



Federal Office
for Information Security



The State of IT Security in Germany in 2021

Foreword

Rapid progress in the field of information technology has brought change – often far-reaching, sometimes radical – to our daily experiences at home and in the workplace. Meetings are now increasingly digital, household appliances are becoming part of the internet and, when planning a trip we are more likely to run a web search than pull out a map. While this makes daily life much easier, there is also a downside to the benefits. This can be seen in the rising number of cyber attacks.

Hacks targeting Microsoft Exchange servers and Solar-Winds have offered a striking demonstration of how much havoc such attacks can wreak in a globally connected world. While Germany was not affected by these incursions to the same extent as some other countries, they have clearly shown that our country's systems are also vulnerable.

Furthermore, cyber attacks are becoming more sophisticated. Both cybercriminals and those active in the fields of cyber espionage and cyber sabotage are constantly developing new techniques while also exploiting recent events and crises (such as the COVID-19 pandemic).

For the Federal Government to fulfil its responsibility to ensure our national security in cyberspace as well, we must adjust continuously to this dynamic threat landscape.

During the current legislative session, we adopted the IT Security Act 2.0 in order to update and modernise the legal framework governing cyber security and information security in Germany. First of all, the Act strengthens the role of the Federal Office for Information Security (BSI) as Germany's central cyber security authority while also widening its remit in relation to the detection of vulnerabilities and defensive measures for cyber attacks. Second, the Act also expands digital consumer protection and provides greater security for businesses. This significantly improves our overall cyber security as a nation.

For our 2021 Cyber Security Strategy, we consulted with entities from the realms of business and society to update our strategy from 2016, which will help ensure we are properly prepared to meet the cyberspace challenges of the future.

In our modern, globally networked world, cyber security requires a mindset that transcends national borders. This is why we work closely with our partners here in the EU and around the world.

As the 2021 Report on the State of IT Security in Germany shows, risks continue to multiply in cyberspace and

now even threaten areas of existential importance for our society – such as the provision of electricity or medical care. Our federal agencies are facing these challenges head on and making every effort to ensure that our citizens, businesses and public authorities have the best protection possible. I believe that the elementary role now played by the BSI as the central authority for information security in Germany deserves special recognition in this regard.



A handwritten signature in black ink, which appears to read 'H. Seehofer'.

Horst Seehofer

Federal Minister of the Interior, Building and Community

Foreword

Germany · Digital · Secure · BSI

The IT Security Act 2.0 was adopted by the German Bundestag in April 2021. This was an important milestone – and not only for the BSI. The Act has provided a clear-cut and urgently needed upgrade to cyber security and information security in Germany, and thereby ensures that the preconditions of secure digitalisation are met. However, these efforts can and will succeed only if cyber security and information security are factored in right from the start. Information security must no longer be misconstrued as an encumbrance. The opposite is true: it is an investment in the future that is also fundamental to a successful digital transition.

While this should be self-evident, the underlying concepts are harder to grasp, not least because successful cyber security is imperceptible. It is an inherent part of systems, processes and products that one only notices when it fails, which can allow a global security incident, a large-scale blackmail attempt or system lock-outs and crashes to occur. This generates the attention and headlines hardly seen when cyber security systems work as they should.

Emotet: The king is dead. Long live the king!

While the number of security incidents is in itself a cause for concern, equally alarming is the rapid development of new and modified types of methods, the mass exploitation of severe software vulnerabilities and the grave consequences that may result from a successful cyber attack. While the take-down of the Emotet network means that the ‘King of Malware’ has vanished from the scene for the time being, there are plenty of other, new attack tools and methods – even some that no longer require interaction.

These new attack vectors would not be possible without vulnerabilities in software and hardware products. This is a particularly serious problem when widely used products with a large market share happen to be affected. Vulnerabilities point to failures in product quality control. Manufacturers should therefore be proactive and work (including in collaboration with others) to protect their own interests by resolving these defects as quickly and efficiently as possible. Users should also be conscious of the need to play an active part in protecting their networks and systems from such vulnerabilities on a daily basis. Anyone who fails to do so is taking a huge risk.

Production downtime can pose an existential threat to businesses. A lack of access to digital citizen services causes headaches for town and district councils. Citizens cannot depend on public services being available with the usual speed and ef-

iciency. Hospitals have to be taken off emergency care rosters and are forced to cancel weeks of operations. This not only puts the lives of individual patients at risk, but also damages the high quality of healthcare provision all across Germany. None of these are fictitious scenarios; they are all real-world consequences of IT security incidents that occurred during the reporting period. As is made very clear by these examples, we are already highly dependent on digital processes as a society, and their failure leaves us highly exposed.

Over the last 18 months, the coronavirus pandemic has brought significant change to our day-to-day lives. COVID-19 has also thrown Germany’s digitalisation deficits into the spotlight. As a society, we have reprioritised key areas of our lives and adapted many of our social customs: we have followed distancing and masking rules, worked and studied at home, and got used to online conferences and virtual family get-togethers. Many of these innovations are likely to become routine even after the pandemic has subsided. This is why it is also appropriate that we properly address the corresponding challenges, especially in relation to cyber security and information security. The Report on the State of IT Security in Germany in 2021 shows where these challenges lie.

The digital transition will proceed apace, with all of the benefits that it brings, and this is a welcome development. However, its potential can and will never be fully realised if we continue to neglect information security. In the worst case, many digitalisation projects may founder entirely.

Germany must thus be resolute in its efforts to stay the course



that it has charted by adopting the IT Security Act 2.0. This legislation has put our country on track for secure digitalisation in public administration, digital innovation in a flourishing economy and reliable computerised apps that benefit all our citizens. As Germany’s federal cyber security authority, we are ready to take the next steps.

A handwritten signature in black ink, reading 'Arne Schönbohm'. The signature is fluid and cursive, with a large, stylized 'A' and 'S'.

Arne Schönbohm

President of the Federal Office
for Information Security

Contents

Forewords

Foreword Horst Seehofer, Federal Minister of the Interior, Building and Community	3
Foreword Arne Schönbohm, President of the Federal Office for Information Security	4

1 Threats to Cyber Security in Germany 8

1.1 Summary and Assessment	9
----------------------------	---

1.2 Malware	10
-------------	----

1.2.1 New Malware Variants	11
1.2.2 Big Game Hunting with Ransomware	12
1.2.3 Spam and Malware Spam	19
1.2.4 Botnets	19

1.3 Theft and Abuse of Identity Data	24
--------------------------------------	----

1.3.1 Phishing and Other Types of Fraud	24
1.3.2 Malware and Data Leaks	25
1.3.3 Cyber Attacks on Videoconferences	25

1.4 Vulnerabilities	26
---------------------	----

1.5 Advanced Persistent Threats	28
---------------------------------	----

1.6 Distributed Denial of Service (DDoS)	31
--	----

1.7 Attacks in the Context of Cryptography	36
--	----

1.8 Hybrid Threats	36
--------------------	----

1.9 Threats to Cyber Security due to the COVID-19 Pandemic	38
--	----

2 Insights and Services for Specific Client Groups 46

2.1 Civil Society	47
-------------------	----

2.1.1 Insights from the Threat Landscape in Civil Society	47
2.1.2 Digital Consumer Protection	48
2.1.3 IT Security Label	48
2.1.4 Educating and Raising Awareness Among Consumers	49
2.1.5 Security in the Internet of Things, Smart Homes and Smart Cities	50
2.1.6 Security of Medical Devices	51
2.1.7 Corona Warn App	51
2.1.8 eHealth and Telematics Infrastructure	52
2.1.9 Security Models for Virtual Meetings and Voting Systems	53
2.1.10 Security of Payment Methods	53
2.1.11 Two-Factor Authentication	54
2.1.12 Assessment of Electronic Identification Procedures	54
2.1.13 Secure, Smartphone-Based Electronic Identities	55
2.1.14 Biometrics in the Age of Artificial Intelligence	56

2.2	Industry	56
2.2.1	Threat Landscape for Critical Infrastructure	57
2.2.2	UP KRITIS	59
2.2.3	Digitalisation in the Energy Sector: Smart Metering System Rollout	59
2.2.4	Modern Telecommunications Infrastructure (5G)	60
2.2.5	Cyber Security in the Automotive Sector	61
2.2.6	Cyber Security in Aviation	62
2.2.7	Cyber Security in the Manufacturing Supply Chain	62
2.2.8	The Unique Role of SMEs in Germany	63
2.2.9	Technical Security Device for Electronic Recording Systems	63
2.2.10	IT Security Certification as an Instrument for Verifiably Secure Digitalisation	64
2.2.11	IT-Grundschutz: Solutions for Information Security	65
2.2.12	IT Security when Working from Home	65
2.2.13	Alliance for Cyber Security	66
2.2.14	Other Solutions/Services for Business	66
2.3	Federal Government / Administration	68
2.3.1	Threat Landscape in the Federal Administration	68
2.3.2	National Cyber Response Centre	70
2.3.3	Computer Emergency Response Team	71
2.3.4	Federal IT Consolidation Project: New Information Security Officer	73
2.3.5	National Liaison System	73
2.3.6	Realisation of the Federal Implementation Plan (UP Bund)	73
2.3.7	Cyber Security for Bundestag and State Parliament Elections	74
2.3.8	Information Security Consulting	75
2.3.9	Smart Borders and Management of Official ID Documents	75
2.3.10	Technology Verification Programme	75
2.3.11	App Testing for Mobile Solutions	76
2.3.12	Countersurveillance	76
2.3.13	Classified Information Product Approval and Manufacturer Qualification	76
2.3.14	Messenger Services for the Secure Communication of Classified Information	77
2.3.15	Implementation of the Online Access Act	78
2.4	International and European Collaboration	78
2.4.1	BSI Engagement in the EU	79
2.4.2	Multilateral and Bilateral Engagement of the BSI	79
2.4.3	National Coordination Centre for European Research Projects	79
2.4.4	eID: EU-wide Recognition of Germany's Online ID Card	80
2.4.5	Crypto-Modernisation for Satellite Systems	81
2.5	Current Trends and Developments in IT Security	81
2.5.1	Artificial Intelligence	81
2.5.3	Quantum Key Distribution	83
2.5.4	Blockchain	84
3	Conclusions	86
4	Glossary	90
5	Bibliography	94

Register of Selected Incidents in the Reporting Period:

<i>Ransomware Attack on a University Medical Centre in North Rhine-Westphalia</i>	15
Theft of Passport Data	16
Darkside	17
<i>Ransomware Attack on a Major German Media Group</i>	18
Emotet Takedown	21
<i>SMS-Phishing</i> ('smishing')	22
Critical Vulnerabilities in MS Exchange	27
SolarWinds	30
<i>DDoS-Extortion Attacks</i>	34
<i>DDoS-Attack on a Belgian Internet Service Provider</i>	35
Cyber Attack on the European Medicines Agency (EMA)	41

1 Threats to Cyber Security in Germany



1 Threats to Cyber Security in Germany

In its role as Germany's Federal Cyber Security Authority, the BSI monitors the IT security threat landscape in the country on a continuous basis. It focuses on attacks targeting companies, state or public institutions and private citizens, as well as ways to prevent and thwart such incursions. This report summarises events and activities that occurred between 1 June 2020 and 31 May 2021 (referred to hereafter as the 'reporting period'). As such, the report addresses recent and potentially still-ongoing security situations and cyber threats. This includes an appraisal of the IT security situation resulting from the impact of the COVID-19 pandemic.

Drawing on a wide variety of real-world examples from many different areas, we trace out the path and typical methods used by attackers as a means of highlighting the ways in which people and organisations can protect themselves. Our review begins with a summary of the general threat landscape and current cyber threats. Attacks not only have an immediate impact on the individuals and organisations affected; they also exert an adverse influence on the lives of all the members of our digital society. Accordingly, it is important to investigate each individual area together with its specific threats and countermeasures. Without wanting to pre-empt our final conclusions, the cyberspace threat landscape remains serious in this reporting period. Cybercriminals use recent methods and technologies to the full when launching attacks on private citizens, companies and institutions. If we wish to enjoy the benefits of a digital society, we must therefore stay alert and ensure our defences are well organised. If not, we will jeopardise the success of Germany's digital transition.

1.1 Summary and Assessment

The overall IT security situation in Germany can be described as serious to critical in the current reporting period. On the one hand, this is the result of an expansion of familiar cybercriminal extortion attacks from simple ransom payments to double extortion (a kind of 'hush money' extortion) and *DDoS* extortion attacks. In addition, the reporting period also provided examples of cases where the impact of an incident extended beyond the victim in question.

Compared to the previous reporting period, attackers have also significantly accelerated their production of new *malware* variants. While an average of 322,000 new variants a day were identified in the previous reporting period, this daily indicator reached an average of 394,000 variants in

the current period – an increase of over 22 percent. Attackers therefore produced around 144 million new *malware* variants in total during the current reporting period (see chapter *New Malware Variants*, page 11).

Ransom fees, hush money and protection rackets: an inventive time for cyber blackmailers

The current reporting period saw a significant expansion in the blackmailing methods utilised by cybercriminals.

DDoS extortion attacks: As early as autumn 2020, a global campaign was underway in which cyber blackmailers threatened wealthy victims with distributed denial of service (*DDoS*) attacks if they failed to pay a specified sum of 'protection money' (see incident *DDoS Extortion Attacks*, page 34).

Ransomware: Autumn and winter also saw additional waves of attacks based on use of the *Emotet malware*. In the case of certain targets, *ransomware* was downloaded after an *Emotet* infection with the aim of extorting ransom fees from wealthy victims on a large scale; this continued until the takedown of the *botnet* in January 2021 (see incident *Emotet Takedown*, page 21).

Exfiltration and hush money: In addition, some individual attacker collectives expanded their strategy by taking steps to ensure data was unlawfully exfiltrated for off-site storage before it was encrypted. In this case, victims who had an effective *backup* strategy (and could therefore ignore attempts to secure ransom payments) were nonetheless threatened with the disclosure of stolen data and told to pay hush money (see Chapter *Big Game Hunting with Ransomware*, page 12). This essentially means that any data involved in a successful ransomware attack must now also be considered permanently compromised – even in cases where a *ransom* fee or hush money has indeed been paid (see chapter *Malware and Data Leaks*, page 25).

During the reporting period, *spam* campaigns also continued to occur that exhibited aspects of hush money extortion efforts, although these targeted end users directly and did not involve the actual exfiltration of data. Instead, attackers simply claimed to possess data belonging to victims and threatened them with its publication (see chapter *Spam and Malware Spam*, page 19).

Critical vulnerabilities in Microsoft Exchange

After a vulnerability in Exchange Server made headlines in early March 2021, Microsoft issued a *patch* that closed no fewer than four critical security holes, combinations of which had already been exploited in targeted attacks. Directly following the publication of these vulnerabilities, extensive scanning activities were observed online as attackers tried to locate and target unpatched Exchange servers. The BSI raised the threat level to ‘Extremely Critical’ – the second-highest level – to reflect both the sheer number of servers open to attack and the easy availability of *exploit kits*. An initial analysis revealed that 98 percent of the systems audited were vulnerable. A high-profile warning campaign by the BSI and Microsoft, combined with a rapid response from system operators, reduced that number by half within a week and below 10 percent only a fortnight later (see incident *Critical Vulnerabilities in MS Exchange*, page 27).

Spectacular supply chain attack

During the reporting period, compromised software supply chains once again proved problematic as an *attack vector* that is particularly difficult to monitor. Here, attackers start by targeting software manufacturers and inserting *malware* into legitimate software products. One especially sophisticated attack campaign targeted the Orion platform from SolarWinds (see incident *SolarWinds*, page 30).

Cyber security under pandemic conditions

As in the previous reporting period, extensive *phishing* campaigns based on references to any number of fake facts and news content involving the COVID-19 pandemic were once again observed (see chapter *Phishing and other Types of Fraud*, page 24).

The outsourcing of business processes to the digital space also continued apace (see chapter *Threats to Cyber Security due to the COVID-19 Pandemic*, page 38). Meanwhile, the potential scope of cyber attacks expanded as a result of the increased use of remote access, VPNs, and videoconferencing systems, as well as trends such as, bring your own device’ (BYOD) or ‘shadow IT’ (i.e. the use of IT equipment procured without the oversight or vetting of IT departmental security teams). These trends have always involved *attack vectors* that are difficult to monitor, but the use of such equipment has likely expanded significantly during the pandemic.

Videoconferences in particular were popular targets during the reporting period (see chapter *Cyber Attacks on Videoconferences*, page 25). One of the variants observed involved eavesdropping attacks in which attackers used

previously obtained access credentials to join videoconferences and thereby obtain company-internal information.

Attacks targeting healthcare organisations

In a much-publicised attack on the European Medicines Agency (EMA), data thieves made off with information concerning the vaccine manufactured by BioNTech and Pfizer. In this carefully planned attack, the criminals utilised a compromised EMA service *provider* account and followed up the attack by publishing parts of the data obtained online. However, the information published had been tampered with in such a way that it can be assumed the disclosure was actually intended to foster doubt about the vaccine’s safety.

1.2 Malware

The term ‘*malware*’ encompasses all computer programs that can execute harmful operations or provide other programs with the means to do so. *Malware* may end up on a computer as a result of email attachments or links in emails. If a PC user clicks a *malicious* attachment or a link leading to a *malicious* website, this results in a *malware* program being installed. Other typical *attack vectors* include downloads that occur unnoticed in the background (known as *drive-by downloads*) and *malicious* extensions for legitimate software programs. *Malware* commonly exploits vulnerabilities to infect IT systems. These vulnerabilities may be found in software or hardware products, or even on network gateways. As in the case of social engineering, the human factor is also becoming increasingly important in cyber attacks.

Individual *malware* programs differ in terms of their functionality, although a single piece of *malware* can boast several different kinds of functions. One common type of *malware* is *ransomware*, which typically uses encryption to restrict access to data or systems so that the attacker can ultimately blackmail the user into paying a ransom fee (see chapter *Big Game Hunting with Ransomware*, page 12). *Malware* that camouflages itself as a harmless software program or conceals itself in legitimate files is known as a ‘trojan’ (for examples, see the incidents *Ransomware attack on a university medical centre in North Rhine-Westphalia*, page 15; and *Emotet Takedown*, page 21), while malware that can be controlled remotely with the aid of command-and-control servers is called a ‘bot’ (see chapter *Botnets*, page 19).

Protection against attacks from these *malware* programs can be achieved with regular security patches and antivirus software, which detects *malware*, prevents its successful execution and can also remove it from systems. However, some kinds of attacks can make far-reaching changes to an

infected system, which then cannot be simply rolled back to a previous state.

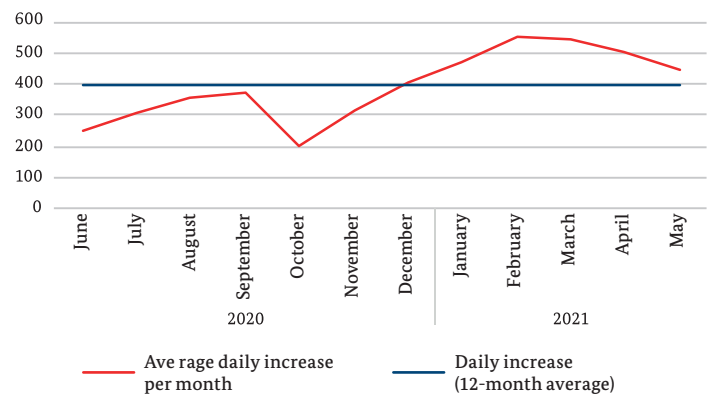
1.2.1 New Malware Variants

Daily increase in new *malware* variants A new variant on a piece of *malware* occurs when changes are made to the

program code. Any variant that has a unique *hash value* is therefore considered new. While detection methods do exist for known *malware* variants, new variants may well be unidentifiable as *malware* immediately after their release – which makes them a particularly dangerous threat.

Average daily increase in new malware variants in thousands

Figure 1: Daily increase in new malware variants
Source: BSI analysis of raw data from the AV-TEST Institute



In the current reporting period, the number of new *malware* variants increased by around 144 million (see Figure 1: Daily increase in new *malware* variants.; source for this and following data: BSI analysis of raw data supplied by the AV-TEST Institute). On average, the number of new *malware* variants increased by slightly more than 394,000 every day. This corresponds to an increase of 22 percent compared to the previous reporting period (see Figure 2). There was considerable variation in this trend, however. In June 2020, only 250,000 new variants emerged per day (i.e. 37 percent fewer than the average value during the reporting period).

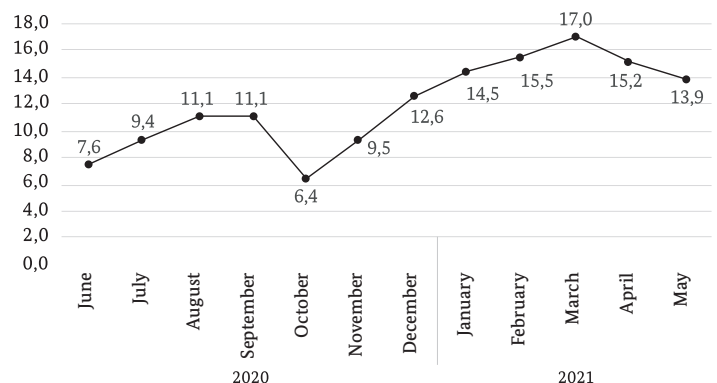
At the turn of the year, attackers then significantly accelerated their production of new *malware* variants: in February 2021, the figure for average new variants per day reached

553,000, which is the highest average daily growth that has ever been recorded (and 40 percent above the average value during the reporting period).

This growth in this daily indicator can be attributed in particular to a considerable increase in attacker productivity within the Windows *malware* category. During the winter months, new peak values were regularly recorded in this category. In September 2020, the appearance of EvilQuest also marked the first time that *malware* targeting Apple's macOS operating system had appeared with any appreciable frequency. Attackers had hidden the new *malware* variants in vast numbers of illegal software copies. As a result, the daily indicator for the macOS *malware* category increased 500-fold in the space of just one month, before then falling

New malware variants from June 2020 to May 2021 in millions

Figure 2: New malware variants
Source: BSI analysis of raw data from the AV-TEST Institute



back to its typical level. Since this *attack vector* was essentially based on product piracy, macOS computers running only legal software were not affected by EvilQuest.

1.2.2 Big Game Hunting with Ransomware

Ransomware refers to malware whose typical mode of operation is to block access to data and systems stored locally or on a network. The commonest approach for attackers is to encrypt user data (such as Office documents or image, audio and video files) or even an entire back-end system, such as a database. The victim is then sent a message explaining that their access will be restored only after they pay a ransom fee. Typically, very short deadlines are set and victims are threatened with the successive deletion of their data. In the current reporting period, attackers also increasingly deployed *ransomware* for new types of cyber extortion (see chapter *Theft and Abuse of Identity Data*, page 24). In such cases, the victim's data was not only encrypted with the aim of demanding a ransom, but also exfiltrated beforehand. This meant that attackers could then threaten the victim with both destruction and disclosure of the data. Ransom payments are usually handled using (virtual) digital currencies such as *Bitcoin* or *Monero* in order to make law enforcement efforts more difficult. Alongside the actual extortion of money, *ransomware* attacks can also be used to conceal or distract from other attacks, or simply deployed as sabotage.

As a rule, cybercriminals use attack strategies that are easy to scale and can be used in large-scale campaigns against a range of victims. As one example, the three-stage attack strategy observed in the previous reporting period from June 2019 to May 2020, which combined features of the former banking trojan Emotet, the TrickBot malware and the Ryuk *ransomware*, was successfully employed by attackers to launch large-scale versions of attack strategies that had previously only been observed as part of strategically targeted APT espionage attacks (see the bibliography¹). In the first stage of these attacks, the Emotet trojan spread itself via Outlook harvesting by analysing the victim's email traffic in order to launch especially authentic-looking social engineering attacks that targeted the victim's contacts. Emotet also had downloader functionality, which allowed the attackers to install the espionage malware TrickBot on infected systems in the attack's second stage. TrickBot gave the attackers the chance to complete extensive espionage on the infected systems. If this data showed that the victim would be worth the extra effort, the Ryuk *ransomware* was then installed and a ransom demanded.

Where possible, cybercriminal attackers are grouped together and differentiated by their preferred malware and attack strategy. As one example, the Ryuk and Clop ran-

software variants tend to be deployed by different types of attacker collectives. In the current reporting period, the BSI observed that numerous attacker groups known to employ a wide variety of *ransomware* variants generally focused on targets from which they would be able to demand the highest-possible ransom. In so doing, the attackers used publicly available information about their targets – such as company size or quarterly financial statements – to set an 'appropriate' amount. This phenomenon is commonly referred to as 'big game hunting' in the security industry. The BSI views big game hunting as a subcategory of cybercriminal attacks. It uses the term to refer to attacks that utilise *ransomware* and associated methods of extortion to target company-wide networks with the aim of blackmailing these companies into paying as high a ransom as possible.

Ransomware is distributed using the usual *attack vectors*, either as an email attachment or a link that takes the user to a malicious website. One *attack vector* that is particularly dangerous for businesses and other institutions with larger-scale IT infrastructure is made possible by vulnerabilities in remote administration/VPN gateways. These vulnerabilities are exploited to launch interactive attacks on systems due for maintenance, for example. During the COVID 19 pandemic, remote working in particular has become a frequently used and necessary approach for many organisations (see *Threats to cyber security from the COVID-19 pandemic*, page 38). By successfully compromising these gateways, an attacker can often obtain an extensive set of rights from the outset. In many instances, *ransomware* is also no longer installed immediately; instead, attackers take the time to investigate the target's network before executing a *ransomware* attack, especially in the case of wealthy organisations.

Additional information on this topic can be found at www.bsi.bund.de/ransomware (see the bibliography^a).



Malware and method proliferation

According to the BSI's research, the *malware* and methods used by cybercriminals are spread within the community by attacker collectives. If the strategies adopted by one collective have proven successful, they are especially likely to be copied soon after by other groups. The BSI refers to this distribution of cybercriminal technologies and expertise as *malware* and method *proliferation*.

In the current reporting period, the BSI observed a further translation of known extortion tactics into cyberspace. Alongside the familiar kinds of blackmail using encryption trojans, attackers also demanded 'hush money' payments to prevent the disclosure of compromising data (also known as 'double extortion'; see chapter *Malware and Data Leaks*, page 25) and payments of 'protection money' to avoid a

subsequent *DDoS* attack (see chapter *Distributed Denial of Service*, page 31). As a rule, attackers would disclose stolen information on leak websites set up specifically for this purpose. This is an example of a successful method that was soon being adopted by other attacker collectives. This *proliferation* is being accelerated by the division of labour and the outsourcing of the various components of cyber attacks to specialised collectives, just as services are outsourced in the private sector. This phenomenon is referred to as *cybercrime-as-a-service (CCaaS)*. The *CCaaS* market was covered in detail by the BKA in its National Situation Reports on Cybercrime 2020 (see the bibliography²).

During the current reporting period, cybercriminals exhibited an alarming degree of resourcefulness, particularly when negotiating hush money payments with their victims. The following section describes some of their various strategies.

1. Drawing public attention from the target's partners, customers or patients. Some attackers actively contact the customers and partners of their victims (as well as media organisations) with the aim of exerting additional pressure. This goes beyond the simple publication of information relating to the victim on a dedicated leak website. Attackers may, for example, contact the target's customers or employees by email and inform these individuals that their personal data has now become public because a specified hush money payment was not made. In the case of one psychological counselling practice, extortion efforts were focused not merely on the practice owner, but also on the individual's patients.

If the target fails to be entirely forthcoming with those potentially affected by a data leak, this can result in a long-term loss of reputation. Proactive and compliant communication helps mitigate this risk.

2. Auctioning or sale of sensitive data. As an alternative to publication, some attackers auction or sell stolen data in cases where the affected party is not prepared to pay any hush money (known as 'double extortion'). Unlike publication on a leak website, this enables attackers to generate additional profit from the harvested data. In addition, the buyers of this stolen data can then use it to extort payment from the target themselves. This is especially the case if the data consists of trade secrets or compromising information relating to specific individuals. In one case affecting a software development company, attackers stole new and unpublished program code and threatened to auction it off to the highest bidder. Typically, it is impossible to track down the final buyer in such black-market data auctions or sales. In addition, once data has been exfiltrated, it must always be considered compromised, even if hush money or a ransom has in fact been paid.

3. Threat of reporting the victim to a data protection or regulatory authority. In the context of a cyber attack, the target may be guilty of a breach of the EU General Data Protection Regulation or other legislation if it has not complied with its reporting duties. Some attackers use these legal obligations and the administrative penalties that may result from non-compliance to exert further pressure on their target by threatening to inform regulators of such infringements.

However, violations of this kind may well become known to the responsible authorities without any direct contact from attackers; they can simply publish the data taken from the target's network and notify relevant members of the press or other media. Proactive and compliant communication helps mitigate this risk.

4. Deployment of *DDoS* attacks in the negotiation phase.

A number of attackers have resorted to additional *DDoS* attacks during ransom negotiations in order to put their victims under further pressure. If a *ransomware* attack were to force an online retailer to move their commercial operations to a web host with less *resilience* against *DDoS* attacks, for example, a subsequent *DDoS* attack would then make managing and countering the *ransomware* attack even more difficult.

This expansion of extortion methods in the reporting period shows that attackers no longer believe encryption alone will put their targets under enough pressure to act. This may be because victims can rely on an effective *backup* strategy or refuse to make ransom payments in accordance with the BSI's recommendations. The BSI expects cybercriminals to continue expanding and developing their attack strategies in the future.

Consequences of a *ransomware* attack

Ransomware attacks are often only detected once data has already been encrypted and computerised processes have come to an abrupt halt. This situation results in various kinds of extensive damage and losses – including those of a financial nature and others that can even affect the health of patients in cases where their treatment options have to be curtailed. Beyond this direct impact, subsequent costs are also incurred in post-attack management and clean-up.

Additional costs also result from data sanitisation work and IT system recovery. To determine the extent of the damage, specialised service providers must often be brought in, since a failure to conduct sanitisation work thoroughly may result in *backdoors* being left in systems. At a later point in time, these backdoors can be used by attackers to once again encrypt data with the aim of

extorting money from the victim. The BSI provides information about how to handle such incidents on its website (see the *bibliography*^{b)}).



Since the exfiltration of data by attackers before encryption takes place has now become a standard procedure in almost all cases, data must always be viewed as permanently compromised in the aftermath of a *ransomware* attack. This increases the risk of further attempts at blackmail, as well as the loss of reputation due to *ransomware*. The potential ramifications are further intensified by the fact that attackers now cast a much wider net in their extortion attempts, which may include the target's partners and the media.

All in all, the damage from a *ransomware* attack may constitute an existential threat to affected organisations.

Recommendations

An effective *backup* strategy is the most important countermeasure against a *ransomware* attack. *Backups* must be checked regularly to confirm that they can be properly restored. It should not be possible to modify or delete *backup* files from the network. In other words, *backups* should always be stored offline.

To counter the increasing risk of data exfiltration and subsequent disclosure or publication (double extortion), a systematic and rules-based approach to data transfer monitoring is required. Such an approach could identify an unusually large outbound flow of data, for example, and terminate it in good time.

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

For companies and other organisations, comprehensive and continuous training that raises the information security awareness of all members of staff should be a matter of course, as should taking steps to restrict the number of individuals with administrative access to systems. Where access permissions are necessary, stringent requirements must be applied in the form of *authentication* and protocol policies.

The consequences resulting from the short-term failure of computerised processes can also be countered by establishing alternative or redundant digital services. For example, content delivery networks (CDNs) can be used to keep a web presence online along with the services it offers. In the event of extended mail server

downtime, a company can compensate by falling back on third-party email services or other alternatives. These and similar measures are intended to ensure that a computerised business-critical process can be restored as quickly as possible in order to minimise the potential damage resulting from a system outage. Here, it is important that such measures account for the fact that a *ransomware* attack may make it impossible to restore a computerised process to its normal state for a long time.

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





Ransomware-Attack on a University Medical Centre in North Rhine-Westphalia

On 10 September 2020, a university medical centre in North Rhine-Westphalia fell victim to a *ransomware* attack with far-reaching consequences. The centre is one of six university hospitals in NRW that together provide a basis for healthcare provision in Germany's most populous state while also contributing to research and teaching work. The centre has more than 1,200 beds across 32 departments and provides treatment to around 50,000 in-patients every year. Since this puts the university medical centre above the healthcare *provider* threshold of 30,000 annual in-patient cases, it is a registered critical infrastructure (CI) operator in accordance with relevant German legislation.

Situation

At around noon on 10 September 2020, the BSI took notice that the university medical centre had become the victim of a *ransomware* attack. The hospitals antivirus server detected several abnormalities in the IT operations on the evening of 9 September 2020. However, these were initially classified as simple operational discrepancies until the first sets of encrypted files were discovered on some servers the following morning. As an initial containment action, the centre went offline and shut down most of its Windows servers to prevent access to the internal network and to stop the encryption of any other files.

The attackers used a *backdoor*, which they installed on the Citrix NetScaler gateway before the security *patch* was applied to attack the hospital with the *ransomwares* DoppelPaymer and Dridex. Citrix NetScaler is a widely used network product that is used for example to provide a secure remote access. The attackers also left behind a blackmail note, although this was actually directed at the university itself rather than the medical centre. When the investigating authorities subsequently informed the cybercriminals that they had targeted a hospital, the latter then provided a digital key for recovering the IT systems and data. One is therefore led to conclude that the university – rather than its in- and out-patient care facilities – had been the attackers' primary target.

Assessment

In the aftermath of the attack, the provision of healthcare at the university medical centre was assured for in-patients, but outages affecting core systems meant that the hospital could not provide services as part of the region's emergency care roster for a period of nearly two weeks. Scheduled and outpatient treatments were cancelled or postponed, and the hospital did not admit new patients during this time. Email communication was restricted and the hospital had only limited phone lines available. The university medical centre incident once again highlights the dangers of cyber attacks directed against healthcare institutions and their IT infrastructure.

Response

At the centre's request, the BSI deployed a mobile incident response team (MIRT) to the site the very same day to organise an initial response as part of incident management. During the incident, a local BSI team helped rebuild the centre's local IT infrastructure with coordination support from a back office team.



Theft of Passport Data

Situation

The Argentinian immigration authority Dirección Nacional de Migraciones became the victim of a *ransomware* attack in which a massive amount of data was stolen, with German citizens among those affected. The bulk of the data consisted of the passport particulars of around 100,000 inbound and outbound private citizens, 12,000 of whom were from Germany (including high-ranking German diplomats). The personal data captured by the attackers included details such as first and last names, passport numbers, dates of birth and travel itinerary, as well as passport types (e.g. diplomatic passports). The data obtained could be easily used for identity theft.

On 27 August 2020, the Argentinian immigration authority announced that it had been affected by technical disruptions and took action by shutting down its IT systems. The NetWalker hacker collective sent a blackmail note stating that the data on the infected IT systems in the network had been encrypted. It demanded payment of a ransom amounting to roughly USD 4 million to surrender the decryption key. The Argentinian immigration authority refused to make the payment. About two weeks later, the data was uploaded to a website and a link with the password to this website was then posted on a darknet blog.

This was followed by a tweet from the Argentinian security service, which stated that the stolen data amounted to roughly one percent of the annual volume of data generated by cross-border travel and that the immigration authority database had not been compromised. According to media reports, around two gigabytes of data were taken from a folder named 'Coronavirus'. This folder had contained a spreadsheet listing the personal details of around 100,000 travellers from various countries, including Argentina, Canada, France, Germany, Israel and Switzerland. The data was checked for authenticity and found to be genuine (see the bibliography [here](#)³ and [here](#)⁴).

Assessment

Originally known as Mailto, the NetWalker *ransomware* has been circulating since August 2019. Since then, the feature set associated with this *ransomware* has continually expanded. In its most recent format, which has been in use since 2020, NetWalker operates based on a *ransomware-as-a-service* model (see the bibliography⁵). *Ransomware-as-a-service (RaaS)* solutions are now in widespread use. Easy to come by on the darknet's underground forums, these services enable users (who no longer need to fully understand the *attack vector*) to piece together a custom *ransomware* variant for later use in targeted attacks or campaigns. Meanwhile, business models are becoming common in which the entities involved share spoils based on their respective input (e.g. 40 percent of a ransom goes to the solution *provider* and 60 percent to the person using the *RaaS*; see the bibliography⁶).

According to the Telemetry Map from McAfee, an increase has been recorded in the global distribution of this *ransomware* (see the bibliography⁷). Almost simultaneously, the NetWalker hacker group tried to extort USD 3.8 million from Pakistan's largest private energy utility, K-Electric, using the same approach they took with the Argentinian immigration authority. When K-Electric did not meet their demands, the collective also published their data online (see the bibliography⁸). Other known cases involving the NetWalker threat group include an attack on an Austrian city council on 24 May 2020 and another on a public health services *provider* in Philadelphia (USA) on 20 June 2020 (see the bibliography [here](#)⁹ and [here](#)¹⁰).

Response

In the case of the Argentinian immigration authority, systems were shut down as a precaution during the attack to limit the extent of the damage and weaken the attack itself. As a result, the attackers had access to less data than they had perhaps planned. In addition, formal charges were brought against them and an investigation was launched by law enforcement with the active participation of the BSI. The Argentinian IT security authority also announced that the systems in question would be hardened to protect against future attacks of this kind (see the bibliography [here](#)¹¹ and [here](#)¹²).

As a general rule, the BSI recommends refusing to pay *ransoms* because it is never certain that data will indeed be decrypted once the requested payment has been made. Paying a ransom also offers no reassurances that the data stolen (or copied, to be technically accurate) will not subsequently be published anyway by the attackers. Important information, recommendations and documents on the topic of *ransomware* can be found on the BSI website (see the bibliography⁴).





Darkside

Situation

On 7 May 2021, the US pipeline operator Colonial Pipeline Company became aware of a cyber attack on its IT infrastructure. The following day, the affected operator reported the cyber attack as a confirmed *ransomware* deployment to the Federal Bureau of Investigation (FBI), the United States Department of Energy (DOE) and the White House. The attack affected the company's administrative network (see the *bibliography*¹³).

According to its own figures, Colonial Pipeline operates the largest pipeline system for refined products in the USA. Its pipeline network spans approximately 8,800 km and is capable of transporting as many as 2.5 million barrels every day. Colonial Pipeline occupies a key position in supplying customers with refined products along the USA's East Coast (see the *bibliography*¹⁴). As the FBI subsequently discovered, the cybercriminals had used the *ransomware* Darkside (also styled as DarkSide) in their attack (see the *bibliography*¹⁵).

Assessment

Cybercriminals offer Darkside in *ransomware-as-a-service* arrangements. At the time of this cyber attack, Darkside was one of the most prominent and advanced *ransomware* variants. Cyber attacks featuring Darkside can be categorised as 'big game hunting'. Alongside ransom demands, targets are also told to pay hush money to prevent attackers from publishing the data they have stolen and encrypted (a practice known as double extortion).

In Germany, the petroleum industry forms part of the national critical infrastructure. Operators of critical infrastructure are assigned specific duties in relation to cyber security and are also required to inform the BSI of cyber security incidents. A comparable cyber attack is considered entirely possible in Germany.

The country's operators of energy supply grids and facilities must ensure an appropriate level of protection for the telecommunications and electronic data processing systems required in order to provide their critical services (German Energy Act (EnWG), sections 11a and b). While some IT incidents reported to the BSI (pursuant to section 8b of the BSI Act, BSIG) have involved isolated IT attacks on energy suppliers, these have only affected office systems to date. In each case, critical services were maintained despite these attacks.

Response

The pipeline operator responded to the attack by taking its administrative network offline and shutting down pipeline operations as a precautionary measure. These shutdowns caused regional shortages and panic buying – of petrol in particular. On the dedicated leak website that cybercriminals primarily use to publish their stolen data, the operators of the *ransomware-as-a-service* (*RaaS*) Darkside posted a statement alleging that the attack had been launched by an affiliate and that the magnitude of the damage caused by the attack was unintentional (see the *bibliography*¹⁶).

Since 15 May 2021, multiple media sources have reported that the cybercrime group responsible for the Darkside *RaaS* has apparently lost control over large parts of its own IT infrastructure. These media reports have been based on a statement that was issued by former Darkside *providers* to their *affiliates*. Control over the IT infrastructure was apparently revoked by the infrastructure *provider* in response to an order issued by a law enforcement agency. Towards the end of the statement, the Darkside *providers* announce the discontinuation of their *RaaS* (see the *bibliography*¹⁷).

Beyond the specific case of Colonial Pipeline and Darkside, this has also had repercussions for *RaaS* in general. While *RaaS* solutions had previously been advertised and showcased on cybercriminal underground forums, many of the established forums summarily banned any *ransomware* topics from their platforms just a few days after the incident. As a result, the *RaaS* offers previously promoted publicly were forced onto private servers. Since then, interested individuals have had to search for new *affiliates* through invitation-only chat groups, for example, or based on word-of-mouth (see the *bibliography*¹⁸).

Some *RaaS providers*, such as REvil (a.k.a. Sodinokibi) or Avaddon, have specified new conditions that their *affiliates* need to fulfil before an organisation can be attacked with their code. These conditions have included specific exclusions such as healthcare organisations, as well as the need to request authorisation from the *RaaS* operators (see the *bibliography*¹⁹).

As of this writing, there is no way of estimating the extent to which the announced restrictions on *affiliates* will lead to an actual decrease or increase in attacks on individual sectors. Apart from the public *RaaS* solutions on offer, any number of established cybercrime groups remain in business that have yet to announce any such restrictions and are also very unlikely to do so. As before, *ransomware* possesses exceptional potential as a cyber threat.



Ransomware Attack on a Major Media Group

Situation

During the night of 22 December 2020, a major German media group became the victim of a *ransomware* attack. This attack had a massive effect on operations throughout the group and prevented it from providing many of its print and online media offerings as usual. The attack was based on the *ransomware* DoppelPaymer. Due to the disruption of both editorial and printing processes, only an 'emergency edition' of each newspaper could be published following the cyber attack.

Assessment

The attackers responsible for the *ransomware* DoppelPaymer (also known as 'Doppel Spider') are a big game hunting collective. Typically, their attacks feature a combination of encryption and publication of data stolen beforehand (double extortion), which makes it possible to exert more pressure on their victims. The same attacker group is probably also responsible for the attack on a university medical centre in North Rhine-Westphalia (see the incident *Ransomware attack on a university medical centre in North Rhine-Westphalia*, page 15).

Response

The media group made every effort to recover its systems as quickly as possible. The local police force and State Criminal Police Office (LKA) conducted investigations of this incident, with the Central Cybercrime Contact Point (ZAC) at the State Prosecutor's Office handling procedural matters. The group affected resumed publishing its newspapers with their normal content at the end of January 2021.

As a rule, the BSI recommends never capitulating to ransom demands because once it is exfiltrated and encrypted, data must always be viewed as compromised, even following payment of a ransom or hush money.

1.2.3 Spam and Malware Spam

Unsolicited emails are generally referred to as *spam*. Apart from unsolicited advertising, some emails – like *malware spam* and *phishing* mails – may constitute cyber attacks. *Spam* can be sent from compromised or commercially rented servers via legitimate email accounts that attackers have compromised (see chapter *Malware and Data Leaks*, page 25) or via infected systems that have been consolidated into *botnets* and then used to provide *spam* services (see chapter *botnets*, page 19).

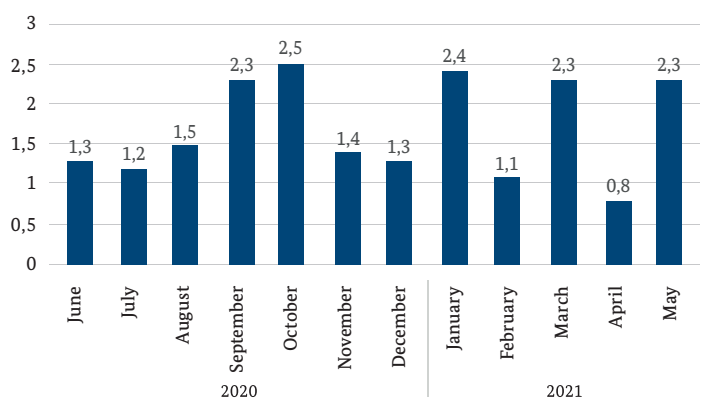
In the reporting period, waves of *spam* involving cyber extortion in particular were observed. In one example, the attackers behind a large-scale sextortion campaign conducted in October 2020 claimed to possess erotic material relating to the email recipients, along with information on all the contacts in their address books. The criminals also asserted that they had gained control of the victims' devices, as well as peripherals such as webcams. The email recipients were threatened with comprehensive disclosure of the alleged compromising material, and attempts were made to extort USD 1,000 in *bitcoin*.

Sextortion campaigns took on significant dimensions in January, March and May 2021. In the emails involved, attackers claimed to possess video clips of the victims that showed them visiting a website hosting pornographic content. A four-figure sum in euros, payable in *bitcoin*, was then demanded. A failure to pay would result in the compromising video being sent to all the victims' contacts. The *spam* ratio, which specifies the volume of *spam* received by businesses in Germany in relation to genuine email, went from one high to another during these *spam* waves in January 2021, ultimately reaching peak values of up to 34 to one in May 2021. In contrast, the average value was 2.3 in May 2021 (see Figure 3). Statistically speaking, inboxes operated by businesses in Germany during the above-mentioned campaign would therefore have received 34 cyber (s)extortion emails for each legitimate email. Of these, no fewer than 80 percent were sent as part of the double extortion campaign campaign.

During the reporting period, the average *spam* ratio amounted to 1.7 *spam* emails for each legitimate email. The threat posed by *spam* was therefore at an average level compared to previous years. Modern *spam* filters were able to handle the threat and disposed of most *spam* before it actually reached the intended inboxes.

Spam-Ratio in German business Number of *spam* mails received per legitimate email

Figure 3: Spam ratio in German businesses
Source: BSI analysis of its own sources



1.2.4 Botnets

The term 'bot' refers to a type of *malware* that gives an attacker remote access to an infected system. The widespread use of *bot* software has given cybercriminals access to a large number of third-party systems (computers, smartphones, routers, *IoT* devices, etc), which they can then misuse for their own purposes. An aggregation of multiple *bots* controlled from a master computer is referred to as a *botnet*. The modular design of contemporary *bot* software gives attackers options for adjusting

a *bot's* functionality to suit the respective attack objective and designated target. Apart from causing damage throughout the infected system itself (through the theft of personal data, online banking fraud, cryptomining, data encryption, and so on), compromised systems can also be commandeered for attacks on third parties (e.g. *DDoS* attacks; see chapter *Distributed Denial of Service*, page 31) or *spam* campaigns (see chapter *Spam and Malware Spam*, page 19).

In the current reporting period, *bots* were primarily used for espionage attacks targeting personal information and for the propagation of other *malware*. In relation to *ransomware*, perpetrators focused consistently on financially appealing targets (see chapter *Big Game Hunting with Ransomware*, page 12). Both Emotet and TrickBot were deployed en masse in order to conduct espionage attacks on well-known companies and institutions, whose data was then encrypted with the help of Ryuk.

As in previous years, the number of known *DDoS botnets* decreased further, but new variants of the Mirai *malware* continued to appear with additional mechanisms of infection for a wide range of hardware platforms. In general, an increasing level of professionalism can be observed in the use of *botnets*, which is helping to keep threat levels high. The vast majority of *bot* software now in operation is being deployed by professional service providers on dedicated platforms as *malware-as-a-service (MaaS)*. Even cybercriminals who lack the necessary expertise can now use the functionality offered by a *botnet* without needing to worry about the technical details.

The trend towards a stronger focus on mobile devices on the part of attackers continued unabated in the current reporting period. Seven of the 10 largest *botnets* observed in the BSI's sinkholing activities target Android tablets and smartphones. The threat posed by *botnets* has also taken on a new quality. Since January 2021, attackers have been attempting to persuade users of Android smartphones to install the MoqHao *malware* as part of comprehensive campaigns conducted using text message *spam*. Following successful installation, this *malware* integrates the affected smartphone into a *botnet* in order to misuse the device for activities such as data theft or the further propagation of *malware*. Other *botnets*, such as ArrkiiSDK or AndroidBauts, track user behaviour or install additional applications without the knowledge or consent of the user. They also offer click fraud functionality, which allows attackers to simulate advertising banner clicks and thereby claim fraudulent commission payments.

The BSI regularly reports information about *botnet* infections to German ISPs, which can then proceed to identify and inform their affected customers. During the reporting period, up to 40,000 infected devices were detected and reported to ISPs in Germany every day. The total number of *botnet* infections is likely to be considerably higher.

This estimate stems primarily from *sinkhole* datasets that have been supplied by external sources or generated by the BSI's own internal *sinkhole* systems. Instead of

contacting the *command-and-control servers* operated by attackers, *sinkhole* systems simply accept contact requests from *bots* and log them without taking further action. A description of the sinkholing procedure is provided on the BSI website (see the bibliography^e).



The website also provides profiles of the *malware* families that are most frequently reported.

As in previous years, the threat posed by *bot networks* remains consistently high. Infection numbers deduced from sinkholing should always be seen as minimum values because it is impossible to obtain a complete set of data for all ongoing *botnet* infections. Depending on the source consulted, the *botnets* selected for observation and the domains utilised for control (*C&C servers*), the figures on visible infections can vary greatly. The insights gained to date from *botnet* takedowns show that the number of unreported cases is significantly higher, and that the total volume of infected systems in Germany must be at least in the low millions. Introduced by the German IT Security Act 2.0, the authority to have *malicious* network traffic stemming from internet service providers redirected now offers the opportunity to significantly improve the visibility of previously DNS-based sinkholing.

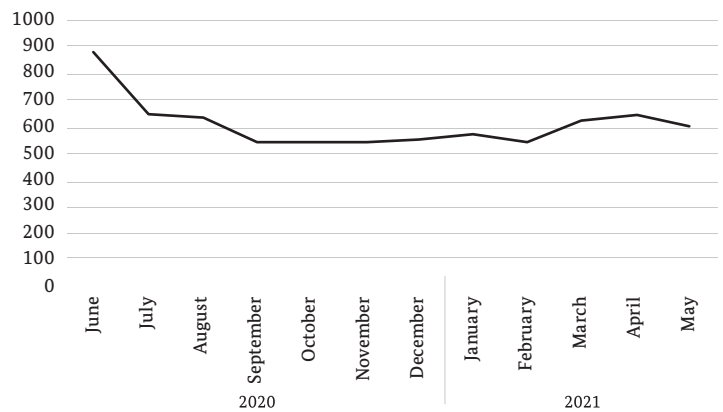
In 2020, for example, steps were undertaken to improve the reporting of undetected cases. The Unique IP Index, which measures the occurrence and development of infection figures in observed *botnets* by means of unique IP addresses, was launched with 884 data points in June 2020. Compared to earlier reporting periods (the figure for 2019 was 100), official figures for observed *botnet* activities therefore rose by a factor of almost 10.

With the BSI using regular reports to warn internet service providers and network operators about affected systems (see chapter *Computer Emergency Response Team*, page 71), a considerable reduction in infections was already achieved in the first year of the effort to expose undetected cases (-31% compared to June 2020). The average figure for the Unique IP Index was 609 points in the reporting period (see Figure 4).

As the number of potential target systems continues to expand (due to inadequately secured *IoT* devices and mobile systems, for example) and the professionalism on the part of perpetrators grows, one can expect infections to increase further in the future.

Unique-IP-Index¹⁾ 2019 = 100

Figure 4: Unique IP Index
Source: BSI analysis of its own sources



Emotet Takedown

Situation

In addition to providing a detailed analysis of Emotet in its 2020 situation report, the BSI has repeatedly issued press releases and cyber security warnings over the last few years that have warned of the risks posed by this particular *malware*. In 2019, the BSI also published detailed recommendations for action to guard against attacks based on Emotet (see the *bibliography*²⁰). Notwithstanding these activities, tens of thousands of home users, as well as many companies, authorities and other organisations, fell victim to new Emotet infections over the past year.

In some cases, additional *malware* subsequently downloaded by Emotet (such as TrickBot) was able to compromise the victim's entire network, requiring weeks of recovery work and causing restrictions to business productivity, along with millions of euros in losses. In other instances, attackers also deployed the *ransomware* Ryuk to the target's networks to encrypt data for extortion purposes, which resulted in significant additional damage.

Assessment

On infected systems, Emotet was able to capture email login details and inbox content for the purpose of propagating itself further using sophisticated social engineering techniques. In 2020 alone, *spam bot* monitoring conducted by the BSI revealed that more than 40,000 email accounts operated within Germany had been compromised by Emotet. The BSI reported this information to the respective service providers so that the affected parties could be informed and further abuse of their accounts for the propagation of Emotet could be prevented. This figure represents only the tip of the iceberg, however: the total number of email accounts compromised by Emotet in Germany is assumed to be significantly higher.

Response

On 26 January 2021, the infrastructure used by the *malware* Emotet was taken over and destroyed as part of an internationally coordinated initiative whose members included the Chief Public Prosecutor's Office/Central Office for Combating Internet Crime (ZIT) in Frankfurt (Germany), the German Federal Criminal Police Office (BKA) and law enforcement agencies in other countries (see the *bibliography*²¹).

¹⁾ Does not include infected IP addresses that were not logged by sinkholing

As part of this takedown operation, the law enforcement agencies were able to distribute a modified binary to a large number of infected target systems that rendered the Emotet *malware* unusable. The communication parameters for Emotet were modified so that infected systems would no longer establish contact with the perpetrators' control servers, but instead report back to a series of *sinkhole* servers operated by the BKA. These *sinkholes* would log evidence of these contact attempts from infected systems by recording the timestamps, IP addresses and Windows computer names reported by Emotet.

The BKA then passed its log records on to the BSI. CERT-Bund (which operates within the BSI) forwarded this information to the network operators and internet service *providers* responsible for these IP addresses in Germany so that the affected customers could be notified about the Emotet infection on their systems. Data relating to IP addresses managed by network operators in other countries were forwarded to the respective national CERTs.

While the takedown does mean that the Emotet *malware* cannot cause any further damage on infected systems, any other *malware* subsequently downloaded (such as TrickBot or Qakbot) still remains active. Affected parties therefore needed to act quickly to sanitise their systems after being notified of an infection so as to avoid any further loss or damage.

The modified Emotet binary uninstalled itself automatically on 25 April 2021. Prior to this date, the authorities in question had three months to notify those affected by infections.

On infected systems, Emotet captured login credentials from system users as they logged into online services using a web browser. As part of further investigative activities conducted after the takedown, law enforcement agencies seized a database containing over 35 million records of login details captured by Emotet from infected user systems all over the world. More than 700,000 data records related to user accounts from over 80,000 online services operated in Germany, including online banking, online shops, booking portals for hotels and flights, customer portals run by internet and mobile service *providers*, and portals for various government services, including economic stimulus programmes and applications for student financial assistance (BAföG). CERT-Bund informed the operators of these online services and their internet service *providers* about the compromised user accounts.



SMS-Phishing („Smishing“)

Situation

Apart from email, *phishing* attacks can also be carried out using SMS text messages as a vector. The neologism ‘smishing’ has been coined to describe this variant. While this phenomenon is not new, most previous campaigns were reported outside of Germany. The attack variants described below have a dual purpose: to ensure the large-scale distribution of *malware* via infected Android smartphones and to conduct actual *phishing* attacks.

In February 2021, a large wave of SMS *phishing* messages was detected in Germany and ultimately traced back to the Android *malware* MoqHao. To propagate itself, MoqHao used German-language text messages resembling notifications from parcel service *providers*. These SMS messages typically contain a notification and a link – for example, ‘Your package is in transit. Please check the details and accept delivery. <Link>’. The link leads to a website where Android users are asked to install what seems to be an update for the Chrome browser *app*. This update, however, contains the MoqHao *malware app*. Immediately after installation, an infected Android smartphone will start sending out texts with the aim of spreading MoqHao further. In addition, MoqHao can conduct *phishing* attacks on infected Android smartphones by showing form fields requesting user input (for example). MoqHao identifies its command-and-control servers from coded content posted to social media profiles.

Since March 2021, MoqHao texts in Germany have been increasingly superseded by SMS messages sent by the Android *malware* 'FluBot', which also sends users texts that appear to be notifications from a parcel delivery service. Users are informed that package tracking requires an *app*, which is the FluBot *app* disguised to look like the *app* from FedEx or DHL. As with MoqHao, installing this Android *app* results in the sending of bulk text messages. In this case, however, the SMS messages are much more varied, and have even included a personalised salutation since early April 2021. FluBot has this information at its disposal because it accesses a smartphone's contacts after installation and sends the data to a command-and-control server. These contact details are then used for sending text messages from infected Android smartphones. Besides propagating itself via text message, FluBot (like MoqHao) also conducts *phishing* attacks on infected Android phones.

Meanwhile, FluBot has a more robust *botnet* infrastructure than MoqHao. As a result, the URLs used in the text messages change on a regular basis. FluBot *apps* are offered from a wide variety of unrelated download websites, all of which are compromised *malware* hosting sites. In order to establish contact with *command-and-control* servers, FluBot uses a domain generation algorithm (DGA). Since the potential domains run into the thousands, this is meant to make it impossible to contain the FluBot *botnet* by taking down individual domains.

The Android *malware* 'TeaBot', which follows FluBot's mechanisms, is also able to access local smartphone contact details and propagate itself by SMS message. TeaBot can disguise itself as one of several Android *apps*, including VLC Media Player, TeaTV, DHL and UPS. Like FluBot, TeaBot conducts *phishing* attacks on infected Android smartphones in order to compromise installed banking *apps* from German financial institutions.

Assessment

Common to the Android *malware* programs MoqHao, FluBot and TeaBot is the fact that they have to be installed from unknown sources and not from legitimate *app* stores. This function is deactivated by default in Google's Android operating system and is not even possible with Apple's iOS. Thanks to social engineering techniques based on personal salutations and the increased volume of parcels sent during the COVID-19 pandemic, however – as well as step-by-step instructions for the necessary Android configuration changes and *app* installation – smishing perpetrators have still managed to achieve widespread penetration within Germany.

Once one of these Android *malware apps* is installed, the phone in question can be considered fully compromised. Apart from sending texts, the *malware* can also access SMS content, and some versions are even able to eavesdrop on text input and *app* content. This means that both *app* data and two-factor *authentication* methods can be affected.

While Apple iOS users are obviously not at risk from Android *app malware*, following the links contained in the text messages received can still take these users to *phishing* websites.

Response

Since the increased incidence of waves of SMS *phishing* attacks in February 2021, the Cyber Response Centre has worked with German mobile service *providers* to contain these smishing campaigns and raise public awareness, including via press releases and social media. A dialogue has also been actively pursued with the international IT security community to enable prompt identification of tactical changes in these SMS *phishing* campaigns and derive countermeasures.

Alongside its measures to increase awareness, the BSI has also adopted strategies to detect infected Android smartphones with the help of *sinkholing* (i.e. the registration of *command-and-control* server domains). *Sinkholing* stops infected smartphones from 'phoning home' by redirecting them to a *command-and-control* server operated by IT security analysts. The information gained is then used to inform German network operators about infected Android smartphones present in their respective networks.

The BSI has also worked with Google to improve the detection of the above-mentioned Android *malware* on smartphones – with the help of Google Play Protect, for example.

1.3 Theft and Abuse of Identity Data

In the context of information security, an ‘identity’ is understood to mean a set of attributes providing evidence that a person or thing is genuine. Accordingly, the identity of a person or thing can be defined by a single attribute or a combination of several discrete attributes. In the online world, the identity of a person is typically deduced from identification and *authentication* data – the combination of a username and password, for example. These kinds of data items hold knowledge about individuals, which is why they are also known as ‘knowledge factors’. The concept of ‘identity theft’ is defined as the unlawful acquisition or usage of such data. In electronic communication and the use of internet services in particular, an internet user’s level of trust in a particular counterpart often depends on whether this party can provide such knowledge factors. This makes any form of data that inspires trust a highly attractive target for a wide range of attackers.

1.3.1 Phishing and Other Types of Fraud

One popular technique used by attackers to acquire such data is known as ‘*phishing*’. In this kind of attack, sophisticated social engineering techniques are used to encourage the victim to disclose sensitive information. In Germany, *phishing* attacks tend to be focused on customers of financial institutions, as well as customers of online retailers like Amazon or payment systems such as PayPal.

In its own observations, the BSI has seen how current *phishing* campaigns closely track social trends and topical issues, such as tax refunds or matters related to the COVID-19 pandemic. Attackers have made good use of the various uncertainties and challenges posed by recent pandemic developments, as well as objective and subjective time pressures and the overall dominance of the topic in society and the media. In their targeted efforts to *exploit* people’s emotions, they have managed to reach a very wide audience.

For example, attackers have taken advantage of the fact that logistics has faced additional obstacles during the pandemic. Attackers have posed as customs officials, for instance, and sent emails demanding payment of a fee – to be paid via an anonymous payment service such as Paysafecard – before goods will be delivered. The much greater number of people placing orders online as a result of the pandemic has also increased the number of potential victims. As new issues and scenarios have arisen, no stone has been left unturned in thinking up ways to *exploit* them. Attackers have set up fake websites to siphon off pandemic support funds, used the cut in the VAT rate to try and trick

users into paying non-existent hikes in bank charges, and invented a host of fictitious online systems to *exploit* impending lockdowns or the temporary closure of local bank branches. They have always been very quick to respond to current or forthcoming developments in the pandemic (see Figure 5).

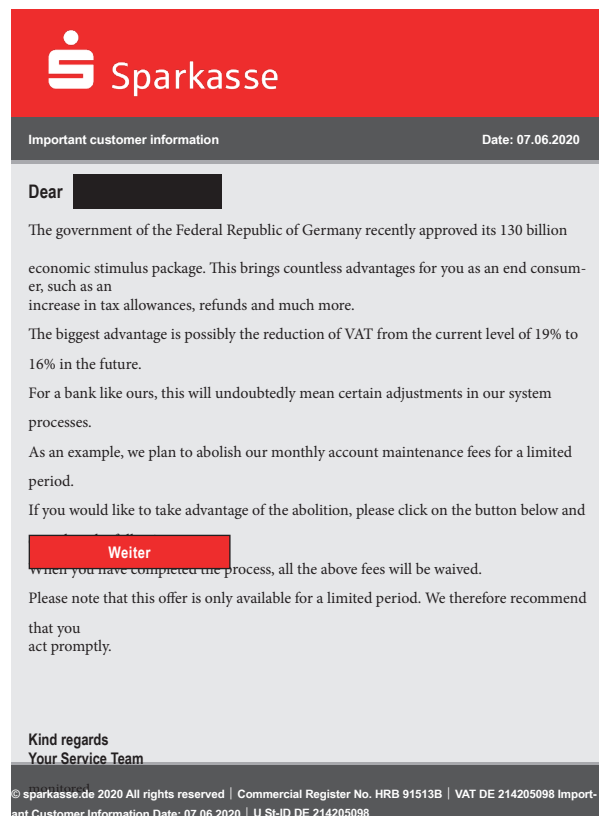


Figure 5: Phishing email
Source: Phishing Radar from the NRW Consumer Advice Centre, in cooperation with the BSI

Attackers’ knowledge of their victims and/or their ability to act convincingly as representatives of trusted organisations or individuals has been a key factor in the success or failure of any particular attack. In the reporting period, incidents were reported to the BSI where attackers managed to gain access to a victim’s online banking service, for example, and then utilise targeted spoof calls to obtain the TAN necessary for a specific transaction. Incidents also came to light where Twitter accounts owned by famous personalities such as Barack Obama, Jeff Bezos and Bill Gates were hacked to make tempting offers related to the *Bitcoin* cryptocurrency, which came with the promise that double the sum of bitcoins deposited would be paid out at a later date (see the bibliography⁴).



1.3.2 Malware and Data Leaks

Alongside *phishing*, special-purpose *malicious* scripts or complex pieces of *malware* are also regularly used to gain access to identity data. The immense volumes of customer data held by online retailers means that they are continually targeted by contemporary attackers using skimming. Web skimming attacks are used to compromise legitimate online retail sites – sometimes without the platform operator even becoming aware of the attack. During the reporting period, Magecart again reared its head in connection with these kinds of skimming attacks on web shops. This particular *malware* lets attackers implant *malicious* JavaScript code that steals credit card data and delivery and invoice addresses from web shop payment processes.

In addition, the ubiquitous threat posed by the encryption of key data by *ransomware* was increasingly accompanied during the reporting period by the theft and publication of this data (see chapter Big Game Hunting with *Ransomware*, page 12). At first, only isolated attacker groups were using this approach to improve their chances of success in blackmailing their victims, but a larger number of collectives have since adopted this *modus operandi* – and the trend shows no signs of slowing down. As a consequence, an attack that deploys *ransomware* must always be assumed to involve the risk of a data leak because the two topics are becoming increasingly intertwined. In addition, once data has been published on a dedicated leak site (DLS), it must be considered compromised even if a hush money payment has been made and the data has been taken down from the site. The data is likely to have been accessed and stored by a wide variety of actors and could well be utilised in future attack scenarios.

In many cases, however, data leaks are not the result of advanced attacks. In the current reporting period, sensitive data also ended up in unauthorised hands due to a lack of adequate protective measures for (online) databases. This often leads to a situation where sensitive (and often personal) data is disclosed without the participation – and in many cases, even without the knowledge – of the data subject.

Organisations affected by these kinds of general data leaks in the reporting period included leading technology companies, doctor's practices and hospitals, transport and logistics firms, public institutions and social networks. One incident in Finland attracted particularly significant attention. As part of a cyber attack on the operator of a Finnish psychotherapy centre, unknown individuals made off with tens of thousands of patient records. The attackers demanded hush money payments, offering to erase the patient records once they were made. In such cases, however, victims can never be entirely sure that the data has indeed been deleted, which is why the data must generally be viewed as compromised.

The Finnish incident made international headlines because it involved a serious breach of particularly sensitive patient data.

Turning to other cases of identity theft in the reporting period, the global COVID-19 pandemic proved to be a recurrent topic. As analogue processes were relocated to the digital space and measures were increasingly introduced to combat the pandemic, this was repeatedly exploited by many incidents (see chapter Threats to Cyber Security due to the COVID-19 Pandemic, page 38). Around the world, targeted attacks and a lack of appropriate security measures led to many leaks of sensitive information associated with the pandemic and related countermeasures. On some occasions, personal data was also accessed at several German testing centres.

Meanwhile, the BSI helped improve the long-term security of Germany's national 'Corona Warn App' by supplying continuous vulnerability analysis and penetration testing during the *app* development process. The BSI then worked with the *app* developers to rectify any vulnerabilities detected before the corresponding release of each new version. The BSI is not aware of any incidents during the reporting period where a leak of personal data occurred in conjunction with the Corona Warn App (see chapter Corona Warn App, page 51).

1.3.3 Cyber Attacks on Videoconferences

All in all, the COVID-19 crisis led to the large-scale relocation of many areas of life into cyberspace. While this change offered the chance to create innovative new models and opportunities, the outsourcing of analogue processes to the digital space also introduced a number of new risks. Social contact restrictions greatly expanded the role played by communication platforms in the reporting period. All over the world, companies and government agencies used videoconferencing platforms to handle a large part of their internal communications. As a result of this much greater usage and the associated public awareness and status of these platforms, videoconferencing has become an attractive target for cyber attacks.

One area of interest for attackers is the procurement of information from invitation-only conferences. In 'credential stuffing' attacks, for example, user details from previous data leaks are tried out with various service *providers* in an automated process that attempts to achieve a successful login. Such attacks have enabled third parties to use previously leaked login details to impersonate legitimate participants and gain access to closed sessions. This kind of intrusion into internal conferences can have fatal consequences for affected organisations. There are many

options available for weaponising the information thereby obtained. In addition to an organisation's confidential information, content discussed in videoconferences may provide valuable insights into internal processes and deployed tools. Alongside extortion and industrial espionage, eavesdropping can therefore offer a springboard for further cyber attacks.

In the reporting period, many users experienced attacks as a result of the theft of their login credentials. In many cases, attackers used *phishing* mails disguised as session invitations, which then redirected the target to fake conference websites. On these websites, users were then requested to enter their password details. Some of the information gained using these methods was then sold on illegal internet platforms. Apart from login data, zero-day exploits were also offered for leading videoconferencing platforms.

Another phenomenon that entered the spotlight as a result of the increased usage of videoconferencing platforms was a technique known as 'Zoom bombing'. This involved third parties gaining access to conferences with the explicit aim of disrupting them. Online education was one sector affected by such attacks, particularly since login credentials were often passed around by lesson participants. A key source of security risks in the use of videoconferencing platforms relates to the lack of knowledge about how to operate certain kinds of system functions. During the reporting period, there were many incidents where public figures published photos of their online sessions on social networks and thereby disclosed their own login data – in the form of URLs clearly visible in the photo, for example. In one case, this resulted in unknown parties disrupting a confidential session attended by European Union defence ministers.

Summary

In a continuation of the trend established in recent years, the BSI noted regular reports of leaks of personal data in the current reporting period. During the reporting period, however, such incidents were aggravated by the fact that *ransomware* attacks and attempts at (double) extortion have now become closely associated with such data leaks. In practice, these are now merging into a single phenomenon. In light of especially serious breaches of patients' confidentiality, giving these kinds of data the appropriate safeguards they require must now be prioritised as a matter of urgency. A loss of sensitive health data can potentially result in lifelong repercussions for the patients involved.

The COVID-19 pandemic has become an important factor in the identity theft threat landscape. As a result of the physical distancing needed during the pandemic, the

trust placed in digital identities has become increasingly important. Accordingly, the loss of confidential information not only undermines safeguards against cyber attacks on the infrastructure of a digital society, but also influences the basic level of trust in digitalisation itself. While a well-considered and secure approach to the handling of personal data is first and foremost the responsibility of internet service providers, each and every one of us must be aware of the risks involved in disclosing our personal data (see the bibliography⁶).



1.4 Vulnerabilities

Services hosted online with vulnerabilities that can be utilised by an attacker as a bridgehead for penetrating a network represent a particularly serious risk. During the reporting period, two prominent examples of such problems were the 'ZeroLogon' Active Directory vulnerability, which affects the NetLogon protocol (CVE-2020-1472); and vulnerabilities affecting the groupware and email server Microsoft Exchange. The criticality of such vulnerabilities is exacerbated by the publication of functional attack code for vulnerable systems ((zero-day) exploits) and/or the integration of such code into known attack tools (*exploit kits*). This makes the wider exploitation of a vulnerability more likely, which was particularly true of the 'Proxylogon' vulnerability that affected Microsoft Exchange during the reporting period (CVE-2021-26855). Perhaps as a result of the increasing number of people working from home due to the pandemic, many companies and institutions started operating Exchange servers for their staff with a public-facing Outlook Web Access (OWA) service. As a result of the publication of these vulnerabilities, validated figures for Germany indicate basic problems with the secure operation of these kinds of DMZ-based systems and the application of key security patches (see incident Critical Vulnerabilities in MS Exchange, page 27). The risk is also clearly illustrated by the Bluekeep vulnerability (CVE-2019-0708) in Microsoft's Remote Desktop Protocol (RDP), which can still be found in the wild as a commonly used *attack vector*, as well as a wide range of vulnerabilities affecting security and VPN applications that regularly go unpatched.

Another increasingly important factor here is the security risk posed by software projects as a result of the now common practice of including software libraries that are themselves not under the control of the developers responsible for a given project. While hard to quantify precisely, this is a type of supply chain risk that is caused (for instance) by vulnerabilities in widely used software components. Important examples of this include the vulnerabilities known as AMNESIA:33 (33 vulnerabilities in

four separate open-source network stacks) and Ripple20 (19 vulnerabilities in a proprietary network stack). Once again, these cases have clearly illustrated the far-reach-

ing implications presented by critical vulnerabilities in software products that are now in frequent use (see the Sidebar: Software Bill of Materials sidebar, page 28).



Critical Vulnerabilities in MS Exchange

Situation

In March 2021, Microsoft published an unscheduled security update for its widely used groupware and email server, Exchange. This *patch* closed four critical security holes, combinations of which had already been exploited in targeted attacks. One of these vulnerabilities allowed attackers to authenticate themselves to Exchange by sending it specially formatted HTTP requests. The other vulnerabilities could then be exploited to execute arbitrary program code and gain far-reaching access privileges. Attackers took advantage of these problems to plant backdoors on thousands of servers in the form of ‘webshells’. If these backdoors were not then removed after installation of the security update, perpetrators retained access to the affected systems and could use them to intercept mail or roll out *malware*, including *ransomware* variants. At the time the vulnerabilities were made public, some 98 percent of systems analysed in Germany were vulnerable. The first wave of exploits was mostly observed in cyber attacks conducted in the USA.

Assessment

Directly after the publication of the security *patch* by Microsoft, attackers were already hard at work scanning the entire internet for vulnerable systems. At the same time, various hacker collectives also started exploiting the various vulnerabilities to install *malware*. As a result, all vulnerable Exchange servers immediately faced a very high risk of a *malware* infection. Even systems that had been patched quickly thus needed to be audited for compromises that could have occurred earlier. The situation was made worse by the fact that many systems were running very outdated software versions for which updates were no longer available, and that many Exchange servers possessed high-level default rights in many networks. Ready-made scripts for exploiting these vulnerabilities were also quickly made available online.

In 2020, the lackadaisical approach taken by many system admins had already been demonstrated by the security update published to *patch* another critical security hole in Microsoft Exchange at the start of the year. Since Exchange servers are operated with high-level rights in many backend setups, exploiting these kinds of vulnerabilities frequently facilitates more advanced attacks that can even compromise an entire Windows domain in some cases. Despite the severity of this risk, two-thirds of the Exchange servers in Germany were running a public-facing Outlook Web Access (OWA) service that was susceptible to attacks exploiting this vulnerability in October 2020 – some eight months after the publication of the corresponding security update by Microsoft. In this year’s case, continuous monitoring of the situation revealed that the responsible system admins had learned from their previous mistakes and responded more quickly and more comprehensively. In the first week after publication of the vulnerability, the number of susceptible systems fell by half.

Response

Owing to the seriousness of the risk, the BSI graded the threat situation as extremely critical and posted regular security information updates on its website. Client groups addressed by the BSI received support for incident handling, and two webinars were offered that provided further updates about the situation. The routine CERT-Bund reports used by the BSI to inform network operators and internet service *providers* in Germany about vulnerable systems in their networks were also expanded to include information about the risks posed by these vulnerabilities. By supplying additional updates for older software versions and publishing scripts for mitigation and auditing systems for indicators of compromise, Microsoft was initially able to defuse the situation to an extent.

In May 2021, however, roughly nine percent of the Exchange servers analysed in Germany were still susceptible to these critical vulnerabilities.

i Software Bill of Materials (SBOM)

Major coordinated vulnerability disclosure (CVD) cases such as AMNESIA:33 and Ripple20 have underlined the extreme difficulty manufacturers face as they attempt to identify the libraries and other third-party software now integrated within their products. These analysis tasks take valuable time and hinder the CVD process.

The international community is receiving dedicated support from the US agency NTIA in drawing up a Software Bill of Materials (SBOM) specification. An SBOM is used to list all of the dependencies pertaining to a specific piece of software. This is intended to enable the effective review of potential vulnerabilities within a product. As the initial users of SBOMs, manufacturers themselves must analyse their supply chains to see whether they use a particular version of a piece of software that is known to be vulnerable. Once armed with this information, they can take measures to resolve the problem. When applied in combination with the Common Security Advisory Framework (CSAF), the process can be largely automated within the supply chain.

The BSI is also supporting this improved level of protection for supply chains in its work on the specification of the VEX format. This format can be used by manufacturers to inform users that a vulnerable software version is used but that the vulnerability in question is not in fact exploitable. One example of a possible scenario here involves the use of compiler options to ensure that only a certain, non-vulnerable part of the code is used by a given product.

1.5 Advanced Persistent Threats

Advanced persistent threats (APTs) are distinguished from other threats to cyber security based on the attacker's motivation and methodology. While *malware*, for example, is typically distributed by cybercriminals en masse and with no particular target in mind (see chapter Big Game Hunting with *Ransomware*, page 12), APTs are often meticulously planned over a long period of time and target a single, carefully chosen victim. The objective of an APT attack is not financial gain, but to procure information about the target, potentially with the aim of sabotage.

Technical approach: In the related literature, APTs are often associated with the exploitation of complex vulnerabilities. In practice, however, this is often not the case, especially for attacks that target end users. Most email-based attacks have moved on from simple exploits of technical security holes. As in the case of criminal attacks, the focus is instead on the user. Attempts are made to trick the user into ignoring warning pop-ups and executing macros and other harmful content. In other cases, the user is fooled into clicking executables and shortcut files in ZIP archives, which is part of an attack technique known as 'DLL sideloading'. In order to avoid detection by security products, some groups have taken to no longer including *malware* directly as email attachments. Instead, they now hide code in remote templates that are downloaded only when the document is opened by the user. This has been observed in particular with the groups Lazarus, APT28 and Gamaredon.

In another clear trend, individual groups are switching from email-based attacks back to server scanning (of remote access or email servers, for example), or have at least included this in their portfolios. The groups BerserkBear, APT41, APT28 and KarmaPanda are just a few examples. This trend was already ongoing before many companies around the world introduced working from home as a result of the pandemic. There are many possible reasons why servers are now being targeted alongside end users and their office software packages. One is that servers are typically not updated automatically with security patches. For security teams, a systematic approach to the planning of update processes is made difficult by the different time frames in which manufacturers release their patches. In addition, it is much simpler for attackers to connect directly to a compromised server over the internet rather than wait while an infected office computer boots up and reports back as being ready to receive new commands.

During the reporting period, compromised software supply chains once again proved problematic as an *attack vector* that is particularly difficult to monitor. Here, attackers first target software manufacturers and insert *malware* into legitimate software products. One especially sophisticated attack campaign targeted the Orion platform from SolarWinds (see incident SolarWinds, page 30).

While many groups are now basing their attacks on known and publicly available tools such as CobaltStrike, Meterpreter and PowershellEmpire, some dedicated, group-specific *malware* is still being developed as before. This is

true of both very technically advanced groups and groups with below-average capabilities. In addition, many groups operating in different parts of the world also went to great lengths to shield their *payloads* from analysts during the current reporting period. To achieve this, infection chains were regularly lengthened by new, intermediate stages that only download further levels of *malware* in gradual steps. This should not be confused with the approach previously observed, which was to download various optional *malware* modules later on. Instead, these attack chains absolutely require all the steps to be completed in a specific order. However, because perpetrators could remove the next *malware* component from attack servers at any step – or make continuing the attack conditional on receiving data from an earlier step – analysts at security firms and government agencies were often unable to analyse the actual *malware* programs involved.

International political measures: Alongside technical security precautions, some countries are now also making use of foreign policy measures as a means of countering APT activities. In light of repeated APT incidents, several countries published statements on international cyberspace law in the reporting period to set out their positions on sovereignty, the right to national self-defence and the question as to when an incident crosses the line and must be considered an act of armed aggression. Germany has also published its opinions on international cyberspace law (see the *bibliography*²²).

The US in particular has adopted a concerted approach to cyberspace actors that involves many government agencies. Measures adopted by the US administration include sanctions targeting suppliers rated as untrustworthy, economic sanctions and legal action targeting individuals suspected of involvement in APT attacks, the creation of legal frameworks for offensive cyber operations and, as a last resort, offensive cyber operations against the infrastructure used for such attacks.

Cases in Germany: During the reporting period, the BSI processed a number of cases that were attributed to APT groups. The vast majority of these groups launched attacks on government agencies. This tallies with the worldwide trend in government agencies being the most common target for targeted attacks. In attributing attacks, the BSI only works at the group level. The APT collectives identified are generally (and virtually unanimously) assigned to one of four countries of origin by the intelligence services, law enforcement agencies and international security companies responsible.

Globally, the defence sector is traditionally a preferred target of such groups. In this area, the APT groups that came to the attention of the BSI during the reporting

period are associated with two separate countries of origin by government authorities and security firms. At least four groups conducted targeted attacks on companies in other sectors.

One growing trend can be observed in the targeting of think tanks and non-governmental organisations (NGOs), including in Germany. Typically, the organisations affected are those that deal with foreign policy or human rights issues.

Foreign opposition figures living in Germany have also become the target of APT attacks.

Personal data in the crosshairs: The attacks mentioned on foreign opposition figures have been confirmed by reports of similar attacks abroad in which personal data was stolen from individuals. Airlines, airports, telcos, public authorities and health organisations were all targeted in order to steal the personal data of both specific individuals and huge groups of random people. Ensuring the protection of such data across all sectors and organisations must continue to be an inherent and integral part of the digital transition.



SolarWinds

One of the attack campaigns that received the greatest amount of political and public attention in the reporting period involved an *exploit* that used the Orion software from US manufacturer SolarWinds to compromise targets in business and government. While the attacker groups generally focused on targets in countries other than Germany, the situation is nonetheless relevant for two important reasons. First, SolarWinds underlines the enormous potential presented to attackers by supply chain attacks, where legitimate software products can be infected with *malware* code even in the manufacturer's own network. Second, analysis reports also confirm that the attack group in question possessed technical expertise of a level rarely seen before, which enabled them to conduct their attacks over a long period without detection.

Situation

One of the products sold by the US-based SolarWinds is Orion, which comprises a monitoring package for networks, systems and applications. In mid-December 2020, US government officials announced that unknown actors had implanted a *backdoor* in Orion update files. To date, this update had been downloaded and installed by up to 18,000 SolarWinds customers. The attackers then used this *backdoor*, termed 'Sunburst' or 'Solorigate', to download additional *malware* code and penetrate the internal networks of a small subset of commercial and government targets (see the *bibliography*²³). According to media reports, several US agencies were compromised, including the Commerce and Treasury departments. Software giant Microsoft reported knowing of at least 40 affected organisations at which attackers had conducted manual follow-up activities. Of these, around half were located in the IT sector (see the *bibliography* here²⁴ and here²⁵). The number of unreported cases is likely to be higher.

According to technical reports from the IT security companies FireEye and CrowdStrike, attackers went to great lengths to avoid discovery (see the *bibliography*²⁶). For example, the *malware* code was not inserted into the actual Orion product source code, where it would have been detected by code audits. Instead, the compilation process (which is used to 'translate' the source code into executable code) was manipulated so that the *malware* was present only in working memory, and then in the final product. The attackers clearly expended a great deal of time and effort in analysing the Orion software before implanting their *backdoor* in legitimate modules and network protocols.

During subsequent attacks on companies and government agencies, the attackers tailored their tools and control servers to each individual target. This indicates a level of effort that other attackers generally try to avoid.

Accordingly, the attacks seemed designed to achieve long-term system compromises. Following installation, for example, the *malware* waited two full weeks before making any contact with a command-and-control server operated by the attackers. The initial attacks are estimated to have been launched in early 2020.

In Germany, the BSI is aware of a double-digit number of facilities that installed the *malicious* Orion update. In these cases, however, the attackers did not then implant any additional backdoors and did not spread further within the internal networks affected.

Assessment

The SolarWinds incident has technical, economic, political and strategic implications.

1. At the technical level, the incident demonstrates the potential of supply chain attacks. Manipulated software installation files and updates are useful *attack vectors* that are capable of 'flying under the radar' of widely used detection techniques. If, as in the case of SolarWinds, attackers then primarily deploy legitimate administration tools and stolen login credentials in later phases of an incursion, it can go undetected for a long time. Depending on the penetration achieved by the manipulated software, attackers may gain access to a great many networks and systems. For software customers, recognising supply chain attacks is particularly difficult. The most important actors capable of preventing *malware* implants in software products are the manufacturers themselves. Development and delivery systems thus require an appropriately high level of security.

The effort and technical expertise utilised by the SolarWinds attackers in staying undetected for so long must also be considered a technical milestone and a particular cause for concern.

2. The economic and political consequences for the affected companies and government agencies depend on the information that the attackers were able to steal. As is commonly the case with such incidents, very little information has been published on the subject. While it is often no longer possible to determine which documents have been exfiltrated, most affected parties are also loathe to disclose any specific details to the public. The kinds of information that attackers are interested in also depend on the specific attacker collective responsible and the mission they want to fulfil. Spokespersons for the Canadian, UK and US governments pinned the attacks on the APT29 group, a collective previously known primarily for conducting long-term espionage against government agencies and think tanks (see the bibliography here²⁷, here²⁸ and here²⁹). All the parties involved in the investigations are in agreement that there are no signs of sabotage to date despite the ample opportunities that have been available.

3. At the strategic level, the SolarWinds case led to discussions in the spheres of policymaking, research and the media – especially in the US – about the circumstances that enabled such a large-scale security incident, how best to respond and whether the US needed to make changes to its cyber policy.

Major IT corporations such as Microsoft called for a greater exchange of information between government agencies and companies, for example (see the *bibliography* here³⁰ and here³¹). Criticism was also levelled at the state-run Einstein project, which had used its generous budget to set up a kind of intrusion detection system for government agencies and businesses, but failed to detect the SolarWinds attack. On the other hand, some commentators noted that such systems show their real strength in detecting prolonged campaigns with familiar characteristics, while the attackers in this case had made every effort to avoid detection based on recurring indicators.

Fundamental questions were also raised, such as whether offensive cyber capabilities are capable of providing a deterrent and should therefore be expanded (see the *bibliography*³²).

Another discussion developed along the lines of whether this kind of large-scale supply chain attack breaches international cyber standards – and if not, whether additional standards need to be developed. Legal or political redress for breaches of such standards is only available when appropriate international codes of conduct have been established.

Political commentators in the US assume that fundamental strategic questions regarding cooperation between business and government, deterrence, defending forward and cyber standards will influence the cyber policy of the Biden administration.

Response

The BSI warned of the possibility of exploits immediately after details of the Orion vulnerability were published. The BSI also informed potentially affected institutions and companies in Germany and supported their analysis work as needed.

1.6 Distributed Denial of Service (DDoS)

A denial of service attack (*DoS* attack) aims to overload an internet service. A *DoS* is therefore a dangerous type of attack that affects the security objective of availability. While these kinds of attacks have a long history and can affect anyone, protection is available. *DoS* attacks target the availability of services, websites, individual systems or entire networks. When these attacks are carried out simultaneously by multiple systems, they are referred

to as a distributed *DoS* (*DDoS*) attack. Such attacks can be executed from a set of compromised systems assembled into a *botnet*, or from a dedicated cluster of computers set up for this exact purpose by willing participants. Another type of *DDoS* attack is the 'reflection' attack: in this variant, publicly available servers (such as NTP servers) are abused to boost the strength of an attack. As a result, the operators of such servers become unwilling co-perpetrators.

With this kind of attack, considerably fewer systems are needed to achieve the same effect as an attack based on a conventional *botnet*.

DDoS attacks are typically used by cybercriminals to damage specific targets, extort money from their victims or attract attention to the attacker's cause (e.g. a specific set of political demands). DDoS attacks may also be used to conceal other kinds of attacks, or even enable them in the first place.

DDoS attacks have been in use for over 20 years. On 22 July 1999, a computer at the University of Minnesota (USA) was attacked by a network of 114 computers running the program Trin00. This incident is considered to be the first DDoS attack (see the *bibliography*³³).

Since then, DDoS attacks have essentially followed an upward trajectory according to DDoS statistics, which clearly indicate a constant and continual increase in attack numbers, bandwidth and packet rates.

In 2020, for example, the Netscout company first logged more than 10 million DDoS attacks in a single year (see the *bibliography*³⁴). Link11 estimates that roughly 50 million DDoS attacks took place worldwide during 2020 (see the *bibliography*³⁵).

Bandwidth expansion is one factor that has favoured this rise, since it enables the launch of attacks with ever-increasing bandwidth.

The continued advance of digitalisation has also created space for new *attack vectors*. As the following examples show, some of them can be used for DDoS.

One measure deployed to contain the COVID-19 pandemic was the digitalisation of many business processes. In one prominent example, countless companies enabled their staff to continue working from their computers at home. However, implementing this often created situations where personal devices were used to work on sensitive business processes without the same high security safeguards as those offered by company firewalls. The increased use of the public internet significantly enlarged the potential scope of DDoS attacks, including both quantitatively and qualitatively. In some cases, for example, remote access had to be set up ad hoc, or mail servers needed to be made accessible for a short time from the public internet. Despite this theoretically larger scope, the BSI is not aware of any indications that DDoS activities have been more frequent in Germany during the COVID-19 pandemic.

As in other areas of cybercrime, however, an increased use of DDoS attacks to support extortion attempts has been observed. This practice has been known since 2015, when a private email *provider* was rendered temporarily unavailable as a result of a DDoS extortion attack (see the *bibliography*³⁶). The expansion of such kinds of extortion attempts to persistent, global DDoS extortion campaigns represents a specialisation that was first observed during the current reporting period. Alongside the familiar kinds of *ransomware*-based blackmail (see chapter Big Game Hunting with *Ransomware*, page 12), this is a new and alarming manifestation of cyber extortion.

During an extortion campaign observed since mid-August 2020, both domestic and international companies increasingly received extortion emails (see incident DDoS Extortion Attacks, page 34). The attacks targeted companies from a wide range of industry sectors and also included operators of critical infrastructure (see the *bibliography*³⁷). Elsewhere in the world, an extortion attempt made against New Zealand's NZX exchange was reported at the end of August 2020. DDoS attacks led to multiple forced interruptions to trading over a period of four days. An attack on a major Fortune Global 500 company at the end of 2020 also made the headlines worldwide (see the *bibliography*³⁸). (The Fortune Global 500 is an annual list of the top 500 companies in the world ranked by revenue. The list is compiled and published by the US business magazine Fortune.) In Germany, multiple attacks of this kind took place, including one targeting a company in the finance sector at the end of August 2020 (see the *bibliography*³⁹). Payment services were also affected by such attacks, including a series that was launched against payment systems such as Braintree, MoneyGram, PayPal, Venmo, Worldpay and YesBank India (see the *bibliography*⁴⁰).

The continued use of outdated technology (including outdated server technology) also presents additional opportunities for DDoS attacks. This effect is multiplied even further when the potential marks also include the declared targets of politically motivated DDoS attackers or DDoS hackers. In one example from the reporting period, DDoS attacks targeted study platforms that had been deployed to maintain the school education system during the COVID-19 pandemic.

The infrastructure used to operate study platforms in Germany is not at all uniform. Study platforms use backends that vary not only between the individual states, but even within the states themselves. This infrastructure ranges from servers that are sometimes outdated and operated by schools or school authorities to host study platform software, to fully fledged *cloud* solutions for study platforms. *Cloud* solutions in particular have seen very strong growth over the last few months.

The choice of the underlying infrastructure also depends on several parameters, including the funding provided by the education system, the technological equipment and degree of digitalisation found in schools, and each school's technical expertise in handling such infrastructure.

The type of underlying infrastructure on which study platforms are operated results in a variety of risk profiles for *DDoS* attacks.

By their very nature (high-bandwidth connections, administration by technically skilled personnel, etc), *cloud* solutions typically offer effective technological safeguards against *DDoS* attacks that can be supplemented with mitigation strategies depending on the business model at hand. In contrast, however, locally managed and often outdated school servers offer virtually no protection against *DDoS* attacks. Such systems are therefore considered to have a high or very high risk profile for the operation of study platforms. In September 2020, an incident was reported where a 16-year-old pupil from Miami had disrupted online lessons organised by his school, South Miami Senior High, for a three-day period by attacking the servers run by Miami-Dade County Public Schools, which is the fourth-largest US school district. The pupil had used Low Orbit Ion Cannon (LOIC) for the attack – a tool which has not been updated for years. The success of the attack was surprising, since LOIC attacks are assumed to present a low threat potential against target systems configured according to modern standards.

In Germany, study platforms had a very high public profile as a result of their importance in maintaining the states' educational systems under pandemic conditions. Study platforms are also experiencing strong growth in terms of user numbers. The Hasso Plattner Institute (HPI) reported that the HPI School *Cloud* passed the million-user milestone during the middle of Germany's second hard lockdown. The HPI study platform had seen its registered users grow by a factor of nearly 30 since March 2020 (see the *bibliography*⁴¹).

This connection between study platforms and measures taken to contain the COVID-19 pandemic is one reason for politically motivated *DDoS* attacks or hacktivism (in the sense of digital vandalism) that targets such platforms. Experience has shown that the extent to which a target has an established public profile and the degree to which the target is protected by effective security measures are strong sources of motivation to conduct such *DDoS* attacks. On 20 January 2021, the BKA published a warning advisory on the subject (see the *bibliography*⁴²).

Overall, events in the reporting period demonstrated that *DDoS* attacks are an established form of cyber attack whose

threat potential has grown consistently over time as a result of the ever-increasing versatility and resourcefulness exhibited by *DDoS* variants. Accordingly, protective measures must be constantly maintained and updated on a regular basis.

As Germany's Federal Cyber Security Authority, the BSI provides up-to-date and comprehensive informational resources to help prevent and counter *DDoS* attacks, and also publishes a list of accredited *DDoS* mitigation service providers with selection criteria (see the *bibliography*^h).





DDoS Extortion Attacks

Situation

As part of a global DDoS extortion campaign conducted in the third and fourth quarters of 2020, both strategic and technical similarities were often observed in many extortion attempts.

Initial contact would often be made with an extortion email, for example, in which a forthcoming DDoS attack on the contacted company was announced that could only be stopped by a corresponding payment in *bitcoin* (BTC) by a stated deadline. To emphasise the seriousness of their threats, attackers also announced warning attacks that were then indeed carried out. Attacks of this kind were characterised by the use of very high bandwidth (up to 200 Gbps) and also lasted for several hours. If the extortion payment was not made, the perpetrators threatened subsequent attacks with alleged bandwidths of more than 2 Tbps at a later point in time. While these often proved to be empty threats, the attackers behind the extortion attempt on New Zealand's NZX exchange did indeed follow through on theirs. The attacks were based on UDP floods, TCP floods and SYN floods. To maximise the size of the attacks, the perpetrators utilised the reflection/amplification vectors WS-Discovery and Apple Remote Control plus DNS (see the *bibliography*⁴³). Attacks utilising the GRE protocol flood and SNMP flood vectors were also observed (see the *bibliography*⁴⁴).

The campaign subsequently expanded to include other industry sectors. From September/October 2020, several German ISPs reported DDoS extortion attempts. A similar methodology was used in many of these cases, as well. The attackers often started by directing SYN flood attacks against reverse proxy servers. These efforts were then amplified by excessively high packet rates whilst the bandwidth was kept low (approx. 1–2 Gbps). Following this, the attacks were continued with a change in tactics, such as with ACK flood attacks in which the force of the attacks was generated by an excessively high number of requests.

In some DDoS extortion attempts, the threat strategy involved attackers impersonating known APT groups such as Fancy Bear (a.k.a. Sofacy or Sednit), Armada Collective (see the *bibliography*⁴⁵) or Lazarus. The DDoS extortion attackers claiming to be Fancy Bear or Lazarus had already emerged as known perpetrators of DDoS attacks in October 2019. The BSI views this strategy as an attempt to pressure victims into negotiating rather than contend with attacker groups that have been the subject of past reports on investigations carried out by intelligence agencies. The correspondence sent by the black-mailers in 2019 and 2020 used virtually identical wording. Only the *bitcoin* addresses for the payment of extortion fees were different in each case (see the *bibliography*⁴⁶).

There were also differences in the payment models adopted by the groups cited: demands made in the name of the Armada Collective frequently started at five to 10 bitcoins (1 BTC ~EUR 48,000 as of March 2021) and then increased by five bitcoins if the fee had not been paid by the stated deadline. After that, the fee rose by five bitcoins a day. In contrast, demands made in the name of Fancy Bear frequently started at 15 to 20 bitcoins, rose to 30 bitcoins if the deadline expired without payment, and then increased by a further 10 bitcoins a day (see the *bibliography* here⁴⁷ and here⁴⁸).

At the end of January 2021, one of the BSI's European partner agencies responded to an article posted by Radware (see the *bibliography*⁴⁹) by stating that DDoS extortion attackers were again contacting victims who had not met their demands in the past. Radware also published the contents of this correspondence, which began as follows: "Maybe you forgot us, but we didn't forget you. We were busy working on more profitable projects, but now we are back." The messages then continued: "We asked for 10 *bitcoin* to be paid at <bitcoin address> to avoid getting your whole network DDoSed. It's a long time overdue and we did not receive payment. Why? What is wrong? Do you think you can mitigate our attacks? Do you think that it was a prank or that we will just give up? In any case, you are wrong."

Assessment

The BSI itself has not become aware of any such cases of 'payment reminders' being received. However, it cannot be ruled out that DDoS extortion attacks will also experience a comparable renaissance in a national context.

Response

The BSI has informed its client groups in government, business and civil society about the extortion campaign described and recommended countermeasures. In particular, extortion victims should investigate the consequences of possible outages affecting the various components open to attack. In the event of an initial test attack, they should provide advance warning to their IT security service *provider* and report the incident to the authorities.

As a rule, the BSI does not recommend meeting ransom or extortion demands, since this works to legitimise the cyber extortion 'business model' and may motivate further attacks on one's own systems or those of other targets.

**DDoS-Attack on a Belgian Internet Service Provider****Situation**

On 4 May 2021, a *DDoS* attack was launched on a major Belgian Internet service *provider* (see the *bibliography*⁵⁰). The attack started at 11 AM and its impact was substantial. According to press coverage, around 200 organisations suffered at least temporary outages. The ISP's typical customers included universities and research establishments, as well as government institutions. As a result, several parliamentary sessions could not be held because remote participants were unable to connect.

Online services were also affected, such as the Belgian web portal for making COVID-19 vaccine appointments.

According to several media reports, some Belgian politicians tweeted that the attack began at roughly the same time as the Belgian Parliament's Committee on Foreign Affairs was about to hold a session.

The ISP introduced countermeasures and was able to mitigate the excessive traffic targeting its network by around 5 PM on the same day. According to an assessment from the BSI's Belgian partners, the technical aspects of the attack made it harder to counter. Corresponding criminal proceedings were also initiated.

Assessment

The BSI currently has no insights regarding the attackers in question or their motivation. However, political designs cannot be ruled out, since the timing of the attack coincided with the Belgian Parliament's committee session.

DDoS attacks remain a form of cyber aggression that, assuming sufficient resources on the part of the perpetrators, can take individual organisations or (in extreme cases) even ISPs offline at least temporarily and limit their ability to go about their work by flooding them with requests. Typically, the length of time until a disruption is resolved depends on the preparations made by the targeted organisation (e.g. by purchasing *DDoS* mitigation services) and its connection to upstream ISPs. While upstream *providers* can throttle or redirect *DDoS* traffic, this does require the nature of the attack traffic to be characterised as precisely as possible. For this reason, perpetrators (as in this incident) modify their attack tactics – sometimes multiple times. Due to the complex defence strategy this requires, *DDoS* attacks continue to pose a major threat.

Measures

The BSI maintained an ongoing dialogue with its international partners in relation to the attack. This incident, which also affected third parties, was a further reminder that organisations should compare and assess their own *DDoS* mitigation planning, preparation and processes and adjust them when necessary.

The BSI has accredited a number of service *providers* that offer *DDoS* mitigation (see the bibliography: <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister-DDos-Mitigation-Liste.pdf>) (see the *bibliography*⁵¹).



1.7 Attacks in the Context of Cryptography

Cryptographic mechanisms are important building blocks required to include security functions in IT products. State-of-the-art cryptographic algorithms can generally guarantee an excellent level of security in this context. In the Technical Guideline TR-02102, the BSI recommends a series of cryptographic methods and protocols that are generally regarded as secure based on rigorous mathematical cryptanalysis.

The following factors can result in a cryptosystem failing to fulfil its intended purpose in practice:

- Weaknesses in cryptographic mechanisms or protocols
- Implementation errors
- Inadequate protection of side channels
- Weaknesses in key generation

One typical application for cryptography is in securing communication over public networks such as the internet. For trusted integrity-protected channels, various cryptographic protocols are available for which it is commonly assumed that an attacker with network access can neither gain access to the secret key nor decrypt messages or tamper with them without the changes being detected. If these cryptographic protocols are to be effective, their correct implementation must first be assured. In addition, any device behaviour that can be monitored at the network interface (such as error messages or response times) must not result in the disclosure of information about processed secrets. In the reporting period, for example, details were published on a new attack that exploits runtime differences in a cryptographic protocol (see the Raccoon attack sidebar, page 37 (if on a different page)).

When securing cryptosystems that are designed to resist attacks even from perpetrators in physical proximity to the systems, side channels other than runtime (such as power consumption or electromagnetic radiation) must also be considered, since these can also leak information. Side-channel analysis (i.e. the analysis of susceptibility to *side-channel attacks*) is now a separate area of research that besides new countermeasures has also produced new *attack vectors*. One current trend in side-channel analysis and mathematical cryptanalysis is the deployment of methods used in artificial intelligence (see chapter Artificial Intelligence, page 81).

A key prerequisite for the secure use of cryptography is the generation of random numbers that meet certain quality criteria. Among other aspects, random numbers are needed to generate keys. For cryptographic applications, random numbers must not be predictable, nor should they exhibit any kind of exploitable statistical defects. To avoid attacks based on weaknesses in random number generation, the BSI defines random number generator functionality classes in AIS 20 and AIS 31 (application notes and scheme interpretations) for various kinds of use cases. One positive development here is that many products now utilise a physical random number generator that has been certified according to the German Common Criteria scheme (see chapter IT Security Certification as an Instrument for Verifiably Secure Digitalisation, page 64).

However, the guarantees of security offered by many cryptographic algorithms in use today will be invalidated by the availability of a sufficiently powerful quantum computer. The chapter Cryptography (page 83) discusses a number of approaches to countering this threat and presents the BSI's activities in this area.

1.8 Hybrid Threats

The term 'hybrid threat' refers to various kinds of attempts on the part of states and their proxies to exert illegitimate influence, for instance through various types of cyber attacks or influencing public opinion and political will by spreading disinformation and propaganda online or by using economic pressure to achieve political goals. Typically, such activities can encompass several areas or levels of engagement, as well as a broad spectrum of both covert and public methods. The resources deployed in the context of hybrid threats often provide perpetrators with a comparatively simple means of concealing or denying all involvement in both the act itself and the motivation behind it. One example of attacks involving hybrid threats are cyber espionage attacks that illegally capture sensitive data from IT systems with the aim of propagating it later in a harmful and manipulative disinformation or smear campaign. Cyber sabotage attacks may also pursue the goal of causing harm in a specific area – for example businesses, in particular critical infrastructures – and then working to *exploit* the subsequent effects within the information space.

During the reporting period, the digitisation continued to be a decisive catalyst for hybrid threats because it has also led to new potential vulnerabilities for nation states, the economy and civil society. Cyberspace is therefore an especially important domain of any hybrid campaign. It also has a cross-domain function, since it



Raccoon Attack

In September 2020, a team of security researchers and cryptologists drawn from Ruhr-Universität Bochum, the University of Tel Aviv, the University of Paderborn and the BSI published details on a new timing attack targeting the TLS (Transport Layer Security) protocol, dubbed 'Raccoon'. The TLS protocol facilitates encrypted communication between a client and a server, such as between a web browser and a web server on the public internet.

Timing attacks utilise runtime differences in cryptographic implementations in order to draw conclusions about the secrets being processed. The Raccoon attack targets the shared secret that is agreed between the client and server when using Diffie-Hellman (DH) key exchange. For TLS 1.2 and earlier versions, the TLS standard specifies that leading null bytes must be trimmed from the shared DH secret. This design weakness in the TLS specification can, in certain circumstances, lead to a situation where secrets with leading null bytes are processed more quickly than secrets without leading null bytes. A network attacker who observes key exchange negotiations between a client and server can therefore conduct sufficiently precise time measurements to determine whether or not the negotiated DH secret starts with a null byte.

Knowing merely one byte of the shared DH secret is obviously not enough to break the encryption used by the TLS connection. However, attackers can record the TLS connection in its entirety and then use modified versions of the client's public DH key in order to establish connections with the TLS server themselves. If the TLS server reuses its DH key on multiple occasions, this can be used to generate a considerable amount of information about the server's response times, which are also relevant in conjunction with the original TLS connection. A mathematical procedure can be applied to calculate the shared DH secret agreed between the client and server based on these individual pieces of information. This secret can then be used to decrypt the recorded TLS connection.

All in all, the Raccoon attack is a complex kind of attack that can be performed only under a specific set of conditions and with considerable effort. In practical terms, the threat it poses is therefore relatively low. However, the Raccoon attack does identify a vulnerability that should be avoided when developing new protocols.

Neither the latest TLS version (1.3) nor the Diffie-Hellman key exchange using elliptic curves (TLS-ECDH and TLS-ECDHE) is vulnerable to a Raccoon-style attack.

Further information about the Raccoon attack can be found at <https://raccoon-attack.com>.

is often a primary enabler of actions in other domains. Within a hybrid campaign, the physical (e.g. hardware and *firmware*), logical (e.g. virtualisation and operating systems) and informational (e.g. applications and data) layers of cyberspace can all be exploited. During the reporting period, the continuing COVID-19 pandemic demonstrated how perpetrators used cyber attacks and disinformation with the aim of influencing EU vaccine campaigns. In December 2020, the European Medicines Agency (EMA) became the target of one such attack. This resulted in a leak of data related to an ongoing authorisation procedure for a COVID-19 vaccine (see incident Cyber Attack on the European Medicines Agency (EMA), page 41). Leaked documents later turned up on the darknet. Through the selective dissemination of these kinds of stolen information, hybrid actors can attempt to illegitimately influence public opinion while creating fertile ground for the spread of false claims.

Disinformation – that is, the targeted propagation of false and misleading information with the intent to deceive – is a common method used in hybrid threats. In our digitalised world, this increasingly relies on the use of technical and digital tools and channels. Wherever data is stored and processed digitally, IT security also serves to protect this data from unauthorised dissemination ('hack-and-leak' operations). In the case of hack-and-leak attacks, the manipulation of authentic information is also possible. This may include counterfeiting photographs, videos or audio recordings or falsifying the source of certain data (an email or a social network post, for example). The BSI contributes its technical expertise to the identification of these kinds of manipulations.

As the cyber security authority of the Federal government, the BSI furthermore supports operators of critical infrastructure, works towards the improvement of IT security

in the context of elections, maintains a dialogue with operators of social media platforms (as in a recent initiative to develop security recommendations, for example) and works to raise awareness of IT security issues in the general population. The BSI also participates in such efforts at the international level, including in dialogue with the international expert community. As a result, the BSI makes a number of important contributions to strengthen both technical and social *resilience* against hybrid threats.

1.9 Threats to Cyber Security due to the COVID-19 Pandemic

The COVID-19 pandemic has served as a catalyst for the digitalisation of both commercial and social life in Germany. As a result, many companies and public organisations have faced the challenge of needing to conduct more of their business operations and provide more of their services in a digital format. While the rapid introduction of digital tools and working from home opened up new opportunities both for businesses and public authorities, this novel, pandemic-driven situation also created many new possibilities for exploitation by cybercriminals. Even during the very first lockdown in early 2020, the BSI logged a number of cybercriminal attacks that attempted to make the most of the pandemic circumstances as a thematic starting point for *phishing* and other social engineering attacks (see the *bibliography*⁵¹).

This trend continued apace during the past year. Despite the much greater scope for exploitation due to the outsourcing of many activities to remote working setups, however, the BSI did not identify a significant rise in the number of attacks. While many cybercriminals adapted the subject matter of their social engineering attacks to the pandemic, they did not develop entirely new types of attack.

Based on its situation monitoring, the BSI assumes that many of the technical and organisational problems identified at the start of the pandemic in introducing decentralised working practices will continue to exist, such as the availability of a central IT support unit. The BSI therefore assumes that many organisations' degree of exposure to attack will be potentially greater than before the pandemic as a result of their relocating activities to the digital space. Accordingly, the BSI encourages organisations to adopt an approach that does not treat IT security as an afterthought when setting up and operating digital solutions, even on short notice.

Exploiting the pandemic for social engineering attacks

During the reporting period, the BSI observed a broad spectrum of social engineering attacks that exploited the COVID-19 pandemic as a topic (see chapter *Phishing* and other Types of Fraud, page 24). In one example, the BSI recorded instances of websites that impersonated official web portals, with the apparent aim of selling a wide variety of counterfeit products. The goods on sale included those in demand during the pandemic, such as protective equipment and COVID-19 vaccines. In at least one case, an official web portal used to apply for COVID-19 economic relief was faked with the aim of capturing the extensive personal data required to submit such applications (see the *bibliography*⁵²). Data of this kind permits criminals to commit identity theft and impersonate victims for their own ends. Such data can be used to apply for support funds in the victim's name, for example, and then have their payments redirected. These treasure troves of personal data may also be sold by criminals to the highest bidder on illegal marketplaces (see chapter *Malware* and Data Leaks, page 25). To counter this threat, the BSI worked with the Consumer Advice Centre in North Rhine-Westphalia to support the police in their investigations into this kind of fake web portal so that they could be taken offline whenever possible.

Meanwhile, a new threat landscape emerged last year as a result of incidents in which cybercriminals or state-supported actors directed targeted attacks against healthcare companies and agencies. In contrast to the early days of the pandemic, the BSI observed targeted IT attacks related to COVID-19 that were conducted in key areas of the health sector during the current reporting period. These included the attack on the European Medicines Agency (EMA), attacks on foreign vaccine producers, a *DDoS* attack on the COVID-19 vaccine portal operated by the State of Thuringia and a *ransomware* attack on a German manufacturer of COVID-19 antigen tests (see incident Cyber Attack on the European Medicines Agency (EMA), page 41).

An increase in potential targets

Attacks on videoconferences: Conferencing solutions constitute an essential tool in working and studying from home. During the previous reporting period, a range of products for organising conference calls and videoconferences played an increasingly important role in supporting work-related and personal communications. Since systems of this kind must to an extent be connected to over the public internet, they are an attractive and highly accessible target for cyber attacks. The BSI has learned of targeted cyber attacks on certain meetings in which unauthorised parties used credentials

stolen beforehand to gain access to internal sessions for the purposes of espionage or sabotage (see chapter Cyber Attacks on Videoconferences, page 25). The BSI has published recommendations on the secure handling of conference calls and videoconferences (see the *bibliography*^{j)}).



VPN security: Typically, an organisation's network will be kept separate from the public internet and use access points known as network gateways for individual services. These kinds of services may include mail servers or proxy servers for internet traffic originating from the organisation's network, as well as VPN servers. VPN servers play a crucial role in accessing an organisation's network: they are intended to ensure that only authorised parties can access the network from the internet and to enable these users to act as though they were sitting in an office on the organisation's physical premises. In this process, users must first authenticate themselves to the VPN server to verify their identity and rights. The connection between the accessing party and the VPN server is also encrypted as an additional measure. This effectively prevents network traffic being accessed in unencrypted form for the purposes of eavesdropping or manipulation. To enable these protective layers to work as they should, both the VPN solutions in use and the organisation's network architecture must be coordinated with one another. As a result of the occasionally last-minute adjustments required when switching to working from home, this coordination – as well as the secure configuration of VPN solutions and remote solutions for similar purposes (e.g. Remote Desktop Protocol, RDP) – is not always completed in full. This situation is worsened by the fact that these kinds of remote solutions were often the target of exploits by attackers associated with known *ransomware* even before the pandemic. Accordingly, attackers can compromise solutions with poor security at short notice without having to acquire additional expertise. Since the BSI considers remote solution security an important topic independently of the ongoing pandemic, it has contributed a set of recommendations to the Alliance for Cyber Security (see *Bibliography*^{k)}).



BYOD: 'Bring your own device' (BYOD) refers to the use of personal IT devices in a professional context. This may involve using a personal mobile phone to make work-related calls, for example, synchronising personal and work calendars between home and office PCs or using a USB drive provided by an employer to store personal files. Particularly when managing the requirements of working from home, BYOD has always been a very convenient solution for employers and employees alike. At the same time, there are considerable risks involved

in using personal devices in professional settings – especially for company networks. Even in the context of a well-secured company device and a highly resilient company network, an email infected with *malware* still constitutes a considerable threat. If a *malicious* email of this kind is then opened – via a web application, for example – on a personal and less well-secured device, the *malware* will often find a much more favourable set of vulnerabilities on the device. Opening and working with email correspondence, which includes potentially *malicious* spam that targets an organisation's email addresses, is therefore very likely to lead to a much easier and more rapid spread of infection on a personal PC than would otherwise be the case. If this occurs, an attacker will have already taken the most important step in gaining a foothold on the company network. In the process of securing an organisation's network, BYOD solutions present a serious challenge from an administrator's perspective because things like ensuring the proper application of the latest patches to personal devices are very hard to guarantee. For these and other reasons, the BSI updated its recommendations on safeguarding security when working from home during the very first lockdown (see the *bibliography*^{l)}).



Shadow IT: Similar kinds of risks are posed by organisations' 'shadow IT' – meaning devices that are procured by individual departments and therefore not managed by a central IT administration. Shadow IT may comprise test equipment, presentation laptops, laboratory servers or similar sorts of devices. In many cases, there are no clear responsibilities established regarding the setup and management of such devices, particularly when it comes to applying security patches. In some circumstances, the security level of such devices may therefore differ considerably from typical company standards. Furthermore, the degree to which shadow IT devices are present in an organisation is often completely unknown. Shadow IT is thus a risk that is hard to quantify, particularly when people are increasingly working from home.

Internet stability during the pandemic: As a result of extensive remote working and the fact that curfews and other restrictions have led people to spend more time at home, the need for internet capacity – whether for VPNs and virtual meetings or video streaming and online gaming – has also risen. This increased usage has also been registered by ISPs. During March and April 2020 in particular, there were regular reports in the media about a significant increase in internet traffic at both internet service providers and internet exchange points (IXPs). Fears were voiced about the possibility of internet infrastructure becoming overloaded as a result

of measures adopted to contain the pandemic. The BSI has observed and assessed the changing requirements being placed on internet infrastructure. It estimates that, apart from changes in usage types and times, the overall traffic volume has also increased. While this increase in traffic is clearly visible at many internet exchange points, the growth can still be handled by planned capacities. This should dispel concerns about outages as a result of the increased load. In Germany, the impact on the major *providers* of internet access services has been marginal: latencies remain virtually unchanged and download rates have even decreased in some cases. Overall, the internet is well able to meet these increased requirements, especially in Germany. That said, the bottlenecks found in rural areas where no broadband connectivity is available (which already existed before COVID-19) have presumably been exacerbated as a result of the increased need for bandwidth.

Cyber attacks: a risk in pandemic management

As initially discussed, the COVID-19 pandemic has affected every organisation and every aspect of life. In the complex interplay among government, business and civil society, digitalisation in particular is of central importance, as it allows us to adjust to the changing requirements caused by such situations when they arise

with so little notice. Accordingly, digital processes and solutions also have a crucial part to play in managing the pandemic.

This means that cyber attacks present a particularly serious risk to these management efforts. In the modern era of highly interdependent production and complex supply chains, the pandemic has meant that any resource – no matter how small – has become critical. Even a single cyber attack can thus lead to a dangerous domino effect that must be avoided at all costs (see incident Cyber Attack on the European Medicines Agency (EMA), page 41). This is why the BSI calls upon organisations to properly prioritise IT security when implementing short-term modifications to digital processes and procedures.

Outlook

The BSI monitors the IT security situation very closely, paying particular attention to the circumstances and risks discussed above, and maintains a constant dialogue with both national and international partners. This enables it to obtain a comprehensive picture of the current circumstances and adopt preventive measures as early as possible. In the foreseeable future, the BSI expects to see further exploitation of the pandemic in cyber attacks, including those involving social engineering, *phishing* and *spam*.



Cyber Attack on the European Medicines Agency (EMA)

Situation

The European Medicines Agency (EMA) handles new drug applications within Europe. On Wednesday, 9 December 2020, the EMA reported that it had become the victim of a cyber attack. Data stolen during the attack included information about the approval application for the COVID-19 vaccine produced by BioNTech and Pfizer.

The attackers had first gained access to the computer of an employee at a service *provider* used by the EMA. This allowed them to obtain the employee's user credentials at the EMA. With this account, the attackers were then able to log into the EMA network remotely and access its document management system. An extensive search was conducted for documents relating to vaccine development and distribution.

The incident did not impact the authorisation procedure for the COVID-19 vaccine manufactured by BioNTech and Pfizer.

On 8 January 2021, it was discovered that data apparently stolen during the EMA attack had been posted to online forums. The approach taken in publishing this information suggested that the disclosure of the data was intended to raise a number of doubts about the vaccine. The leaked information did not achieve broad dissemination on the internet, however.

Assessment

This attack shows that information about COVID-19 vaccines is of interest to attackers, and that the motivation behind it was not simply a case of industrial espionage. Some of the data taken in the attack was clearly utilised in order to undermine confidence in the vaccine. Whether this was designed to further the attackers' economic interests or some other objective has not been established. However, the public debate in relation to the AstraZeneca vaccine does demonstrate the impact that a low level of trust in a vaccine can have on a corresponding rollout in Germany.

In addition, the incident again underlines the growing importance of the human factor as an Achilles heel targeted in cyber attacks. In this case, for example, two-factor *authentication* was required for service *provider* access to the EMA system, but the user of the targeted client system had stored both factors on the very same system, which undermined the security 2FA is meant to provide. If basic IT security precautions had been properly implemented, the attack could have been prevented, or at least made much more difficult.

Response

The BSI contacted BioNTech as a matter of urgency in order to assess the threat situation resulting from the data leak. As a further measure, all the information provided to the BSI in this context was continuously forwarded to companies and organisations in Germany that play a key role in the development, production and distribution of COVID-19 vaccines.

Since the start of the pandemic, the BSI has worked with departments at the National Cyber Response Centre to identify companies and organisations that are playing a role in combating the pandemic and offer them protection against cyber attacks. A task force has also been set up for this purpose.

The State of IT Security in Germany in 2021: Overview

RANSOMWARE/DDOS

Significant expansion of cyber-criminal extortion methods

New trend

+ 360%
Data leak
pages



Hush money
blackmail



Ransom
blackmail



Protection money
blackmail



13 days

was the amount of time for which a university hospital was unable to admit emergency patients after a *ransomware* attack

144 million

new malware variants

+ 22%

compared to 2020:

117.4 MILLION

AN AVERAGE OF

394,000

2020: 322,000

new
malware
variants
every day

WITH A PEAK OF

553,000

2020: 470,000

TWICE AS MANY

BOTINFECTIONS ON GERMAN SYSTEMS
per day at the daily peak

20,000 > 40,000

98%



of all tested systems were susceptible
to vulnerabilities in **MS Exchange**

14.8 MILLION

reports of malware infections forwarded by the BSI to German network operators, more than
DOUBLE THE NUMBER
 of the previous year

approx.
7 million

2020

2021

44,000

emails containing malware
were intercepted per month
on average in German
government networks

2020 35,000



74,000

websites containing malware
programs were blocked by
web filters protecting
government networks

2020 52,000

Germany among the **TOP THREE**
NATIONS in Common Criteria certificates



5,100

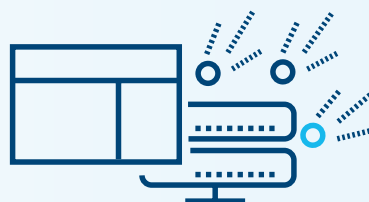
MEMBERS OF THE ALLIANCE
FOR CYBER SECURITY

▶ 2020: 4,400

▶ 2019: 3,700

▶ 2018: 2,700

< 10%



still contained
vulnerabilities in
MS Exchange after
warnings from the
BSI and Microsoft

Overview

Cyber security over the past 12 months

- Agreement between BSI and consumer protection agency
- BSI brings the topic of cyber security into Germany's EU Council Presidency
- Presentation of the Corona-Warn-App
- BSI and VDA work together for more cyber security in cars

- Argentina: *Ransomware* attack at immigration office results in outflow of passport data
- New Zealand: Blackmail attempt via *DDoS attacks* on New Zealand's Exchange (NZX)
- Blackmail attempts via *DDoS* attacks in the financial sector and on payment service *providers*
- Security requirements published for telecommunications networks
- Recommendations for the migration to post-quantum cryptography updated

- Cyber blackmail with sextortion campaign
- BSI and Federal Motor Transport Authority reach administrative agreement on cyber security in automotive sector
- Publication of the Cyberfibel by BSI and the 'Deutschland sicher im Netz' ('Germany safe online') association
- ECSCM: livestream series with the Federal Agency for Civic Education on cyber security, disinformation and *deep fakes*
- BSI publishes 'Guidelines for Your Virtual Event'
- BSI publishes security requirements for online social elections

June

August

October

2020

Global *DDoS* blackmail campaign

July

September

November

- BSI publishes audit specifications for broadband routers
- BSI contributes to European standard for networked smart home devices
- Proof of security deficiencies in telematics infrastructure due to misconfigurations

- Ransomware* attack on a university medical centre in North Rhine-Westphalia
- EvilQuest: malware targeting the Apple macOS operating system
- DDoS* blackmail of Internet service providers (also in October)
- BSI team succeeds at the CHES-Challenge crypto conference
- BSI and EASA work together for more cyber security in aviation
- BSI and ProPK publish Digital Barometer 2020
- Launch of the BSI 'Update available' podcast

- Ransomware* attack on Saarbrücken Airport
- Official cyber security conference for the German EU Presidency by BMI and BSI
- Symposium on digitalisation, cyber security and first-person perspectives in healthcare at University Hospital Bonn
- Cooperation agreement between BSI and Fraunhofer IAIS on joint development of audit processes

- Cyber attack on the European Medicines Agency (EMA)
- Ransomware attack on a major German media group
- USA: APT attack on monitoring provider SolarWinds
- Information Security Guideline agreed as part of the German federal government's IT consolidation project
- Chief Information Security Officer appointed for the German federal government's IT consolidation project
- First version of the Artificial Intelligence roadmap presented at Digital Summit
- Highest average daily increase in new malware variants ever measured: 553,000
- 'Smishing' (SMS phishing) messages sent using the Android malware MoqHao
- BSI organises 17th German IT Security Congress – first to be held digitally
- Publication of the Criteria Catalogue for AI-based cloud services (AIC4)
- Adoption of the German IT Security Act 2.0
- Deep-fake manipulation: successful deception of several European politicians
- EU Commission and 18 other states succeed in integrating online ID function into eID scheme
- Launch of eMergent project for digitalisation in emergency services
- Alliance for Cyber Security reaches 5,000-participant milestone
- Presentation of results of BSI business survey on working from home

December

February

April

2021

January

March

May

- Emotet malware infrastructure smashed
- Cyber blackmail with sextortion campaign
- Bundeskartellamt (Federal Cartel Office) and BSI work together to protect digital consumers
- Draft of the new BSI Standard 200-4 on business continuity management published
- Security update for vulnerabilities on Microsoft Exchange servers
- Cyber blackmail with sextortion campaign
- BSI publishes 'Minimum Standard for Video Conferencing Services'
- Launch of the BMI-BSI campaign #einfachBSIchern ('simply secure')
- USA: Cyber attack (DarkSide) on IT infrastructure of Colonial Pipeline Company
- Belgium: DDoS attack on major Internet provider
- Cyber blackmail with sextortion campaign
- UP KRITIS: 750 organisations now participating in the platform
- IT-SiG 2.0 comes into force

2 Insights and Services for Specific Client Groups



2 Insights and Services for Specific Client Groups

As Germany's Federal Cyber Security Authority, the BSI is working with our country's citizens and businesses, government and public administrations, and international institutions to ensure a secure digital transition. Since its formation in 1991, the BSI has developed into a national centre of excellence for the full spectrum of information security issues. The IT Security Act 2.0 (2021) has once again expanded the remit of the BSI to meet the challenges of the continued advance of digitalisation, which also include establishing the BSI as a centre for digital consumer protection. In this role, the BSI provides support to consumers in evaluating the risks associated with technologies, products, services and media offerings.

2.1 Civil Society

Digitalisation is crucial to Germany's future success as a nation state. The success of this digital transition is strongly dependent on information security, which is something the BSI works hard every day to improve in all areas of our lives. The citizens of our country can thus rest easy knowing that their personal data is in good hands and make secure use of IT to navigate with confidence through our highly networked world. To achieve this, we deploy a comprehensive set of expertise drawn from the areas of prevention, detection and reaction in order to create specific information resources for both groups in civil society and individual citizens.

2.1.1 Insights from the Threat Landscape in Civil Society

The BSI works with the State and Federal Police Crime Prevention Commission programme (ProPK) to ensure that consumers are comprehensively informed about online risks and appropriate steps to protect themselves. This work is based on the Digital Barometer, a representative online survey that has been conducted jointly by these organisations every spring since 2019. The survey collects data on the importance of online security when using the internet as a consumer; the extent to which consumers protect themselves from digital dangers; and how they inform themselves about vulnerabilities, risks and protective measures.

One in four has experienced cybercrime

As in the previous two years, the general rate of cybercrime affecting citizens remained constant in this reporting period, with one in four respondents stating that they had

been a victim of cybercrime online (24%). The commonest experience that respondents reported was third-party access to at least one of their online accounts (31%), followed by a *malware* infection (29%). *Phishing* attempts targeting the disclosure of login or account details affected one-fourth (25%) of victims. While 40 percent of victims of online crime stated they had been affected by online shopping fraud in 2020, the figure for 2021 fell to just 19 percent. In addition, one in 10 respondents reported receiving *phishing* emails on the subject of the COVID-19 pandemic.

As before, the conscious application of protective measures by consumers still offers room for improvement. While the use of antivirus software (62%), secure passwords (60%) and an up-to-date firewall (53%) is now widespread, these figures also show that coverage remains well below 100 percent. At the same time, the number of respondents who stated that they use automatic updates rose from one in four in 2020 to nearly one in three (32%) in 2021. The situation is similar with two-factor *authentication*, which had been activated by a third of respondents (33%) in 2020 and has risen slightly (to 40%) in 2021.

Response to security recommendations

Around two-thirds of the respondents (67%) are familiar with security recommendations on how to protect themselves against online crime (65%), with 37 percent implementing such recommendations at least partially and over one in 10 fully (12%). Those who are aware of security recommendations but have not implemented them (12%) stated that this would require too much effort, or that the recommendations were too complicated to understand.

A large portion of the respondents (40%) stated that they read up on internet security once in a while, but over one in five never do (22%). For many of the respondents, security in online banking (88%) and online shopping (67%) is especially important, as is security in relation to *cloud* services (66%). While a third of the respondents know about the BSI's information services about protecting themselves against online crime, a significant number of them (43%) stumbled on this information rather by accident.

'What to do in an emergency' a key need

Most victims of cybercrime stated that they had sorted things out themselves. This also tallied with their need for information: most of those affected needed a checklist of steps to take in an emergency, while others wanted a

website with explainer videos or a person to contact at the police in such cases. There was also a general interest in information services addressing online security as a specific area of concern. This topic was raised by over half of the respondents, who cited identifying internet crime (57%) and protecting sensitive data (48%) as key points of focus. This group was also interested in recommendations on software offering such protection and what to do as a victim of online crime (each at 48%).

2.1.2 Digital Consumer Protection

Consulting health apps to obtain information, an analysis of physical parameters or personal motivation is a growing trend that has only strengthened due to the COVID-19 pandemic. However, these apps need to offer a high level of IT security to appropriately protect users' personal health data. In December 2020 and January 2021, the BSI examined a number of health-related apps on Android and iOS that are not medical devices and/or not listed in the official German directory of Digital Health Applications (DiGA). Apps were analysed from the categories of chronic illness management, fitness, nutrition, and relaxation and mindfulness.

The market segment in question is characterised by very dynamic growth and a rapid pace of technological progress and innovation. More importantly, however, the study results show that these apps have significant shortcomings in terms of IT security.

The basic principle of *security by design* was only accounted for in some parts of the development processes followed by the 84 app providers considered. A lack of processes for updates or for handling published vulnerabilities went hand-in-hand with a failure to properly implement technical and organisational measures. Specific test categories in an analysis focusing on the IT security level (see fig. 6) of seven selected apps highlighted other risks, including the transfer of passwords in plain text [see chapter Theft and Abuse of Identity Data, page 24] and inadequate protection against interception, eavesdropping and manipulation attacks on communication content transferred between the apps and the respective providers' cloud backends.

Alongside raising awareness of the potential risks involved in health apps, a better level of protection for consumers in this market can only be ensured by providers that take action to significantly increase the level of IT security offered by their apps. [Source: www.bsi.bund.de, <https://www.bsi.bund.de/TR-3161>] The full analysis and detailed results of the study 'IT Security in the Digital Consumer Market: A Look at Health Apps' can be accessed here (see Bibliography^m).

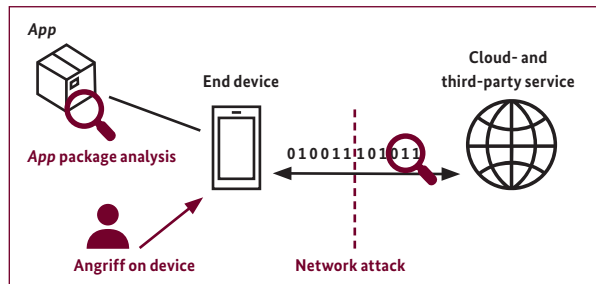


Fig. 6: Test categories in the IT security analysis

2.1.3 IT Security Mark

In passing the IT Security Act 2.0 (which entered into force in 2021), the Bundestag and Bundesrat paved the way for Germany's introduction of the IT Security Label. This label is intended to make the IT security properties of consumer products more visible, while also establishing IT security as a product feature that is relevant for consumers.

BSI experts have developed the internationally recognised Technical Guideline for broadband routers (BSI TR 03148). Further, BSI was involved in the specification of European Norm ETSI EN 303 645 which defines requirements for a minimum level of Cybersecurity for all consumer *IoT* devices (see chapter Security in the Internet of Things, Smart Home and Smart Cities, page 50).

The IT Security Label will subsequently be extended to products in the field of consumer *IoT*. Starting with routers. Generally, the security label is also applicable for web services.

By applying for the right to use the IT Security Label on their products, manufacturers will officially and formally confirm to the BSI that their product complies with a technical standard, which is intended for the corresponding product group, or web service. Using the documents submitted, the BSI will check each manufacturer's declaration for completeness and plausibility. Product-specific (technical) audits, which are required for certifications in line with other BSI Technical Guidelines, will not be conducted as part of the IT Security Label application procedure.

Once manufacturers have successfully completed the application procedure, they will be authorised to display the IT Security Label on their product packaging. A QR code and short link will be provided as a quick and simple way for consumers to access the most recent product-specific security details on a BSI website. The provided information includes e.g. the length of time for which the manufacturer will provide updates for the product and if there are any known vulnerabilities.

Once the IT Security Label is in use by the manufacturer, the product in question will be monitored by the market surveillance of the BSI, which means that the BSI will provide notification of any known product vulnerabilities on the respective product page and will get in touch with the manufacturer in such cases.

With the support of companies that have understood the importance of consumer protection and information security as a key criterion for their own business, the IT Security Label will work to improve the overall security and transparency of products offered on the consumer IT market. In the future, the BSI will work to have the IT Security Label incorporated into a binding, pan-European labelling system.

2.1.4 Educating and Raising Awareness Among Consumers

At regular intervals, the BSI informs consumers about recent developments and topics in relation to baseline protection, highlights risks and makes recommendations about day-to-day IT security so that all citizens can act securely and independently when using networked information systems.


At the start of the reporting period in summer 2020, particular attention was given to the question of how secure digital participation can be enabled during the time of the COVID-19 pandemic and the resulting absence of face-to-face meetings. To this end, the BSI posted a series of articles on its website aimed at designing a secure daily routine involving videoconferences or other digital communication formats. The guideline for virtual events that was developed in October 2020 also offers clubs and voluntary workers advice and assistance on questions relating to cyber security.

From autumn 2020, the BSI worked with the Federal Agency for Civic Education on a three-part live streaming series as part of European Cyber Security Month. Experts discussed topics such as cyber security, disinformation and deep fakes. With a nod to the US presidential election, those watching the live stream also learned more about the topic of 'truth and relevance in the digital space'.

Cyber security

In the services it offers to consumers, the BSI focuses on the current issues and requirements faced by ordinary citizens. Its numerous informational services provide regular updates on baseline protection for hardware and software. This is important work: according to the Digital Barometer (see chapter Insights from the Threat Landscape in Civil

Society, page 47), important baseline protection measures are still not being deployed to the full by all internet users. As a result, one in four citizens have already been a victim of online crime.

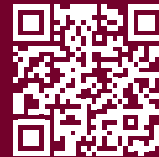
- The website [bsi-fuer-buerger.de](https://www.bsi-fuer-buerger.de) has been a part of the new consumer area of the BSI website (<https://www.bsi.bund.de/VerbraucherInnen>) since February 2021. Visitors are provided with a comprehensive overview of all the key topics within cyber security, as well as recommendations for digital day-to-day life (see *Bibliography*ⁿ). 
- The free warning and information service Bürger-CERT offers technical warnings and the fortnightly newsletter 'Stay Secure · Stay Informed'. The BSI uses the service to announce vulnerabilities and recent incidents, and to offer corresponding tips. Around 112,000 people are currently subscribed to Bürger-CERT.
- The BSI posts regular updates and recommendations on its consumer-focused social media profiles on Facebook (around 43,700 subscribers) and YouTube (around 3,000 subscribers). The explainers and animated videos on YouTube were viewed for a total of around 700 hours during the reporting period. Topics such as security updates, information on critical vulnerabilities and the 'Update Available' video podcast were especially successful.
- A BSI service centre handles user enquiries on the topics of IT and internet security. It can be contacted by calling 0800 2741000 or by sending an email to mail@bsi-fuer-buerger.de.
- In April 2021, five brochures that explain how consumers can stay safe while using the internet, smartphones, tablets and other devices, social networks, cloud services and the Internet of Things were redesigned with updated content. These brochures are available as downloads from a corresponding website, and free print versions can also be ordered.
- The 'Cyber Primer' was launched in October 2020. This reference work is for people working in consumer counselling or public information services. The Cyber Primer brings together information on digital environments and recommendations on basic skills in relation to IT security, and also serves as a basis for workshops or individual consultations. The product was developed jointly with 'Deutschland sicher im Netz' ('Germany safe online', DsiN).

- Since October 2020, the BSI podcast 'Update Available' has appeared at the end of every month on popular online platforms. It discusses current incidents in non-technical language from a consumer

perspective. The topics covered so far have included deepfakes, healthcare security, secure remote schooling and account protection.

i CIS/IT campaign

On 22 March 2021, the BMI and the BSI launched their joint awareness and information campaign on IT security for consumers under the hashtag #einfachaBSIchern (#simplysecure). The aim is to increase consumers' awareness of online risks while also improving their skills in dealing with them. On the corresponding website (<https://einfachaBSIchern.de>), visitors can learn more about topics such as secure email communication, smart home security and secure online shopping (see *Bibliography*⁶).



2.1.5 Security in the Internet of Things, Smart Homes and Smart Cities

Networked devices from the *Internet of Things (IoT)* are taking on an increasingly important role in the design of the digital future, including for consumers, industrial entities, and other types of businesses. The number of households that have installed smart IoT products is rising fast. According to the latest Digital Market Outlook from Statista (see the *bibliography*⁵³), the number of smart homes in Europe will already pass the 60 million mark in the coming year. Since IoT components also present risks to privacy, information security and cyber security, they also intensify the corresponding threat situation. Furthermore, this trend is being accompanied by a rise in *malware* variants, among other developments (see chapter *New Malware Variants*, page 11).

The BSI believes urgent action needs to be taken to reduce the proportion of products that are affected by security holes (see chapter *Botnets*, page 19). Here, prevention is a key area that needs to be addressed, including by new standards.

In this context, EU-wide initiatives focused more strongly on the cyber security of network devices in the reporting period. This topic duly became the subject of several conclusions adopted by the European Council, particularly during the German European Council Presidency in the second half of 2020.

A European approach to strengthening cyber security has the advantage of raising the security level of IoT products throughout the European Single Market in line with European values to make a valuable contribution to a global challenge.

"The Council of the European Union [...] notes that the increased usage of consumer products and industrial devices connected to the internet will also raise new risks for privacy, information- and cybersecurity [...]. Cybersecurity and privacy should be acknowledged as essential requirements in product innovation, the production and development processes, including the design phase (security by design), and should be ensured throughout a product's entire life cycle and across its supply chain. [...] [The Council] acknowledges that the certification of connected devices would require relevant norms, standards or technical specifications for cybersecurity evaluations under the CSA [...] and recommends strengthening efforts undertaken by European Standards Organisations in this matter. At the same time, [the Council] notes the ETSI EN 303 645 cybersecurity standard for consumer IoT devices as an important step in this direction."

In this sense, the BSI's engagement in the creation of ETSI EN 303 645 and the corresponding test specification ETSI TS 103 701 (whose completion is expected in the second half of 2021*) is laying key groundwork for the establishment of European certification schemes and the improvement of cyber security in Europe.

The Internet of Things is not merely limited to consumer IoT devices, but also encompasses devices deployed within public IoT. Public IoT plays a decisive role in digitalisation, especially in municipal public services (e.g. in connection

with smart cities). The dramatic rise in *malware* variants and infected devices is also having an impact on this sector.

Within these digital transformation processes, the consumer sector faces comparable basic technological challenges. However, local governments have a responsibility to their citizens to provide a basic set of public services and must therefore make every effort to avoid risks or threats to public welfare. Such efforts therefore need to support the establishment of an appropriate level of cyber security in digital infrastructure. To achieve the goal of operating secure *IoT* infrastructure while accounting for underlying risks, both local governments and participating businesses need standards and recommendations for action. The BSI maintains a close dialogue with proactive local authorities to help design and ensure IT security.

2.1.6 Security of Medical Devices

Attacks on institutions in the healthcare sector (see the *ransomware* attack incident targeting a university medical centre in North Rhine-Westphalia, page 15) and vulnerabilities in health apps can have far-reaching consequences, and may even pose a serious threat to the health of patients. A related project, 'ManiMed – Manipulation of Medical Devices', started in early 2019 and concluded in December 2020. The project aimed to represent the cyber security situation in relation to networked medical devices currently available on the German market as realistically as possible by applying in-depth tests focused on IT security. Overall, the project identified more than 150 vulnerabilities in 10 products across five categories (implantable pacemakers, defibrillators and their accessories, insulin pumps, ventilators, patient monitors and infusion pumps), as well as in their associated infrastructure.

Most vulnerabilities affected the accessories or the infrastructure components, but not the actual medical devices themselves. This shows that any such analysis must look beyond individual components and consider the overall medical device ecosystem. In addition, vulnerabilities are generally dependent on a product's specific operating environment. In the event of a vulnerability, the manufacturer must evaluate and prioritise the necessity, feasibility, and cost-effectiveness of addressing it. The vulnerabilities identified were communicated to the respective manufacturers in the course of the project and can be grouped roughly into three categories.

Configuration errors, for example, include the disclosure of information such as software version numbers or the use of default accounts for *authentication*. In many cases, the vulnerabilities discovered involved the use of

outdated software. These types of vulnerability are typically fairly simple to resolve. However, one basic problem is that while such fixes can generally be implemented quickly and appropriately, basic security mechanisms or configuration models are often entirely lacking.

The large number of vulnerabilities identified confirms previous research in this field and clearly highlights the need for improvement in the IT security of medical devices. In the future, manufacturers in this field should follow the principle of 'secure by design'. In addition, the IT security of complex ecosystems should be investigated regularly as an overall system through in-depth testing and analysis.

The ManiMed project has provided an overall view of the state of security in networked medical devices. Several follow-on projects are planned that will offer a more detailed look at other sub-areas that were evaluated only superficially by the ManiMed project.

One such endeavour – eMergent, which is specifically analysing digitalisation in emergency services – already began on 12 April 2021. In this project, the focus is on ground-based, mobile medical devices and record-keeping systems that are not able to access a secure infrastructure. These devices are therefore subject to requirements such as a robust design, accessibility for personnel with modest IT skills and high availability. The eMergent project aims to provide a situation report about an area of healthcare digitalisation that has not been the subject of much research thus far and identify both opportunities and challenges where the BSI could contribute to enhancing IT security.

2.1.7 Corona Warn App

The Corona Warn App (CWA) is an important part of the digital toolbox for pandemic management. The BSI has conducted security assessments of the *app* since its development began. It is also providing support for the ongoing development of the *app* in the form of penetration tests and code reviews, which take place on a fortnightly basis and last for seven days. All *app* development is fully documented and utilises a publicly accessible source-code management system hosted on GitHub. The BSI also uses GitHub to report any identified vulnerabilities to the developers. Since the CWA was released, numerous enhancements, such as a contact diary and event registration, have been provided in a process closely coordinated among the BSI, RKI, Deutsche Telekom and SAP. The *app* has also been harmonised with the overall EU system, as well as with the system used in Switzerland. The enhancements have extended the functional scope offered by the

*Until the publication of ETSI TS 103 701, public drafts can be viewed at http://docbox.etsi.org/CYBER/CYBER/Open/Latest_Drafts

CWA and resolved identified vulnerabilities. Thanks to the activities of the BSI, over 70 security vulnerabilities were identified within the space of a year.

2.1.8 eHealth and Telematics Infrastructure

The digital transition in healthcare has proceeded rapidly from 2020 to the present day, especially with regard to applications of the Telematik Infrastructure (TI). The last 12 months have seen the launch of the Electronic Patient Record (ePA), the Health Insurers' Frontend (FdV), Emergency Data Management (NFDm) and Safety in Drug Therapy (AMTS) in Germany. Progress has also been made on E-Precription (E-Rezept), and the interplay between Telematik Infrastructure and digital healthcare/nursing apps, as well as on implants and EU-wide collaboration on emergency services. Ancillary service providers such as nursing staff and midwives will also soon be included.

This wealth of new use cases requires a redesign of the Telematik Infrastructure, which is reflected primarily in the current draft of the German Act on the Digital Modernisation of Healthcare and Nursing (DVPMG) and in gematik's plans for Telematics Infrastructure 2.0. Throughout all these various developments, the BSI is providing consulting, testing and security certification services to civil society, government and business, while also representing their various interests. The current release (4.0.2, available from the gematik extranet) provides 93 specifications, 15 models and 95 summaries that were created with the BSI's support.

Meanwhile, a change in mindset is needed with regard to documenting how secure specific applications of Telematik Infrastructure are. The certification processes still in use today for the Konnektor (such as the current certifications for product type version 4) offer only limited applicability for smartphone applications such as the Health Insurers' Frontend. As a result of the sheer variety of operating system versions and frequent updates to both apps and operating systems, established testing mechanisms now face major obstacles. In response to this need, the BSI has issued the 'Health Insurers' Frontend - Electronic Patient Record test specification' (see the *bibliography*⁵⁴), which defines an alternative test procedure tailored to the app in question.

The original approach to ensuring the security of the Telematik Infrastructure is essentially based on a secure network in which service providers interface with the Telematik Infrastructure by means of a Konnektor (comparable to a VPN) without any other form of internet access. This resulting environment is inherently secure and protects providers from unauthorised external agents. Despite this high level of security, there were a number of potential or actual vulnerabilities:

- The Telematic Infrastructure offers multiple ways to connect (see the *bibliography*⁵⁵). Many service providers do implement a serial connection as recommended by gematik. Here, the service provider's network is connected directly to the certified Konnektor, which can therefore offer a high level of protection thanks to its firewall and other integrated security functions. Instead, operation-in-parallel is often used, meaning the Konnektor (just like any other IT device used at doctor's practices) is plugged into a router that is connected directly to the internet. This type of operation is envisaged for major IT-service providers with their own security mechanisms and does not offer any integrated protection from attacks originating from the internet.
- Closely associated with the above were security deficiencies due to misconfiguration that security researchers announced in July 2020 and also presented at the Chaos Communication Congress in December 2020. The researchers demonstrated that admin interfaces of some Konnektoren could be accessed over the internet.
- In the middle of 2020, a configuration error occurred that caused disruptions in Insured Master Data Management (VSDM) in Konnektoren from a number of manufacturers (see the *bibliography*⁵⁶). VSDM is required in order for patients to identify themselves as insured to their doctors with the help of their electronic health insurance cards (eGK). In particular, the affected connectors' inability to connect to the Telematik Infrastructure made it impossible to compare patients' data against online data repositories. While the infrastructure itself was not at risk, its availability in doctors' practices was nonetheless restricted.
- In December 2019, deficiencies in the supply chain for HBA and SMC-B security cards were presented at the Chaos Communication Congress (see the *bibliography*⁵⁷). While these weaknesses applied to organisational processes outside of the actual IT systems themselves, any exploit that targeted these weaknesses would nonetheless have posed a direct risk to information security.

The TI's redesign in Telematik Infrastructure 2.0 involves a number of major interventions into its security architecture, which in turn require rethinking and reassessing many related issues. This is another area where the BSI will work to ensure the development of an optimal solution.

The following key pillars of IT security have already been identified:

- At minimum, the previous security level will be maintained.
- Protective mechanisms will be defined as part of a global consideration of processes and systems by means of appropriate security and risk analyses.
- Devices used to process medical data must be provided with an appropriate level of security (use of a Secure Element, for example).
- Cryptographic security must be based on a hardware trust anchor under the sole control of the data owner.
- All communication channels must be encrypted and use mutual *authentication*.
- All users must be authenticated using two-factor *authentication* with a high assurance level.
- A suitable alternative must be provided for users who are unable to guarantee the required level of security on their own devices.
- The transition from TI 1.0 to TI 2.0 must follow a migration plan in which all the interim states fully uphold the security level.

Together, eHealth and the introduction of Telematics Infrastructure 2.0 remain key drivers of the interplay among service *providers*, health insurers, patients and other stakeholders. Only through continuous change can the digital transition in healthcare keep pace with the IT security landscape.

2.1.9 Security Models for Virtual Meetings and Voting Systems

The COVID-19 pandemic has led to a situation where many meetings, voting sessions and elections have not been possible during in-person events. As a result, there has been a sharp rise in the demand for virtual alternatives. Alongside practical questions regarding things like the technical handling of videoconferencing software and data protection issues, a key focus in this transition has been on information security. How can virtual events be designed with this in mind? What aspects need to be considered to ensure that information can be transferred and exchanged securely? What risks arise and which requirements apply in cases involving confidential voting? In dialogue with the interested public, the BSI early on drafted guidance for all the relevant

client groups in government, society and business. On this basis, it also advised the German Bundestag and various political parties on the secure organisation of virtual party conferences and voting (see *Bibliography*^p).



Online elections

Online elections present an even more complex situation. As part of a pilot project, German health insurers will be offered the opportunity to conduct online elections alongside the traditional practice of postal voting for the social elections scheduled for 2023. Electors will therefore be able to choose between casting their vote online or postal vote. In Technical Guideline TR-03162 (IT Security Requirements for Conducting an Online Election for the Pilot Project According to Section 194a of Book V of the Social Code (Online Elections)), the BSI has set out specifications for information security and thereby created an important basis for the secure digitalisation of the 2023 social elections. This directive also includes cryptographic requirements that are intended to ensure that the basic election principles can be upheld (see the *bibliography*⁵⁸). While this project was initiated independently of the COVID-19 pandemic, it has now taken on a more important role in light of the current situation. Accordingly, the BSI is now also investigating options for ensuring the secure digitalisation of other non-political elections (see *Bibliography*^q).



Information about the cyber security of Bundestag and state parliament elections can be found in the corresponding section which starts on page 74.

2.1.10 Security of Payment Methods

Strong customer *authentication* (SCA) for payments made with digital or physical cards at the point of sale (POS), for transactions at cashpoints or for payments in e-commerce has been standard practice for some years now. Chip cards used in combination with a PIN or the combination of a digital card and a biometric factor (such as a fingerprint) are now used on a day-to-day basis almost without afterthought.

In contrast, the introduction of SCA specifically for credit card payments made for online purchases was continually postponed or not yet made mandatory in all cases because its integration with shop systems and banking communications raised a number of problems. In the case of many online purchases, errors made in implementing security features resulted in credit card payments being rejected and transactions being cancelled. Customers thus looked for shops that did not require additional factors, or even switched to other payment methods.

In the meantime, 3-D Secure has become the security standard that must be implemented to accept credit card payments online.

The 3-D Secure procedure is suitable for use both on the web and in mobile apps. For *authentication*, the procedure makes use of biometric interfaces such as fingerprint scanners or facial recognition.

The data stored on the credit card itself is exchanged only between the bank and the 3-D Secure website; the merchant is not given access to this information.

While customers must register with their bank before being able to use 3-D Secure, they do not incur any additional costs. The BSI considers this procedure more secure than simply entering the data displayed on a credit card. In addition, fraud is made more difficult because customer *authentication* does indeed take place (see *Bibliography*⁵⁹).



2.1.11 Two-Factor Authentication

Even today, password entry is far and away the commonest form of authenticating oneself to an online service. In this scenario, users are required to provide just one *authentication* factor. While passwords are simple to implement, they have disadvantages. First of all, only this single factor needs to be known to circumvent the *authentication* mechanism. Second, it takes a great deal of effort to select a secure and individual password for each service.

As a result, an increasing number of services now require a second factor, such as an *authentication* code that is sent to the user's phone. However, this approach only improves the level of security if the devices in question are actually physically separate and the factors cannot be attacked simultaneously. If a smartphone application were to use a password, for example, and a code sent to the phone as a second factor, both of these factors could be intercepted by *malware* on the smartphone, making the system insecure. Other usability problems can also arise, such as when users switch to a different phone or change their mobile phone number.

A more advantageous approach is to request two factors from different categories (possession, knowledge and biometrics) as part of two-factor *authentication*. Combining the strengths of these individual factors makes attacks much more difficult. In the process, biometric features should be used locally and not stored with an online service.

As a member of the Fast Identity Online (FIDO) Alliance, the BSI is involved in the definition of verifiably secure *authentication* tokens. Proof of a high level of security can be provided

by Common Criteria certification. Following the successful certification of a FIDO U2F token of its own design, the BSI published a protection profile of this kind with a high test depth for secure FIDO U2F tokens. This token fits seamlessly into existing web infrastructures, since physical possession of the authenticator is proven in the second step by means of successful password *authentication*. Without testing and related security certification, there is a real risk of implementation errors being overseen. Certification according to the FIDO security standard will also be available soon (see *Bibliography*⁶⁰).



2.1.12 Assessment of electronic identification procedures

Contact restrictions introduced due to COVID-19 have underlined the need to digitalise public administration at the federal and state levels. To create a digital interface between citizens on the one hand and public officials on the other, the Online Access Act (OZG) adopted in 2017 also establishes a legal requirement to offer online access to public services by the end of 2022 (see chapter Implementation of the Online Access Act, page 78).

This new digital state of play for public services can only come about if citizens and businesses alike are able to identify and authenticate themselves in a user-friendly and secure way at the online interfaces to these services. Accordingly, both citizens and companies must be able to place their trust in suitable and secure access solutions for public services in the digital space.

Through the establishment of a federated portal network and user accounts (see the *bibliography*⁵⁹) at the federal and state levels to implement the OZG, digital federal cooperation is simultaneously being advanced in Germany. The BSI assesses both the underlying technologies and specific implementations to minimise any associated risks (resulting from identity theft, for example) for government, business and civil society.

It has also published two Technical Guidelines that enable the systematic appraisal of procedures for electronic identities and trust services for online processes. TR 03107 1 covers assurance levels and mechanisms for electronic identities as well as trust services in e-government, while TR 03147 complements this with procedures for confirming the identity of natural persons. Assessment processes are differentiated according to the assurance levels 'Normal', 'Substantial' and 'High'.

To date, the BSI has assessed two procedures from the private sector; in the reporting period, assessment also started for two other electronic identification procedures. For the BMI,

this technical assessment process offers a basis on which it can decide whether to approve the use of a given procedure within e-government.

Of particular interest here are procedures that are able to achieve at least the assurance level of 'Substantial' as defined by TR-03107-1. Suitable procedures and established assessment criteria are available for the cryptographic algorithms and protocols required. Meanwhile, assessing the level of assurance at interfaces to the analogue world or in cases of media discontinuity is a more complex issue. This is often the case during the initial identification or registration of individuals for electronic identification procedures. In addition to procedures in which ID documents are still presented conventionally in person, video-based procedures are frequently used where individuals are filmed holding their ID documents and thereby verified. The BSI is also collaborating with the Federal Criminal Police Office to evaluate whether the video-based verification of ID documents can also achieve the assurance level of 'Substantial'.

2.1.13 Secure, Smartphone-Based Electronic Identities

More and more of our daily routines now take place in the digital space, and smartphones are used to access many services. Users require a digital identity to use everything from online banking and shopping to digital public services and social networks. To ensure these identities can be used securely on phones, the German federal government is making further improvements to the country's online ID card. The new Smart eID, which is based on Germany's personal ID card technology, facilitates the secure storage of identity data and the secure use of services involving sensitive data, even on a smartphone.

To be able to use many online services, citizens require an electronic identity (eID) – an umbrella term that can be used to refer to a wide variety of online accounts:

- A pseudonym in online forums
- A profile in social networks
- A customer account in an online shop
- An account holder in online banking

Each of these eIDs must be protected against abuse, and the protection required will vary according to the type of electronic identity in question. In some cases, simple login credentials (i.e. a username and password) are all that is required. This is insufficient protection for sensitive data, however. An eID with a better level of protection should be

used by those wishing to conduct banking on their phone or control access to company premises, for example.

Introduction of Smart eID

As with any networked device, smartphones are continuously exposed to the risk of a cyber attack. Accordingly, particular requirements must be fulfilled in order to ensure that eIDs are stored securely on smartphones.

The basis for Smart eID is an eID applet that may only be executed within a security component located on the user's mobile device. The security component is a dedicated chip that is optimised for the secure storage of cryptographic keys and the secure execution of cryptographic operations or applications. It can be implemented on mobile devices either as a Secure Element (SE) or by a permanently installed SIM card, which is often referred to as an eUICC or eSIM. The applet itself is based on established cryptographic protocols that are already deployed as part of the electronic personal ID card. This has the advantage of ensuring that Smart eID is compatible with services that already offer online ID card functionality.

The next step is to ensure that the eID applet can be utilised and installed only on Secure Elements that offer an appropriate level of security. To this end, the Trusted Service Manager (TSM) is being used to create a non-discriminatory infrastructure that is accessible to all *providers* of secure applets and meets the very highest security and data protection standards. As an interface among the ID card issuer, mobile device manufacturers and end customers, the TSM is tasked with validating the suitability of the Secure Elements on mobile end devices and securely installing the eID applet on these devices. To achieve this, the BSI is involved in the standardisation of the necessary components, interfaces and processes so as to ensure that the technology developed can be made available to as many mobile devices and end users as possible.

Before Smart eID can actually be used, the eID applet must ultimately be furnished with valid identity data from the end user. This is enabled by a service in which the user utilises their personal ID card's online *authentication* function to read the data from the card and have it stored in the applet, where it can be verified and protected against manipulation.

The BSI is acting as a technical project manager for contractors who are working on the implementation of Smart eID, and it is also supplying security specifications in the form of Technical Guidelines and protection profiles. In a parallel process, the BSI has talked to many mobile device manufacturers and contributed its expertise to a large number of standardisation bodies. These activities were

pursued with the goal of raising awareness among manufacturers about security requirements for smartphones, tablets and wearables, as well as anchoring the BSI's own requirements within international standards. A set of appropriate, mandatory standards is the only way to establish an environment where any buyer of a mobile device is able to obtain the security functions they need in order to protect their eID. Smart eID will be rolled out to the first smartphone models in the autumn of 2021.

2.1.14 Biometrics in the Age of Artificial Intelligence

A 'medial identity' is understood to refer to an individual present within a digital medium who can be identified by biometric attributes such as their face or voice. Methods for manipulating these kinds of medial identities have existed for many years now. Through the application of techniques from the field of artificial intelligence (AI), however, it has become significantly easier to create high-quality fake identities with comparatively little effort or expertise. Due to the utilisation of deep neural networks, such techniques are conventionally referred to as 'deepfakes'. With the help of such techniques, it is possible to replace the face of someone shown in a video with the face of another person (face swap) or exchange the voice on the audio channel with a different person's voice (voice conversion). The procedure used to achieve a face swap is sketched out in figure 7. The person intending to create a *deepfake* will need material (such as video or audio recordings) from the person whose identity is to be faked.

With the help of this procedure, even a layperson with moderate technical skills can manipulate medial identities for the purposes of bypassing remote identification systems, perpetrating defamation or fraud (especially *CEO fraud*) or simply creating 'fake news'. In April 2021, a case became known in which several European politicians had been fooled by a *deepfake*: in a videoconference, these politicians believed that they were talking to Leonid Volkov, a confidant of Russian opposition leader and Putin critic Alexei Navalny, only noticing some time later that the person they were talking to was in fact someone else (see the *bibliography*⁶⁰). The case marked a milestone in the quality of deepfakes, which must now be countered by appropriate detection technologies and defensive measures.

Current developments in the field of medial identity manipulation are focused on optimising the quality of the results obtained and reducing the number of data items required about the target individual. This work is typically conducted by academic institutions, including with

corporate funding in some cases, although the resulting software is typically not published. In the future, however, it can be assumed that methods will also be available to the general public with which high-quality fakes can be created in real time without any obvious artefacts.

AI is also an important basis for countermeasures to the counterfeiting of medial identities. That said, one problem with many of these strategies is that they return good results for a specific usage scenario, but often respond poorly to changes in general conditions, such as a change in manipulation method.

Procedures for the manipulation of medial identities are being enhanced all the time. Accordingly, countermeasures must also improve to keep pace. The BSI tracks the development of these attack strategies to better estimate the kinds of real-world attack they could enable. Ultimately, this also permits the development and recommendation of countermeasures that are in line with current research.

2.2 Industry

Networking and the exchange of information are key economic factors in Germany. At the same time, the economy also depends on a functional and secure IT infrastructure. This is especially true for the operators of critical infrastructure (CI). The BSI therefore monitors

Sources: J. Naruniec et al. High-Resolution Neural Face Swapping for Visual Effects, EGSR 2020, 39, 4 (2020)

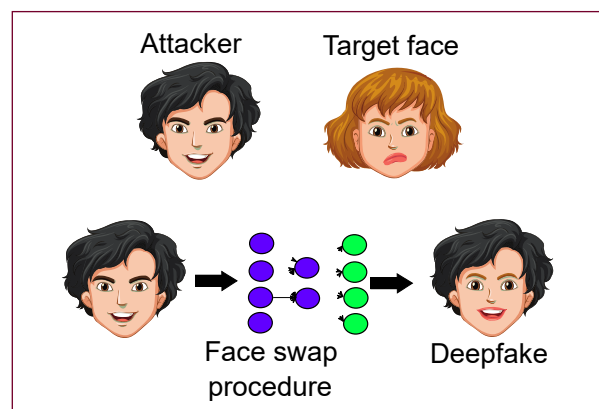


Figure 7: During a face swap, the face of a target person is used to replace that of an attacker. The technique also attempts to retain the facial expressions of the attacker.
Source: brgfx / Freepik

the situation to determine whether the corresponding protective measures are adequate while also creating the environment needed to improve these types of infrastructure. Through the Alliance for Cyber Security and its current membership of around 5,000 institutions, the BSI is also helping to strengthen Germany's *resilience* against cyber attacks. Small and medium-sized businesses in particular benefit from the exchange of expertise and practically oriented IT security recommendations. To increase the information security of new technologies, part of the BSI's remit is designing security requirements, standards and recommendations for real-world scenarios. As the country's central certification and standardisation body, the BSI also assumes responsibility for Germany as a hub of digital business. Last but not least, the BSI plays a leading role in ensuring the success of major digitalisation projects.

2.2.1 Threat Landscape for Critical Infrastructure

Critical infrastructure (CI) refers to organisations of vital importance to the wellbeing of our society. These organisations operate critical services in areas such as medical care and the supply of food, water and electricity. Critical services also include the processing and storage of data in data centres and ensuring citizens can make withdrawals at cashpoints. While public attention has focused on incidents affecting the healthcare system due to the COVID-19 pandemic, cyber attacks are regularly experienced by CI operators in all sectors.

Critical services of all kinds are heavily dependent on IT systems working without any disruptions. Any fault, impairment or failure affecting these core services can lead to supply bottlenecks with lasting repercussions, considerable disruptions to public security and all sorts of other dramatic consequences. For CI operators, the BSI Act (BSIG) therefore sets out measures for the prevention (section 8a) and management (section 8b) of IT security incidents and disruptions.

IT Security Act introduces burden of proof to strengthen IT security in critical infrastructure

In 2015, the IT Security Act introduced a requirement for CI operators to document the implementation status of security requirements pursuant to section 8a (3) of the BSI Act. Every two years, operators must now submit proof of compliance to the BSI that they are operating state-of-the-art IT security systems. These documents provide details not only on the security measures implemented, but also on any security deficiencies discovered through independent security audits.

During the last audit cycle, each of which runs for two years, a total of 1,805 security deficiencies were discovered in the sectors of information technology and telecommunications, finance and insurance, and water and energy as part of routine implementation audit work.

These security deficiencies in the sectors of information technology and communications, finance and insurance, and water and energy are presented in the following sections for each of these sectors according to the categories specified in the BSI's orientation guide for security audits in CI operators.

In the **CI sector Information Technology and Telecommunications**, deficiencies were discovered relatively often in the areas of technical information security, human resource and organisational security, and checks conducted as part of normal operations. Security deficiencies relating to information security management systems (ISMS) were identified significantly less often than in the energy and water sectors.

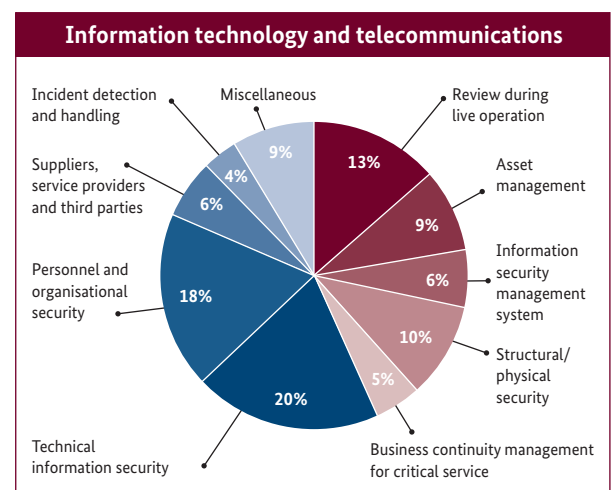


Figure 8: Deficiencies by category in the Information Technology and Telecommunications sector.

In the **CI sector Finance and Insurance**, the deficiencies most commonly encountered were in the categories of technical information security, checks conducted as part of normal operations, asset management and ISMS. In the finance and insurance sector, deficiencies relating to technical information security were frequent compared to other sectors. This also applied to the absolute frequency of deficiencies.

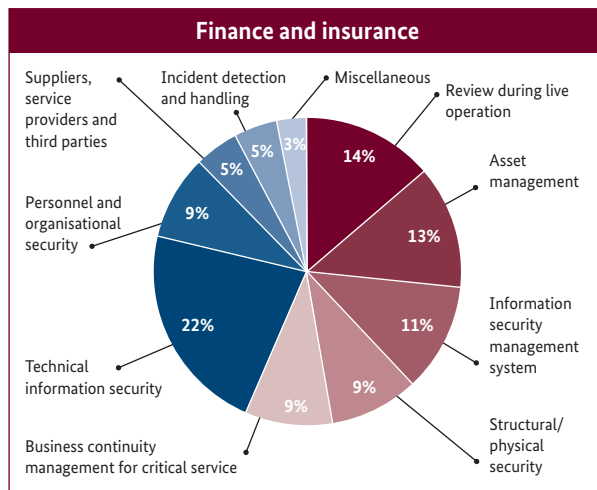


Figure 9: Deficiencies in the Finance and Insurance sector by category.

cies involving technical information security. One reason for this could be that, in this highly computerised sector (which was already tightly regulated even before the enactment of the IT Security Act), IT security has achieved a higher level of maturity with correspondingly fewer deficiencies in the other categories. It should be noted, however, that the category of technical information security is very extensive and therefore encompasses a wide range of deficiencies. Deficiencies relating to asset management frequently result from the fact that operators are required to first uniquely identify and classify their critical infrastructure systems.

Around a third of all deficiencies in the CI sector Water can be assigned to ISMS. There is clearly room for improvement in relation to ISMS in the Water sector, and much more needs to be done. In contrast to information technology and communications or finance and insurance, only one in 10 of the deficiencies discovered during an implemen-

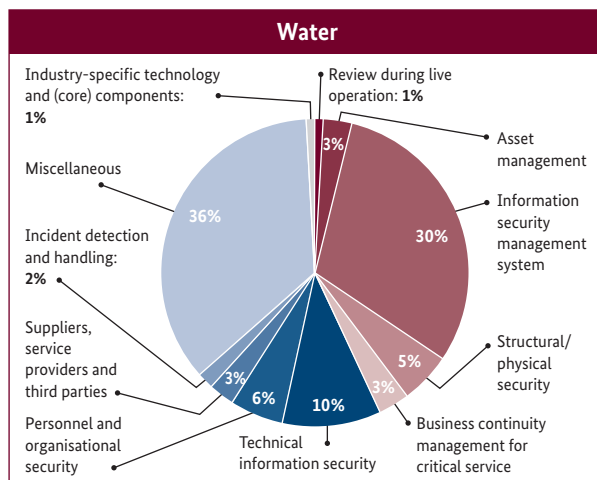


Figure 10: Deficiencies by category in the Water sector

tation audit in this sector can be ascribed to the category of technical information security. However, the sector also

has a relatively low level of digitalisation and is accordingly less dependent on IT.

In the CI sector Energy, the picture is similar to the Water sector. Around a quarter of the deficiencies identified in this sector can be ascribed to ISMS. As in the water sector, the number of deficiencies related to technical information security in the energy sector is low in relation to the total

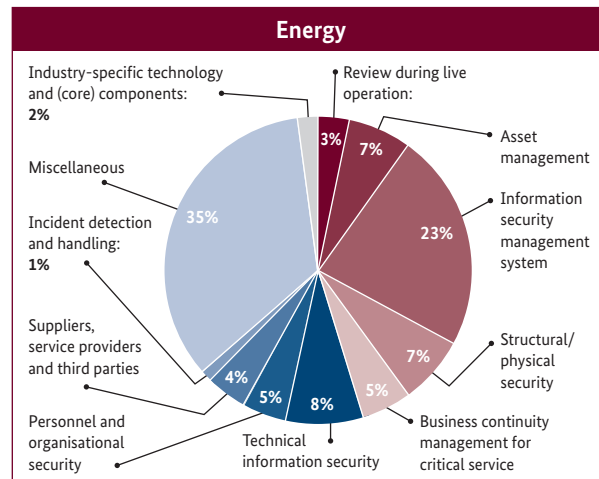


Figure 11: Deficiencies by category in the Energy sector.

number of deficiencies. Unlike the water sector, however, this sector exhibits a very high degree of digitalisation and is very dependent on IT systems.

Insights from the audit documents

Insights gained from the audit documents submitted to the BSI assist the BSI's Critical Infrastructure Branch in providing specific advice to CI operators in affected industries on how to improve their IT security. The knowledge obtained by CI operators and the BSI from the audit documents is also used to prepare new sector-specific security standards (B3Ss).

There are plans to expand the pool of the categories of security deficiencies to obtain a more detailed picture of the frequency and the underlying causes. This will enable the CI operators required to submit proof of compliance to receive specific guidance from the BSI on potential improvements to their IT security.

2.2.2 UP KRITIS

UP KRITIS is a platform that supports cooperation and information exchange among CI operators, their industry associations and the regulatory authorities responsible for CI in Germany. The overall aim is to protect critical infrastructure, especially in the area of cyber security. The participants in UP KRITIS, which included 750 organisations as of May 2021, have been working together for over 10 years. The BSI has been a member of the UP KRITIS partnership since its formation and also acts as its operative arm.

Successful cooperation between CI operators and government to protect critical infrastructure

Cooperation in UP KRITIS takes place at both an operational and at a conceptual level. At the operational level, participants engage in dialogue about the current cyber security situation. For its part, the BSI issues warnings, situation reports and background information. Within UP KRITIS working groups, security incidents are discussed in a confidential setting. The BSI also stays in touch with the operators of critical infrastructure through a dedicated CI contact at the National IT Situation Centre to ensure a rapid response in the event of anomalies or incidents. In addition, the members of UP KRITIS share a great deal of information with one another, especially on major incidents (such as the Exchange vulnerability in early 2021 – see incident Critical Vulnerabilities in Microsoft Exchange, page 27).

Advancements in the cyber security of CI operators in UP KRITIS working groups

Conceptual and contextual questions are addressed primarily in the thematic working groups (TAKs) within UP KRITIS. One such recently formed group is TAK Detection, which focuses on the increasing importance of detecting cyber attacks. It is currently developing guidance on issues relating to detection with the participation of the BSI. Meanwhile, TAK Operational Information Exchange has been working on improvements to the risk matrix used by UP KRITIS. The matrix makes use of a threat catalogue to help industries assess industry-specific vulnerabilities and probabilities of their manifestation. Risk trends can be determined by a system of cyclical risk analyses (which are completed in sessions held by industry working groups, for example). Reporting on the results of the CI industries creates a high-level threat landscape for all CI sectors that can also indicate trends.

New committee structure within UP KRITIS

After more than 10 years of successful cooperation, UP KRITIS was restructured in 2021. Alongside its thematic and industry working groups, it includes two overarching bodies: the Plenum and the Council (see Figure 12).

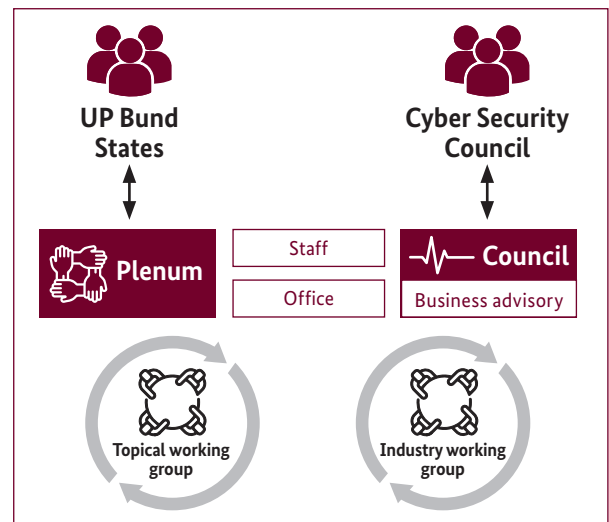


Figure 12: UP KRITIS committee structure

Consisting of delegates from working groups, the Plenum is the decision-making body within UP KRITIS. Since the restructuring of the Plenum in 2021, any CI industry can delegate a spokesperson to the Plenum. This means all the CI industries are now represented in the Plenum.

The Council, meanwhile, is the board that advises UP KRITIS on policy. It provides input and feedback on strategic goals and projects within UP KRITIS, thereby strengthening the partnership and cooperation of business and government. Council candidates from business-side are proposed by CI industries and confirmed for a two-year period by the Plenum (most recently in early 2021). (See Bibliography⁴).



2.2.3 Digitalisation in the Energy Sector: Smart Metering System Rollout

In the future, critical systems in the energy grid are interconnected by a secure communications infrastructure due to the use of certified smart meter gateways as a trusted communications platform within intelligent metering systems. This will also provide an effective countermeasure to the kinds of cyber attacks that were again on the rise in the reporting period.

Four manufacturers of Smart-Meter-Gateway have now successfully completed the BSI's product certification procedure, with two manufacturers (Power Plus Communications and EMH metering) also completing the recertification procedure with additional functionality within a few short months.

With the help of the two Smart-Meter-Gateways that are currently capable of supplying grid status data and feed-in values, distribution network operators can now operate intelligent metering systems that give them key data about

the current load on their grids, which enables them to identify and avoid potential bottlenecks in good time. This information also helps ensure that power grid expansion is designed to be efficient and cost-effective. The used devices ensure to support information security at the very highest level.

In the future, flexible consumption points (heat pumps, electric vehicles, etc) and decentralised power generation plants can be controlled via Smart-Meter-Gateways and thus deployed to the advantage of the grid and market.

Together with the Federal Ministry for Economic Affairs and Energy, the BSI is working with industry associations and companies to specify the key technical cornerstones and the resulting BSI standards that will help establish the secure energy grid of the future. This in turn will make it possible to monitor current trends and innovations in a goal-oriented manner, ensuring that the gateway technology is continuously improved for deployment in other areas.

2.2.4 Modern Telecommunications Infrastructure (5G)

Modern mobile network standards based on 5G/6G, which enable faster connections, lower latency and higher data speeds, form a key technological basis for the continuing digital transition. The BSI has been tasked with creating the environment needed to ensure that these networks achieve the highest possible level of confidentiality, integrity and authenticity. The current basis for the development of secure 5G/6G networks is the catalogue for security requirements specification that the Federal Network Agency, the BSI and the Federal Commissioner for Data Protection and Freedom of Information (BfDI) have revised in line with section 109 of the Telecommunications Act, which will be applied to the new 5G/6G networks being set up.

Catalogue for security requirements

The German Telecommunications Act (TKG) sets out the legal framework for operators of telecommunications networks. In terms of IT security, section 109(6) of the Act is most relevant, since it stipulates national security requirements for telecommunications infrastructure in the form of the catalogue for security requirements. These criteria are prepared by the Federal Network Agency in consultation with the BSI and the Federal Commissioner for Data Protection and Freedom of Information (BfDI). They are updated regularly to reflect the latest technical and regulatory circumstances.

The newly published annex to the catalogue for security requirements focuses on topics such as the assurance level of manufacturers and suppliers, safeguarding the integrity of components throughout their entire lifecycle and requirements for ensuring that the secure operation of networks is maintained by means of security monitoring and key management. In addition, operators are required to obtain security certification for their critical network components.

Certification strategy

The BSI is currently preparing a certification strategy for 5G to ensure that discrete and interrelated certification schemes can be deployed for both products and systems within the various network contexts. In this work, the BSI is referencing established, internationally recognised standards to minimise the related effort for manufacturers and operators.

The basis for this product certification is provided by the Network Equipment Security Assurance Scheme (NESAS), a testing/auditing scheme developed by the Global System for Mobile Communications Association (GSMA). The BSI is currently working together with the GSMA to extend the NESAS scheme with the aim of establishing it as a European certification scheme in the context of the Cybersecurity Act. The two organisations are also seeking to integrate other auditing requirements into the standard, such as a secure product lifecycle that also accounts for the supply chain. In accordance with the further development of the corresponding technology and market, product certification will be extended to include the Accelerated Security Certification (BSZ) and Common Criteria (CC) schemes at a later date. The aim is to ensure the creation of CC-based protection profiles for selected critical network functions, and to standardise and harmonise them at the European level (3GPP/GSMA).

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

Further developments have been made to the BSI's related Technical Guidelines, which summarises the schemes for product and system certification that were selected as part of the 5G certification strategy.

European harmonisation

The EU Commission has recommended a concerted approach to the security of 5G networks. In its Recommen-

dation 'Cybersecurity of 5G networks' ((EU) 2019/534 of 26 March 2019), the Commission published a roadmap for developing a common, EU-wide toolbox of measures to increase security in 5G telecommunications networks. In particular, these measures include the establishment of a Cooperation Group, the creation of a coordinated European approach to risk assessment and the development of a common toolbox of management measures to mitigate identified security risks.

Within the Cooperation Group, the BSI has worked to promote the introduction of appropriate certification schemes (e.g. the NESAS scheme mentioned above) as EU certification schemes. The corresponding proposal to develop a 5G certification scheme in the context of the Cybersecurity Act was submitted to ENISA by the EU Commission in January 2021. The BSI will participate in the subsequent design process to be handled by ENISA's ad hoc groups.

Technical expertise and funding

The BSI is concentrating its work on various 5G activities at its new premises in Freital (near Dresden). It has also already begun expanding its technical capacity in this field. Meanwhile, plans have been made to set up a 5G Security Lab within the BSI. From the outset, broad-based contact and dialogue will be sought with corresponding research institutions, testing bodies, manufacturers and operators. With products and solutions for 5G Release 16 set to become available in 2021, there will be a significantly wider spectrum of use cases for 5G, which will also become more strongly established in campus networks. The BSI is therefore increasing its monitoring of this field from a security perspective.

One topic of note here is Open RAN. The O-RAN Alliance is working to develop international specifications that will bring radical change to the use of radio access networks (RANs) as part of mobile telephony. Leading mobile network operators in Europe also intend to build on Open RAN for future 5G network rollouts. The BSI believes that further work is needed when considering IT security in the context of Open RAN, and that the current Open RAN specifications need improvement in this regard. At the same time, 'opening the RAN' offers new opportunities for security aspects in relation to radio access networks.

Open RAN also has an important part to play in the German federal government's recovery programme (combating the impact of COVID-19, securing prosperity, strengthening future viability and 'Ziffer 45'). The BSI is participating in the design of specific funding programmes for IT security and 5G – and for the 6G wireless

networks that will follow. Open RAN security will naturally also be a point of focus here.

2.2.5 Cyber Security in the Automotive Sector

On Germany's roads, increasing interconnectedness and automation – along with requirements for e-mobility – are creating entirely new threats as a result of potential attacks targeting vehicle IT, which were previously unaccounted for in the vehicle type approval process. In recent years, many attacks on vehicle systems – particularly those using wireless interfaces – have made the headlines and highlighted the inherent potential threat.

In June 2020, regulations for vehicle cyber security were accordingly adopted at the international level and subsequently entered into force at the start of 2021 (source: United Nations Economic Commission for Europe: ECE/TRANS/WP.29/2020/79, 'UN Regulation on uniform provisions concerning the approval of vehicles with regard to cyber security and of their cybersecurity management systems', June 2020). These new regulations have been transposed into EU law and will become binding from July 2022. As a result of this legislation, vehicle makers will be required to account for potential IT-related risks through measures that include appropriate development and response processes.

In light of the above, the BSI signed an administrative agreement with the Federal Motor Transport Authority (KBA) in October last year to bring together competencies related to the cyber security of networked and autonomous vehicles. The BSI is assisting the KBA with type approval processes in accordance with the new UNECE regulation mentioned above, and with IT security issues in market surveillance. To this end, both the BSI and the KBA are establishing processes for the joint assessment of IT security incidents and vulnerabilities in motor vehicles. They are also building up analysis expertise, drawing up requirements for inspections and developing test guidelines.

In June 2020, the BSI and the German Association of the Automotive Industry (VDA) signed a memorandum of understanding in which they agreed on regular exchanges on the topic of IT security. The aim is to develop a shared understanding of the various sub-areas within automotive cyber security and to highlight any need for action – in areas such as standardisation, for example. Following initial talks, IT security in the supply chain is one topic that the parties have agreed to address.

Vehicle-to-vehicle and vehicle-to-infrastructure communication for cooperative intelligent transport systems

(C-ITS) is also now enjoying wider adoption in the market. As part of the effort to secure C-ITS, the BSI has prepared drafts of Technical Guidelines for the interoperable implementation of EU-level criteria. These documents provide guidance on the communication components used in roadside units and vehicles, as well as for the associated public key infrastructure. Work on the drafts is currently being coordinated with representatives of the affected industry sector and the corresponding authorities.

The BSI is also working on the security aspects of the AI techniques that are increasingly being used in the context of (semi-)autonomous vehicles (see chapter Artificial Intelligence, page 81).

2.2.6 Cyber Security in Aviation

The Implementing Regulation (EU) 2019/1583 lays down detailed measures for the implementation of common basic standards of cyber security in aviation at the EU level. With the adoption of this Implementing Regulation by the Commission, companies regulated by sections 5, 8, 9 and 9a of the German Aviation Security Act (LuftSiG) will be required to ensure the fulfilment of their duties in relation to IT security in addition to their existing legal responsibilities from January 1st 2021. These duties include establishing preventive measures in relation to cyber security (e.g. taking precautions against and detecting cyber attacks) and communicating information on vulnerabilities and *malware* in an appropriate, practicable and timely manner. The aim is to protect civil air traffic from cyber attacks, aircraft hijacking, acts of sabotage and terrorism.

As a result of the increasing digitalisation and networking of systems, accounting for IT security as part of the conventional understanding of security and safety has never been more important. Apart from outages, even impairments to the integrity and authenticity of IT systems can have a disastrous impact on flight operations. In November 2020, an incident in Saarbrücken demonstrated how airports in Germany could become victims of cyber attacks. A *ransomware* encrypted the airport's IT systems and were accordingly unavailable for some time afterwards. This incident shows that the threat landscape regarding IT security in aviation should be considered as nothing less than critical.

In Germany, the BSI is responsible for the organisation and management of measures relating to information security for companies regulated by LuftSiG sections 5 and 8. These companies include the roughly 200 German airport operators, as well as passenger and baggage security. As regards LuftSiG sections 9 and 9a, which cover aviation companies and parties involved in the secure supply chain,

the Federal Ministry of Transport and Digital Infrastructure has the responsibility. As defined by LuftSiG, parties involved in the secure supply chain include regulated agents, known consignors, hauliers, subcontractors of regulated agents, regulated suppliers and known suppliers working in the airfreight industry.

The BSI will draw up criteria and requirements in relation to cyber security in aviation for companies regulated by LuftSiG sections 5 and 8 and, as part of the National Aviation Security Programme (NLSP), specify which of these companies must verify within the new cyclical approval procedure.

The BSI will also draw up the requirements needed for auditing compliance and conformity with statutory criteria, and specify these as part of the NLSP.

2.2.7 Cyber Security in the Manufacturing Supply Chain

As Industry 4.0 becomes more widespread, digitalisation is affecting more and more supply chain processes. In addition to helping to protect goods in the supply chain – whether software or material goods – from product counterfeiting and manipulation, the digitalisation of the supply chain is driving new business models, advanced analyses and automated cooperation.

However, this can also lead to an increase in potential targets and vulnerabilities that may expose various areas of companies – including their production environments. The disastrous impact that this can have on entire corporate networks has been demonstrated by the SolarWinds hack (see incident SolarWinds, page 30). This example clearly shows that IT security is something that must be tackled collectively. To support a shared dialogue and coordinated response mechanisms, in-depth formats for active communication and cooperation must be developed in compliance with competition law.

The IT Security Act 2.0 will work to further promote cyber security efforts, including those focused on the supply chain. The Act introduces the concept of a 'business of special public interest', which encompasses companies with key economic significance that should therefore – as with critical infrastructure operators – be subject to special protection and reporting regulations in the future.

Small and medium-sized enterprises (SMEs) must also digitalise their business processes, however, if they want to avoid being forced out of the market by digitalised supply chains. One difficulty here is that the general

shortage of specialists means that SMEs have fewer resources and less knowledge at their disposal to manage cyber security challenges (see chapter The unique role of SMEs in Germany, page 63).

Strategy

A digitalised supply chain must not result in a closed market that excludes certain competitors. To ensure that all the data and participants along the supply chain can be trusted, however, a sufficient level of cyber security must be achieved.

For this reason, the BSI is working with the realms of research and business on digitalisation strategies for the supply chain. One focus of this work is Plattform Industrie 4.0, which brings together more than 300 actors from over 150 companies, associations and trade unions, as well as the fields of research and policymaking. The platform is steered and managed by the Federal Ministry for Economic Affairs and Energy and the Federal Ministry of Education and Research in cooperation with senior representatives from business, research and trade unions.

In addition, the BSI is driving standardisation and the certification of security measures at all enterprise levels. To provide SMEs with support for digitalisation and the rollout of security measures, the BSI is producing best-practice guides that contain recommendations for action and checklists for specific technologies and standards, such as eIDAS or IEC 62443.

European and international collaboration

Together with the Japanese Robot Revolution & Industrial IoT Initiative (RRI), Plattform Industrie 4.0 and the BSI are developing a trustworthiness profile demonstrator for the exchange of eIDs and digitalised company certificates.

Within the International Standardisation Organisation (ISO), the BSI is working on the standardisation of a programming interface for Secure Elements in industrial devices (ISO/IEC TS 30168 ED1: 'Internet of Things (IoT) – Generic Trust Anchor Application Programming Interface for Industrial IoT Devices').

2.2.8 The Unique Role of SMEs in Germany

According to the EU classification of an SME, this sector encompasses around 2.6 million companies in Germany, which is around 99.4 percent of all the country's active businesses. The BSI, meanwhile, extends the classification of an SME according to the definition used by Institut für Mittelstandsforschung (IfM) Bonn, which sets the limit for

medium-size companies at 499 employees (instead of 249). This allows for better representation of the unique status of medium-sized, family-run businesses within Germany. Many of these family-run and owner-managed businesses can be considered 'hidden champions': this grouping accounts for about 1,500 companies in Germany, or roughly half of all the hidden champions in the world.

The contribution made by SMEs is fundamental to the success of the German economy. Failings in IT security that affect SMEs can therefore cause a direct and significant impact on the country's overall economic output. Although standard in larger corporations, SMEs typically do not maintain a dedicated IT security team. They often do not even have an internal IT department. As a result, SMEs often lack the expertise to properly assess threats to IT security. At the management level, there is often an insufficient basic awareness of the risks and dependencies that the deployment of information technology involves. This means SMEs are particularly exposed to threats originating in cyberspace. As digitalisation continues apace, this threat landscape also grows more critical by the day, as has been reflected in the BSI's analyses of update practices in businesses. In March 2021, for example, a warning campaign conducted by the BSI in relation to vulnerabilities in Microsoft Exchange Server identified a large number of at-risk systems in Germany (see incident Critical Vulnerabilities in Microsoft Exchange incident, page 27). However, many of these systems had not merely been rendered vulnerable by the security holes announced in early March; they were also susceptible to attacks for which patches had been available for some time. In the vast majority of these cases, the vulnerabilities affected systems at SMEs.

Urgent action must therefore be taken to strengthen the security of SMEs in Germany in light of their important status for the economy. The BSI is meeting its obligations in this regard by expanding its activities on behalf of this key client group.

2.2.9 Technical Security Device for Electronic Recording Systems

As part of the digital transformation, business transactions are increasingly being recorded using electronic systems. Among other things, the retail trade is characterised by the use of a very wide variety of cash registers: from traditional tills to tablets, smartphones and even 'cash till server farms', every conceivable type is represented. The technical challenges faced in tax inspections have thus changed radically, since subsequent manipulation of electronic records can be practically undetectable if appropriate safeguards are not used.

To counter this kind of tampering, the Fiscal Code of Germany and Cash Register Security Ordinance have stipulated the protection of electronic recording systems in Germany with a certified technical security device from 2020 onwards. After being contacted by the electronic recording system, this device secures the data to be recorded and files the secured records using a uniform format. Thereto, the technical security device is equipped with a security module that prevents records from being unrecognizably erased, modified, or created anew at a later point in time.

The new legislation also explicitly facilitates a technology neutral approach for the design of technical security devices. A standardised digital interface simplifies integration with existing and future electronic cash register systems, while also guaranteeing the necessary interoperability in the context of tax inspections. There are no specific requirements for the physical interface are not specified to ensure that typical standard interfaces such as USB, Ethernet and (micro) SD cards can be used. To complement these purely local security devices, scalable solutions – for deployment in branches or as part of an online service setup, for example – have been planned from the outset by means of an optional client/server architecture for the security module.

The technical requirements and testing standards for the components used in the technical security device have been specified by the BSI in Technical Guidelines and protection profiles.

Seven different technical security devices have successfully completed the certification process and are now available on the market. Four of these can be integrated directly into tills and mobile devices by means of USB drives and (micro) SD cards. The three other solutions can be integrated as ‘cloud-based technical security devices’ that are hosted in data centres.

2.2.10 IT Security Certification as an Instrument for Verifiably Secure Digitalisation

The COVID-19 pandemic has brought digitalisation topics into sharper focus and emphasised the need to ensure that products and services fulfil a minimum standard of information security. To support providers and operators of digital solutions, the BSI offers a range of certification programmes an organisation can use to verify that its product or service meets a certain set of predefined security requirements. An independent audit conducted by the BSI creates trust and provides evidence of integrity, confidentiality and authenticity.

In principle, both manufacturers and suppliers can apply for certification of an IT product. An audit can be conducted in accordance with the internationally recognised Common Criteria (CC), a Technical Guidelines (TR) or the new Accelerated Security Certification (BSZ) procedure. Product certification according to CC or TR confirms that a product version fulfils certain functional and security-relevant properties, which are specified in protection profiles, security specifications or Technical Guidelines. To reach security verdicts, the BSZ adopts an approach based on penetration testing with fixed evaluation periods and fewer documentation requirements.

Alongside product certification, the BSI also offers a second key pillar in the form of information security management system (ISMS) certification. This is modelled on the commonly used certification according to ISO/IEC 27001 and conducted on the basis of the BSI’s internally developed IT-Grundschutz. In addition, the BSI offers a wide range of services for individual certification: auditors for various specialist subjects, IS auditors and IT-Grundschutz consultants are just some of the types of certification in demand.

Current challenges

When the Cybersecurity Act (CSA) entered into force in June 2019, the European Commission laid the foundation for the EU-wide recognition and harmonisation of IT security certification programmes. One challenge the BSI now faces is transposing the demanding requirements already established in national digitalisation projects into the new EU-wide scheme, together with those from the previous SOGIS-MRA recognition agreement. Some examples of both established and new digitalisation projects run by the German federal government and the EU in which certification is now firmly entrenched include the digitalisation of healthcare, official documents, the digitalisation of the energy transition, digital trip recorders, digital signatures and protection against the manipulation of digital original records (cash registers).

Certification in figures

In the reporting period, the BSI issued Common Criteria certificates to a total of 69 products, 19 sites and six protection profiles. In addition, there were five ALC re-evaluations and 21 CC maintenance procedures.

In international comparison, the BSI occupies a leading position in CC certification and, depending on the certificate trustworthiness level or application area selected, consistently ranks among the top three countries in terms of CC certificates issued.

In addition, 77 certificates were issued according to Technical Guidelines in 14 testing categories, 51 of which were initial or re-certifications, 15 were maintenance procedures and 11 were surveillance audits.

In the area of IT-Grundschutz, a total of 87 procedures were completely successfully in the reporting period, of which 31 were ISO 27001 certificates based on IT-Grundschutz. A total of 56 surveillance audits were also conducted. The Accelerated Security Certification procedure is currently in the pilot phase.

2.2.11 IT-Grundschutz: Solutions for Information Security

The manifold and ever-changing nature of the attacks described in section 1 illustrates once again the importance of an integrated approach in obtaining a level of security that meets the needs of all an organisation's business processes and the data handled within them. The approach proved to be the most effective is establishing an information security management system (ISMS) based on IT-Grundschutz. The application of IT-Grundschutz helps detect threats, reduce risks and significantly elevate the level of information security at hand by means of appropriate measures.

So far, businesses and public authorities can draw on the expertise of over 100 trained and accredited IT-Grundschutz consultants. These BSI-accredited consultants can help in the development of a security model or provide support during the rollout of an ISMS. For organisations that have limited time and personnel available for the first steps in ensuring information security, an IT-Grundschutz consultant can offer assistance and make a key contribution to prevention. In terms of day-to-day operations, these experts can work with an organisation's assigned teams to define measures based on IT-Grundschutz before putting them into practice.

Well-prepared for an emergency: business continuity management

The value of a well-organised business continuity management (BCM) system is best demonstrated when the security goal of availability is targeted. Many attacks have resulted in the failure of an organisation's critical business processes. *Ransomware* attacks in particular now constitute a very serious threat. This illustrates the need to establish both a BCM system and an ISMS in order to be able to respond quickly in any situation. In this way, organisations can achieve lasting *resilience* even when facing an emergency or disaster. In light of the significance of this topic in efforts to improve efficiency and deal with dependencies among functional business processes – including multiple

locations – the BSI has subjected BSI Standard 100-4 to a detailed analysis and revision process. The very title of the future Standard 200-4 will reflect the focus on business continuity management. A BCM system aims to ensure that, even if exposed to significant damage due to an incident, business processes will not be interrupted or can be restarted after an outage within an appropriate time frame. In order to achieve this BCM takes both a preventive and reactive approach. Within IT-Grundschutz, establishing ISMS and BCM systems is viewed as a long-term undertaking that involves clearly assigned responsibilities, processes and tasks to achieve long-term *resilience* in businesses and public authorities.

2.2.12 IT Security when Working from Home

At the beginning of the COVID-19 pandemic, the changeover to working from home – sometimes at very short notice – introduced new technical and organisational challenges. The BSI undertook a series of specific measures to secure home working environments from the outset. At the same time, the challenges posed by this new kind of workplace were investigated in a survey examining IT security when working at home, particularly in the context of the COVID-19 pandemic (see *Bibliography*^u).



Technical and organisational measures when working at home

While working from home is set to play a significant role in our day-to-day working lives going forward, all too few technical and organisational measures are being adopted to secure home environments adequately against cyber attacks. Micro-enterprises and small enterprises have much work to do in this regard. For example, only 66 percent of the survey respondents had deployed a virtual private network (VPN). Just half of the companies surveyed had implemented multi-factor *authentication*, and only 38 percent of them are currently managing their mobile end devices (phones, tablets, etc) centrally via mobile device management (MDM). Many businesses nonetheless seem to understand the importance of their awareness of cyber and information security, and that their employees – the 'human factor' – must play a central role in their IT security strategies. No fewer than 81 percent of the businesses were investing in awareness campaigns both before and during the pandemic and are working to educate their employees now. Training is not enough on its own, however. Regular drills for cyber or IT emergencies are another important aspect – and there is still much to do here. Only 24 percent of the companies surveyed conduct regular drills that simulate the impact of an IT emergency on their processes. Particularly striking is the

fact that only around half of the respondents have adopted the most important principle when it comes to corporate IT security: that cyber security is a board-level issue.

Threat landscape and IT budget

As employees transitioned to working from home due to COVID-19, eight percent of the companies surveyed had to take action against cyber attacks. SMEs in particular are more likely to view the ensuing damage as severe. For companies with fewer than 50 employees, the losses from one in four cyber attacks posed a serious or existential threat. The survey also revealed an inadequate level of investment to date: more than half of the businesses (55%) are currently earmarking as little as 10 percent or less of their IT budget for information security. The BSI recommends assigning 20 percent of IT expenditure to cyber and information security. Meanwhile, only 16 percent of the companies responded to the coronavirus crisis by increasing their budget for information security.

Support services for working from home

The BSI responded quickly by providing support services for the ad hoc transition to working from home, and also provided tips for initial security measures and a checklist for company managers. This checklist gives companies a quick way to assess their own information security level, which can be improved as needed with the services provided.

The use of videoconferencing solutions has increased during the pandemic. The BSI has responded by developing a compendium for the use of videoconferencing systems and a community draft of minimum standards for videoconferencing solutions. Facilitator cards from the Alliance for Cyber Security provide a useful set of aids for virtual communication and have already proven their worth on many occasions as an analogue fall-back – in the event of audio dropouts, for example. Working from home is also a point of focus for the national IT security campaign #einfachaBSIchern ('simply secure'). Important tips and information about working from home securely can be found on the BSI website (see *Bibliography*).



Figure 13: Five simple actions to take
Quelle: BSI

2.2.13 Alliance for Cyber Security

The Alliance for Cyber Security (ACS) is the biggest business-focused public-private cooperation platform for cyber security in Europe. The initiative employs a number of traditional and new digital formats to meet the growing need for information, with examples including the Cyber Security Web Talk and the ACS podcast CYBER-SNACS (see *Bibliography*).



True to its slogan, 'Networks Protect Networks', the ACS draws on the resources of more than 150 partners and 100 thought leaders in business to offer a wide range of information and opportunities for dialogue. Companies can use the partner services offered, including (online) seminars, training and publications on many different specialist topics, to expand their cyber security expertise or share it with the network. Another important information channel is the ACS newsletter, which circulates at regular intervals to more than 7,000 subscribers. In the case of the Microsoft Exchange vulnerabilities, a special newsletter was issued to quickly provide businesses with related information.

The alliance passed the 5,000-member mark in April 2021, and its numbers continue to grow. The ACS welcomes all companies and other organisations deploying IT systems in Germany.

2.2.14 Other Solutions/Services for Business

BAFA Export Controls

The BSI assists the Federal Office for Economic Affairs and Export Control (BAFA) with applications for export and shipment authorisation. The overall legal basis for these powers of oversight is provided by the Foreign Trade and Payments Act (AWG), the Foreign Trade and Payments Ordinance (AWV) and the EU Dual-Use Regulation. In these support services, the BSI focuses on cryptographic export control, which is subdivided into the following individual topic areas:

1. Support and (self-)protection of the German cryptography industry
2. Protection of certified IT security products, components such as smart cards and other related technology (against re-engineering, manipulation, etc).

During the reporting period, the BSI processed 96 applications representing roughly EUR 70 million in total revenue.

Investment Monitoring

Pursuant to sections 4 ff. of the Foreign Trade and Payments Act (AWG) and sections 55 ff. and 60 ff. of the Foreign Trade and Payments Ordinance (AWV), the Federal Ministry of the Interior, Building and Community (BMI) tasks the BSI with auditing foreign direct investment in domestic companies. Growth in the volume of audit procedures, which has been rising sharply since 2015, continued in 2020, and a further increase is expected for 2021. The reasons for this include the expanded legal basis for audits, as well as heightened public awareness of how trade policy impacts the national security situation and technological sovereignty.

In a joint initiative involving France, Germany and Italy, the EU Screening Regulation (2019/452) was promoted at the European level to achieve more effective audits of direct investment from non-EU countries and establish an EU-wide regulatory framework. On 17 July 2020, the amended AWG entered into force following a parliamentary resolution from the Bundestag for the transposition of EU Regulation 452/2019; the associated 16th and 17th amendments to the AWV were adopted in 2020 and 2021.

Key changes from the EU Screening Regulation and the amended German legislative framework include the following:

- A lowering of the threshold for intervention to foreseeable impairment rather than an imminent endangerment of public order and security
- A newly introduced reporting duty in relation to key industries
- A lowering of thresholds in many contexts in terms of ownership percentage (from 25% to 20% or 10%)
- Consideration of atypical takeover/controlling relationships
- Explicit specification of factors to be accounted for, such as state-controlled takeovers
- The establishment of an EU mechanism of cooperation

This significant enlargement of the audit base and the new case groups that affect the BSI's remit (such as IT security companies) will lead to a further increase in investment activities requiring the attention of the BSI. Meanwhile, a significant increase in case numbers has already been seen over the last few years. Over 180 cases were registered under the auspices of the BMWi in 2020, representing a four-fold increase since 2016. Since the new legal situation

has not yet had much of an impact, an even greater increase is expected for 2021.

In the case of procedures with potential relevance for cyber security, the BMI involves the BSI to assess/counter the risk at hand and perform associated audits (assignments). When acquisition procedures are complex or particularly sensitive – because they require requests for additional documents, a deeper level of risk analysis, negotiations involving the acquisition parties and other potentially affected stakeholders, or contractual negotiations in relation to official regulations – the various steps involved may also result in new audit assignments for the BSI.

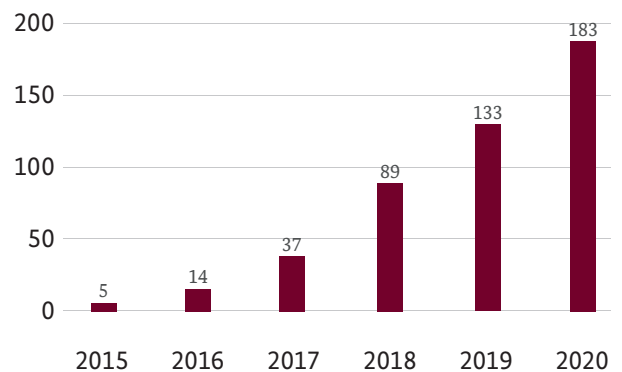


Figure 14: Development of audit / assignments within the framework of AWG procedures

Source: BSI

Taking into account the respective economic, legal and technological situation of the buyer and the target company, the BSI analyses and assesses potential risk situations, and develops position and solution proposals to avert risk. Potential IT security risks can involve leaks of sensitive information to unauthorised third parties, the implantation or concealment of vulnerabilities, the endangerment of critical infrastructure or the loss of key technologies. As is also emphasised by the EU Screening Regulation, the level of protection required for key technologies (in relation to semiconductors, telecommunications, quantum mechanics or artificial intelligence, for example) will continue to pose a major and novel challenge in investment auditing procedures beyond 2021. Since these key technologies also involve the field of IT, the BSI's remit will encompass a large part of this work.

Security of Cloud Services

BSI's Cloud Computing Compliance Criteria Catalogue (C5) was revised, updated and published as BSI C5: 2020 last year (see the *bibliography*⁶¹).

Some initial attestations have now already been issued and the total number of attestations of *cloud* services continues to grow, as does the overall number of auditors / auditing firms issuing attestations according to BSI C5.

Assessing the security of *cloud* services is no simple matter: because the services offered are subject to constant change and based on other services, pinning down the data actually processed is a difficult task. Accordingly, the BSI C5 attestation consists of a report (in line with the International Standards of Assurance Engagements 3000 auditing standard) that permits users to form their own opinion of the security offered by a *cloud* service and the trustworthiness of the *cloud* service provider. Since these reports can be very comprehensive and different structures might be used, the BSI offers support in the form of a published Evaluation Guide (see the *bibliography*⁶²). This document describes a structured approach to extracting the information that will be needed by users of a *cloud* service. Based on this information, an informed decision can then be made as to whether the security offered by the *cloud* service is adequate for the target requirements and use case at hand.

EU cloud certification and BSI C5:2020

A *cloud* certification scheme (the EU Cloud Services Scheme, EUCS) is now being prepared within the scope of the EU Cybersecurity Act. The BSI has played an active part and been able to integrate key parts of C5 in this process, which has taken over two years so far. As one example, the security objectives and requirements for *cloud* services in the certification scheme are largely based on the security criteria taken from BSI C5:2020. Many other elements, such as the assessment of the operating effectiveness of controls, the integration of sub-service providers and the audit methodology, have also been successfully brought into the draft scheme. These elements originate from the auditing standards on which BSI C5 is built, which are widely applicable to *cloud* services. One of the last major challenges remaining in the standardisation process is to apply this audit methodology to a certification scheme that corresponds to the provisions of the ISO 17065 standard 'Conformity assessment – requirements for bodies certifying products, processes and services'. This standard is stipulated by the EU Cybersecurity Act. Since requirements from the EU Cybersecurity Act have already been introduced into BSI C5:2020, this means that *cloud* services with a BSI C5:2020 attestation now approximate the current EUCS draft to a degree not attained by any other security audit on the market.

A minimum standard for the German federal administration

If German federal agencies intend to use services from public clouds, this use is governed by the BSI's 'Minimum

Standard for the Use of External *Cloud* Services' (see the *bibliography*⁶³). This standard describes the steps to be taken when selecting *cloud* services. The BSI also provides public authorities with domain expertise to ensure that they can use the advantages of *cloud* computing securely.

2.3 Federal Government / Administration

Another core task of the BSI is defending against cyber attacks on government networks and the federal administration. Organisations in the federal government, state agencies and other administrative entities also benefit from the updated IT-Grundschutz; from minimum standards and services related to information security consulting, certification and accreditation; and from the support of CERT-Bund, Mobile Incident Response Teams (MIRTs) and the National Cyber Response Centre in the event of IT security incidents. The main points of contact for Germany's states and municipalities are the National Liaison Offices located in Berlin, Bonn, Hamburg, Stuttgart and Wiesbaden.

2.3.1 Threat Landscape in the Federal Administration

Government networks are exposed to attacks from cyberspace on a daily basis. This includes both untar-geted mass campaigns and attacks targeting the federal government's various agencies.

In almost every case, the perpetrators use *malware* to launch their attacks. This *malware* may be propagated as email attachments or hidden in download links sent via email, posted on social media accounts or embedded in webpages (see chapter *Malware*, page 10). As a general rule, attackers proceed by utilising social engineering techniques to trick users into clicking a particular link or piece of content. This is followed by an attempt to install *malware* code on the user's system. The BSI employs a set of varied and complementary measures to protect government networks from these attacks.

Centralised filters are used to block access to webpages hosting *malware* from within the federal administration, which prevents *malware* being downloaded in a multi-stage attack. During the current reporting period, such blocks needed to be added for almost 74,000 *malicious* websites – an increase of 42 percent compared to the previous reporting period. As is shown by the Defence Index for these new blocks, attackers activated a large number of new websites hosting *malware* last year, particularly in September and November. In September 2020 alone,

three times as many *malicious* websites were blocked as the average figure for 2018 (see Figure 15).

As had been seen in earlier years, waves of attacks involving email-based *malware* were observed in late summer and autumn in 2020. These waves were particularly strong compared to last year. The average Defence Index figure for *malware* attacks on the federal administration was 94 points for the reporting year, although strong fluctuations were seen in this figure during the year. During the attack waves from August to November 2020, the indicator occasionally rose as high as 180 points (see Figure 16). An attack wave detected in March 2021 took advantage of email bouncing. Attackers had spoofed email addresses used by the federal administration in a *malware spam* campaign in order to make the emails appear trustworthy. However, most of the recipient addresses targeted did not in fact exist, which caused the corresponding mail servers to return the

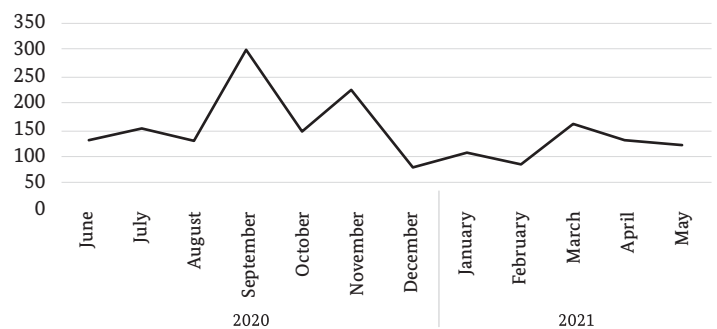
emails to the supposed senders – which were the federal administration addresses specified by the attackers. Since the mail attachments included *malware*, they were identified as a *malware* attack and sanitised at a central server.

During the reporting period, an average of around 44,000 *malware* emails per month were intercepted in government networks by automated antivirus countermeasures before they could reach the inboxes of their intended recipients. Antivirus signatures created by the BSI itself were responsible for intercepting an average of around 9,700 emails every month and therefore made a major contribution to these countermeasures.

Downstream from these automated antivirus measures, the BSI operates another system for detecting *malware* in government network data traffic. The system is tasked with sniffing out targeted attacks and novel *malware* variants.

Index of newly blocked malicious websites

Figure 15: Index of newly blocked malicious websites
Source: BSI analysis of its own sources

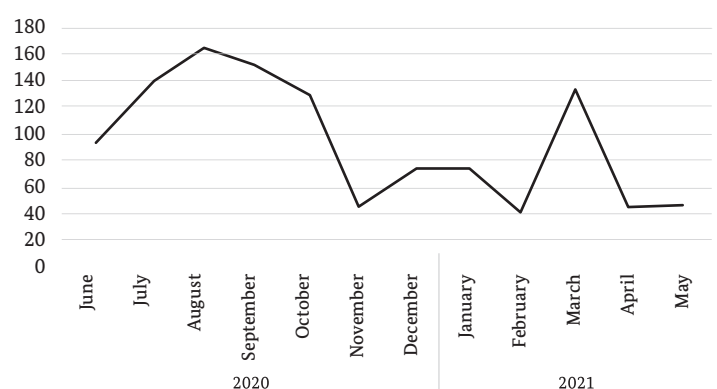


To do so, a combination of automated testing procedures and manual analysis is utilised. With this system, the BSI's internal analysts have detected an average of another 5,100 attacks every month. These attacks had not been identified or blocked by the commercial products that are used in the automated antivirus countermeasures mentioned above.

The security of government networks is also enhanced by centralised protection against unsolicited *spam* mail. This strategy is effective against both unsolicited advertising email and cyber attacks such as *phishing* mails.

Index of malware attacks on the federal administration

Figure 16: Index tracking malware attacks on the federal administration
Source: BSI analysis of its own sources



Does not include spam sent to public authorities that do not take part in the BSI's centralised protection measures

The *spam* ratio (i.e. unsolicited *spam* mail as a proportion of all email received) averaged 58 percent during the reporting period.

Volumes and trends in *spam* mail on federal networks are tracked by means of the *Spam* Mail Index.

After experiencing a lull over the summer with below-average values, the index rose rapidly in autumn 2020, reaching values of over 130 points on several occasions. In March 2021, a record value of 181 points was achieved (see Figure 8). Compared to the previous

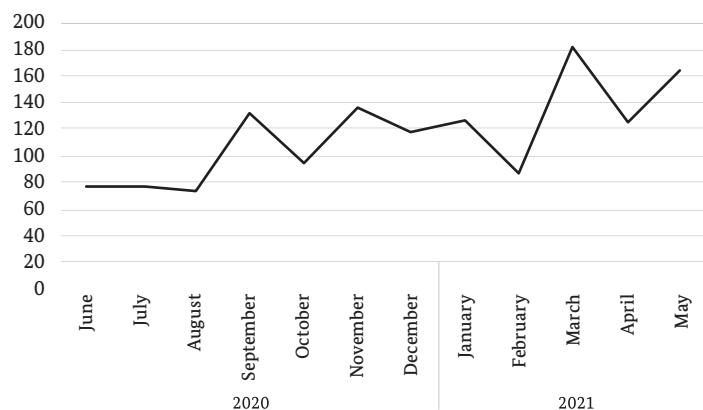
reporting period, the *spam* volume received by the federal administration was nonetheless average overall (115 points).

2.3.2 National Cyber Response Centre

The National Cyber Response Centre (CRC) is a federal-level collaboration platform that supports the day-to-day exchange of information among agencies with various responsibilities in the field of cyber security. The core agencies working at the CRC are: the Federal Office of Civil Protec-

Spam mail index for the federal administration

Figure 17: *Spam* Mail Index
Source: BSI analysis of its own sources



Does not include spam sent to public authorities that do not take part in the BSI's centralised protection measures

tion and Disaster Assistance (BBK), the Federal Office for the Military Counterintelligence Service (BAMAD), the Federal Office for Information Security (BSI), the Federal Office for the Protection of the Constitution (BfV), the Federal Criminal Police Office (BKA), the Federal Intelligence Service (BND), the Federal Police Presidium (BPOLP), and the Cyber and Information Space Command (KdoCIR) at the Federal Armed Forces. Other government bodies participate as associated units. Partners from other levels of the administration are involved on a case-by-case basis. At the state level, this includes the state CERTs, the State Criminal Police Offices and the State Offices for the Protection of the Constitution; State Prosecutor's Offices are also likely to join in the future. The BSI is represented by several liaison officers at the CRC and, as the host agency, also supplies core personnel for the operative arm of the CRC, as well as premises and the shared IT infrastructure that is located at the Bonn site.

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

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

As a result of the increased relocation of many activities online during the COVID-19 pandemic, two key points of focus in the reporting period were the joint evaluation of developments in relation to cyber security and the coordination of measures to protect at-risk facilities. In particular, these include companies from the pharmaceuticals sector and organisations providing medical services (see chapter Threats to Cyber Security due to the COVID-19 Pandemic, page 38). Within the newly formed 'Zukunftsbild' working group at the CRC, extensive development work was completed last year regarding collaboration among public authorities.

2.3.3 Computer Emergency Response Team

The Computer Emergency Response Team for Federal Agencies (*CERT-Bund*) was originally formed as an internal emergency team tasked with assisting the agencies within the federal administration in handling IT security incidents. However, it soon became clear that the growing pace of digitalisation in society and the resulting interconnections between information and communication technology would require a broader approach. As the BSI's remit has been continuously expanded by successive legislation, *CERT-Bund*'s responsibilities have also been expanded to other client groups. Of these, critical infrastructure is perhaps one of the most important, although *CERT-Bund* also provides services to SMEs and the general public.

During the reporting period, around 70 IT security incidents were handled. In 10 cases, the BSI deployed an MIRT to provide local support and assistance to those affected.

In addition, the portal for the Warning and Information Service (WID) run by *CERT-Bund* and *Bürger-CERT* – both of which are overseen by the BSI – supplied around 1,050 individual and collective reports about vulnerabilities (as well as additional update reports). A further 40 cases were considered especially relevant for individual client groups, which then received corresponding cyber security warnings.

In individual cases, the BSI provides support to security researchers, vulnerability discovery experts and manufacturers in resolving vulnerabilities. When a security researcher discovers a vulnerability in a product, the uncoordinated publication of this weakness poses a particular threat, since this is often how attackers first learn of such security holes.

In the reporting period, the BSI notified manufacturers of 25 coordinated vulnerability disclosure cases reported by external parties, as well as of other vulnerabilities detected during its security studies. These included vulnerabilities in a range of office applications, energy metering (smart meters) and industrial control systems, medical devices and administrative and information handling software used in healthcare (see *Bibliography**).



In the BSI's experience, few manufacturers are adequately prepared to organise and handle CVD processes themselves. Even establishing contact with the person responsible within an affected company often proves to be something of a difficult undertaking for the security researchers involved. At the same time, more and more CVD processes are being conducted in which the number of affected manufacturers is comparatively high as a result of the increasing integra-

tion of external software components. Coordinating bodies such as the BSI provide regular procedural support to manufacturers and security researchers by guiding the involved parties through the process as a neutral third party. The CVD procedure is based to a great extent on a collaborative approach. The manufacturers in question are typically granted a grace period before a vulnerability is published. To be able to respond appropriately to a reported vulnerability within this period, adequate preparations must be made – particularly on the part of the manufacturer. This work includes publishing the contact details required, preparing analysis and response processes and ultimately ensuring that users are informed appropriately and effectively (see sidebar on the Common Security Advisory Framework (CSAF), page 72). In addition, the BSI recommends that *providers* publish a company-specific CVD policy. A guideline of this kind creates transparency and sets out a framework for reporting vulnerabilities in much the same way as a bug bounty programme. The BSI has published recommendations to help companies that want to improve their organisational preparations for handling vulnerabilities (see the bibliography⁶⁴).

Meanwhile, *CERT-Bund*'s reports constitute a regular service offered to internet service *providers* and network operators. These reports contain details of systems that are very likely to be infected with *malware* (see chapter *Botnets*, page 19), list systems that contain critical vulnerabilities (see the Critical vulnerabilities in MS Exchange incident, page 27) and report on systems that are publicly reachable over the internet or have openly configured server services that could be abused to conduct cyber attacks (see chapter *Malware and Data Leaks*, page 25). Due to the sheer number of such systems, these reports are created by an automatic process. During the reporting period, an average of 9,100 reports were sent out on a daily basis.

With this multi-faceted approach, *CERT-Bund* makes an important contribution to secure digitalisation in Germany.

i Common Security Advisory Framework (CSAF)

A reported and resolved vulnerability only marks the beginning of the vulnerability handling process on the operator side. In order to protect themselves, users must install a corresponding update. Since the installation of updates may have far-reaching consequences, it is advisable to conduct a risk assessment first. To be able to perform such an assessment, users need to be provided with all the relevant information about the vulnerability at hand in a timely and efficient manner. To date, human-readable security information (commonly referred to as security advisories) have been published by manufacturers and the various coordinating bodies for this purpose.

To be able to assess the risks to their IT infrastructure and the products they deploy, operators need to read through these security advisories. Searching for newly published advisories and evaluating them to assess their relevance routinely involves a high investment of both time and personnel. This results in part from the fact that manufacturers and other bodies that publish these details use a great variety of channels to notify their customers and the general public. For example, email notifications may not be sent out immediately or customers may need to subscribe to an RSS feed, or they may have to retrieve new advisories manually from a website (which may require a login). Furthermore, an increasing number of bodies are now publishing more and more security advisories. In particular, assessing whether the products referenced in the advisories are actually being deployed in an area for which the company is responsible is often not straightforward.

Since security advisories produced by different sources typically vary in terms of their file format, structure and quality of information, and formatting, automated processing is only possible to a limited extent (if at all). On the other hand, manual processing wastes skilled company resources on what is largely routine work. The previous approach to this problem also does not scale as the number of security advisories increases, since the same human resources then need to analyse an increasingly complex set of advisories. As a result, this important source of information is often analysed only on an ad hoc or occasional basis – following a report in the media or a BSI notification, for example – and not as a regular activity.

Accordingly, the BSI is working with national and international partners on establishing a solution for providing users with a simpler approach to find, evaluate and implement security advisories. The machine-readable format for security advisories, known as the Common Security Advisory Framework (CSAF) 2.0, will make a decisive contribution to achieving a situation where companies can keep abreast of advisories and ensure their systems are secure. With this approach, security advisories can be automatically retrieved from vendors and compared against the company's own asset database. The BSI has already published the first tool for creating CSAF documents (Secvisogram) on its GitHub page (link to <https://secvisogram.github.io>). With these activities, the BSI is helping to enhance information security in companies and thereby ensure Germany's successful digital transition.

2.3.4 Federal IT Consolidation project: New Information Security Officer

Launched in 2015, Federal IT Consolidation is an ongoing major project in which the German federal government is aiming to consolidate common information technology and IT procurement at the federal level with a few core service providers. The BSI has supported the project from the outset, especially by advising the other participants and contributing to project committees.

The adoption of the Federal IT Consolidation Information Security Policy by the Federal IT Consolidation Steering Committee of the IT Council on 10 December 2020 marked the implementation of a key requirement from UP Bund 2017. In 2020, the policy was prepared under the auspices of the BSI as Germany's Federal Cyber Security Authority together with the Federal Ministry of the Interior, Building and Community; the Federal Ministry of Finance; the Federal Agency for Public Safety Digital Radio (BDBOS); and the core IT service provider ITZBund.

A day after the adoption of the policy, the BSI appointed Christoph Lauffer as the Information Security Officer for Federal IT Consolidation (ISO ITKB) and Sven Schneider as his permanent deputy. The Information Security Officer is tasked with coordinating the various information security activities as a central point of contact and integrating the existing information security management systems with the aim of achieving a suitable level of information security within the Federal IT Consolidation project. A cluster risk management system creates transparency in relation to cyber risks and also permits the ongoing monitoring and improvement of the information security level of the consolidated IT in question.

2.3.5 National Liaison office

In the digital era, information security requires a common approach from the federal and state governments in order to be successful. For this reason, the BSI has expanded its support for the German federal states and promotes collaboration between federal and state administrations at various levels. The goal of this reinforced cooperation is to improve the level of cyber security throughout Germany.

The national liaison office with its five established locations – Berlin, Bonn, Hamburg, Stuttgart and Wiesbaden – eases as immediate point of contact for all 16 federal states the dialogue and cooperation among the various stakeholders. It provides information about products and services of the BSI for the government, economy and

civil society, thus helps to raise general awareness for the topic of information security.

This close cooperation between federal and state administrations has been reflected in the signing of initial cooperation agreements with the federal states in 2021. These build the basis for the implementation of specific cooperation projects that will greatly enhance the level of cyber security.

2.3.6 Progress in the Federal Implementation Plan (UP Bund)

The Federal Implementation Plan (UP Bund) is a roadmap regarding information security for the federal administration. The primary goal of UP Bund is the continuous improvement of information security in the federal administration through monitoring and targeted interdepartmental control. Progress of the UP Bund implementation is therefore evaluated annually. Since the new UP Bund came into force in 2017, the method of data collection was redesigned based on a process-oriented approach and conducted for the second time last year.

With the help of a selected maturity level methodology, it was possible to identify concrete measures and present them in form of a report in a prioritised manner in order to effectively and efficiently increase information security in institutions and departments. The division into two areas – the maturity level methodology and the flexible collection of individual and quantitative data outside of the maturity model – has proven successful and will therefore be pursued and optimized on an annual basis. Furthermore, concrete developments could be identified in individual comparisons during the second implementation.

The evaluation is backed by close user support during the survey, for example through accompanying documents or FAQs, but also with the possibility of individual contact when required.

The annual implementation of the survey therefore reveals cross-institutional, department-wide trends in information security, which promotes the effective and efficient prioritization, planning and implementation of measures and sustainably supports the goals of the UP Bund.

2.3.7 Cyber Security for Bundestag and State Parliament Elections

In a democracy, the government's mandate and the actions taken by legislators are ultimately based on elections. In September 2021, six state parliament elections were also held alongside the Bundestag election. Four other state parliament elections will follow in 2022, while the social insurance election in 2023 represents another nationwide vote. Election-related cyber attacks in other countries have demonstrated that both state and non-state actors will attempt to attack, disrupt or even sabotage democratic processes. Examples such as the 'Macron hack' in the 2017 French presidential election vividly illustrate the threat posed to elections by cyber attacks: in this incident, over 20,000 emails stolen from a member of a campaign team were published by attackers one day before the second round of voting.

Alongside state-controlled attempts that specifically target election environments and the processes that shape and inform public opinion (see chapter *Advanced Persistent Threats*, page 28), cybercrime activities such as *ransomware* attacks (see chapter *Big Game Hunting with Ransomware*, page 12) and *malware spam* can also affect voting. In the latter case, attackers are not primarily interested in disrupting or undermining democratic elections, but rather in extorting some form of payment from the organisations involved in the election process. Such activities can significantly weaken public confidence that correct voting procedure has been followed. If a *ransomware* attack targeting a city or district administration were to make email communication temporarily impossible, for example, this could result in delays in voting or the counting of votes. Loss of trust in the voting process on the part of the population is casually accepted as collateral damage by attackers, or may even be the actual purpose of the attack.

While votes are cast in Germany using an analogue format – pen and paper – a wide range of information technology is nonetheless deployed as part of the voting process and environment and to provide information to the electorate. IT, for example, is used for the internal and external communication of both public and non-public information. Voting processes and the voting environment are also becoming increasingly digital. This trend is being amplified further still by the COVID-19 pandemic: party conferences are being held virtually, citizens are increasingly looking to the internet to research their voting choices and election campaigns themselves have long since been fought online – especially on social media platforms.

While organisations and other entities consciously publish and disseminate information such as manifestos or information about the election process in digital formats as part of their communications with citizens who are eligible to vote, they also work with internal, non-public data that is intended for (and therefore only released to) a restricted audience. These types of data are provided with varying levels of protection.

However, information technology is also utilised to conduct attacks against the state, the economy and civil society. Attacks targeting the election process, the voting environment and information provided to the electorate can threaten the availability, confidentiality, integrity and authenticity of information technology in this context.

- To secure the formal voting procedure and the IT support provided to it, the BSI works closely with the Federal Returning Officer and the state return-ing officers. For the numerous parties and candidates participating in elections, the BSI uses its web services and client group services (for public administration, consumers, businesses and critical infra-structure) to provide a comprehensive set of information and recommendations, such as on making further improvements to existing security measures, promoting networking as a source of current information and warnings, utilising IT service providers, and much more.
- Political parties themselves are accorded particular relevance by the Federal Electoral Act, and both they and their leading candidates are particularly at risk of cyber attacks as a result of their public prominence. Accordingly, the BSI provides them with more focused support services that address subjects such as securing their social media channels.
- Monitoring measures are also extended during elections. In particular, these involve a widening of the 24/7 situation monitoring that encompasses the various public, non-public and social media. The BSI also participates in the various federal working groups that seek to identify and assess threats, and also contributes to the design of specific counter-measures. Corresponding reports, warnings, notifications and more are provided across the various channels the BSI maintains for its various client groups.

2.3.8 Information Security Consulting

The BSI's information security consulting for the federal government advises federal agencies on all information security issues. During the last year, the pandemic largely shaped the topics of focus. While initial questions concentrated on the secure design of working-from-home infrastructure and safeguarding remote workstations, the focus shifted towards the security concept for the Corona Warn App and, most recently, towards digital proof of vaccination. The security consulting division also helped secure Germany's national parliamentary elections. Guidelines and handouts for those affected by unauthorised publications on the internet were continuously modified, amended and updated by the BSI. In the field of digitisation, the BSI supported the judiciary in particular. Through intensive cooperation with the Federal Academy for Public Administration, the BSI also supported the training and continuous education of information security officers.

The BSI's information security consulting service for federal states and municipalities provides target-group-specific advice to users at federal state and municipal level on all information security issues, focusing on information security management, security concepts and IT Grundschutz.

During the past year, cooperation among federal, state and local government was further expanded and deepened, particularly in the development of practice-oriented solutions. This included, in particular, support for the development of the requirements catalogue for information security in determining the preliminary election results of nationwide parliamentary elections and the implementation of the associated workshops in the context of information security in state government elections.

2.3.9 Smart Borders and Management of Official ID Documents

The goal of the European Smart Borders programme and EU-wide regulations on the interoperability of European IT systems in terms of security, migration and border control is the secure identification and verification of third-country nationals at the border and within the Schengen Area. To achieve this, the European Entry/Exit System (EES) and the European Travel Information and Authorisation System (ETIAS) are technically connected with the Schengen Information System (SIS) for law enforcement, the Visa Information System (VIS) and other IT systems at the European level. This facilitates centralised and uniform identity management for third-country nationals throughout the EU. Alongside work to increase security within the

Schengen Area, especially in the context of cross-border crime, illegal migration and epidemics, a further objective in this area is the establishment of more efficient border control processes.

In 2020, effective countermeasures against pandemics came to dominate the headlines. This topic is already addressed by the ETIAS Regulation in the version adopted in 2018. Issues such as combating cross-border crime and illegal migration continue to attract attention, since passenger numbers for international flights rose by roughly 50 percent between 2009 and 2019 (see the *bibliography*⁶⁵). The need for effective border controls will therefore continue to be significant once the pandemic is over.

The BSI plays an active part in implementing these various European projects. In 2020, Germany submitted the largest proportion of comments on technical specifications of those EU systems by a wide margin – largely thanks to the BSI's expertise. In relation to European work on related legislation, the BSI maintained a focus on the security of digital identities, drawing attention to potential logical vulnerabilities affecting cross-system processes within European identity management (see chapter Theft and Abuse of Identity Data, page 24). In a national context, November 2020 saw the publication of version 5.1 of Technical Guideline TR-03121, which addresses in particular the new biometrics requirements for border control processes and serves as a basis for national invitations to tender. In 2021, a cooperation of federal agencies under the auspices of the BSI prepared a guideline on digital identity management for the immigration authorities. In parallel to its design of a corresponding specification, the BSI is setting up data analysis for sovereign systems that handle official documents to support the correct and efficient implementation of their components at all levels.

2.3.10 Technology Verification Programme

The Technology Verification Programme puts the BSI in contact with numerous manufacturers of information and communications technology. This technical dialogue is intensified further by 'Security Labs', which serve as a platform for holding meetings and videoconferences with development departments around the globe. They can also be used to pursue more in-depth technical discussions and achieve insights that extend to the perusal of products at the source code level. In this work, BSI employees are supported by experts from accredited audit labs who specialise in code audits and other areas. Thanks to this close collaboration with development units at manufacturers, trends and risks can be identified at an early stage. Customers within public administration represent the TVP's primary client group. The programme constitutes

part of the BSI's responsibility to help shape information security in Germany.

Meanwhile, the TVP focuses primarily on manufacturers, which means that the BSI cooperates closely with these companies on questions of IT and cyber security and receives profound insights into their working practices and internal structures. This work involves regular meetings at corporate head offices and the active shadowing of various positions in these companies by BSI specialists.

As part of the Technology Verification Programme, regular technical discussions are held with international manufacturers from the information and communication technology (ICT) sector to improve the BSI's technical expertise in selected key technologies. These include platform security, virtualisation, hardware security chips and AI. Thanks to its close cooperation with research departments at manufacturers, BSI makes an active contribution to the design of new technologies with an eye towards setting up industry-wide security standards. Meanwhile, the TVP also seeks to make connections between verified key technologies and the operational networks of customers. Since these goals can be achieved only with the support of manufacturers, the BSI invests in long-term partnerships.

During the reporting period, the implementation of key technologies was primarily investigated in relation to 5G network components. A corresponding Technical Guide-line is now in preparation. In addition, audit catalogues are currently being drawn up based on existing Technical Guidelines.

2.3.11 App Testing for Mobile Solutions

While the use of apps extends the usefulness of mobile devices, it also presents security risks to both the data processed and the overall device in question. These risks need to be properly assessed.

The BSI's *app* testing service, which is provided to federal agencies in partnership with Deutsche Telekom Security GmbH, offers a set of criteria to aid decisions about whether to deploy an *app* and under which conditions.

The *app* tests performed take into account issues relating to both security and data protection. The test reports may also include information and recommendations for *app* users concerning the settings they should consider to enhance security.

If test results justify such a decision, the BSI also reserves the right to warn explicitly against the use of a specific *app*.

People at government agencies who take advantage of this *app* testing service can access a wide-ranging repository of test results already available and initiate new tests if required. Requests can also be made to have apps tested on a continuous basis to ensure that results for apps previously approved for use can be kept up to date.

As of this writing, the BSI's *app* testing service is now being used by registered individuals from over 50 government agencies and organisations. Test results are now available for more than 650 apps.

For around 70 percent of these test results, information and recommendations have been provided that should be observed while using the *app* in question. A warning against use has been issued for around one in six apps.

2.3.12 Countersurveillance

The BSI's countersurveillance unit advises organisations on wiretapping security and inspects facilities secured against wiretapping pursuant to classified information regulations (VSA) for the federal government, federal agencies and companies that handle classified information; assistance is also provided to state administrations. The unit is also consulted for political conferences or those of a similarly important nature when their agendas involve the discussion of topics that require a high level of secrecy.

During the last period, the coronavirus pandemic meant that no high-level political conferences took place face-to-face, where a discussion of classified information would have required the support of the BSI. For the same reason, only a limited number countersurveillance audits were conducted on-site. During this period, the focus was instead on basic research and project work.

2.3.13 Classified Information Product Approval and Developer Qualification

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

The BSI issued or extended over 91 approvals in the reporting period, which is in line with previous years. There are now a total of 209 approved IT security products and product versions. Products with general approval can be found by consulting the latest BSI Publication 7164.

As a result of the COVID-19 pandemic, the BSI has observed a sharp rise in the need for approved solutions that permit the secure handling of classified information even when working within a home environment. In particular, the approval instrument “Freigabeempfehlung” defined by VSA section 51 has ensured an efficient approach to supplying government customers with such solutions in a targeted manner at short notice. For the federal armed forces, the procedure for scenario-specific approvals (VSF) was used on multiple occasions in this context. By using the VSF procedure, the BSI was able to legitimise the armed forces’ handling of classified information while working from home in a matter of days.

To implement the VSA, which was revised in 2018, the BSI has published a Technical Guideline TL-IT 01, ‘Duties of Cooperation in Approval Procedures’, as well as a catalogue of the product classes and types relevant for approval. BSI TL-IT 01, which is based on VSA section 52(1), specifies the duties of cooperation for all parties participating in an approval procedure. The catalogue of product classes and types is a reference document for the types of IT security products requiring approval and the security functionality these products must provide. It is designed to be easy to update and extend.

Further information about approvals, including the above-mentioned publications and BSI Publication 7164, can be found on the BSI website (see *Bibliography*⁹⁾.



Developer qualification

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

Classified Information Requirements Profiles

Classified Information Requirements Profiles (VS-Anforderungsprofile, VS-AP) define IT security requirements for IT security products that are subject to approval. These requirements are defined as part of a cooperative process involving governmental users, operators and the BSI. This approach ensures that security requirements are defined by means of an approach that is harmonised, efficient and tailored to clients’ needs. A total of 16 VS-APs for various product types have now been finalised, and there is already a range of IT security products that conform to these BSI specifications. During the reporting period, three VS-APs were published and work began on two further profiles. Since VS-APs represent a standard that is continually adapted to recent technical developments, one VS-AP is now being revised and amended. Many other VS-APs are also currently in preparation.

A detailed description and listing of completed and pending CIRPs can be found on the BSI website (see *Bibliography*²⁾).



2.3.14 Messenger Services for the Secure Communication of Classified Information

There are many opportunities to use contemporary communication channels in the work performed by the federal administration – whether to ensure easy availability when working from home; coordinate work among agencies for a security incident; or communicate with businesses, citizens or European partner agencies. Alongside data protection aspects, enhanced security may also be required in an agency context, especially when work involves transferring data that is sensitive or defined as classified information (VS-NfD) by the VSA (see chapter Classified Information Product Approval and Manufacturer Qualification, page 76). For this reason, the BSI has been evaluating messaging solutions for some time now, and the Wire messenger in particular.

Just before the start of the German EU Council Presidency, a VS-NfD release recommendation for the on-premise use of Wire in the federal administration was issued in early June 2020. Alongside further development on the product itself, a more in-depth evaluation is also planned with an eye towards VS-NfD approval. Other messengers that aim to obtain VS-NfD approval in the future include BwMessenger from the federal armed forces (which is based on the Matrix protocol) and the SecureCOM messenger from Virtual Solution AG.

Wire is a fully featured messenger that, in addition to sending text and voice messages, files and images, can host conference calls and videoconferences and share screen content. To ensure that it can maintain a very high level of security, Wire guarantees the end-to-end encryption of all data and also minimises the collection of metadata. Encryption is based on the Double Ratchet protocol (see the *bibliography*⁶⁶), which is currently considered to be the state-of-the-art approach for messaging solutions.

Outside of the agency context, there is also a keen interest in both the economy and civil society for secure communication when working with the authorities or among one another so as to prevent corporate espionage (for example) and avoid leaks of personal data. The Wire project is working towards meeting this need in the future by exploring the possibility of combining various systems. One key aspect of this work is a migration to the cryptographic protocol based on the MLS (Messaging Layer Security) standard (see the *bibliography*⁶⁷). This is currently being finalised within an IETF working group (see the *bibliography*⁶⁸) and will, among other aspects, enable interoperability among different messaging solutions.

2.3.15 Implementation of the Online Access Act

Following its entry into force in 2017, the German legislation to improve online access to administrative services (the Online Access Act, OZG) requires federal, state and local administrations to extend their service provision to digital administration portals and to link these together into a portal network by 2022. To make use of these services, it is essential that both private citizens and organisations be able to identify and authenticate themselves online against the user accounts provided at the federal and state levels as stipulated by the Act.

Criteria for the secure integration of identification and authentication procedures with these user accounts are set out in part one of BSI Technical Guideline TR-03160, 'Service accounts'. These criteria guarantee the identity of these users at the respective assurance level for the business processes connected to the corresponding user accounts without requiring the users to know the exact details of the identification and authentication. Part two of TR-03160 defines criteria for guaranteeing the interoperability of federal and state solutions so as to ensure that users only need to complete the identification procedure in one state to utilise the services of a different state or those provided at a federal level. Both parts have been approved by the

federal and state administrations in their role as operators and published on the BSI website.

As regards linking electronic proof of identity on smart-phones (Smart eID) with the service accounts offered at the federal and state levels, a guideline for integrating Smart eID with a user account has been published. (See the *bibliography*⁶⁹)

The user accounts pursuant to the OZG provide inboxes for the electronic delivery of official documents created by business processes. Requirements for the security and interoperability of the various inbox solutions are currently being consolidated into Technical Guideline TR-03160-3, 'Interoperable inboxes'.

Cryptographically secure barcodes can also be attached to these documents so that their integrity can be confirmed when they are submitted as printouts or displayed on mobile devices. These kinds of digital seals conforming to TR-03137 are already being used on official documents such as proofs of arrival to verify that the printed data is indeed genuine. The new Technical Guideline TR-03171 also enables certificates, notifications and other administrative documents issued at the federal, state and local levels to be secured by means of an optically verifiable digital seal.

2.4 International and European Collaboration

IT security is an issue that transcends national borders. This means countries must join forces to effectively counter threats in cyberspace. The BSI firmly believes that cyber security in Germany is strengthened by international collaboration and worldwide exchange. Whether bilaterally, multilaterally or in committees and working groups, the BSI has worked with global partners since its formation over 30 years ago. Its own experts are also sought out for their expertise and advice, and as speakers at industry events.

Complementing its national mandate as the cyber security agency for the German federal government, the BSI also aims to shape international developments in the field while strengthening its own competencies in technological assessment. To properly fulfil its responsibilities in this context, the BSI continues to intensify and expand its relationships with agencies, organisations and companies, as well as key actors in research and civil society around the world. It also opened a liaison office in Brussels in December 2019. Participation in various expert committees addressing information/cyber security in the context of the EU, NATO and the world at large forms an important part of BSI's international engagement.

2.4.1 BSI Engagement in the EU

During the reporting period, the German EU Council Presidency in the second half of 2020 formed the key point of focus for BSI's engagement within the European Union. The BSI substantially contributed to the development of the key issue in cyber security, namely the definition of minimum requirements for the security of connected devices (see section, 'Security in the Internet of Things, smart homes and smart cities', page 50). The topic was then showcased as part of a digital EU cyber security conference organised by the BSI together with the BMI, which was attended by over 400 delegates from European cyber security agencies. This German initiative culminated in the adoption of Council conclusions. Since then, the topic has been on the European agenda and was, for example, also addressed in the new cyber security strategy adopted by the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy. At the end of 2020, owing in part to the contribution made by the BSI's liaison officer, the German Council Presidency achieved a consensus with the European Parliament on a European Cybersecurity Industrial, Technology and Research Competence Centre. The BSI also played an active role in preparations for the establishment of the corresponding National Coordination Centre (see section 2.4.3).

Negotiations on a 'Proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148', known as the NIS Directive 2.0, have been ongoing since the start of 2021. Under the auspices of the BMI, the BSI has played an active part in these negotiations. At the same time, the BSI has also been active in various European cyber security bodies, including the NIS Cooperation Group, the CSIRTs Network, the European Cybersecurity Certification Group, and the various committees and working groups of the European Union Agency for Cybersecurity (ENISA).

2.4.2 Multilateral and Bilateral Engagement of the BSI

The BSI's multilateral and bilateral engagement is multi-faceted and encompasses a wide range of topics. As part of these activities, it maintains close and mutually beneficial relationships with many foreign partner agencies. The spectrum of this work ranges from the day-to-day exchange of operational information and dialogue on technical matters to strategic discussions in a policy context.

The BSI also performs a key function both within and vis-à-vis NATO in its roles as the National Communication Security Authority (NCSA) and National Cyber

Defence Authority (NCDA) for Germany. In the corresponding NATO committees, the BSI contributes its national insights and strategies and also helps shape and steer core topics such as cyber and information security within the Alliance.

Brexit was another important topic in 2020. The BSI believes that a good working relationship with the UK is important in the realm of IT security in the international context as well as for Europe's pursuit of digital sovereignty. In light of this, the BSI intensified its dialogue with its British partner agency, the National Cyber Security Centre (NCSC), on a range of technical topics. Roughly one year post-Brexit, the results have been very positive, and the long-standing and trusted working relationship between the NCSC and the BSI was certainly a contributory factor. Technology leadership and digitalisation both have key roles to play as part of the Integrated Review, a strategic repositioning of the UK in terms of foreign and security policy that was presented by Prime Minister Boris Johnson in March 2021. The BSI is tracking these developments closely to sound out opportunities for additional cooperative projects, such as in the secure design of new technologies.

Of particular note in 2020 was the BSI's work with the Polish Ministry of Digital Affairs regarding the implementation of the EU toolbox for 5G security. As part of the NIS Cooperation Group, the BSI took on a leading role with Poland in implementing the measures in relation to certification and standardisation. In one notable achievement, the EU Commission entrusted the BSI to produce EU-wide certification schemes within the scope of the Cybersecurity Act.

2.4.3 National Coordination Centre for European Research Projects

At the end of 2020, the Council and the European Parliament adopted a decision to set up the European Cybersecurity Industrial, Technology and Research Competence Centre, along with a network of national coordination centres. The corresponding Regulation entered into force in May 2021. From its headquarters in Bucharest, the competence centre help consolidate investments in research, technology and industrial development. In particular, this should improve coordination in planning the European subsidy schemes Horizon Europe Programme (HEP) and the Digital Europe Programme (DEP) in relation to cyber security.

The competence centre will also pursue its own research and innovation measures (with support from HEP), as well as capacity-building measures (with support from DEP) as an independent body. In addition, the centre and the net-

work of national coordination centres are to work towards achieving stronger synergy effects and tighter coordination between the civil sectors and the defence sector in cyber security. The needs of SMEs are to be properly accounted for all these activities.

The competence centre will be managed by the Member States and the European Commission. An advisory council will be set up for this purpose, with the BSI representing German interests. The competence centre is intended to ensure greater coordination in the field of research and innovation, and in relation to rollout strategies at the European and national levels. The Member States will decide on common measures and projects for the centre.

For its part, the network of national coordination centres is intended to intensify dialogue between the Member States to ensure that international project partnerships can be identified and agreed more rapidly and effectively. This will help strengthen digital sovereignty within Europe. These centres will promote communication among the Member States on relevant national entities in the fields of research and the economy relating to cyber security and cyber defence. They will also consolidate the flow of information to the European Cybersecurity Industrial, Technology and Research Competence Centre with the aim of providing an optimum level of support to the national cyber security communities. At the same time, this will facilitate the incorporation of national interests in the planning of European research programmes.

The German National Coordination Centre for Cybersecurity in Industry, Technology and Research (NKCS) will be set up by the Federal Ministry of the Interior, Building and Community (BMI), the Federal Ministry for Economic Affairs and Energy (BMWi), the Federal Ministry of Defence (BMVg) and the Federal Ministry of Education and Research (BMBF) as a shared collaboration platform. The BSI will be appointed as the project lead and single point of contact (SPoC). Direct use can also be made of existing structures within the departments and institutions involved – those for awarding grants, for example. This national coordination centre will be responsible for creating a comprehensive service catalogue that will reference current services at the federal level and offer open-access services to support the cyber security community. In the field of cyber security, this is intended to create a national digital ecosystem and, with the national coordination centre under the aegis of the BSI, to consolidate all the relevant information required for the promotion of German cyber security research and development.

In this role, the BSI will work closely with the participating departments, as well as with the European competence centre and the coordination centres of the other Member

States. For the German cyber security community, this will result in a broad-based overview comprising designated contacts, support services, events, projects, research institutes and potential research partners, research programmes, grants and research proposals. In carrying out this new role, the BSI will be able to steer the targeted awarding of European funding in an even more active way and provide support to fields of research from both a national and a European perspective. All this will make a direct contribution to improving cyber security within Germany and the EU.

2.4.4 eID: EU-wide Recognition of Germany's Online ID Card

To achieve a successful digital transition, the secure identification of people and things is of critical importance (see chapter Smartphone-based Secure Electronic Identities, page 55). As regards digitalisation within the European Single Market, the eIDAS Regulation (which was adopted in 2014) therefore moved to establish a uniform framework valid across Europe for the mutual trans-boundary recognition of electronic identification methods and trust services at the EU level.

With the active involvement of the BSI, Germany's introduction of the online function for its ID cards and electronic residence permits in 2017 made it the first Member State to complete the notification procedure that is the precondition for recognition. The notification of this online function at the highest assurance level according to the Regulation was accordingly published in the Official Journal of the EU in September 2017. This notification was expanded in 2020 to include the new EU eID card. A mutual obligation of recognition has therefore existed since 2017 (or will from the end of 2021 in the case of the EU eID card). Since this time, all EU/EEA Member States that operate corresponding online services must recognise and integrate the German online ID card for public-sector applications, particularly in the context of e-government.

As a result, 18 countries (Austria, Belgium, Croatia, Denmark, the Czech Republic, Estonia, Finland, Greece, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Slovakia, Slovenia, Spain and Sweden) had already successfully integrated the German online ID card into their own eID schemes by April 2021, with technical support being provided by the BSI. This means that it is already possible to use the online ID card for online services in over half of the other EEA Member States. While some of the remaining Member States do not operate online services and are therefore exempted from the recognition obligation, eight countries (as of April 2021) are now running or preparing to run pilot systems. Further growth in coverage can thus be expected in the near future.

Other countries are also making efforts to have their eID schemes notified. By the end of April 2021, a total of 14 other countries had done so (Belgium, Croatia, the Czech Republic, Denmark, Estonia, Italy, Latvia, Lithuania, Luxembourg, the Netherlands, Portugal, Slovakia, Spain and the United Kingdom). Other procedures have now been initiated or are nearly complete.

Key differences can be seen among the eID schemes of these various countries. While many of the ID systems assessed do in fact use national ID documents based on chip cards, others are based on the use of certified SIM cards or other hardware- or software-based security properties possessed by end devices. App-based procedures are now an increasingly common type of solution, although their evaluation depends heavily on the security functions offered by the mobile device used. This diversity of approaches naturally entails a range of different evaluations as part of the appraisals conducted during the notification procedure, and the results represent the full spectrum of possible assurance levels.

The notified electronic identities of the other countries will be integrated into German e-government (and thereby recognised) with the aid of the user accounts and citizen portals implemented as part of the Online Access Act (OZG).

In 2020, a formal review of the eIDAS Regulation began, which will aim to retrospectively assess the successes and failings of the Regulation and prepare any amendments that prove necessary. In 2021, the EU Commission submitted a proposal for a revision of the eIDAS Regulation.

2.4.5 Crypto-Modernisation for Satellite Systems

To function as intended, our public administration, economy and civil society are increasingly dependent on digital services for communication, navigation, geolocation and timekeeping, as well as for climate monitoring and weather forecasting. In many cases, only satellite-supported infrastructures can implement these services.

Information forms the basis for planning, knowledge and decision-making in private, economic and public administrative settings. This incentivises hackers or criminal groups to try to capture this information or disseminate incorrect information. The availability of systems, services and information – as well as their integrity and confidentiality – are essential to all users of our government, industry and society.

This makes the cyber security and IT security of satellites a key field of operations for the BSI. While one major focus is the EU's GALILEO navigation system, the BSI maintains an interest in the satellite sector as a whole. Together with other Member States, under its auspices BSI developed a criteria catalogue to prepare satellite systems and their communications infrastructure for future challenges. One important requirement here is resistance to the threat posed by quantum computing. In 2020, the GALILEO programme successfully incorporated demands to modernise the IT and cyber security of satellites and their ground-based infrastructure into development work on the second generation of the EU's GALILEO navigation system. They will launch the first satellites equipped with modernised cryptography systems in 2024.

2.5 Current Trends and Developments in IT Security

The rapid pace of technological development presents IT security agencies with a constant stream of challenges for which definitive answers must be found. In some cases, however, these answers can also be derived from the novel technologies themselves, which sometimes give security experts a set of new and practical options for the identification and timely interception of security-relevant incidents. In fields such as artificial intelligence (AI), *blockchain*, quantum computing or cryptography, the BSI works closely with technical and research universities and other research institutions in order to come up with new answers to the latest security issues.

2.5.1 Artificial Intelligence

Methods from the field of artificial intelligence have long since matured into key technologies as a result of their capabilities in many application domains. AI techniques are increasingly gaining ground in government, business and society and making an important contribution to digitalisation. However, many important questions about the security properties of AI systems and the potential use of AI for IT security applications have yet to be fully resolved. The BSI engages in answering these questions as part of its responsibility to ensure the secure design of technology.

To ensure the secure deployment of AI, organisational and procedural specifications are needed, as are technical requirements for the development and operation of AI systems. In relation to these technical requirements, the BSI continued its comprehensive analysis work on the security properties of AI systems in the previous reporting period. In an overview document (see the *bibliography*⁷⁰) that can serve as an initial starting point for AI providers

and professional users of such systems, the various measures and action areas for the secure, robust and plausible deployment of AI were summarised and introduced. The two types of requirements mentioned above (namely organisational/procedural and technical) were also taken into account (see *Bibliography*^{aa}).



AI in standardisation and certification work

The BSI also applies its expertise and working results to standardisation activities at the national and international levels. In this context, it contributes to AI-related initiatives and bodies within the DIN, the ISG SAI (Securing Artificial Intelligence) working group (see the *bibliography*⁷¹). At the end of 2020, an AI standardisation roadmap was presented at the Digital Summit (see the *bibliography*⁷²). This roadmap, which the BSI also helped prepare, represents in particular a significant national contribution to the development and establishment of AI-specific standards. In the future, the BSI will also be closely involved in the standardisation and transposition of the EU Artificial Intelligence Act.

To ensure that the use of AI can be designed to be verifiably secure and trustworthy, it is important to develop corresponding audit criteria, procedures and methods. The BSI is working closely with the areas of business and research in this field. One milestone on this path was the signing of a strategic cooperation agreement between the BSI and Fraunhofer IAIS on the joint development of audit procedures in November 2020. In early 2021, the first project in this collaboration was completed with the inauguration of the 'Certified AI' flagship project for the AI Competence Platform run by the State Government of North Rhine-Westphalia (KI.NRW; see the *bibliography*⁷³). The results obtained by this project will form the basis for a uniform set of auditable standards.

Domain- and application-specific results

Audit procedures and methods, as well as the standards themselves, are being developed under consideration of the domain- and application-specific characteristics of AI systems. In two key application domains, namely transport and *cloud* services, the BSI has worked hard to promote the secure deployment of AI in the relevant user groups.

In the context of digitalisation, AI techniques continue to play an increasingly important role in the execution of security-critical functions. The use of these systems in the biometric identification and verification of individuals (see chapter Biometrics in the Age of Artificial Intelligence, page 81) is already ubiquitous, for example. AI techniques are also being increasingly deployed in transport solutions

such as (semi-)autonomous driving. Here, the relevant application areas include the processing of imaging data, such as for the detection and recognition of traffic signs or other road users. Since 2019, the BSI has been running a working group with the Association of TÜVs (VdTÜV), which develops models for the secure deployment of AI techniques in the automotive sector. In October 2020, the working group organised an international workshop with the participation of a number of distinguished speakers, which focused on the question of auditing AI techniques. The results of the workshop were published in a white paper in May 2021. In addition, the BSI organised the execution of exemplary robustness tests for AI techniques in traffic sign recognition (see the *bibliography*⁷⁴). The BSI views tests of this kind as one component in approaches to guarantee the secure use of AI techniques in the automotive sector. It plans to develop these tests further and generalise them to include other use cases.

With the publication of the AI Cloud Service Compliance Criteria Catalogue (AIC4; see the *bibliography*⁷⁵) in February 2021, the BSI took an important initial step towards applying organisational and procedural requirements to strengthen information security in the use of machine learning and *cloud* services. The catalogue extends the established BSI C5 (see chapter Security of *Cloud* Services, page 67) to include AI-specific requirements. It defines a minimum level of security and trustworthiness for AI *cloud* services and formulates criteria that can be checked as part of a standardised audit procedure. A corresponding audit report not only establishes a high degree of transparency between *cloud providers* and professional *cloud* users. When the findings are interpreted correctly, it can also form the basis for an independent assessment of the information security level of the service in question. The criteria catalogue will be developed gradually by the BSI as part of a broad-based, participative process and also adapted to reflect recent research findings (see *Bibliography*^{bb}).



AI in cryptography and side-channel analysis

The BSI continues to track the use of AI techniques to resolve questions in cryptanalysis and side-channel analysis, and has once again made significant contributions to this domain. In September 2020, for example, a BSI team enjoyed considerable success as participants in the CHES* Challenge. AI techniques were used to break implementations that had been specifically shielded against *side-channel attacks*. At the end of the day, the BSI team had won every prize on offer and was hence crowned the overall winner. The results produced in both cryptanalysis and side-channel analysis are being used to update and

supplement existing requirements for the security of cryptographic methods and implementations.

Expansion of AI unit at Saarbrücken support office

The BSI's activities in the field of AI to date will be further intensified by the establishment of a new BSI support office in Saarbrücken and by new thematic areas to be addressed. Apart from expanding the BSI's technical examinations of AI security, the Saarbrücken office will also work on the technical principles of digital consumer protection in the field of AI. In addition, the new support office will facilitate improved dialogue with French and other European partners to also ensure that AI security standards are also being promoted at the international level.

2.5.2 Cryptography

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

The standardisation of post-quantum cryptography essentially stems from a process initiated by the US National Institute for Standards and Technology (NIST) that includes broad international participation. NIST has announced some initial draft standards for 2022–23. Alongside standardisation, many activities are now focusing on the migration to post-quantum cryptography. That said, the topic of quantum computer resistance is also picking up speed in the field of public key infrastructure and application scenarios for digital certificates. A number of approaches are now being discussed (hybrid certificates, mixed PKI, alternative signatures, etc).

In addition to some initial key transport mechanisms with quantum computer resistance, Technical Guideline TR-02102 (issued in March 2021) recommends the hash-based signature schemes LMS and XMSS. The BSI also updated its recommendations in migrating to post-quantum cryptography (see the *bibliography*⁷⁶) in August 2020. A long version of these recommendations for action is planned for publication in autumn 2021. Further information on the topic can also be found on the BSI website (see the *bibliography*⁷⁷).

2.5.3 Quantum Key Distribution

Quantum key distribution (QKD) is a technique for quantum computer-resistant key exchange that is based

on the theoretical security derived from the principles of quantum mechanics. The BSI considers QKD a potential supplement to post-quantum key exchange schemes. This only pertains to specific application fields, however, since the technical requirements for QKD are very restrictive.

Unlike conventional and post-quantum algorithms for key exchange, special hardware is required to be able to exchange quantum states. Alongside the theoretical security of QKD, its implementation security must also be considered. This means that it is important to develop evaluation criteria for QKD modules. The BSI is currently working with ETSI to have a Protection Profile (PP) prepared according to the Common Criteria. This Protection Profile is, however, limited to point-to-point connections and a certain class of QKD protocols ('prepare-and-measure' protocols). The PP will not initially consider entanglement-based QKD or network aspects. It aims to comply with Evaluation Assurance Level EAL-4+AVA_VAN.5+ALC_DVS.2, which assumes a high attack potential and also factors in the lifecycle of each product. Initial drafts have been distributed to groups such as the ETSI QKD Industry Specification Group for comment. For the subsequent applicability of the Protection Profile, a QKD product certification system needs to be set up in which audit criteria and evaluation methods – such as for *side-channel attacks* – can be coordinated and developed further.

Numerous projects in the field of QKD are being funded within Germany and Europe at the moment. The EU's EuroQCI project, which now includes the participation of 25 EU Member States, aims to establish an EU-wide quantum communication network. Both terrestrial and satellite-based components are planned here. The BSI is represented in the project's Security Group, and it is also playing an advisory role in an EuroQCI architecture study that is currently being prepared for a quantum communication network.

The QuNET initiative, which is funded by the Federal Ministry of Education and Research (BMBF), is investigating various aspects of quantum communication. Several demonstration networks are planned for the next project phase. The BSI is supporting this research initiative as a member of its advisory board. The BSI is also an advisory board member in the BMBF-funded project Q.Link.X, which is focusing its research efforts on quantum repeaters. In the medium term, these devices should ensure the end-to-end security of fibre-based QKD over longer distances.

In light of the interest and funding that QKD is currently attracting, the BSI sees a need for action in a number

***Conference on Cryptographic Hardware and Embedded Systems

of areas to achieve the ambitious security objectives of planned implementations. Standardisation activities in the field of QKD should be intensified, for example, and further effort should be made to research and evaluate implementation security. Given the importance of digital

sovereignty, European manufacturers of QKD products also enter the market. For its part, the BSI is planning further studies to examine several aspects of the theoretical and practical security of QKD.



Quantum computers: development status

To obtain a sound assessment of the current state of development and the potential future availability of quantum computers, the BSI commissioned a study entitled 'The State of Quantum Computing' from researchers at Saarland University (Germany) and Florida Atlantic University (USA).

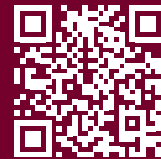
The study examines current technological approaches and quantum algorithmic innovations in detail and discusses their implications in the context of cryptography currently in use.

The two revisions of the 2019 and 2020 study showed that algorithmic and technological advances can reduce the number of physical quantum bits (qubits) required, as well as the size of the quantum circuits needed for a given task.

Specifically, the Google experiment on quantum supremacy and other optimisation heuristics were described and evaluated in the cryptographic context in the second 2020 revision.

The study, together with an executive summary, can be downloaded from the BSI website at <https://www.bsi.bund.de/qcstudie>.

A continuation of the study is being planned.^{dd)}



2.5.4 Blockchain

Blockchain remains a hotly debated topic in the field of information security. As with all new technologies, the security of *blockchain* should be considered from the outset and a secure-by-design approach should be pursued.

Cryptocurrencies represent one of the fields in which *blockchain* is used. In 2021, the BSI accordingly published a position paper on the security of DLT-based cryptocurrencies as part of its 'Designing Secure Blockchains' series of publications. DLT stands for distributed ledger technology, which (like *blockchain* itself) implements a decentralised, publicly accessible record of transactions.

The BSI had already addressed the secure design of DLT applications in detail in several earlier publications.

Owing to the current interest in this topic, however, its latest position paper once again explicitly summarises the aspects that have been identified as core factors in establishing the IT security of DLT-based cryptocurrencies.

In the study 'Security Analysis of Selected *Blockchain* Applications', the BSI prepared a market overview of *blockchain* applications and provided sample evaluations of selected products from various product classes. Key findings from the study have been published on the BSI website (see *Bibliography*^{dd)}). All the BSI's other publications on *blockchain* technology can also be downloaded there.



3 Conclusions



3 Conclusions

Digitalisation needs defending

This year's report on the state of IT security in Germany has again been marked by the effects of COVID-19. The impact of the pandemic throughout society has also had consequences for the working environment in almost all public authorities, organisations and businesses. Meanwhile, the challenges that have arisen in information security have not resulted solely from the tremendous increase in people working from home. Thanks to the special role they took on in combating the pandemic, businesses suddenly found themselves confronted with an entirely new threat landscape – and with necessary protective measures that changed virtually overnight. This new situation has naturally also affected work at the BSI over the last 12 months.

The BSI's working from home study revealed the risks to which companies are exposed, for example: up to 25 percent of the companies surveyed that needed to respond actively to a cyber attack described this attack as either a serious or an existential threat. In COVID-19 test centres, serious vulnerabilities were also repeatedly discovered in web applications. Sensitive data such as test results and addresses could be viewed online and therefore abused. Of particular concern were the attacks that targeted essential facilities such as the European Medicines Agency, vaccine manufacturers or hospitals.

The BSI works closely with IT security researchers to detect and respond to these kinds of attacks, and is therefore often able to prevent a worst-case scenario. The underlying problem remains, however: digitalisation projects born of necessity rather than strategy neglect information security and therefore endanger entire company networks. Software applications that are quickly cobbled together present a security risk to sensitive data – one that may often go entirely undetected by affected consumers. All too often, functionality is provided quickly rather than securely. This can backfire and endanger the success of digitalisation as a project.

The combination of speed and security is possible, however – as the Corona Warn App (CWA) has demonstrated to impressive effect. The BSI has supported the app's development and security modelling from the outset and continues to provide regular auditing and testing. To date, no IT security incidents are known to have occurred in connection with the CWA app. The BSI has also provided specific recommendations on maintaining security when working from home, operating corporate

networks and many other kinds of digital applications. As Germany's Federal Cyber Security Authority, the BSI sees itself as the architect of a secure digital transition that will only succeed through the combination of information security and digitalisation. These are the two sides of the same coin – and of the BSI.

Cyber extortion attempts becoming the number-one threat

The threat landscape is not merely the result of a failure to implement IT security measures, however. As the BSI observed during the reporting period, the numbers of *malware* variants regularly hit record highs, and significant developments were also seen in the quality of attacks. Attempts at cyber extortion in particular are now an increasingly common phenomenon. With ever-greater frequency, cybercriminals are encrypting data at businesses and organisations in sophisticated, multi-stage attacks aimed at extorting ransoms. The consequences are often extreme and can result in network outages lasting days or weeks – periods in which production or the provision of services is either extremely limited or no longer possible.

A decisive role has been played by the Emotet *malware* in this context. Security experts estimate that Emotet alone is responsible for losses of some USD 2.5 billion worldwide, with this sum reflecting both its crippling effects on IT infrastructure and the ransoms it has extorted. While the infrastructure for this particular *malware* was successfully taken down and destroyed in January 2021, the underlying threat remains. The BSI's situation report clearly shows how cybercriminals continue to hone and refine their attack strategies.

Vulnerabilities remain one of the greatest challenges

A security hole in Microsoft Exchange servers that remained open until March 2021 is symbolic of one of the greatest challenges facing information security, namely the handling of vulnerabilities. With the technical means at their disposal, cybercriminals are well positioned to *exploit* these kinds of flaws. One particularly alarming fact is that while Emotet still needs a user to click on a link or a file attachment, the kind of vulnerability found in Microsoft Exchange can be exploited without any intervention on the part of the user. Immediately after news of the hole was published, a wave of attempts at sniffing out and compromising vulnerable Exchange servers was observed. The BSI assessed the situation as

extremely critical and assigned it the second-highest threat level – ‘IT crisis (limited)’. This was only the third time in its history that the BSI had issued a warning in this category. While the high proportion of vulnerable servers (98%, with a total of around 65,000 servers affected in Germany alone) was reduced to less than 10 percent after two weeks, this was only possible thanks to urgent warnings issued by both the BSI and Microsoft to the affected companies. Despite these efforts, scans still revealed over 4,000 vulnerable servers in May 2021. While an update has successfully closed the security hole itself, further measures must nonetheless be taken: the BSI considers it entirely plausible that *malware* infections may have taken place before the vulnerability was actually patched. As these compromised systems continue to be operated, they may lead to damaging cyber attacks even weeks or months later. Such systems are therefore a ticking time bomb on the servers of affected organisations.

Through the Warning and Information Service (WID) provided by the federal administration’s Computer Emergency Response Team (CERT-Bund), the BSI provides regular, timely and free information about vulnerabilities, security holes, and other current threats to IT systems for government, business and civilian subscribers. For these information services to be effective, however, companies, organisations and ordinary citizens need to take these threats seriously and implement the necessary countermeasures. Unfortunately, progress still needs to be made in this regard. Related failings have been demonstrated not only by the Exchange incident, but also by the BSI’s own study on cyber security when working from home. Small and medium-sized businesses in particular are still falling short of the security measures that would adequately protect their home working environments from cyber attacks.

Cyber security made in Germany

Cyber security is increasingly being seen as a competitive advantage for companies in Germany. Ensuring that a business can continue as a going concern (business continuity management) and confirming the security of IT products are two issues that are addressed by support services from the BSI. Information security must also be seen – and sold – as a feature because it encourages consumers to accept and trust corresponding products.

This can be clearly seen in the case of autonomous driving, where secure networks and technologies are absolutely essential: no-one will get into a self-driving car if their safety and that of other road users is not guaranteed! The BSI contributes to numerous national and international bodies and committees working on

the standardisation and certification of technologies in this field (such as AI) and also cooperates closely with both business and research. For these and other fields of application for AI, the BSI has also completed important groundwork for the improvement of cyber security in AI in its Criteria Catalogue for AI-Based *Cloud* Services (AIC4). Prior to its publication, there had been no comparable, ready-to-use audit standard available for secure AI systems.

Another aspect is the security of medical devices. These can also be improved by a greater degree of networking and the use of AI, but they are only deployable in practice when they do not pose a risk to patient safety. While successful BSI projects such as ManiMed (‘manipulation of medical devices’) are very important, they are still only able to address individual aspects of the much larger topic of cyber security in healthcare.

This is why the BSI always keeps an eye on the future. Alongside the ‘Quantum Computers – The State of Play’ study that was completed together with researchers from Saarland University and Florida Atlantic University, the BSI is also actively assessing and evaluating quantum key distribution (QKD), for example, and working to support its deployment. The list of new technologies that are the subject of BSI research goes on to include *blockchain*, smart homes, smart cities and more.

To concentrate its expertise in key topics, the BSI is also setting up competence centres at its main sites and support offices. Its Freital office, for example, focuses on 5G/6G. In this case, the BSI benefits from its strong networking with local partners, whose knowledge is further reinforced by the presence of other key technology companies in the region. With the opening of its support office in Saarbrücken in June 2021, the BSI is now pursuing further activities in the field of artificial intelligence, as well.

While this work on research, communications and prevention is certainly important, however, it is not enough in isolation. As well prepared as an organisation may be, its protection against attacks can never be complete. The most recent reporting period has once again demonstrated the rapid pace of development and the professionalism with which cybercriminals go about their work. For public authorities, businesses and organisations, this means preparing for the worst-case scenario. Information security needs to be structured and implemented with the aid of an information security management system and understood as an investment in the future success of any business. Every technical implementation must always reflect the current state of the art if it is to adequately protect business operations. This is the only way that digitalisation will succeed.

Looking to the future

The last 12 months have underlined the fact that the threat posed by cybercriminals to our digital society continues to grow. On the one hand, these attackers are able to cause widespread damage, as in the case of the oil pipeline attack in the USA, which caused several days of oil shortages in some regions. Attacks targeting companies can cause massive losses of revenue and, in the worst case, even lead to bankruptcy. Cyber attacks on hospitals can cause life-threatening situations. On the other hand, cybercriminals also weaken the trust placed in digital technologies. Without this acceptance on the part of users, the digital transition will not succeed. Successful digitalisation can be achieved only if cyber threats are actively countered and people in Germany – whether in a private or professional capacity – are able to act as alert, informed and prudent citizens. Proactively addressing cyber threats while raising awareness and providing support to the people of Germany are core responsibilities of the BSI, which plays a central role as the architect of the country's secure digital transition.

In her opening address to this year's German IT Security Congress, Chancellor Angela Merkel neatly summarised the situation as follows: "Digitalisation and information security belong together. We need to be strong in both of these areas, as our performance here will have a significant impact on Germany's future success. In light of these facts, the BSI clearly has an important role to play and will continue to do so in the future."

The secure development of the Corona Warn App, the development of AIC4 as the world's first standard for secure AI applications, and the modernisation of the IT Security Act underline the Chancellor's words and highlight the potential of the BSI. However, these positive developments stand in contrast to the fast-paced trends in cyber threats: attacks are growing more and more potent, the proportion of cyber extortion is rising and, in February 2021, the highest average daily growth to date in new *malware* variants was recorded. Such trends are being fuelled as our networks spread ever further, causing an ever-increasing degree of digital dependency that is still all too often accompanied by a lack of digital literacy. While a digitalised world is full of opportunities and potential, it also creates many risks and a constant rise in potential targets.

Germany is not alone in its observation of these trends. All over the world, digitalisation is now proceeding apace. The massive rise in data volumes is merely one marker among many, and these developments show no signs of stopping. Now, some 80 years after Konrad Zuse powered up the world's first functional computer in

switching on his Z3 right here in Germany, it is time to rethink the digital transition. Information security must be placed front and centre and form the basis of any and all digitalisation projects we undertake. The present report is a stark reminder to us all that the successful digitalisation of government, business and civil society can only succeed with cyber security in its proper place.

4 Glossary

Advanced persistent threats

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

Affiliates

In the case of cybercrime-as-a-service, the cybercriminals making use of the service are commonly referred to as 'affiliates'. The term is derived from affiliate marketing, a practice in which one commercial provider provides its sales partners (affiliates) with advertising material and offers a commission for its use. In the context of cybercrime, ransomware is provided instead of advertising material and the affiliate is promised a share of the ransom extorted.

Attack vector

An attack vector is a combination of an attack route and method that a perpetrator uses to gain access to IT systems.

Application/app

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

Authentication process

An authentication process is a procedure to verify the identity of a person or a computer system by means of a particular attribute. This attribute may be a password, a chip card or biometric characteristics.

Authentication

Authentication is the process of proving authenticity. A person's identity can be authenticated by means of a password, a chip card or biometry, for example; data authentication can be carried out based on things like cryptographic signatures.

Backdoor

A backdoor is a program typically installed by a virus, worm or trojan that grants third parties unauthorised access to a computer, but remains concealed and also bypasses the computer's normal security defences.

Backup

A backup involves the copying of files or databases to physical or virtual systems at a different storage location. These resources are kept at this separate location so they can be recovered in the event of a device failure or some other catastrophic incident.

Bitcoin

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

Blockchain

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

Bot/botnet

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

CEO fraud

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

CERT/Computer Emergency Response Team

A CERT team is a team of IT specialists. CERTs have become established in many companies and institutions to mount a defence against cyber attacks, respond to IT security incidents and implement preventive measures.

CERT-Bund

CERT-Bund (the Computer Emergency Response Team for Germany's federal agencies) is located within the BSI and functions as the central coordinating body for both preventive and responsive measures in the event of security-related incidents affecting computer systems.

Cloud/cloud computing

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

Command-and-control server (C&C server)

Server infrastructure with which the attacker controls the infected computer systems (*bots*) that are integrated into a *botnet*. *Bots* (infected systems) typically report back to a *C&C server* after infection has taken place in order to receive subsequent commands.

Cybercrime-as-a-service (CCaaS)

Cybercrime-as-a-service (CCaaS) describes a type of cybercrime phenomenon in which the criminal acts perpetrated by cybercriminals are contract-based or facilitated as part of a service-oriented system. Within a subtype of *CCaaS* known as *malware-as-a-service (MaaS)*, for example, one cybercriminal is provided with the malware required to perpetrate a crime by an external party – perhaps an attacker group specialising in malware – for a fee, and may even be provided with malware updates and similar services in the same way as in the legal software industry. A further subtype of *MaaS* is *ransomware-as-a-service (RaaS)*, where malware required to encrypt an infected system, updates for this malware, the handling of ransom negotiations and payments, and other methods of extortion are often all provided to a cybercriminal for a specified fee. Since *CCaaS* breaks down a cyber attack into constituent services, it also allows less IT-savvy attackers to conduct technically advanced cyber attacks.

Deepfake

The word ‘deepfake’ is a colloquial term for methods that can be used to achieve the targeted manipulation of identities in medial content with the aid of techniques taken from the field of artificial intelligence. One example involves methods that are capable of swapping the face of a person depicted in one video with the face of some other person while still retaining the original person’s facial expressions.

DoS/DDoS attacks

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

Drive-by download/drive-by exploit

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

Exploit

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

Exploit kit

Exploit kits or exploit packs are tools for cyber attacks that are placed on legitimate websites. A variety of automated exploits are used in an attempt to discover vulnerabilities in web browsers or their plug-ins and exploit them in order to install malware.

Firmware

Firmware is software that is embedded in electronic devices. Depending on the device, firmware can offer operating system or application software functionality. Firmware is tailored to a specific piece of hardware and is not interchangeable.

Hash value

A hash value is an alphanumeric character string that results from the application of a specific hash function. A hash value has a defined length and can therefore represent large volumes of data (e.g. a malware program) within the space of comparatively few characters. A hash function is a mathematical function for data conversion. Converting a hash value back into the original data is essentially impossible, or possible only with an exorbitant use of computing power.

Internet of Things/IoT

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

MaaS

Malware-as-a-service (see also *CCaaS*).

Malicious

In the field of IT security, programs or websites capable of executing harmful operations on a computer system are referred to as ‘malicious’. The general term for harmful software, ‘malware’, is itself formed from ‘mal(icious)’ and ‘(soft)ware’.

Malware

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

Patch/patch management

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

Payload

The term 'payload' generally refers to the usable/user data in a data transfer. In the context of information security, a distinction is made between malware code that opens up a system to further attacks, malware code that serves as a temporary vehicle and malware code that is intended to remain on the system. A payload involves this last type of malware code.

Phishing

The term 'phishing' is a combination of the words 'password' and 'fishing,' i.e. 'fishing for passwords'. An attacker attempts to access the personal data of an internet user via bogus websites, emails or messages and to abuse this data for their private purposes, usually at the victim's expense.

Phishing Radar (NRW Consumer Advice Centre)

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

Plug-in

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

Potentially unwanted application (PUA)

Application software (often distributed as bundled software) that cannot be classified definitively as malware. While PUAs are typically installed by the user, they then exhibit unexpected behaviour or execute certain functions covertly that could be construed as 'undesirable': these include the collection of information and the sharing of user behaviour, the display of advertising banners, and so on.

Proliferation

This term was originally used by militaries to refer to the spread of weapons of mass destruction, including related technical expertise and the material required to produce them. Accordingly, IT security experts now refer to the spread of cyber weapons (both software and methods) among attackers as 'prolifera-

tion'. The process of proliferation enables attack resources and strategies to spread rapidly among discrete attacker collectives without individual groups needing to build up specific technical expertise.

Provider

A service provider can act in a number of roles, including as a network operator that supplies infrastructure for data and voice traffic in the manner of a mobile network provider, internet service provider or carrier. Alternatively, a service provider may offer services that go beyond network provision and include the operation of networks within an organisation or the provision- ing of social media.

Public key cryptography

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

Ransomware

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

RaaS

Ransomware-as-a-service (see also CCaaS).

Resilience

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

Responsible disclosure

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

Security by default

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

Security by design

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

Side-channel attack

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

Sinkhole

A sinkhole is a computer system to which queries from bot-net-infected systems are redirected. Sinkhole systems are typically operated by security researchers in order to detect botnet infections and inform affected users.

Social engineering

In cyber attacks involving social engineering, criminals attempt to mislead their victims into voluntarily disclosing data, bypassing security measures or willingly installing malware on their personal systems. In the areas of both cybercrime and espionage, such attackers are skilled at exploiting perceived human weaknesses such as curiosity or fear in order to gain access to sensitive data and information.

Spam

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

UP KRITIS

The Critical Infrastructure Implementation Plan (www.upkritis.de) is a public-private partnership of critical infrastructure (CI) operators, 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 this network. In VPNs, the integrity and confidentiality of data can be protected and communication partners can be securely authenticated with the help of cryptographic procedures, even when several networks or computers are connected to each other over leased lines or public networks. While the term 'VPN' is often used to refer to encrypted connections, other methods can also be used to secure the transport channel, such as special functions that are available in the transport protocol used.

Two-factor or multi-factor authentication

In two- or multi-factor authentication (2FA, MFA), an identity is authenticated by means of various authentication factors that are taken from separate categories (knowledge, possession or biometric attributes).

5 Bibliography

- ¹ The State of IT Security in Germany in 2020, page 11
- ² <https://www.bka.de/SharedDocs/Downloads/EN/Publications/AnnualReportsAndSituationAssessments/Cybercrime/national-SituationReportsOnCybercrime2019.html>
- ³ <https://www.br.de/nachrichten/netzwelt/hacker-veroeffentlichen-passdaten-von-12-000-deutschen,SArrtc5>
- ⁴ <https://www.bleepingcomputer.com/news/security/netwalker-ransomware-hits-argentinian-government-demands-4-million/>
- ⁵ <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-defenders-blog-netwalker/?hlite=%27ransomware%27%2C%27netwalker%27>
- ⁶ <https://www.bleepingcomputer.com/news/security/princess-evolution-ransomware-is-a-raas-with-a-slick-payment-site/>
- ⁷ <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-defenders-blog-netwalker/?hlite=%27ransomware%27%2C%27netwalker%27>
- ⁸ <https://www.bleepingcomputer.com/news/security/hackers-leak-files-stolen-in-pakistans-k-electric-ransomware-attack/>
- ⁹ <https://www.heise.de/news/Hacker-veroeffentlichen-Daten-nach-Cyberangriff-auf-staedtische-IT-in-Oesterreich-4727538.html>
- ¹⁰ <https://cyberflorida.org/threat-advisory/netwalker-ransomware-targets-philadelphia-health-system/>
- ¹¹ <https://www.br.de/nachrichten/netzwelt/hacker-veroeffentlichen-passdaten-von-12-000-deutschen,SArrtc5>
- ¹² <https://www.bleepingcomputer.com/news/security/netwalker-ransomware-hits-argentinian-government-demands-4-million/>
- ¹³ <https://www.colpipe.com/news/press-releases/media-state-ment-colonial-pipeline-system-disruption>
- ¹⁴ <https://www.bleepingcomputer.com/news/security/largest-us-pipeline-shuts-down-operations-after-ransomware-attack/>
- ¹⁵ <https://www.nytimes.com/2021/05/08/us/cyberattack-colonial-pipeline.html>
- ¹⁶ <https://edition.cnn.com/2021/05/12/politics/colonial-pipeline-ransomware-payment/index.html>
- ¹⁷ <https://www.intel471.com/blog/darkside-ransomware-shut-down-revil-avaddon-cybercrime>
- ¹⁸ <https://www.intel471.com/blog/darkside-ransomware-shut-down-revil-avaddon-cybercrime>
- ¹⁹ <https://www.intel471.com/blog/darkside-ransomware-shut-down-revil-avaddon-cybercrime>
- ²⁰ <https://www.bsi.bund.de/emetet>
- ²¹ https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2021/Presse2021/210127_pmEmotet.html
- ²² Federal Foreign Office, 'On the Application of International Law in Cyberspace', <https://www.auswaertiges-amt.de/blob/2446304/2ae17233b62966a4b7f16d50ca3c6802/on-the-application-of-international-law-in-cyberspace-data.pdf>
- ²³ FireEye, 'Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor', <https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html>
- ²⁴ Brad Smith, Microsoft, 'A Moment of Reckoning: The Need for a Strong and Global Cybersecurity Response', <https://blogs.microsoft.com/on-the-issues/2020/12/17/cyber-attacks-cyber-security-solarwinds-fireeye/>
- ²⁵ FireEye, 'Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor', <https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html>
- ²⁶ CrowdStrike, 'SUNSPOT: An Implant in the Build Process', <https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/>
- ²⁷ <https://home.treasury.gov/news/press-releases/jy0127>
- ²⁸ <https://www.gov.uk/government/news/russia-uk-exposes-russian-involvement-in-solarwinds-cyber-compromise>
- ²⁹ <https://www.canada.ca/en/global-affairs/news/2021/04/state-ment-on-solarwinds-cyber-compromise.html>
- ³⁰ Brad Smith, Microsoft, 'A Moment of Reckoning: The Need for a Strong and Global Cybersecurity Response', <https://blogs.microsoft.com/on-the-issues/2020/12/17/cyber-attacks-cyber-security-solarwinds-fireeye/>
- ³¹ Paul R. Kolbe, New York Times, 'With Hacking, the United States Needs to Stop Playing the Victim', <https://www.nytimes.com/2020/12/23/opinion/russia-united-states-hack.html>
- ³² Lawfare Blog, 'The Strategic Implications of SolarWinds', <https://www.lawfareblog.com/strategic-implications-solarwinds>
- ³³ <https://www.link11.com/en/blog/threat-landscape/20-years-of-ddos-a-brief-look-at-the-past-and-what-the-future-will-bring/>
- ³⁴ <https://it-online.co.za/2021/03/04/new-record-for-ddos-attacks-in-2020/>
- ³⁵ <https://www.link11.com/en/security-wiki/link11-report-reveals-ddos-attacks-reached-record-high-in-2020/>
- ³⁶ <https://techaeris.com/2015/11/08/protonmail-hit-massive-ddos-attack-pays-bitcoin-ransom/>
- ³⁷ <https://www.link11.com/en/blog/threat-landscape/warning-ddos-threat-fancy-bear/>; <https://blogs.akamai.com/sitr/2020/08/ransom-demands-return-new-ddos-extortion-threats-from-old-actors-targeting-finance-and-retail.html>
- ³⁸ <https://blog.cloudflare.com/ransom-ddos-attacks-target-a-fortune-global-500-company/>
- ³⁹ <https://www.welivesecurity.com/2020/08/27/ddos-extortion-campaign-targets-financial-firms-retailers/>
- ⁴⁰ <https://www.zdnet.com/article/ddos-extortionists-target-nzx-moneygram-braintree-and-other-financial-services/>
- ⁴¹ https://ga.de/news/digitale-welt/schul-cloud-des-hpi-mit-ueber-einer-million-nutzern_aid-55700185

- ⁴² https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Warnhinweise/210120_DDos.html
- ⁴³ <https://www.link11.com/de/blog/bedrohungslage/fancy-bear-warnung-ddos-erpressung/>
- ⁴⁴ <https://blogs.akamai.com/sitr/2020/08/ransom-demands-return-new-ddos-extortion-threats-from-old-actors-targeting-finance-and-retail.html>
- ⁴⁵ <https://www.link11.com/de/blog/bedrohungslage/armada-collective-ddos-erpressung-hostinganbieter/>
- ⁴⁶ <https://www.link11.com/de/blog/bedrohungslage/fancy-bear-warnung-ddos-erpressung/>
- ⁴⁷ <https://blogs.akamai.com/sitr/2020/08/ransom-demands-return-new-ddos-extortion-threats-from-old-actors-targeting-finance-and-retail.html>
- ⁴⁸ <https://www.link11.com/de/blog/bedrohungslage/armada-collective-ddos-erpressung-hostinganbieter/>
- ⁴⁹ <https://dd80b675424c132b90b3-e48385e382d2e5d17821a5e-1d8e4c86b.ssl.cf1.rackcdn.com/external/...>
- ⁵⁰ <https://belnet.be/fr/nouvelles-evenements/nouvelles/update-reseau-belnet-a-nouveau-disponible-nos-equipes-restant>
- ⁵¹ The State of IT Security in Germany in 2020
- ⁵² The State of IT Security in Germany in 2020, page 34
- ⁵³ <https://www.statista.com/forecasts/887705/number-of-smart-homes-per-segment-in-europe>
- ⁵⁴ https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/DigitaleGesellschaft/Pruefvorschrift_Produktgutachter_ePA-Frontend.pdf
- ⁵⁵ https://fachportal.gematik.de/fileadmin/Fachportal/DVO/Informationsblatt_Betriebsarten-Konnektor_V1.0.0.pdf
- ⁵⁶ <https://fachportal.gematik.de/ti-status/stoerung-vsdm>
- ⁵⁷ <https://e-health-com.de/details-news/ccc-hackt-bestellprozess-gematik-nimmt-stellung>
- ⁵⁸ <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03162/BSI-TR-03162.pdf>
- ⁵⁹ https://www.it-planungsrat.de/DE/Projekte/Koordinierungsprojekte/Portalverbund/Portalverbund_node.html
- ⁶⁰ <https://www.heise.de/news/Deep-Fake-Politiker-fallen-auf-gefaketen-Nawalny-Vertrauten-rein-6027713.html>
- ⁶¹ https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/C5_AktuelleVersion/C5_AktuelleVersion_node.html
- ⁶² https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cloud-Computing/Anforderungskatalog/2020/C5_2020_Auswertung-sleitfaden.xlsx
- ⁶³ https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_Nutzung_externer_Cloud-Dienste.html
- ⁶⁴ https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_019.html
- ⁶⁵ https://www.destatis.de/EN/Themes/Economic-Sectors-Enterprises/Transport/Passenger-Transport/_node.html
- ⁶⁶ <https://signal.org/docs/specifications/doubleratchet/doubleratchet.pdf>
- ⁶⁷ <https://messaginglayersecurity.rocks/>
- ⁶⁸ <https://datatracker.ietf.org/wg/mls/about>
- ⁶⁹ https://www.personalausweisportal.de/SharedDocs/downloads/Webs/PA/DE/informationsmaterial/weiterefuehrendes-material/Handlungsleitfaden_Integration_Smart-eID_Nutzerkonto.html
- ⁷⁰ https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KI/Herausforderungen_und_Massnahmen_KI.html
- ⁷¹ <https://www.etsi.org/committee/sai>, ETSI and the ad hoc working group on the topic of AI at ENISA (see the bibliography: <https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges>)
- ⁷² <https://www.din.de/de/forschung-und-innovation/themen/kuenstliche-intelligenz/fahrplan-festlegen>
- ⁷³ <https://www.ki.nrw/en/flagships/certified-ai/>
- ⁷⁴ https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/ArtificialIntelligence/Empirical_robustness_testing_of_AI_systems_for_traffic_sign_recognition.html
- ⁷⁵ <https://www.bsi.bund.de/aic4>
- ⁷⁶ <http://www.bsi.bund.de/PQ-Migration>
- ⁷⁷ <https://www.bsi.bund.de/Quanten>

List of QR codes included in the report

- a) <https://www.bsi.bund.de/ransomware>
- b) https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/Unternehmen/Ich-habe-einen-IT-Sicherheitsvorfall-Was-soll-ich-tun-ich-habe-einen-it-sicherheitsvorfall-was-soll-ich-tun_node.html
- c) <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.html>
- d) <https://www.bsi.bund.de/ransomware>
- e) 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
- f) https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/spam-phishing-co_node.html
- g) https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Elektronische-Identitaeten/elektronische-identitaeten_node.html
- h) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefahren/DDoS/ddos_node.html
- i) <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister-DDos-Mitigation-Liste.pdf>
- j) https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/KoViKo_140420.html
- k) https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Remote/remote_node.html
- l) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/empfehlung_home_office.html
- m) <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publicationen/DVS-Berichte/gesundheitsapps.html>
- n) <https://www.bsi.bund.de/VerbraucherInnen>
- o) <https://einfachabSIchern.de>
- p) <https://www.bsi.bund.de/viva>
- q) <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publicationen/TechnischeRichtlinien/TR03162/BSI-TR-03162.pdf>
- r) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publicationen/Broschueren/Sicher_zahlen_im_E_Commerce.html
- s) https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0096_0096V2_0096V3.html
- t) <https://upkritis.de>
- u) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Lageberichte/Cyber-Sicherheitsumfrage/IT-Sicherheit_im_Home-Office/it-sicherheit-im-home-office_node.html
- v) https://www.bsi.bund.de/DE/Themen/Kampagne-einfach-absi-chern/Home-Office/home-office_node.html
- w) https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Netzwerk-Formate/Medien/Cyber-Sicherheits-Podcast/cyber-sicherheits-podcast_node.html
- x) https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_019.html
- y) <https://www.bsi.bund.de/Zulassung>
- z) https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Zulassung/VS-Anforderungsprofile/vs-anforderungsprofile_node.html
- aa) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KI/Herausforderungen_und_Massnahmen_KI.html
- bb) <https://www.bsi.bund.de/aic4>
- cc) <https://www.bsi.bund.de/Quantenw>
- dd) <http://www.bsi.bund.de/blockchain>

Legal Notice

Published

by Federal Office for Information Security (BSI)

Source

Federal Office for Information Security (BSI)

Godesberger Allee 185–189
53175 Bonn, Germany

E-Mail

bsi@bsi.bund.de

Telephone

+49 (0) 22899 9582-0

Fax

+49 (0) 22899 9582-5400

Last updated

September 2021

Printed by

Appel & Klinger Druck und Medien GmbH, Schneckenlohe
Germany

Concept, editing and design

Faktor 3 AG

Texts and editing

Federal Office for Information Security (BSI)

Image credits

Titel, p. 8, p. 44–45, p. 46, p. 86: AdobeStock ©Inna;
p. 3: BMI; p. 4: BSI;

Graphics

Federal Office for Information Security (BSI)

Article number

BSI-LB21/510e

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

