made available to the general public. The manufacturer is usually given a fixed time frame for this, usually a few months at the latest, after which it will be published.

RSA
This term refers to a public-key cryptography method that is used for signatures and encryption and is named after the developers Rivest, Shamir and Adleman. Part of the RSA public key consists of the RSA module n, a natural number that is the product of two secret prime numbers p and q. The security of RSA is based in particular on the difficulty of factorising the RSA module n, i.e. calculating the two prime factors p and q from knowledge of n only.

RNG
This is an abbreviation for Random Number Generator.

Security Advisory
Recommendations to IT security managers on how to deal with vulnerabilities that have been found.

SCAS
Security Assurance Specification

Scam Email
Fraud email. A category of spam emails with which attackers pretend to collect donations, for example.

Security by Default
A product that is delivered with Security by Default is already in a securely pre-configured delivery state without any additional measures being necessary.

Security by Design
With Security by Design, information security requirements are taken into account during the development of a product.

Side-Channel Attack
Attack on a cryptographic system that exploits the results of physical measurements on the system (for example, energy consumption, electromagnetic radiation, time consumption of an operation) to gain insight into sensitive data. Side-channel attacks are highly relevant for the practical security of information processing systems.

SIM-Swapping
Ordering another SIM card for a mobile phone number in the name of the user so that mTANs are sent to several devices.

Sinkhole
AA sinkhole is a computer system to which requests from botnet-infected systems are redirected. Sinkhole systems are typically operated by security researchers to detect botnet infections and inform affected users.

Smart Grid
A smart grid is a grid in which the actions of generators, consumers and storage units are intelligently integrated. The aim is to ensure an efficient, sustainable, economical and safe supply of electrical energy.

Social Engineering
BIn cyber attacks involving social engineering, criminals try to entice their victims to disclose their data, bypass protective measures or install malware on their systems on their own. In both cybercrime and espionage, attackers are clever in their approach to exploit perceived human weaknesses such as curiosity or fear to gain access to sensitive data and information.

Spam
Spam refers to unsolicited messages sent en masse and in an untargeted manner by email or via other communication services. The harmless version of spam messages usually contains unsolicited advertising. However, spam messages often also contain malware in the attachment, links to contaminated websites or they are used for phishing attacks.

Scraping
Extraction of content from web pages.

SIM Swapping
With SIM swapping, attackers order another SIM card for the mobile number on behalf of the user, so that mTANs are sent to several devices

Trusted Execution Environment (TEE)
A Trusted Execution Environment (TEE) is an isolated part of a system that provides a specially protected runtime environment. A TEE can, for example, be part of a main processor (CPU) or part of a smartphone's System-on-Chip (SoC). TEEs protect the integrity and confidentiality of the stored data and key material from unauthorised third parties, e.g. also the user of a device. Only authorised bodies are allowed to introduce or modify applications in the TEE.

UP KRITIS
UP KRITIS (www.upkritis.de external link) is a public-private cooperation between operators of critical infrastructure (CI), their associations and government agencies such as the BSI.

VPN
A Virtual Private Network (VPN) is a network that is physically operated within another network (often the internet), but logically separated from that network. In VPNs, the integrity and confidentiality of data can be protected with the help of cryptographic procedures and communication partners can be securely authenticated, even if several networks or computers are connected to each other via leased lines or public networks. The term VPN is often used to describe encrypted connections, but other methods can also be used to secure the transport channel, for example special functions of the transport protocol used.

Webshell
Malicious code that attackers install on a web server after breaking in. Webshells allow attackers to remotely access servers and can be used to execute malicious code.

Wiper
Malware that destroys data. Unlike ransomware, wipers are not aimed at encryption and extortion, but at sabotage through the final destruction of data.

Witnessing
A witness assessment of a technical service refers to the monitoring of an audit carried out by the technical service by KBA staff in order to evaluate the auditing, the associated internal procedures and the competence of the auditors, among other things.

Two- and Multi-Factor Authentication
In two- or multi-factor authentication, the authentication of an identity is done using different authentication factors from separate categories (knowledge, possession or biometric characteristics.

Bibliography

1) https://therecord.media/ransomware-tracker-the-latest-figures/
2) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2021.pdf
3) https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/Fragen-und-Antworten/fragen-und-antworten_node.html
4) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2021.pdf
5) https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-269486-1032.pdf
6) https://www.bsi.bund.de/Schwachstellenmeldung
7) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf
8) Bundesamt für Verfassungsschutz, "Sicherheitshinweis für die Wirtschaft | 01/2022 | 04.03.2022": https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/wirtschafts-wissenschaftsschutz/2022-03-04-Sicherheitshinweis.pdf
9) https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr
10) https://de.radware.com/2021q3-ddos-report/
11) https://www.link11.com/de/bedrohungslage
12) https://azure.microsoft.com/en-us/blog/business-as-usual-for-azure-customers-despite-24-tbps-ddos-attack/
13) https://blog.cloudflare.com/cloudflare-thwarts-17-2m-rps-ddos-attack-the-largest-ever-reported/
14) https://www.inforisktoday.com/meris-how-to-stop-most-powerful-botnet-on-record-a-17574; https://www.cysecurity.news/2022/01/russia-recorded-largest-botnet-attack.html
15) https://www.documentcloud.org/documents/7070798-FLASH-MU-000132-DD.html
16) https://www.zdnet.de/88395308/erneute-welle-von-ddos-erpressungen-durch-fancy-lazarus/
17) hhttps://www.link11.com/de/blog/bedrohungslage/cyber-angriffe-am-black-friday-wochenende-brechen-rekorde/
18) https://fermatattack.secvuln.info
19) https://securitylab.github.com/advisories/GHSL-2021-1012-keypair/
20) https://www.spiegel.de/wissenschaft/technik/russland-ukraine-was-der-ausfalleines-satellitennetzwerks-mit-deutschen-windkraftanlagen-zu-tun-hat-a-22850ad5-dee2-42c4-8c5a-c2b39ac42da4 (Stand: 20.04.2022)
21) https://www.viasat.com/about/newsroom/blog/ka-sat-network-cyber-attack-overview/ (Stand: 29.04.2022)
22) https://www.lefigaro.fr/secteur/high-tech/les-telecoms-victimes-de-cyberattaques-russes-20220228 (Stand: 20.04.2022)
23) https://www.viasat.com/about/newsroom/blog/ka-sat-network-cyber-attack-overview/ (Stand: 29.04.2022)
24) https://cert.gov.ua/article/39518 (Stand: 13.05.2022); https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf (Stand: 13.05.2022); https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ (Stand: 13.05.2022)
25) https://www.vzbv.de/pressemitteilungen/anbieter-und-hersteller-zu-it-sicherheit-verpflichten
26) https://cdr-initiative.de/uploads/files/210503_Umfrage_FInal_Faktenblatt_CDR.pdf
27) https://www.bmj.de/DE/Themen/FokusThemen/CDR_Initiative/_downloads/cdr_plattform.pdf
28) https://cdr-initiative.de/kodex
29) https://www.bundesnetzagentur.de/DE/Fachthemen/Digitalisierung/start.html
30) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/messenger.html
31) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Magazin/BSI-Magazin_2022_01.html
32) https://www.bsi.bund.de/SharedDocs/Videos/DE/BSI/VerbraucherInnen/statementvideo-messenger-verschluesselung.html
33) https://datatracker.ietf.org/wg/mls/about/
34) https://www.europarl.europa.eu/factsheets/de/sheet/45/energiebinnenmarkt
35) https://www.bmwk.de/Redaktion/DE/Publikationen/Studien/it-dienstleister-als-akteure-zur-staerkung-der-it-sicherheit-bei-kmu-in-deutschland.html
36) https://www.bmwk.de/Redaktion/DE/Publikationen/Studien/it-dienstleister-als-akteure-zur-staerkung-der-it-sicherheit-bei-kmu-in-deutschland.html
37) auch BKA-Veröffentlichung: https://www.bka.de/SharedDocs/Downloads/DE/UnsereAufgaben/Deliktsbereiche/InternetKriminalitaet/CyberattackenUnternehmen.pdfl
38) https://ntia.gov/SBOM
39) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html
40) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Sichere_Nutzung_Cloud_Dienste.pdf
41) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5_node.html
42) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03160/tr03160_node.html
43) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03107/TR-03107_node.html
44) https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Elektronische-Identitaeten/Identitaetspruefung/identitaetspruefung_node.html
45) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03116/TR-03116_node.html

Register of QR codes included in the report

a) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.html
b) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Technische-Sicherheitshinweise-und-Warnungen/technische-sicherheitshinweise-und-warnungen_node.html
c) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-CC/itsicherheitszert.html
d) https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/Bewertung-2FA-Verfahren/bewertung-2fa-verfahren_node.html
e) https://www.bsi.bund.de/DE/Service-Navi/FAQ/IT-SicherheitskennzeichenVerbraucher/faq_it-sik-verbraucher_node.html
f) https://www.bsi.bund.de/DE/Themen/Kampagne-einfach-absichern/kampagne_node.html
g) https://www.dialog-cybersicherheit.de/
h) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SmartCity/Handlungsempfehlungen_Smart_City.pdf?__blob=publicationFile&v=3
i) https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Moderner-Staat/Online-Wahlen/online-wahlen_node.html
j) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Sicher_zahlen_im_E_Commerce.pdf
k) https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/zwei-faktor-authentisierung_node.html
l) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html
m) https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/Stand-der-Technik-umsetzen/Uebersicht-der-B3S/uebersicht-der-b3s_node.html
n) https://www.bsi.bund.de/DE/Home/home_node.html
o) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/ohsza.html
p) https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/UP-KRITIS/up-kritis_node.html
q) https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Weitere_regulierte_Unternehmen/UBI/ubi_node.html
r) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/KMU/KMU_node.html
s) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03163/tr-03163.html
t) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-NESAS/NESAS-CCS-GI_node.html
u) https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_node.html
v) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/5-G/KoPa45/Cyber-Sicherheit-digitale-Souveraenitaet-5G-6G_node.html
w) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/Onlinekurs/Onlinekurs_node.html
x) https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Moderner-Staat/Online-Zugangsgesetz/IT-Sicherheitsverordnung_PVV/IT-Sicherheitsverordnung_PVV_node.html
y) https://www.bsi.bund.de/DE/Service-Navi/Publikationen/BSI-Magazine/bsi-magazine_node.html
z) https://cybersecurity-centre.europa.eu/index_de
aa) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Profil_Weltrauminfrastrukturen.html
bb) https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/KI/Towards_Auditable_AI_Systems_2022.pdf
cc) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Kryptografie-quantensicher-gestalten.html
dd) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Eckpunkte_SSI_DLT.pdf
ee) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Kryptografie-quantensicher-gestalten.pdf?__blob=publicationFile&v=5

Legal Notice

Published by
Federal Office for Information Security (BSI)

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

E-Mail
bsi@bsi.bund.de

Telephone
+49 (0) 22899 9582-0

Fax
+49 (0) 22899 9582-5400

Last updated
October 2022

Printed by
Appel & Klinger Druck und Medien GmbH, Schneckenlohe

Concept, editing and design
Faktor 3 AG

Texts and editing
Federal Office for Information Security (BSI)

Illustrations
Koivo c/o kombinatrotweiss.de
Instagram: koivo | kombinatrotweiss_illustration

Graphics
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Article number
BSI-LB22/511e

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