The State of IT Security in Germany in 2023

Federal Office
for Information Security

Foreword

Nancy Faeser, Federal Minister of the Interior and Community

Digital transformation is opening up new horizons for our country. It offers diverse ways to strengthen our economy, enable greater societal participation and simply make our public administration efficient and responsible to public needs.

However, the use of artificial intelligence, the much-cited "Internet of Things" and the ability to digitally control complex processes do not only offer opportunities. They also pose risks. These risks increase as these technologies become more widespread. The potential for misuse is growing and new vulnerabilities are emerging. Knowing this is important – and it needs to be better anchored in the public consciousness. Only those who know and recognise the potential dangers are in a position to make the right decisions and take appropriate measures to protect themselves and others. This is fundamental for our digital and thus public security.

This report by the Federal Office for Information Security (BSI) on the state of IT security in Germany in 2023 makes an important contribution towards raising our awareness of the risks.

This is the only way to enable society, business, policy makers and public administration to effectively prevent cyber attacks. Only then can they take the necessary precautions in order to respond to a possible incident. Only then can they realistically practise and simulate such emergencies. This is vital, because citizens must be able to trust that we are well prepared.

Together with all the federal states, the Federal Ministry of the Interior and Community once again conducted an interstate and interministerial crisis management exercise (LÜKEX) this year. A large number of federal authorities were involved, as were operators of critical infrastructure. The exercise focused on how to maintain state and government functions after a cyber attack. And it showed that we are well prepared for emergencies.

But we also learned that it requires intensive information sharing and coordinated action to successfully counter threats from cyberspace. That is why the federal and state governments must work together to counter these dangers. The BSI is a key partner in this effort. It not only issues warnings of possible threats and risks, but also ensures reliable cyber security together with the other security agencies. This makes the present report even more deserving of many interested readers. I wish you an exciting read!

Foreword

Claudia Plattner, President of the Federal Office for Information Security

In June 2023, the National Security Strategy of the Federal Government was adopted. The word "cyber" appears 62 times throughout the 76-page document. This alone underscores the importance of cyber security for the overall security of Germany and consequently for every citizen. And it aligns with the tense to critical situation identified in the BSI's report:

The ongoing digitisation and increasing connectivity continue to increase attack surfaces – and these are being exploited. In the report, we see a rise in the threat level in the area of vulnerabilities. Nearly 70 new vulnerabilities in software products are being discovered every day – around 25 per cent more than in the previous reporting period. The rapid development of new and adaptive attack methods and the increasing nature of services offered (Cybercrime-as-a-Service) are also causes of concern. Ransomware, in particular, remains the primary threat.

So what can be done? We need to:

- build resilience as quickly as possible in order to prevent attacks.
- actively shape cyber security to get 'in front of the curve'.
- simultaneously advance digitisation, as this is the only way we can assure safety and competitiveness in the technologies of the future.

Our aim is to increase resilience by strengthening the adoption of our recommendations, guidelines and support. The most pressing issues for implementation are patching, updates and secure identity access management to prevent attacks. Additionally, backups, data protection and emergency plans must be created and, above all, tested in response to an incident. To achieve this, we need to provide products and services that meet the necessary security requirements and are easy to use as self-help-tools, we need to be able to promote and demand their use.

By helping to shape important standards and products for more and more cyber issues and technologies at European level as well, we will get ahead of the curve. This systematically increases cyber security for both organisations and consumers.

As the BSI, we are also involved in the development and research of the key technologies required for digitisation – from AI, cloud, eID or smart metering to secure modern networks. By quickly establishing clarity on security features and secure usage, we provide a sense of direction. In this way, we contribute to secure digitization and accelarate it simultaneously.

For all of this, we are and want to continue to be enablers and shapers! We can be a strong partner in Germany's security architecture.

As the BSI, we will exercise our authority: It is essential that we are able to identify security issues and provide solutions. Because cyber security is complex and – as this report shows – it affects everyone, from government authorities and SMEs to individual citizens.

Our top priority is to make Germany more digital and more secure. This can only be achieved with the coordinated cooperation of all stakeholders at the municipal, state and federal levels and throughout Europe! In doing so we should also engage with business, science and society. For us, cyber security is a joint task that is built on transparency as the foundation for trust!

Table of contents

Incidents & Figures

List of Selected Incidents:

List of Figures:

1. — Introduction

As the Federal Cyber Security Authority, the Federal Office for Information Security (BSI) continuously monitors the threat landscape of IT security in Germany. The BSI focuses on cyber attacks against government and public institutions, companies and private individuals, as well as on measures for preventing and combating these situations. This report provides an overview of the period from 1 June 2022 to 30 June 2023 (reporting period).

The reporting period differs from that of the report "The State of IT Security in Germany 2022" due to changes in the periods during which the data is collected and evaluated. To ensure comparability of the data with the previous reporting period (1 June 2021-31 May 2022) and the reporting period of the report "The State of IT Security in Germany 2024" (1 July 2023-30 June 2024), daily averages values are used where possible or the figures are compared with those of the same period from the previous year.

This report addresses current and ongoing cyber threats and assesses the state of IT security in the context of Russia's war of aggression on Ukraine. Using specific examples across different sectors, the report traces the path and typical methods used by attackers, while at the same time showing how users can protect themselves.

Part A of this report provides an overview of the general threat landscape and current cyber threats, divided into attack methods, attack types and vulnerabilities. This includes a summary of developments in the field of artificial intelligence (AI) and their impact on threats. When a cyber threat, such as malware, encounters a vulnerability, a risk is created. While threats exist independently of specific attack surfaces in the industry, government, and society, and thus describe general phenomena on the attacker's side, specific risks arise from increasing attack surfaces on the potential victim's side. These risks to the state, the industry and society are presented in Part B. Lastly, Part C describes current trends in the field of cyber security using salient topics as examples.

The "The State of IT Security in Germany 2023" report focuses on the work of the BSI for the first time. More in-depth information on other topics such as digital consumer protection, automotive and cyber security in the healthcare sector can be found in the respective reports as well as in other BSI publications.

Look here for further information:[a]

Situation Report Health

Situation Report Automotive

Digital Consumer Protection Report

Further BSI publications

Threat Landscape

Part A: Threat Landscape

2. — Summary and Assesment

Overall, the situation in the current reporting period was tense to critical. As a result, the threat in cyberspace is higher than ever before. As in previous years, a high level of cybercrime threats was observed. Ransomware remained the main threat. On the attacker side, observations revealed a black market economy involving the cybercriminal division of labour and characterised by mutual dependencies and competitive pressure. Small and medium-sized enterprises (SMEs) and especially local administrations and municipal enterprises were attacked disproportionately more frequently. In the context of the Russian war of aggression in Ukraine, the threat was mainly posed by pro-Russian hacktivist attacks, which, nevertheless, did not cause any lasting damage and should instead be seen as a propaganda tool. An increase in threats was also noted in the area of vulnerabilities. 68 new vulnerabilities were registered in software products every day during the reporting period – around 24 per cent more than in the previous reporting period.

Expansion of the Cybercriminal Black Market Economy

The reporting period was marked by the continued expansion of a cybercriminal black market economy. The specialisation of the cybercriminal "value chain" of ransomware attacks, which had already begun in previous reporting periods, was further developed by the attackers in the current reporting period. From gaining access to a victim's network to the necessary ransomware to support in ransomware negotiations, attackers can now buy tools for every step of a complex attack as a service. The division of labour among the cybercriminals who offer these tools results in a doubling of the scale of the threat: Firstly, cybercriminal providers are able to specialise in individual tools and thus develop and improve them more quickly. Secondly, this also allows the improved tools to be made available more quickly to a larger number of interested attackers. They specialise in actually carrying out the ransomware attacks and pay commissions from the ransoms collected to the cybercriminal providers of the services used.

Cyber Resilience

Cybercriminals increasingly took the path of least resistance during the reporting period and increasingly chose victims who appeared easy to attack. The focus was no longer on maximising the potential ransom, but on making a rational cost-benefit calculation. As a result, small and medium-sized enterprises as well as state and local administrations, scientific institutions and schools and universities increasingly fell victim to ransomware attacks. That is why cyber resilience is imperative.

DDoS hacktivism

In the context of the Russian war of aggression in Ukraine, there were a number of pro-Russian hacktivist attacks in Germany during the reporting period. The hacktivist groups exclusively used Distributed Denial-of-Service attacks (DDoS attacks) for this, which are designed primarily to affect the availability of internet services and cannot cause any lasting damage like ransomware attacks. DDoS hacktivism is therefore essentially a propaganda tool designed to create social insecurity and undermine confidence in the state's ability to protect and provide for the population.

Advanced Persistent Threats

Advanced Persistent Threats (APTs) aimed at obtaining information were prevalent during the reporting period. While for example telecommunication providers were targeted in Southeast and Central Asia, government institutions were among the targets in Europe and North America. The situation was different in Ukraine, where both cyber espionage and simple cyber sabotage were observed. From a technical point of view, there is a growing shift from attacks via spear phishing to attacks against vulnerable servers at the network perimeter.

Vulnerabilities

During the reporting period, an average of almost 70 new vulnerabilities were discovered in software products every day – around 15 per cent of which were critical.

Cyber extortionists, for example, used two vulnerabilities in file sharing products to grab data from numerous victims in Germany and around the world and then threaten to publish it. Because of the prevalence of products with vulnerabilities, it is safe to assume that a very large number of people are affected. Moreover, an attack on the web portals of various vehicle manufacturers illustrated the possible damaging effects caused by insufficiently secured web servers: This made it possible for attackers to impersonate dealers and gain access to the vehicle functions of other people's cars and control them via the official manufacturer's app.

A detailed consideration of the above points is provided in the following chapters..

3. — Means of Attacks

Cyber attacks are carried out with the help of malware. These are used in a wide variety of ways (for example, e-mail attachments, malicious web servers, exploits, etc.) and thus enable the most diverse types of cyber attacks (see chapter *Types of Attacks*, page 14). If numerous computer systems are infected with a malicious program and can thus be controlled remotely, this is called a botnet, which in turn can be used for cyber attacks.

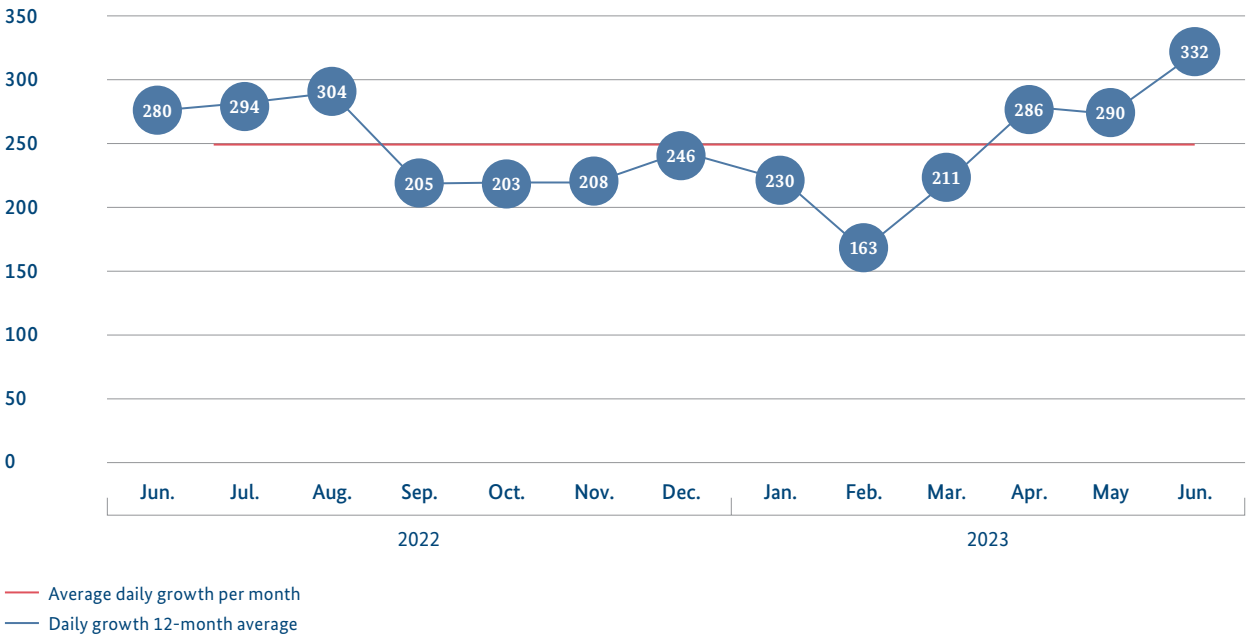
3.1 — New Malware Variants

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

The individual malware programmes differ in terms of their functionality, but a malware programme can also have several functionalities. Ransomware is, for

Average daily growth of new malware variants
Amount in thousands

Figure 1: Average daily growth of new malware variants
Source: *BSI malware statistics based on raw data from the AV-Test GmbH Institute*



example, malware that restricts access to data or systems by encrypting them so that the attacker can then extort a ransom (see chapter *Ransomware*, page 14). Malware that disguises itself as benign software or hides in legitimate files is called a Trojan Horse. Bots are malware that can be controlled remotely, for example, with the help of Command-and-Control servers (see chapter *Botnets*, page 13).

If an attacker makes changes to the malware programme code, a new variant is created. Any variant with a unique checksum (hash value) is therefore considered new. While detection methods exist for known malware variants, new variants may not yet be recognisable as malware immediately after their appearance, making them particularly threatening. During the reporting period, an average of 250,000 new malware variants became known every day. This was 22 per cent less than in the previous reporting period - a figure that indicates a return to the average threat level after the major Emotet surges in 2021 and 2022.

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

3.2 — Botnets

Any system infected with malware that can be remotely controlled via a central control system, the Command-and-Control server, is called a bot. A botnet is an association of several bots that are centrally controlled by a botmaster. Nowadays, almost all systems with internet capability can be infected by bot software. This means that in addition to classic computer systems, smartphones, tablets, routers or even Internet of Things (IoT) devices such as webcams or smart TVs can be compromised and taken over.

Since current bot software is modular, attackers can tailor the botnet's functionalities to their needs and adapt them dynamically via updates. In addition to targeted attacks on the personal data of the victim systems (information theft), the resources of the controlled system can also be used for the attacker's own purposes (e.g. cryptomining) or for attacking third parties (e.g. DDoS attacks, sending spam, etc.).

During the reporting period, as in previous years, botnets were primarily used to steal personal information (see the topic of *Information Stealer* in the chapter *Ransomware*, page 14) as well as to distribute other malware. The botnets observed by the BSI are clearly focused on Android-based mobile operating systems. Classic desktop operating systems continue to lose importance.

During the reporting period, an average of around 21,000 infected systems were detected in Germany every day and reported by the BSI to German providers. The daily values fluctuated significantly. At the peak, 45,000 infected systems were reported. The providers identified and notified the affected customers. However, the number of total infections is likely to be significantly higher, as in many cases there are multiple infections. The infection data mainly comes from the BSI's own and external sinkhole systems, which receive and log the contact requests of bots instead of the regular Command-and-Control servers. A description of the sinkholing procedure and profiles of the most frequently reported malware families are available on the website of the BSI.

Further information can be found here:[b]

Based on experiences from shutting down botnets, it is safe to assume that the number of unreported infections is significantly higher and is at least in the seven-digit range for Germany. Due to the increasing professionalisation of attackers and their focus on specific victims, there has been a decline in the number of infections detected in large botnets compared to previous years. Nevertheless, due to the increasing number of vulnerable mobile and IoT devices and the availability of malware code on the internet, it is reasonable to assume that *script kiddies* or politically motivated opportunists are infecting systems to build botnets for DDoS attacks.

As in previous years, the threat posed by botnets is high. The infection figures calculated through sinkholing represent a lower limit, partly because only a section of the currently known botnets can be actively recorded. Botnet families such as Emotet, FluBot or Glupteba implement countermeasures to circumvent classic domain name-based sinkholing, for example by using IP addresses, tunnelled DNS connections (DNS over HTTPS, DoH) or blockchain techniques to obfuscate communication between control servers and bots.

4. — Methodes of Attacks

The development of the situation in the reporting period is described below for the main types of attacks. Due to the high threat potential, the focus of the presentation is on the threat situation in the phenomenon area of "ransomware". This is followed by situational findings around advanced persistent threats and in the context of the Russian war of aggression against Ukraine, as well as in the area of "distributed denial of service" and the new phenomenon of politically motivated DDoS hacktivism. Furthermore, spam and phishing as well as attacks in the context of cryptography are addressed.

4.1 — Ransomware

A ransomware attack is a form of digital extortion. For example, attackers exploit errors such as incorrect operation, misconfigurations, outdated software versions or inadequate data backups to infiltrate deep into systems and encrypt data. The attackers demand a ransom for decryption. Such extortion is often combined with threatening to publish previously stolen data. This form of extortion is also known as double extortion. The ransom also usually acts as hush money in such cases. Payment is usually requested in electronic currencies (usually Bitcoin or Monero).

The effectiveness of ransomware is based on its immediate impact. Unlike classic malware such as banking Trojans, botnets or phishing emails, the damage occurs right away and has concrete consequences for those affected. In the event of a ransomware attack, for example, all stored documents may be lost and important company data or critical services may no longer be available. Preventive measures are the best way to counter such attacks. Prevention is always better than trying to fix it.

Because the pressure to limit the damage of those affected is enormously high after a ransomware attack, many victims pay the demanded ransom in the hope of quickly being able to function again. However, there is no guarantee that the cyber extortionists will actually release the encrypted data or actually delete the stolen data. There is also a chance that the decryption tool provided by the attacker is defective. The BSI therefore expressly advises against paying any ransoms. Moreover, once data has been leaked, it should always be considered compromised.

Institutions of every type and size are potential victims – from microenterprises to public authorities and KRITIS companies to international corporations, from local administrations and hospitals to scientific institutions, schools and universities. Furthermore, every now and then the BSI becomes aware of mass campaigns that also directly affect consumers, for example targeting network-attached storage (NAS) systems.

There is no complete protection against ransomware attacks, because attackers can also use new attack paths for which no detection and defence methods have yet been developed. However, certain attacks, for example on companies, government agencies and IT service providers, can certainly be prevented. Backups and contingency plans help to limit or even completely compensate for any impacts in the event of an emergency.

4.1.1 — Attack Motives and Process of an Attack

Ransomware attacks are predominantly perpetrated by cybercriminal attackers for financially motivated reasons. Nevertheless, APT attackers can also use ransomware to disguise or divert attention from other attacks. In addition, ransomware can also be used for outright sabotage. If this is the case, the ransomware acts as a wiper and the encrypted data cannot technically be restored (see chapter *Advanced Persistent Threats and Threats in the Context of the Ukraine War*, page 24).

4.1.1.1 — Cybercriminal Attacks on State Institutions

Due to the increasing provision of services in the cybercrime black market based on the division of labour (see chapter *Cybercrime Black Market Economy*, page 16), these services have also become available to other cyber attackers, especially APT groups.

Larger ransomware attacks against important state institutions occurred in Montenegro in August 2022 with the Cuba ransomware and in Bosnia-Herzegovina in September with a ransomware that is still unknown. In both states, the parliament was attacked, among other things.

During the reporting period, several ransomware incidents also became known which, according to public reporting, were probably state-sponsored. For example, attacks were reported on Albanian government institutions between July and September 2022 using the ransomware GoneXML and the wiper ZeroShred. The specialist community has attributed these attacks to the Iranian group Banished Kitten. Moreover, there have been repeated reports of the use of ransomware against Israeli organisations by Iranian attackers, where the financial motivation has been called into question. In October 2022, the Microsoft Threat Intelligence Center (MSTIC) revealed the use of the Prestige ransomware against companies in Poland, among others. In November, MSTIC attributed these attacks to IRIDIUM/ Sandworm with high probability. This state-sponsored group had also carried out sabotage attacks in Ukraine under the guise of ransomware. As the war in Ukraine progressed, however, the group abandoned its disguise as ransomware and directly deployed wipers. In the context of the war in Ukraine, the IT security community suspects that some cybercriminal attackers are acting on behalf of the Russian state. However, the BSI has no evidence of this.

In cybercriminal attacks against state institutions, a purely financial motivation has often been questioned. Especially in the case of higher state authorities, the willingness to pay a ransom is becoming increasingly unlikely. It can be assumed that such attacks have other motives, such as the interests of another state, ideologically motivated attackers or the attackers' desire for recognition in the cybercriminal community and attention in the press. The attackers may also have mistaken the target of the attack. According to the BSI, the majority of cybercriminal attacks are opportunistic attacks (see incident *Ransomware Attacks on Local Administrations and Municipal Utilities*, page 69).

In most cases, there is no clear answer to the motivation of the attackers. However, the attacker's motives can make a significant difference in how the attack proceeds and also in how the attack is handled, such as whether it is about a ransom in the first place or, for example, about the attacker's desire for recognition.

4.1.1.2 — Process of an Attack

Cybercriminals are grouped together according to the malware they use and their modus operandi. For example, the ransomware Alphv (also known as BlackCat) is used by a different group than the ransomware LockBit 3.0.

Attack phase 1 - initial infection: A ransomware attack often begins with a malicious email, compromising remote access such as Remote Desktop Protocol (RDP) or exploiting vulnerabilities (see chapter *Vulnerabilities in Software Products*, page 33). This initial infection is the starting point for subsequent action by the attacker. If the intrusion originated from an access broker, weeks and months can sometimes pass before the access is sold to a ransomware attacker.

Attack phases 2 and 3 – rights expansion and spreading: After the breach, the attacker only has the access rights that the compromised account has. For this reason, attackers usually download additional malware to extend the access rights they have gained and, for example, to gain administrator rights. For example, an administrator is allowed to install or uninstall software. With extended access rights, the attacker is able to spread (semi-)automatically throughout the network of the affected organisation – right into the central components of rights management (e.g. Active Directory) – and attempts to take them over completely. If this happens, the corporate or government network will be completely compromised and no longer trustworthy. The attackers then have all the rights needed, for example, to create user accounts with administrator rights, to view data or even to set up backdoors (malware that allows permanent access to the compromised system).

Attack phase 4 – data leak: Attackers can then steal data (data exfiltration) so that they can later threaten to publish it if a victim is not willing to pay a ransom or hush money.

Attack phase 5 – encryption: Data is encrypted on as many systems as possible, especially on backup systems, usually without affecting the operating system itself. Instead, the attackers leave behind messages with instructions for victims to make contact for ransom or hush money negotiations. Individual attacker groups have begun to dispense with encryption altogether and blackmail directly with the stolen data.

Attack phase 6 – incident response: Victims are faced with the challenge of restoring their systems and data. Depending on the extent of the incident, a transitional operation may have to be organised and the incident communicated to the stakeholders, that is, to the owners, customers and partners. Typically, an IT security service provider who has experience in dealing with IT security incidents is called in at this stage.

4.1.2 — Cybercrime Black Market Economy

Ransomware attacks continue to be the biggest threat of cybercrime. In this case, the increasingly professional division of labour of the attacker groups meets the increasingly connected world of partly multinational companies. In the event of a successful ransomware attack, damage is often no longer limited to regional operating units, but may spread worldwide throughout the corporate network regardless of national and territorial borders.

Due to the millions of dollars in ransoms that ransomware attacks yield, a cybercrime black market economy based on the division of labour and characterised by mutual dependencies and competitive pressure is developing on the attacker side: from the necessary technical infrastructure and malware to access brokers and cybercrime call centres. If a new method becomes suitable for attacks, eventually a cybercrime service will be formed from it, which makes this method accessible to many attackers.

Various elements of a cyber attack are outsourced to specialised groups of attackers, much like the outsourcing seen in the service sector. It is referred to as Cybercrime-as-a-Service (CCaaS). CCaaS allows an attacker to source almost every step of an attack as a service from other cybercriminals, or at least the malware needed to do so. This is a prominent factor in the evolving nature of the threat landscape, as specialisation in a particular service allows attackers to target it and develop its effectiveness. Moreover, the services become available to many attackers at the same time. As a result, the time between the development of a new method and its widespread use is greatly reduced or eliminated. This also partly explains the dynamic developments observed in the cybercrime space in recent years.

An example of this is the phenomenon of Access-as-a-Service (AaaS). These attackers are often referred to as access brokers. They capture identity data or access to specific computer systems in a variety of ways. In the context of ransomware, two forms of AaaS are particularly prevalent: identity and access data theft via information stealers on the one hand, and network compromise on the other.

Identity and access data theft: Information stealers are malicious programmes that attackers distribute via emails with malicious attachments or links to a malicious web server (so-called malware spam). Moreover, attackers disguise information stealers as legitimate software that they offer for download on the internet. Information stealers aim to collect a wide variety of information on a compromised system. This includes, for example, access data stored in browsers, any crypto wallets and information from other software products that could provide information about a person or access to assets. This data is collected after a system has been infected and is then forwarded to the attacker. This compiled data set is called a log and is sold, for example, on underground marketplaces such as Russian Market, 2easy or Genesis Market for 10 to 60 US dollars per log. The logs contain mainly identity data and can be used for identity theft attacks. If these logs contain access data to a company network or session cookies of a cloud application, they can be a gateway for a ransomware attacker to enter the corresponding network.

Compromising networks: Unlike a ransomware attack, an access broker does not cause any immediate damage. Their goal is to create persistent access into the compromised network. This access is then sold on underground forums and private channels to ransomware attackers or APT groups, for example. If the access broker has already succeeded in expanding the access rights obtained, the sales value of this access increases.

Until the last reporting period, malicious Office documents were still the most common means of attack for the initial infection. During 2022, attackers replaced these with malicious container files with formats such as ISO or IMG. Victims still received emails with malicious attachments or links to download the attachments, but the attackers changed the choice of files used for this purpose. The reason for this was probably the standard deactivation of macros in Office products by Microsoft.

The use of malicious container files was particularly promising for attackers because a vulnerability ensured

that the *Mark-of-the-Web (MOTW*, an additional protection measure for end devices) was not applied to files within the container. The vulnerability was fixed on 8 November 2022. As a result, malicious container files were used less frequently in attack campaigns. In early 2023, the majority of attackers then switched to malicious OneNote files for spam and phishing emails.

OneNote files are designed to contain various other files. Using similar methods to malicious Office documents (e.g. social engineering), victims can be tricked into running these embedded malicious files.

In addition to the use of spam and phishing emails to distribute malware, call-back phishing, SEO poisoning and malvertising occurred more frequently during the reporting period.

Call-back phishing: In this case, the attacker sends a fictitious invoice or similar document to persuade the victim to call a call centre under the attacker's control. The call centre then directs the victim to download and execute the malware.

SEO poisoning and malvertising: Both methods often rely on legitimate software as a cover. For example, the attackers imitate the websites and web domains of legitimate software products. If a victim falls for this, they will end up downloading malware in addition to the legitimate software, which will be executed in the background without the victim noticing. SEO (Search Engine Optimisation) poisoning is the term used to describe the attacker's website's position in the search results of a search engine. To achieve it, the attacker tries to achieve the highest possible ranking in the search results. Malvertising, a combination of malware and advertising, involves malware being displayed together with legitimate advertisements. Again, a user is tricked into downloading a mostly legitimate piece of software that has been combined with malware. This is in contrast to drive-by exploits, where simply visiting a website leads to a compromise.

In principle, attackers modify their approach promptly when the circumstances change.

Ransomware-as-a-Service

The most active and thus also the most threatening ransomware families were operated and offered in the form of Ransomware-as-a-Service (RaaS) during the reporting period. The RaaS LockBit 3.0 and the RaaS Alphv stand out in particular. They focus on the development of exclusive services for particularly successful affiliates. This involves providing affiliates, who bring in high commissions in ransoms, with additional services beyond the ransomware.

Both LockBit 3.0 and Alphv, for example, offered additional ransomware variants to selected affiliates during the reporting period, which were based on a different source code and included additional functions. More advanced services such as DDoS attacks, negotiation support or exclusive access brokers were also offered by operators of some RaaS.

Cybercrime groups definitely compete for their affiliates, which is why the reputation of one's own "brand" also plays an important role in the scene. This kind of rivalry leads to an ever increasing intensification of the threat level. For example, a decisive factor for an affiliate when choosing a RaaS is how much pressure can be exerted on an affected person. As a result, the competition between cybercrime groups leads to the maximisation of pressure on affected victims. Other distinguishing features between RaaS offers include the percentage of the ransom that remains with the affiliate or the ongoing improvement of the ransomware itself. For one thing, such exclusive services can bind the most successful affiliates to a particular RaaS for a longer period of time. Furthermore, these services are likely to motivate other affiliates to become more active or to demand higher ransoms.

One notable feature of the RaaS LockBit 3.0 was the introduction of a monetary reward for finding vulnerabilities (bug bounty) for the RaaS itself in the summer of 2022. Very similar to legitimate bug bounty programmes, the attackers call on people to report vulnerabilities in the ransomware or the RaaS offering, as well as if it is possible to identify the attackers, in exchange for a bounty.

Too Big to Stay Afloat

Parallels are thus emerging between the legal economy and the cybercrime black market economy, which has evolved in recent years, driven by ransomware attacks. This division of the different aspects of an attack, such as AaaS and RaaS, is similar to the outsourcing of tasks within the service sector. Maximising the pressure of extortion also allows the attackers to collect as much ransom as possible, which is not unlike the pursuit of profit in business.

Many large and important companies and institutions are commonly deemed "too big to fail". During the global financial crisis of 2008, for example, this included numerous banks that could only be saved from insolvency through state aid. Unlike companies and institutions, however, cybercrime groups cannot become "too big to fail". Instead, they become "too big to stay afloat". When a group of cybercriminals is successful, their public profile increases and with it the attention they receive from security professionals and law enforcement. Therefore, until now, it was only a matter of time before such groups could be rendered harmless or were forced to go into hiding. Emotet, for example, was shut down for the first time in January 2021. The RaaS DarkSide dissolved after a particularly successful cyber attack and the RaaS REvil also disappeared after a particularly successful attack. The "Conti Syndicate" splintered in May 2022, presumably because of differing views on the Russian war of aggression in Ukraine.

4.1.3 — Hush Money Extortion with Data Leaks and Other Extortion Methods

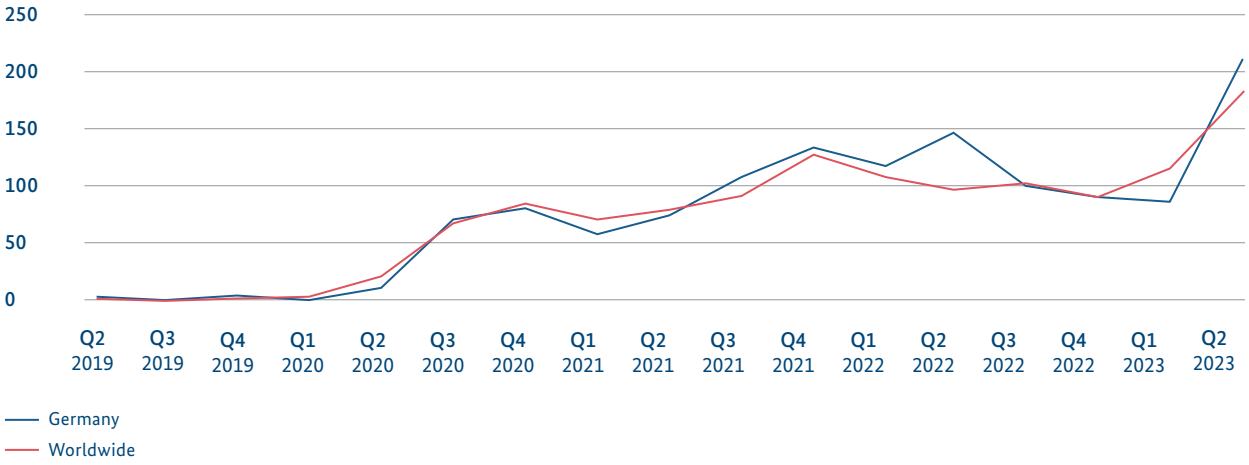
Since 2021, ransomware attacks have usually been accompanied by data leaks. This practice is known as hush money extortion or double extortion. The BSI's leak victim statistics provide information on the victims of hush money extortion. The BSI monitors leak sites for this purpose, on which attackers publish the names and captured data of victims of their ransomware attacks if they do not pay a ransom. By publishing their data on a leak site, ransomware victims become victims of cyber extortion for the second time, so to speak.

These leak pages can therefore be used to record presumed victims who have been threatened with the publication of their data. In this respect, the leak victim statistics are not statistics about ransomware attacks, but about victims of hush money extortion. This is why we also use the term "presumed victims", because being named on a leak page under the control of an attacker does not necessarily mean that an attack actually took place. In some cases, attackers even mention names solely for the purpose of blackmail, without an attack actually having taken place.

The monitoring of leak sites only covers some of the ransomware victims. This means that, generally, only the organisations that refuse to pay a ransom or a hush money are named and published on leak sites. This leaves a large dark field of ransomware victims. Consequently, this data collection does not provide any information on how many of the actual victims decide to pay a ransom or hush money. Moreover, the time of publication does not provide any information about exactly when the

Presumed victims in leak sites
2021 = 100

Figure 2: Presumed victims on leak sites from Germany and worldwide in comparison (2021=100)
Source: Federal Office for Information Security 2023



ransomware attack took place, which may have been a long time before. On top of that, the categorisation by country of the alleged victims recorded in this way is only an approximation, as it is usually done according to the location of the alleged victim's main place of residence. This means that the attacked network segment may have been located in other parts of the world, especially in the case of globally active companies.

The first cyber attacks involving hush money extortion and leak sites were observed in 2019. In the first quarter of 2019, the cybercrime group calling itself "Team Snatch" attacked some victims. In the fourth quarter of 2019, the cybercrime group behind the RaaS Maze began combining ransomware attacks with leaks.

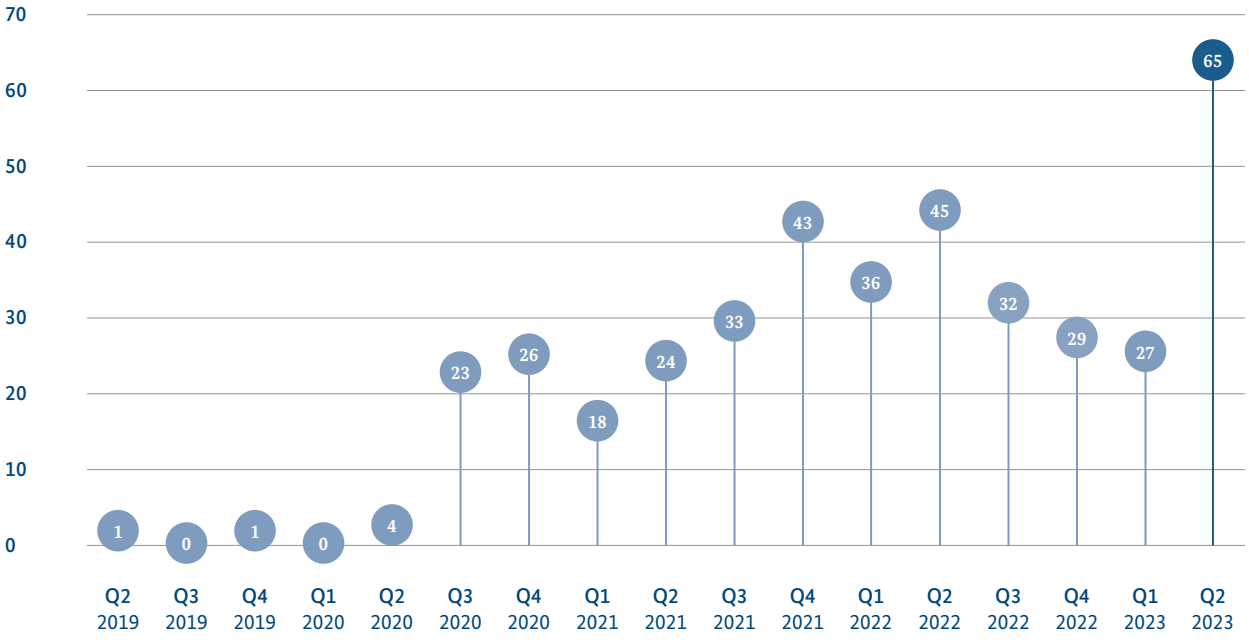
In 2020, this approach gained acceptance among various cybercrime groups, which the BSI reported as a *proliferation* of cybercrime approaches (see The State of IT Security in Germany 2022). By 2021, double-extortion attacks became the norm in a ransomware attack. This development was reflected in the steady increase up to the fourth quarter of 2021.

For the time being, the time series has reached its peak with 1,003 presumed victims recorded worldwide in the fourth quarter of 2021 and 45 victims from Germany in the second quarter of 2022. Both when considering the world as a whole as well as restricting the analysis to the victims assigned to Germany, a slight decrease and subsequent stabilisation can be observed in the following quarters. Then, in the second quarter of 2023, the highest number of leak victims since recording began was recorded. The reason for this were two new leak pages. MalasLocker was previously a one-time campaign with a presumably hacktivist background. The site 8Base, on the other hand, is associated with at least two ransomware families and is likely to have become well established.

The five most active leak sites are regularly responsible for around 50 per cent of the alleged victims. The RaaS LockBit 3.0 is the most active ransomware, both when limited to Germany (see Figure 4) and when viewed globally (see Figure 5). LockBit's leak page named a total of over 800 presumed victims spread around the world during the reporting period.

Presumed victims from Germany on leak sites
Amount

Figure 3: Presumed victims form Germany on leak sites (number)
Source: Federal Office for Information Security 2023



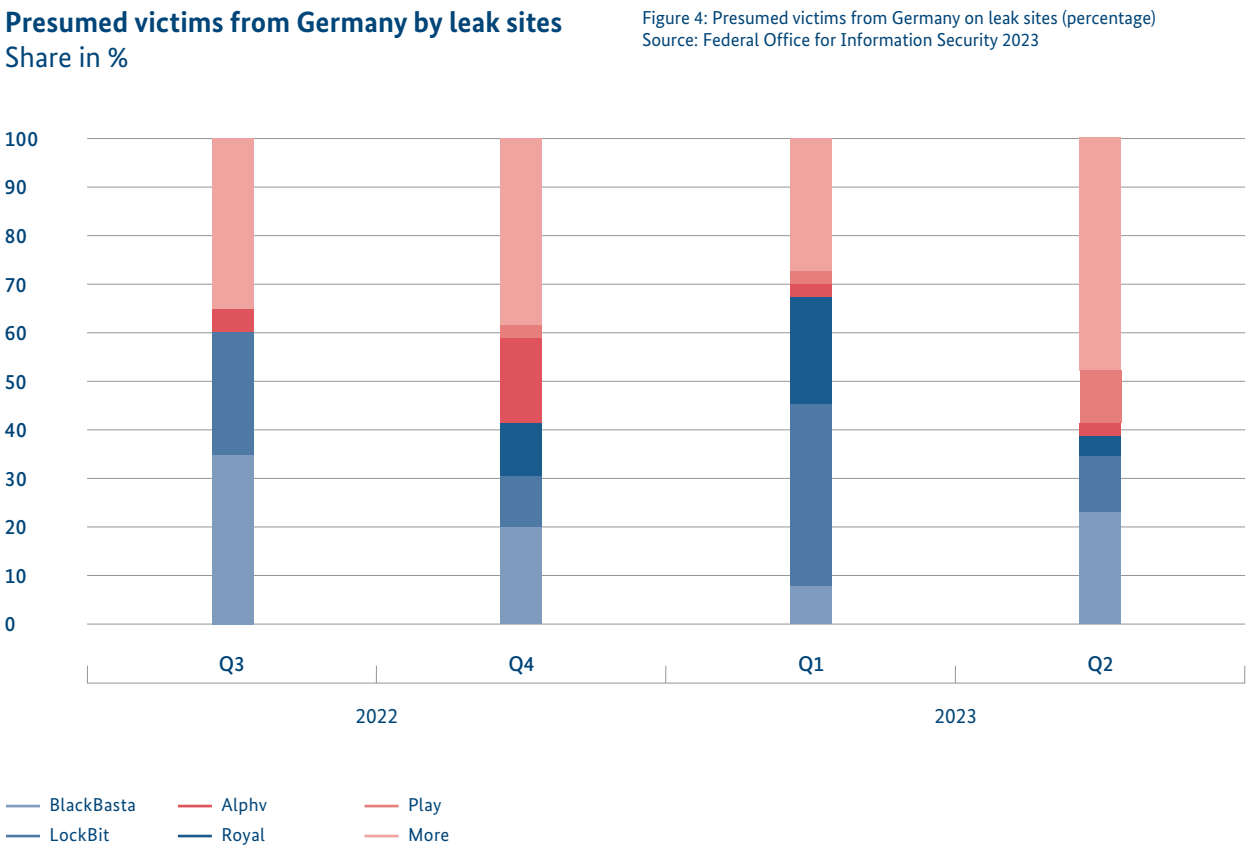


Figure 4: Presumed victims from Germany on leak sites (percentage)
Source: Federal Office for Information Security 2023

The two RaaS Black Basta and Royal are being monitored in the IT security community as a kind of successor to the defunct RaaS Conti. Both RaaS first appeared in 2022 and quickly became part of the top 5 most active ransomware families.

The RaaS Alphv (also known as BlackCat) was first observed in November 2021 and is one of the most threatening ransomware families along with LockBit. In 2023, the cybercriminal group Vice Society took 5th place in the ranking. What is remarkable about Vice Society is that this group did not develop its own ransomware, but uses the ransomware of other RaaS.

In addition to the ransom and hush money extortion described above, attackers often use additional extortion methods to put additional pressure on the victim to pay. Compared to past reporting periods, these other extortion methods described below have remained largely unchanged (see The State of IT Security in Germany 2022). Only the attackers behind the RaaS Alphv tried a new extortion method in individual cases during the current reporting period. This involved the attackers making the data of those affected available in searchable form on a website via the open internet. This allowed any user of the internet to access the data. It is possible that this method will be spread and adopted by other attackers, but it has not yet been observed by the BSI.

Attraction of public attention: Some attackers actively approach the victim's customers or the public to exert additional pressure. This goes beyond publishing the information of victims on leak pages set up for this purpose. For example, attackers might contact a victim's clients or employees by email and inform them that sensitive data about them has become public due to unpaid hush money. This can damage the victim's reputation in the long term, especially if the victim is not transparent in its dealings with the data leak. Dutiful notification of competent data protection or regulatory authorities can limit the negative impact (see chapter *Findings on the Threat Landscape in Society, page* 51).

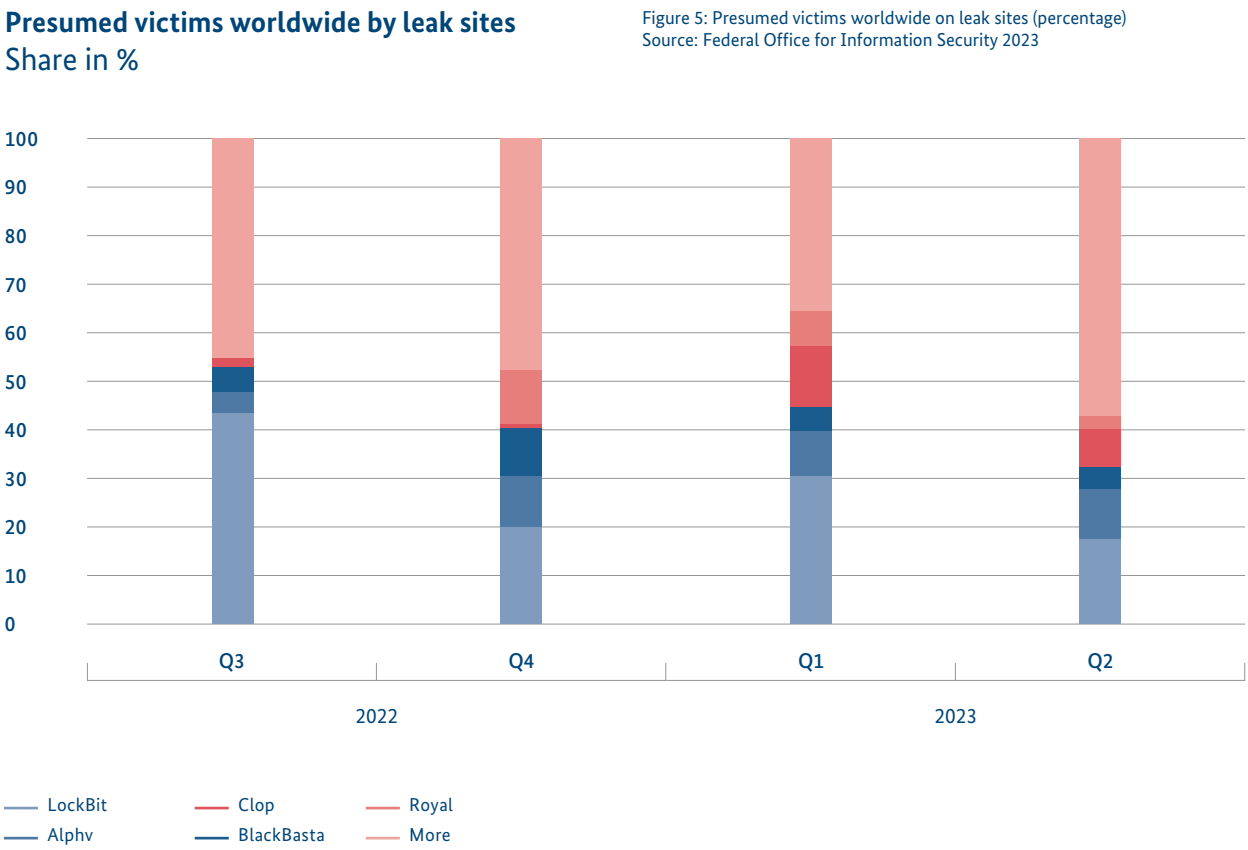


Figure 5: Presumed victims worldwide on leak sites (percentage)
Source: Federal Office for Information Security 2023

Sale or publication of sensitive data: If the victim is not willing to pay, some attackers may auction off or sell captured data to third parties. With this data, the buyers can then blackmail the victim. This is especially true when it involves valuable trade secrets or compromising information about individuals. It is usually no longer possible to determine to whom such data is ultimately auctioned off. If the attackers do not find a buyer, they publish the data on a designated leak page. Once data has been leaked, it is considered permanently compromised, even if hush money or a ransom has been paid.

Apart from the combination of this extortion method with ransomware in the context of double extortion, the BSI also monitors leak pages of attackers who extort their victims without the use of ransomware. In this case, the attackers compromise the victims in the same way as in a ransomware attack, but refrain from using ransomware. The BSI assumes that this allows the attackers to move more quickly from the initial infection to the extortion of hush money.

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

Use of DDoS attacks in the negotiation phase: Individual attackers additionally use DDoS attacks during the negotiation of a ransom to put further pressure on the victim. These attacks may require additional incident response measures and thus also hinder the response to the ransomware attack.

4.1.4 — Measures

Ransom payments generally offer no guarantee that encrypted data will be released. They also contribute to the professionalisation and growth of criminal organisations and black market economies. Therefore, the BSI advises against paying ransoms. It is more important to take effective precautions against ransomware attacks.

4.1.4.1 — Protective Measures According to Attack Phases

A ransomware attack consists of several steps (see chapter *Process of an Attack*, page 15). For each phase of this type of attack, countermeasures are possible to prevent the penetration of networks or the encryption of data and to limit possible damage. These measures are presented according to the respective attack phase.

Attack Phase 1 – Break-in

The three most common vectors of entry for ransomware groups are malware spam or links to malicious servers, exploitation of vulnerabilities and access via poorly secured external access points. Effective measures exist for each of these gateways.

Malware Spam Countermeasure: Emails and Raising Awareness
Any received emails should always be displayed coded as "text only" or "plain text". This can be set up properly by the end user or the system administrator. In contrast to displaying as "HTML mail", no macros or hidden commands that may be contained are output, if the email is displayed as plain text. Moreover, web addresses cannot be disguised in this way either. In an HTML-coded mail, for example, a link labelled "www.bsi.de" could actually point to a website containing malicious code. If text-only encoding is not possible or not desired, at the very least execution of active content in HTML mails should be disabled so that malicious scripts can no longer be executed.

Employees should receive practical training on the risks of interacting with emails as part of awareness-raising measures. This is especially true for employees from public authorities and corporate departments who have to deal with a high volume of external email communication (for example, in the human resources department or in marketing).

Vulnerabilities Countermeasure: Patches and Updates
In order to avoid infections resulting from the exploitation of vulnerabilities which already have security updates available, the updates should be applied to the IT systems immediately after they have been made available by the software provider - ideally also to all desktop computers and notebooks belonging to the company network via the central software distribution of the network. Updates that close vulnerabilities of high criticality or relate to particularly sensitive software such as firewalls or web servers (or both) should be prioritised.

Remote Access Countermeasure: Multifactor Authentication (MFA)
Cybercriminals often try to install ransomware on systems via compromised remote access. For this reason, access from outside should also be secured – usually via virtual private networks (*VPNs*) in combination with multifactor authentication.

Attack Phase 2 – Rights Extension

Countermeasure: Secure Administrator Accounts
As a rule, privileged accounts should only be used for administrator tasks. This should not include reading emails or surfing the internet. Administrators should also create additional user accounts with limited rights for such activities that do not require extended access rights. Privileged accounts should always be protected via multifactor authentication. Furthermore, domain administration accounts should not be used for the administration of clients.

Attack Phase 3 – Propagation

Countermeasure: Segment Network
Clean network segmentation helps to limit damage, as any ransomware that may be introduced can initially only reach the systems in the respective segment. This also requires the secure use of administrator accounts.

Attack Phase 4 – Data Leak:

Countermeasure: Anomaly Detection
With network anomaly detection it is possible to promptly detect a potentially unwanted data leak. For this, it is necessary to know the regular network traffic very well. Threshold values can then be selected on the basis of this normal state and the system will respond if these values are exceeded or not reached. The time

zone and location can also be taken into account. The thresholds should also be different outside the regular working hours for an operating site than during regular operation.

Attack Phase 5 – Encryption

Countermeasure: Backups and Data Security
Backups are the best protection against the effects of encryption by ransomware because they guarantee the immediate availability of data even if this happens. For this, however, the data must be saved in an offline backup, which is kept separate from the other systems in the network after a backup. Only then are you protected from attacks and encryption. A backup always includes the planning and preparation of the restart and the restoration of the data. This should be tested regularly to identify recovery complications and challenges before an emergency occurs.

Attack Phase 6 – Incident Response:

Countermeasure: Emergency Plan
Contingency planning for emergency operations and recovery should be in place in the event of a worst-case scenario of a successful attack in which all systems on the network are encrypted. The processes for responding and for recovering systems that are critical to the business should be practised at regular intervals. In particular, critical systems must be identified in advance and alternative communication options outside the compromised network must be prepared. Telephone numbers and important contact information should be kept offline in paper form.

4.1.4.2 — Support from the BSI

Within the scope of its legal mandate, the BSI can support certain affected parties in dealing with IT security incidents. The legally defined target groups of the BSI are

- the operators of critical infrastructure (in accordance with the BSI Kritis Regulation – BSI-KritisV),
- Institutions of the federal administration / agencies of the federal government,
- Companies of Particular Public Interest.

In justified individual cases, the BSI can also take action with institutions that do not belong to the three target groups mentioned. A justified individual case is deemed to exist in particular if the attack is of a special technical quality, the swift restoration of the security or functionality of the affected information technology system is of special public interest or an important office of a federal state is affected.

Incident handling at the BSI is carried out by the specialist units of the *CERT-Bund*. If necessary, the entire expertise of the BSI can also be enlisted. These include experts from the areas of forensics and malware reverse analysis, incident response (Mobile Incident Response Team (MIRT)), cyber security in industrial plants, detection (Bundes Security Operations Center, BSOC) and operating systems as well as penetration testers.

Other security agencies can also be called in to exchange, assess or process cyber security incidents via the National Cyber Defence Centre (Cyber-AZ), which is based at the BSI.

The National IT Situation Centre conducts an initial assessment of an incident report together with the CERT-Bund. For this purpose, a triage meeting is usually held with the persons involved. In this meeting, a common understanding of the incident is developed and possible measures are discussed. Based on this, appropriate further measures are then agreed upon.

The BSI offers a wide range of products and documents that can be made available to those affected both for prevention and for reaction in the context of incident handling. These include, for example, prevention, detection and response documents for APT incidents, incident handling assistance documents for serious IT security incidents such as ransomware incidents, and much more.

Further information and help documentscuments:[c]

The BSI can also advise authorities and companies on a coordinated and structured approach to security incidents, the implementation of suitable measures, the execution of appropriate IT crisis management and suitable crisis communication.

In particularly high-profile cases, the BSI can carry out an on-site mission with a Mobile Incident Response Team (MIRT). The MIRT can assist the victim in a variety of areas, such as initial assessment, rough analysis and assessment of consequences, and review of log data and alarms. In addition, the BSI can also take action in the context of technical evidence gathering, such as creating hard disk images or recording network traffic, as well as technical analysis in the back office, and advise local operations staff on clean-up. Furthermore, recommendations can be made to harden the systems against cyber attacks.

Not only is the BSI able to support victims with its own expertise, but it can also help in the search for suitable incident response service providers. The BSI has published a list of qualified service providers for this purpose. All service providers on it were reviewed for their competence in dealing with serious IT security incidents using the criteria defined by the BSI and were able to qualify accordingly.

The list of qualified service providers can be found here:[d]

4.2 — Advanced Persistent Threats and Threats in the context of the Ukraine War

Advanced Persistent Threats (APT) differ from other cyber security threats in regards of the motivation and modus operandi of the attackers. For example, while malware is usually distributed en masse and opportunistically by criminal attackers (see chapter *Ransomware*, page 14), APT attacks are often planned over the long term and with great effort on individually selected, singled-out targets. APT attacks are not for criminal gain, but for obtaining information from the target and, if necessary, for sabotage.

Observations from Cyber Operations in Ukraine

In the current reporting period, there were a number of developments that shaped the APT threat landscape. The Russian war of aggression in Ukraine, for example, created the first situation in which a state with strong cyber capabilities was in armed conflict with another highly digitalised state. A wide range of phenomena were observed in cyberspace, including cyber espionage, hacktivism, disinformation including publication of stolen data, and cyber sabotage. This gave the first empirical look at the role of cyber capabilities in a war between an aggressor and a partner state of Germany.

Cyber sabotage: In terms of the threat level, the types of targets that are attacked are always relevant. For example, the threat actors in Ukraine did not limit their cyber sabotage to critical infrastructure in the narrower sense. Instead, acts of sabotage were carried out across a relatively wide area in various sectors and industries in Ukraine. Wiper malware was used to delete data. These malware families were designed for sabotage in office networks. There was only one case where special malware for process control systems such as Industroyer2 was discovered, and that was in the Ukrainian energy sector, specifically during attempted attacks on transformer stations in Ukraine. The attempted attack on the substations did not occur until a few months after the start of the war. In contrast, one of the first targets to be attacked - on the day of the invasion, in fact - was a satellite communications operator that, according to media reports, provided services to the Ukrainian military (see The State of IT Security in Germany 2022). Since then, there have been hardly any reports of cyber attacks on military systems, although this is probably due to the incomplete availability of information.

Cyber espionage: Another key finding is that cyber sabotage against Ukrainian targets was limited to a few threat actors. There were other groups active in Ukraine during the reporting period, but most of them were aimed at gathering information. This division of labour between attacker groups is likely due to organisational or strategic reasons rather than technical ones.

In order to deploy malware in the first place, attack vectors are needed. Several publicly documented cases show that in the early days of the war, attackers used compromised network access that was already in place before the war. No new attack vectors such as new vulnerabilities or new supply chain attacks were observed.

Hacktivism and Disinformation Campaigns in Germany and Other Western Countries

One phenomenon that received greater media attention in Germany in connection with the Russian war of aggression in Ukraine is pro-Russian DDoS hacktivism, which only had limited harmful effects (see DDoS hacktivism chapter *Distributed Denial of Service*, page 28).

Pro-Ukrainian hacktivism occurred in a few cases, most notably at the beginning of the war when a German company with connections to Russia was compromised (see The State of IT Security in Germany 2022).

Unlike DDoS hacktivists, who can only temporarily disrupt internet services with limited damage, cyber spies or saboteurs penetrate deep into IT networks to destroy or leak data. This is an approach that offers further potential for attackers in the future, because depending on the sensitivity of the stolen data, it can be used in disinformation campaigns to influence public opinion. The growing network of hacktivist groups also makes it increasingly possible for state-controlled threat actors to pose as hacktivists in the future.

Furthermore, operations were observed where information gained through the use of phishing or malware was used for disinformation. While this was already common in Eastern European states such as Poland and the Baltic states with regard to the Ghostwriter group before the war, since the beginning of the Ukraine war the Callisto group has also reportedly carried out such operations in the UK according to reports from security agencies and security companies. Due to the heterogeneous level of IT security in German political institutions and media, these kinds of data leaks could also occur in Germany.

Beyond the war in Ukraine, there were other developments in cyberspace that showed the efforts of threat actors to disguise and optimise their attacks.

Anonymisation Networks as a Service for APT Groups

The establishment of several botnets consisting of routers, IoT devices and virtual private servers operated by APT groups for unauthorised access from the internet (scans, exploitation and webshell access) is noteworthy. These botnets serve to anonymise attack traffic, similar to legitimate proxy server systems. This builds on a development that had already been observed in the previous reporting period: Servers that are directly accessible from the Internet are increasingly being attacked. In other words, there is a shift from spear phishing emails to exploiting vulnerabilities in web servers, firewalls or VPN servers. In order to identify and then compromise these systems, the attackers need anonymised internet connections, which they create via these new botnets.

Overview of Relevant APT Groups

During the reporting period, the APT groups named in Table 1 posed a threat to German targets. The list is not necessarily exhaustive. The groups are usually active mainly against targets in the specified sectors. If institutions that have already implemented basic IT security measures want to add threat intelligence to their resources, they can evaluate threat reports particularly about the following threat actor groups. However, the typical attack techniques listed refer to the first phase of an attack and are therefore not complete. Moreover, some of the groups act in a very versatile way, so that other techniques can also be used in the initial attack phase.

APT group	Preferred targets	Preferred techniques
APT15 | VixenPanda | Mirage | Ke3chang	Government institutions | NGOs	*Exploits* against systems accessible from the internet
APT27 | Emissary Panda | LuckyMouse	Energy, telecommunication, pharmaceuticals	*Exploits* against systems accessible from the internet
APT28 | FancyBear | Sofacy	Government institutions | military | media | NGOs	Emails with links to phishing sites; bruteforcing; password spraying
APT29 | Nobelium | DiplomaticOrbiter	Government institutions	Emails with archive files as attachments containing LNK files
APT31 | JudgementPanda | ZIRCONIUM	Government institutions | NGOs	*Exploits* against systems accessible from the internet; bruteforcing
Ghostwriter bzw. Untergruppe UNC1151	Politicians | NGOs | media	Email with links to *Phishing* sites
Kimsuky | VelvetChollima	Defence industry | law firms	Word documents that download remote templates; *Social Engineering*
Lazarus | SilentChollima	Defence industry | aviation	Emails with archive files as attachments; *Social Engineering*
MustangPanda (oder VertigoPanda)	Government institutions	Emails with archive files as attachments containing LNK files
Snake | VenomousBear | Turla	Government institutions | exports	*Exploits* against systems accessible from the internet
UNC2589	Logistics	Emails with documents containing macros in the attachments

Table 1: APT groups relevant to Germany
Source: BSI

Supply Chain Attack as a Result of Another Supply Chain Attack

Situation

In a particularly interesting case, an APT group succeeded in a supply chain attack that was made possible by a previous successful supply chain attack. On 29 March 2023, several IT security companies reported that detections and log files of their customers indicated a supply chain attack targeting a business voice-over-IP (VoIP) communications provider with several hundred thousand customers. It turned out that several installation packages of a VoIP software for Windows and MacOS signed by the manufacturer contained and executed a manipulated software library. It went through several stages to download additional malicious code from actor-controlled servers. These installation packages were officially provided and signed by the manufacturer, so that it was safe to assume a supply chain attack, that is, a successful compromise of the manufacturer. The provider's CEO subsequently confirmed the media reports and the successful attack on the company in a forum post.

A security firm commissioned to investigate the incident found the following: The original attack vector for compromising the VoIP communications provider was the installation of another legitimate financial transaction software. This financial software, which contained malware, had been downloaded by the provider from the website of its manufacturer. This means there had already been an attack on the manufacturer of the financial transaction software, resulting in a concatenation of supply chain attacks: The financial software company was attacked first, and malware was added to its legitimate software. This legitimate but malicious software was then installed at the VoIP communications provider, which in turn added a malicious programme to their software, which was detected at their customers' premises at the end of March 2023.

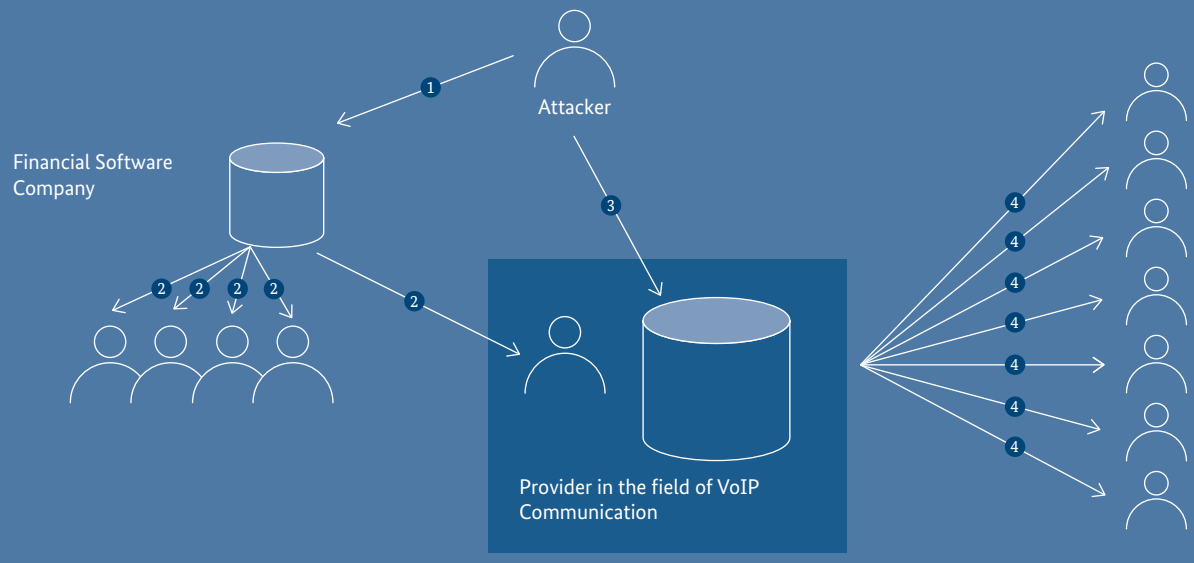


Figure 6: Supply Chain attack as a result of a supply chain attack

1. Attacker infiltrates manufacturer of financial transaction software and compromises legitimate software.
2. Victims download compromised software for financial transactions, including an employee of a VoIP software provider.
3. Attackers compromise VoIP software in order to be able to extend the attack to a large number of potential further victims.
4. More victims download the compromised VoIP software.

Assessment
A supply chain attack has the potential to compromise a large number of victims simultaneously. Measures such as signing software packages and downloading from official websites are not effective in this case, because the attacker is already able to embed their malware in the build process of the software, so that it is signed and made available like official programme code.

The several hundred thousand customers involved in this case demonstrate the impressive potential of such an attack. Ransomware attacks or spying on customers would also be possible in this case, although the actual motivation behind the case described is unclear up to now.
The concatenation of various supply chain attacks, as in this case, is worth highlighting: It shows that attackers are willing and able to analyse accesses in great detail, observe them over a longer period of time and assess if such access can be used systematically and with considerable effort for follow-up attacks.

According to public reporting, the attack has been attributed to the "Labyrinth Chollima" subcluster, part of the APT groups often referred to as Lazarus.

Response
After the attack became known, the VoIP communication provider recommended uninstalling the affected software versions and provided cleaned installation packages. The BSI also warned its constituency. Moreover, the infrastructure for downloading further malware was quickly blocked, so that the infection chain was interrupted at an early stage. Afterwards, the manufacturer dealt with the incident in a transparent manner and provided information on the status of the incident investigation and its results.

4.3 — Distributed Denial of Service

Denial-of-Service attacks (DoS attacks) are attacks on the availability of internet services. Websites are often targeted by such attacks. Their respective web servers are flooded with so many requests that the website becomes inaccessible. If such an attack is carried out by several systems in parallel, it is called a distributed denial-of-service attack (DDoS attack).

Attackers pursue different goals with DDoS attacks. It could be a form of extortion that has been transferred to cyberspace. Attackers demand money from the victim to stop the attacks. DDoS can also be used in the context of a ransomware incident to increase pressure on the victim and extort a ransom for encrypted data. In addition, attackers can also use DDoS attacks to directly harm institutions. Reasons for this can be, for example, competition among competing companies or activism (for example, by so-called *script kiddies*). A DDoS attack can also be used to distract from another, more sophisticated attack such as ransomware (see chapter *Ransomware*, page 14) or APT (see chapter *Advanced Persistent Threats and Threats in the Context of the Ukraine War*, page 24). Politically motivated DDoS attacks, which fall under the phenomenon of hacktivism, have also occurred internationally in the context of the Russian war of aggression against Ukraine.

The consequences of a DDoS attack are, firstly, financial damage for service providers or online shops if they cannot be reached. Secondly, impairments due to hacktivism, critical services and websites, for example of banks or the police, may result in a damaged reputation or an insecurity in the population.

The number of known DDoS attacks in Germany is measured by an index (see Figure 7). An index of 95 points in February 2023, for example, means that the number of DDoS attacks in Germany in February was 0.95 times the annual average in 2021.

The indicator shows DDoS attacks by pro-Russian hacktivists in Germany in September 2022 as well as in spring 2023, which overall had only a minor damaging effect and also fell short of the frequencies of criminal DDoS attacks in previous reporting periods in terms of numbers. Unlike ransomware or APT attacks, attackers cannot hack or hijack networks with DDoS, but only temporarily impair internet services. Therefore, it is safe to assume that the interest of DDoS hacktivism in Germany

Known DDoS attacks (measurement number) in Germany
2021=100

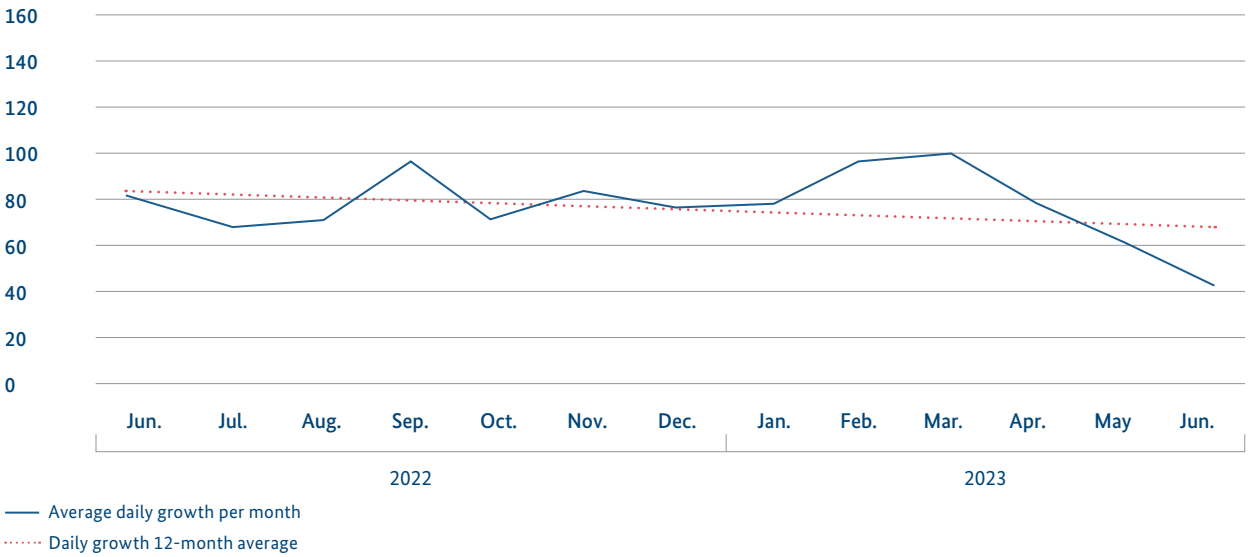


Figure 7: Known DDoS attacks (measurement number) in Germany (2021=100)
Quelle: *DDoS* statistics, BSI

was not to actually cause extensive material damage. Rather, the attackers' aim may have been to stir up social uncertainty and damage confidence in the state's ability to protect and provide for the population.

In contrast to the previous reporting period, there was no increase in DDoS attacks during the current reporting period on high-selling promotion days such as Black Friday, Cyber Monday or the pre-Christmas period. Overall, the number of DDoS attacks decreased significantly in the second half of 2022 compared to the first half of 2022. After the hacktivist campaigns in the first quarter of 2023, the declining trend of cybercriminal DDoS attacks, which was already evident for quite some time, continued in the second quarter of 2023.

In December 2022, law enforcement agencies struck against DDoS-as-a-service provider: Europol reported the shutdown of about 50 websites that offered services for targeted DDoS attacks. One of these services is said to have been responsible for over 30 million DDoS attacks worldwide. Several administrators of these websites were arrested. Authorities from the USA, the UK, the Netherlands, Germany and Poland were involved in the operation[1].

Information on DDoS prevention and mitigation as well as a list of qualified service providers for DDoS mitigation can be found.

Look here for further information:[e]

DDoS Hacktivism

Situation
During the Russian war of aggression against Ukraine, various groups of pro-Russian hacktivists formed and carried out DDoS attacks including targets in Germany. In the summer of 2022, the hacktivist group Killnet made a name for itself (see ***The State of IT Security in Germany 2022****). Moreover, the group NoName057 launched the project "DDoSia". This is a botnet that was deliberately set up for hacktivist attacks. In the autumn of 2022, the providers of DDoSia began recruiting affiliates to use the botnet to attack the internet services of Western authorities. Potential affiliates were offered the prospect of a cash reward.*

The various hacktivist groups are responsible for many DDoS attacks in Germany as well; including websites and internet portals of airports, police forces and state governments. A characteristic feature of these attacks is that the groups announced them in advance on their social media channels. The DDoSia project's target list included, for example, web services of several state police forces and institutions of the federal states. The websites of the police forces in Brandenburg, North Rhine-Westphalia, Lower Saxony, Bremen, Hesse, Mecklenburg-Western Pomerania, Rhineland-Palatinate and the domains of Saarland and Saxony-Anhalt were listed. The websites of federal authorities and the website www.ukraine-wiederaufbauen.de were also attacked

Assesment
The effects of the abovementioned attacks were limited. The reason for this is that DDoS attacks generally do not enable deeper infiltration of networks or sustained damage, such as that caused by data encryption. However, they can lead to short-term outages or slower access to websites for a limited period of time. Such attacks can be effectively mitigated by activating appropriate DDoS protection mechanisms.

Thus, it is safe to assume that the aim of the attackers was to foment social insecurity and damage trust in democratic institutions as well as in the state's ability to protect and provide for the population.

Response
The BSI informed the responsible state CERTs about the findings and was in direct exchange with the state CERTs throughout the entire period.

4.4 — Spam and Phishing

An unsolicited email is generally referred to as spam. Spam is often sent via compromised or rented servers. Likewise, stolen email addresses that originally belonged to a legitimate account can be exploited for this purpose. Moreover, other systems connected to the Internet can be infected in order to misuse them for spam services. For example, IoT devices and private home automation devices can be interconnected and abused as parts of a botnet.

Spam during the reporting period by type
Share in %

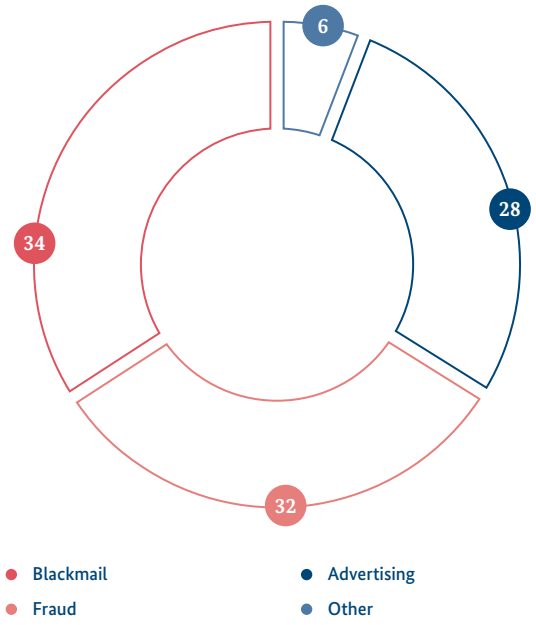


Figure 8: *Spam* during the reporting period by type
Source: Email traffic statistics, BSI

Spam can be split into different categories. There is a distinction between unwanted but basically harmless advertising spam (28%) and harmful cyber attacks, including blackmail (34%) and scam emails (32%). The main distinguishing feature is that blackmail messages threaten to pass on alleged or actual knowledge about the victim and demand hush money this way. This usually happens regardless of whether or not there is any real risk of being blackmailed with information. In contrast, fraud involves feigning a need to act on behalf of an institution or person without extorting any hush money. The aim is to intercept sensitive personal data in order to sell it on or use it for their own criminal activities.

Phishing emails account for the largest percentage of fraudulent emails (84%). These messages aim to use social engineering techniques to get the victim to reveal their identity or authentication details.

Additional attack variations can be distinguished based on the channel chosen for the attack. Smishing (phishing via SMS) and vishing (voice phishing) are particularly noteworthy. Smishing is evidenced through the sending of countless SMS or short messages via Messenger to a multitude of phone numbers, for example with alleged delivery notifications or instructions on how to download a voice message. The aim of this method is usually to trick the recipient into clicking on a link that contains malicious apps or malicious websites. Vishing, on the other hand, involves contacting the target person by phone and using a conversation script to trick them into revealing information or making a payment. Widespread and still current contents of the phone calls are fake calls from alleged IT support or authorities, suggesting to the victims that they have to make a payment or release personal data for verification.

Areas of Focus and Monitoring in Phishing and Spam

As is clear from the phishing techniques described, criminals usually exploit certain topics through which they want to reach their victims. Most fraud attempts are attributed to monetary motivation. As a result, the largest percentage of spam messages sent can be found in the area of finance phishing. Phishing emails are sent out that pretend to be from well-known banks or financial service providers with a corresponding corporate design. The aim is to convince consumers that there is something they need to do. Supposedly threatening to block accounts, requiring verification of online banking or outstanding payments are just a couple of examples that are used to persuade victims to divulge their payment and account data. The BSI also monitors phishing campaigns relating to crypto wallets and FinTechs.

Social emergencies and major events during the reporting period provided criminals with further opportunities for phishing and scamming. The tense situation on the energy market in winter 2022/23 as well as the relief packages decided by the government led to phishing messages with subject lines such as "Secure stipend for energy

now!" and "We will transfer your stipend for energy". These attackers posed as energy providers or part of the government itself and wanted to take advantage of consumers' financial distress. Alongside this, charity scams increasingly appeared in the name of aid organisations, promising assistance in the context of the war in Ukraine and the earthquake in Turkey and Syria, for example. The aim here was to arouse feelings of emotional concern among consumers in order to collect money in the context of fake appeals for donations via social media or email.

The use of large AI language models to improve the quality of phishing and scam attacks is another growing challenge (see chapter *AI Large Language Models*, page 40). Due to technological progress and the increasing availability of AI systems, there is a risk that they will be misused. For example, this can lead to phishing messages being made more authentic. In addition, speech can be imitated better and sounds more human. The use of chatbots, which can imitate conversation processes more authentically, can also tempt people to divulge information and data.

4.5 — Attacks in the Context of Cryptography

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

The Technical Guideline TR-02102:[f]

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

- Weakness in cryptographic mechanisms or protocols
- Implementation errors
- Inadequately secured side channels
- Weakness in random number and key generation
- Inadequately protected key material

The classic application of cryptography is to protect the confidentiality and integrity of data, for example when it is transmitted over open networks such as the internet. Various cryptographic mechanisms and protocols are available for this purpose, for which it is generally assumed that an attacker with access to the network traffic can neither learn the secret keys nor decrypt the exchanged data or manipulate it unnoticed. In order to guarantee the effectiveness of cryptographic mechanisms and protocols, suitable procedures must be selected and implemented correctly. Furthermore, it must be ensured that the behaviour observable at the network interface (e.g. response times of a server) does not reveal any information about processed confidential information.

When securing cryptographic systems that are intended to withstand even attackers in close proximity, further side channels (e.g. power consumption or electromagnetic radiation of the devices) must be taken into account, via which confidential information can also be leaked. Side-channel analysis, that is, analysis for susceptibility to side-channel attacks, is now a separate branch of research that has produced new attack vectors in addition to countermeasures. The attack described in the HERTZBLEED info box (page 32) exploits a novel side channel in modern processors where differences in power consumption lead to different runtimes. This attack demonstrates that side channels, which actually require physical access, can also be exploited by a remote attacker in some situations.

An essential prerequisite for the secure use of cryptography is the generation of true random numbers, which must fulfil certain criteria of quality. Random numbers are needed, among other things, for key generation. For cryptographic applications, random numbers must not be predictable and must not have exploitable statistical defects. In order to prevent attacks by weak random numbers, the BSI defines functionality classes of random number generators for different purposes in the documents AIS 20 and AIS 31. A new draft of the mathematical and technical annex of AIS 20/31 was published in September 2022.

However, the security guarantees of many cryptographic algorithms used today no longer apply as soon as a sufficiently powerful quantum computer is available. The chapter Quantum Technologies (page 73) shows ways to counter this threat and presents the BSI's activities in this area.

HERTZBLEED – Timing Attack on SIKE through Clock Frequency Side Channel in Processors

The power consumption of a processor generally depends on the data that is processed in the processor's registers. By measuring power consumption, it is thus possible to draw conclusions about the data processed and, in the case of cryptographic operations, also gain knowledge about the confidential information being processed. To reduce power consumption and heat generation, some processors dynamically adjust their clock frequency. Adjusting the clock frequency in this way influences the runtime of the calculations performed by the processor. The runtime of a calculation can therefore also depend on the processed data. This novel timing side channel was exploited in the HERTZBLEED attack, which was released in June 2022.

In the publication of HERTZBLEED[2], the dependence of the clock rate on the processed data was described, systematically investigated and verified in experiments. Moreover, the researchers have demonstrated that a remote attacker can completely determine the secret key of the SIKE (Supersingular Isogeny Key Encapsulation) key exchange method by exploiting such timing information. It is worth noting that the SIKE implementations that were attacked were hardened against previously known timing attacks.

SIKE has long been considered a promising candidate in the National Institute of Standards and Technology's (NIST) standardisation process for post-quantum methods. However, an attack by Castryck and Decru[3] published in July 2022 ultimately completely broke SIKE cryptoanalytically. The chapter Quantum Technologies (page 73) contains more detailed information on post-quantum cryptography and the NIST selection process.

5. — Vulnerabilities

In order to infiltrate computer systems, attackers need vulnerabilities in the IT infrastructure that can be exploited for an attack. Malware that exploits a vulnerability to carry out a cyber attack is called an exploit. Exploits are used, for example, by cybercriminals for the initial infection of systems and to prepare a ransomware attack.

Vulnerabilities arise, for example, from errors in programming, from weak default settings of IT products in live operation or also from misconfigured security settings. IT systems are becoming more and more complex and production conditions more and more divided and modular, so vulnerabilities are very common. They can therefore also occur in operating systems and applications (see chapter *Vulnerabilities in Software Products*, page 33) as well as in hardware (see chapter *Vulnerabilities in Hardware Products*, page 39). With the expansion of the Internet of Things, vulnerabilities are increasingly appearing in networked devices (see chapter *Vulnerabilities in Networked Devices*, page 39).

When a vulnerability is discovered in an IT product, manufacturers usually provide security updates (patches) to close the vulnerability and prevent its exploitation for cyber attacks. Structured patch management is therefore one of the most important preventive measures to successfully counter the risks of digitisation.

5.1 — Vulnerabilities in Software Products

Vulnerabilities in software products often serve as the intrusion gateway to compromise systems and entire networks – as they are often exploitable via the internet and thus allow attackers maximum anonymity and flexibility from afar.

During the reporting period, an average of 68 new vulnerabilities became known every day, around 24 per cent more than in the previous reporting period. This means that a total of almost 27,000 new vulnerabilities became known in all kinds of software products, from specialised technical applications to complex server infrastructure and mobile phone apps. As in previous years, the increasing modularisation and division of labour in software production impacted the threat level in the current reporting period. This is because if a vulnerability in a software component that is used in a large number of different applications becomes known, then it will be possible to exploit this single vulnerability for cyber attacks against all of these applications.

The vulnerabilities that became known during the reporting period differed in terms of their criticality as well as the damage that attackers can cause by exploiting the vulnerabilities. The Common Weakness Enumeration (CWE classification), a list of different types of vulnerabilities in hardware and software maintained by the IT security community, is used below to quantify the harmful effects. Criticality is measured using the Common Vulnerability Scoring System (CVSS score).

Harmful effects: The execution of unauthorised programme codes or commands is one of the most important harmful effects. Around 47 per cent of the vulnerabilities that became known during the reporting period were susceptible to this. They allowed, for example, the initial infection in a ransomware attack (see chapter *Attack Motives and Process of an Attack*, page 14). Many vulnera-

Known vulnerabilities by possible harmful effect*
Share in %

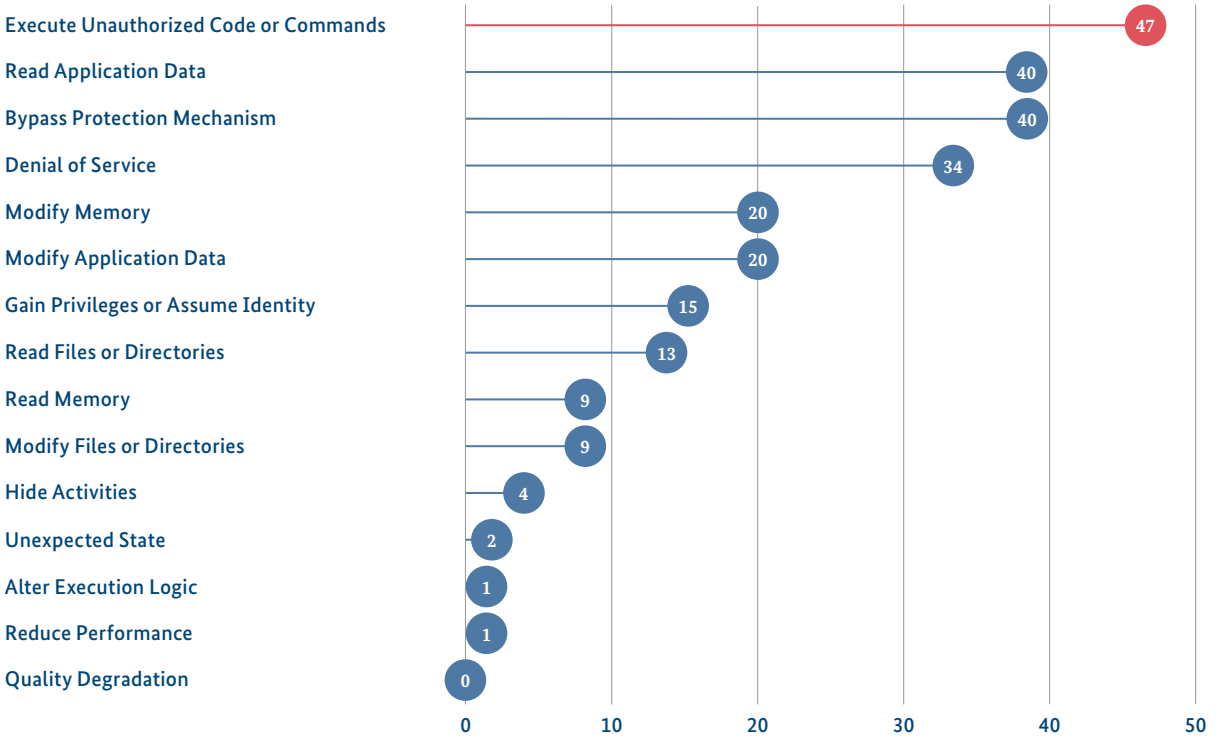


Figure 9: Known vulnerabilities according to harmful effect
Source: Vulnerability statistics, BSI

*Multiple answers possible

bilities also allowed attackers to bypass security measures (40%). With each 20 per cent of the vulnerabilities, attackers were able to manipulate memory and application data, for example, to extend the access rights they had gained. And around 40 per cent ultimately enabled data to be retrieved. Attackers can use such data for cyber extortion (see chapter *Hush Money Extortion with Data Leaks and Other Extortion Methods*, page 18) as well as sell it on to other attackers, who can then use this data for their own cyber attacks. Furthermore, every third vulnerability that became known during the reporting period was exploitable for a DoS attack.

Criticality: The criticality of a vulnerability, however, does not only result from the possible harmful effects that attackers can achieve with it. Attack vectors and other factors are also included in the CVSS score, an internationally recognised industry standard that assesses the criticality of vulnerabilities in an internationally comparable manner. The criticality of the vulnerabilities that became known varied greatly. About three per cent had low scores and 45 per cent had medium scores on the ten-point scale (see Figure 10: Known vulnerabilities according to criticality, source: Vulnerability statistics). More than half – 53 per cent – had high (7-9) or critical (9-10) CVSS scores. The proportion of critical vulnerabilities was around 15 per cent. As in the previous reporting period, the most common attack vectors were cross-site scripting (13%), out-of-bounds write (8%) and SQL injection (7%).

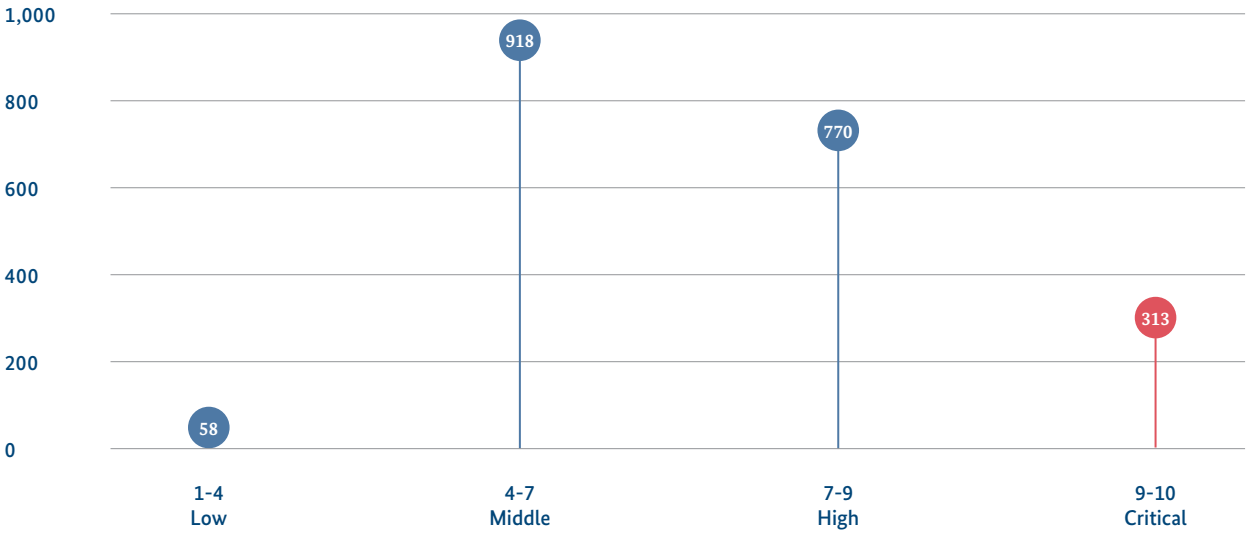
Not every vulnerability is easy to exploit for attacks. For example, a vulnerability in a local application without a connection to the internet can only be exploited by a local attacker. In contrast, vulnerabilities in software products that are directly accessible from the internet, for example, can be abused more easily and by a higher number of cybercriminals for attacks. Of the 13,500 vulnerabilities with a high or critical CVSS score in the reporting period, just under half (49%) were easily exploitable for cyber attacks.

In cyberspace, there is a constant race between security researchers and the various attacker groups: The first to discover vulnerabilities can either use them for cyber attacks or offer them for sale to other attackers on the darknet, or report them to the manufacturer to push for the provision of a patch.

During the reporting period, the BSI received an average of around 20 reports per month from security researchers about software products with vulnerabilities and clas-

Average monthly vulnerabilities disclosed by the CVSS score[1] for criticality

Figure 10: Known vulnerabilities according to critically
Source: Vulnerability statistics, BSI
* Risk assessment according to CVSS version 3.1

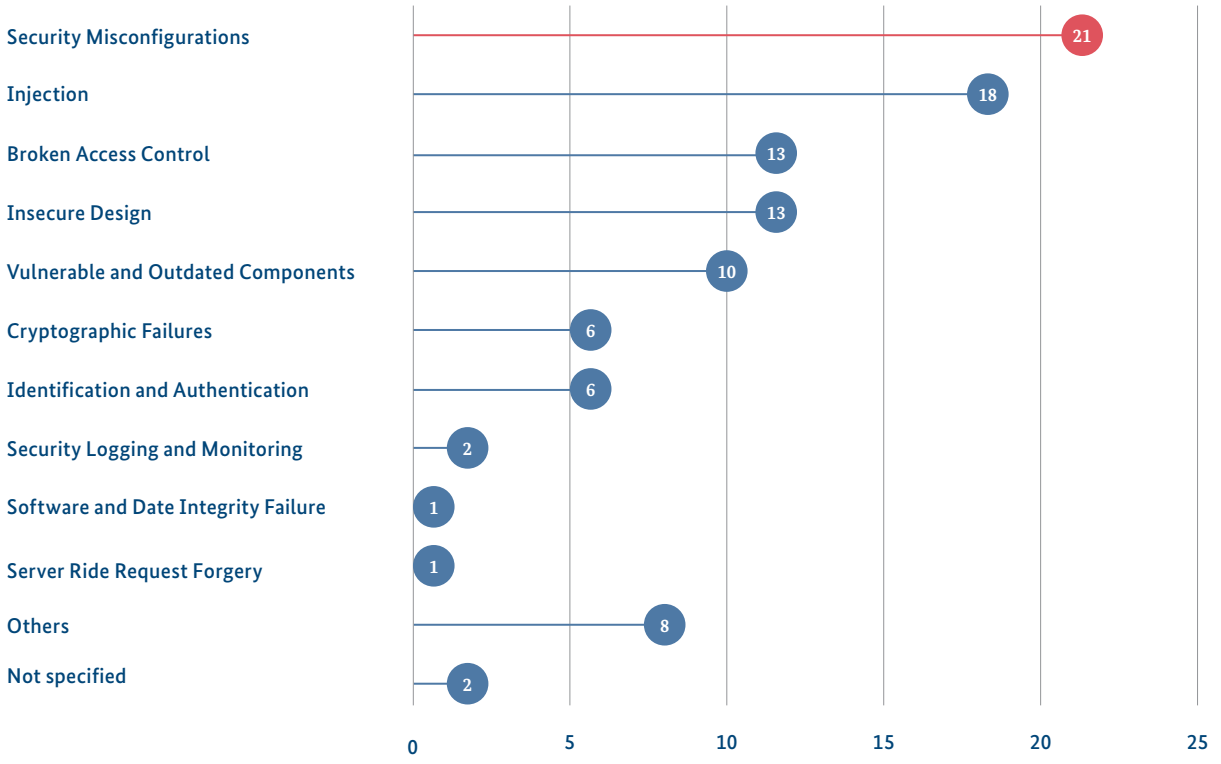


sified them according to the Open Web Application Security Project (OWASP) system. While CWE and CVSS describe the vulnerabilities themselves, OWASP allows a description of the vulnerable product. According to this, most of the reported products in the reporting period had misconfigurations (security misconfiguration, see Figure 11), accounting for around 21 per cent of the reports. These include, for example, a lack of security hardening of the product, unnecessary features such as open ports, access rights or services, or unchanged default accounts from the development phase. In around 18 per cent of the reported cases, the product affected by the vulnerability allowed attackers to inject malicious code because user input was not validated, filtered or sanitised by the software. Software products without functioning access controls (broken access control) followed in third place in the ranking with 13 per cent. They violated the principle of denial of access by default and allowed access to any user without further access control, enabled circumvention of access controls or granted authenticated users to use the software with administrator rights. Around 13 per cent of the reported products violated security-by-design principles (insecure design). One in ten reported products had vulnerable or outdated components, and cryptographic failures occurred in six per cent of the reported products. Other products had vulnerabilities in security monitoring or allowed data to be manipulated. With a part of six per cent, products with vulnerabilities in their identification and authentication systems were still reported comparatively rarely. Multi-factor authentications also fall under this category. There are now, however, known malware programmes that can bypass this form of user authentication (see incident *Identitiy Theft with Phishing-as-a-Service (PhaaS)*, page 54). Therefore, it is likely that more products in this category will prove to be vulnerable in the future.

In addition to the vulnerabilities in software products mentioned above, the BSI also received reports of vulnerabilities in Industrial Control Systems (ICS). Industrial Control Systems are systems for controlling industrial production, for automation control, for human-machine interaction and more. In the reporting period, a total of 24 ICS systems with vulnerabilities were reported to the BSI.

Reports on products with vulnerabilities
Share in %

Figure 11: Reports on products with vulnerabilities
Source: Federal Office for Information Security 2023



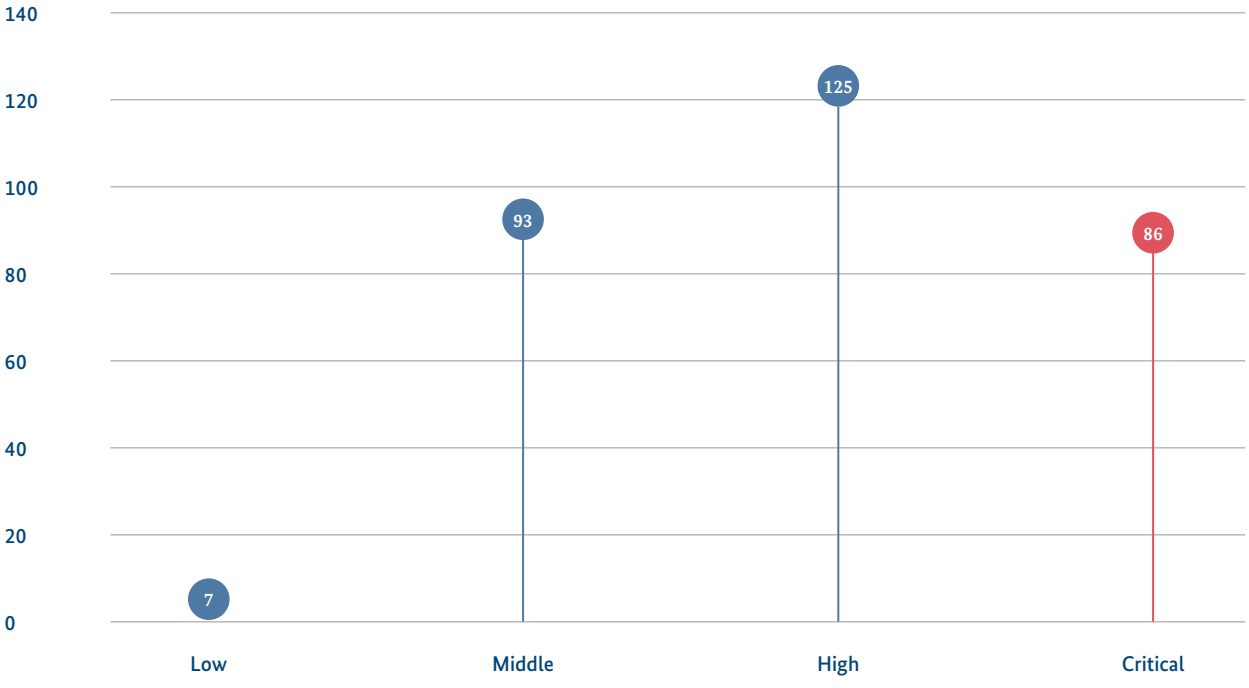
The BSI's Warning and Information Service (WID) sifts through the various sources on new vulnerabilities in software products on a daily basis and publishes the identified issues via the WID portal. It is important to distinguish between advisories (comprehensive vulnerability information provided exclusively to the federal administration) and quick reference guides that summarise facts in abbreviated form for organisations from other sectors. Both formats can be used in government offices, companies and other institutions to provide support for patch management and to drive the roll-out of security updates. Technical warnings for consumers supplement this service offer."

During the current reporting period, the web service was considerably expanded. The portfolio of software products being monitored has also grown significantly, so that the figures for the current reporting period are not comparable with previous reporting periods.

The flood of newly disclosed vulnerabilities is a daily challenge for IT security managers. In the future, the BSI sees the potential to further accelerate the patch management processes through (partial) automation. Among other things, it may be possible to cope with the mass of vulnerability reports by automatically filtering all reports according to those that are of particular interest to one's own organisation. The technical basis for this is the Common Security Advisory Format (CSAF), which the BSI was involved in specifying. This new standard makes Advisories machine-readable so that they can be processed automatically.

Average monthly WID reports, including updates
Amount

Figure 12: WID reports
Source: Federal Office for Information Security 2023



Attack Campaign Against Vulnerability in File Sharing Software GoAnywhere

Situation

On 30 January 2023, the zero-day vulnerability CVE-2023-0669 was disclosed in the GoAnywhere Managed File Transfer (MFT) product. The GoAnywhere MFT software is used to operate a file sharing server and is therefore usually accessible from the Internet. The exploitation of this vulnerability allowed remote access and the execution of, for example, malware by an attacker. On 6 February 2023, a security researcher publicly reported the vulnerability and published proof-of-concept (PoC) code that allowed the vulnerability to be exploited. Shortly after this publication, the Metasploit penetration testing framework was extended to include a corresponding module, enabling any attacker to exploit it. On 7 February 2023, the manufacturer provided an emergency patch to close the vulnerability. Since 8 February 2023, attempts to exploit the vulnerability have been observed.

At the beginning of March 2023, attackers of the Clop ransomware published the names of several suspected victims on their leak page. The attackers claim to have compromised and stolen data from 130 organisations through this vulnerability. These alleged victims were subsequently blackmailed by the attackers for hush money.

Assesment

To the BSI's knowledge, the attackers did not use ransomware in this attack campaign. They were presumably limited to stealing data from compromised GoAnywhere servers. Targets were likely opportunistically selected from vulnerable servers.

This incident was similar to an attack campaign from late December 2020. In this case, the same cybercriminal group exploited a vulnerability in another file sharing software. In this campaign, too, the attackers did not use ransomware, but only used stolen data as blackmail.

Response

To prevent compromises like in this case, active patch management and the implementation of preventive measures are necessary. Moreover, steps should be taken to check whether vulnerable servers can be taken offline until a patch is made available.

Attack Campaign Against File Sharing Software MOVEit

Situation

On 31 May 2023, the software manufacturer Progress published information about a vulnerability in its file sharing product MOVEit and an active attack campaign against it. MOVEit servers are often used for uploading data by external users. Attackers exploited the CVE-2023-34362 vulnerability in an attack campaign lasting multiple days since at least 27 May 2023. The attackers' goal was to steal data from the file sharing server. The attack was attributed by several IT security service providers to the attacker group behind the Clop ransomware.

On 5 June 2023, the attack group behind Clop claimed responsibility for the attacks according to the news website Bleeping Computer. The attackers placed a webshell that served to steal the data. This ***webshell*** *has been named Lemurloot by IT security service provider Mandiant.*

Since 14 June 2023, the attackers published data from several companies on the leak page of the Clop ransomware. These publications probably go back to this attack campaign. However, there may also be victims among them who are not connected to the attack campaign against MOVEit. It is unknown how many organisations are actually affected by this attack campaign. Due to the proliferation of MOVEit, hundreds of organisations were probably vulnerable.

Assessment

The BSI has no indications of the use of ransomware in this attack campaign. Vulnerable MOVEit servers were opportunely attacked with the aim of stealing data. This incident is similar to two other attack campaigns by the same group against vulnerable file sharing servers: on the GoAnywhere server in January 2023 (see incident Attack Campaign against Vulnerability in File Sharing Software GoAnywhere, page 37) and on the file sharing software of the manufacturer Accellion in December 2020.

This attacker group usually extorts victims with double extortion, that is, encryption with ransomware and the publication of stolen data. However, the repeated attack campaigns against file sharing servers were distinguished by the fact that they did not use ransomware. It is also not known if the attackers reused the access established for an attack for a later ransomware attack. In these campaigns, the attackers aimed to compromise as many servers as possible in a short time and to leak data. This is because as soon as the attack campaign becomes known, the vulnerable servers can be disconnected from the internet until a patch is made available. Therefore, it is safe to assume that the attackers deliberately aimed for a high attack speed when exploiting the vulnerability.

Depending on the intended use of the MOVEit server, sensitive information may have been stolen for the organisation concerned.

Response

The BSI published a BSI IT security warning in response to the attack campaign on 1 June 2023. The IT threat level was initially rated 4 / Red, as there was an immediate need for action. On 2 June 2023, the security warning was downgraded to 3 / Orange after the software manufacturer provided a patch.

5.2 — Vulnerabilities in Hardware Products

Hardware vulnerabilities normally not be fixed by software patches because their root cause lies in the way the products are manufactured and in their architecture. There are several ways to attack, e.g. by targeting the functionalities of the transistors that are the basis for the integrated circuits, and thus the microarchitecture of processors. Other ways are provided by the various steps in the production and the supply chain. If the hardware has already been taken into operation, vulnerabilities can normally not be fixed easily, so the potential benefit for a possible attacker is very high. However, in contrast to vulnerabilities in software, the financial effort to exploit them is also higher.

Since the MELTDOWN and SPECTRE attacks were publicised in 2017, there have been more and more versions of these attacks that take advantage of the speculative execution in modern processors. Therefore, new vulnerabilities in this attack class can still be expected as long as the microarchitecture of the processors is not fundamentally changed. However, speculative execution is responsible for a substantial part of the processors' performance. Any other design would lead to a considerable reduction in computing power. As in previous years, the variations developed from these attacks are still dominant. In 2022, for example, the Retbleed, SPECTRE-BHB, SQUIP and PACMAN attacks were published. Either no countermeasures exist against these vulnerabilities, or they lead to large reductions in performance.

Unlike SPECTRE-based attacks, the ÆPIC leak vulnerability is a real flaw in the microarchitecture of the processor where secret key data can be read, but only by users with administrator rights.

New cryptoalgorithms should be quantum safe (post-quantum cryptography, PQC). PQC procedures must withstand not only attacks carried out with quantum computers, but also hardware side-channel and fault injection attacks, as they are implemented on classical platforms. For example, it has been shown that key material can be retrieved in a hardware implementation of the CRYSTALS-Kyber PQC cryptographic method using side-channel analysis in combination with neural networks (see also chapter *Post-Quantum Cryptography*, page 74). For the future use of hardware implementations, appropriate countermeasures must be developed so that secure PQC procedures can be implemented in hardware products.

In March 2023, critical zero-day vulnerabilities were published in Exynos modem chips, which are not only installed in smartphones but also in vehicles. These vulnerabilities allow attackers to execute code on the mobile devices without the owner noticing or being able to do anything about it. For a successful attack the knowledge of the telephone number is sufficient. However, according to current knowledge, this vulnerability is not being widely exploited in the field.

Since the exploitation of hardware vulnerabilities is relatively elaborate compared to the numerous software vulnerabilities, hardware is less often the target of cyber attacks. As shown in several studies, the use of dedicated security elements or completely logically separated processing units for storing and processing sensitive data can greatly reduce the potential for an attack. An indicator for good security functionality in IT products is provided by independent security testing and certification, for example according to the ISO standard 15408: Common Criteria for IT Security Evaluation.

5.3 — Vulnerabilities in Networked Devices

In addition to software and hardware, Internet of Things devices and components can also have vulnerabilities. With the degree of networking and the complexity of the products, the digital attack surface in the field of IoT is constantly increasing. Every additional interface and every additional controller offers potential attack vectors. In modern vehicles in particular, a large number of control units are installed that are connected to each other. Moreover, the already large software coda basis is growing due to the additional functionalities, which typically also results in a higher number of vulnerabilities. In the case of an app or cloud connection and targeted manipulation, it is possible in principle for an attacker to disrupt or deactivate essential functions remotely.

The large attack surface offered by the IoT requires active protection, especially through measures taken by manufacturers such as security concepts and penetration tests. There are many vulnerabilities that enable the attack vectors: First of all, there are many originally conventional products on the market that have existed for gen-

erations and have become more and more digitalised and networked over time. As part of this, additional interfaces have been introduced. The original product did not require cyber security measures due to the lack of networking. In the meantime, however, a fundamental security concept is required in most cases for effective protection, which must already be taken into account in the design of the product (*security by design*). For example, many components are not designed to be protected by transport encryption and do not contain firewalls that protect against unauthorised access. It is often not possible to effectively retrofit such measures due to hardware limitations and backward compatibility.

Another cause is the lack of experience of manufacturers in dealing with cyber security and potential vulnerabilities. Since no IT security measures were necessary for conventional, non-networked products, many manufacturers have so far had neither the structures nor the expertise to counteract digital attacks on their products. Due to the increased awareness of cyber security issues and especially due to new regulatory frameworks such as type approval regulations on cyber security in vehicles, this situation has changed recently. Automobile manufacturers, for example, are required to establish appropriate processes for managing cyber security in production and remediating vulnerabilities.

Vulnerabilities in the Automotive Sector

During the reporting period, new vulnerabilities became known in the automotive sector. The security researcher Sam Curry was able to show[4] that inadequately secured web portals of various manufacturers allowed attackers not only access to manufacturer and customer data remotely, but also access to vehicle functions. Manipulating web requests, for example, allowed attackers to impersonate dealers on the web portal. Dealers enjoy special trust on the part of the manufacturers and can assign vehicles to specific customers by name. Accordingly, an attacker could assign already registered vehicles to their own account and control vehicle functions of other people's cars via the manufacturer's official app. This allowed an affected vehicle to be opened remotely or its engine to be started. In another case, it was possible to receive live images from the rear camera. Manipulation of this kind only required the vehicle identification number (VIN), which in some cases can be found on the windscreen of the vehicle.

In the case of a large North American telematics operator, vulnerabilities enabled the execution of vehicle functions of entire fleets. Ambulances and police vehicles were among the more than 15 million vehicles affected, and their use would have been hampered if these vulnerabilities had been exploited.

These incidents show that more than just the vehicle itself and its internal systems need to be considered. In addition, the whole ecosystem in which the vehicle is embedded, including the trust relationships between different market players, must also be secured.

Further information on the automotive sector can be found in the situation report Automotive:[8]

6. — AI Large Language Models

The technical evolution of AI large language models (LLMs) experienced a key moment in the current reporting period. The release of the application ChatGPT by Microsoft-backed OpenAI in November 2022 was the first broadly distributed, public available application based on an AI large language model. The model's text generation capabilities have surprised not only the general public, but also experts. A dynamic development has been observed since then, both in terms of technology and in the fields of application of this and comparable models.

6.1 — Technical Evolution

Language models can now do much more than create texts, as they are integrated into larger contexts. Through integration in various applications or the use of plug-ins, these models can also operate on the internet, for example, send emails, book flights or pay. Language models are built into corporate IT infrastructures to take over primarily repetitive tasks and support employees in their work.

The ease of automation and the range of variation in the output now go far beyond previous IT products. Whereas programming skills were previously required to create automated archiving, for example, it is now technically possible to delegate this task to a language model simply by using a natural language input: "Every Friday at 4pm, please create an Excel spreadsheet with the week's sales amounts grouped by area and territory. Attach an appropriate two-tiered pie chart to it and email it to the board." LLMs with access to the relevant company data and mail servers can easily implement such a task. Language models now screen applications for their suitability for advertised positions, create business letters with direct financial implications, make bookings or hire service providers.

When LLMs are used by programmers to support the development of complex IT products by generating source code, another significant threat arises: The quality of the results may not be sufficiently ensured by human cross-checking.

The undoubtedly great opportunities presented by LLMs are accompanied by equally high risks. Such models can either be misused as tools for cyber attacks or they themselves can be attacked or exploited as a vulnerability. Since such models can not only be used in legal applications, but also in the context of cybercrime, significant scaling effects can be expected for already known cyber threats. The following narrative provides a perspective on emerging threats and hazards that can be foreseen from the state of development of AI large language models as of the editorial deadline of this report.

6.2. — New Threats

New, previously unknown threats essentially arise from the outstanding importance of training data on the one hand and the use of AI in software development on the other. These new threats will be addressed in the following.

6.2.1 — Training Data

The outputs and behaviour of AI large language models depend significantly on the training data used to teach the AI. In the case of language models that are developed and used in a closed, limited company context, this can be the information of individual departments or divisions, or possibly also data and infrastructure metadata of the entire company. In contrast, LLMs such as GPT-3 or GPT-4, on which applications such as ChatGPT are based, use training data from the entire internet. The more training data there is and the more diverse it is, the more universally the model can produce helpful output in completing queries and tasks. Various threats can arise from the training data.

Biased training data: If training data contains a bias, the model can deliver unbalanced outputs. This can include statements about certain brands or products, but also, for example, evaluations of people, institutions or political tendencies, for example when models adopt biased statements from social media. When training data is manipulated, it can also trigger false news and disinformation campaigns that can influence public opinion and in the long run even social values.

Self-reference: If LLMs are trained with content from the general, public internet, the self-referencing of language models increases exponentially as the amount of AI-generated content on the internet increases. In other words: The more AI-generated content is available on the internet, the more the training data of large AI language models will also consist of AI-generated content.

False news or disinformation campaigns then become increasingly difficult to detect, as different sources, which may also appear reputable, pick up similar content distortions through the use of language models. The type and number of referenced sources, after the prolonged establishment of unreflective language model use, increasingly reduces the quality in terms of the authenticity or correctness of a piece of information when the same language model is used in many places.

Automated social engineering: Language models can generate responses to human reactions (currently in text form, but in the future presumably also as sound, image or video) and gain credibility through this ability to engage in dialogue in a society that is not quickly and comprehensively educated. There is a risk that this could lead to automated social engineering, as text attacks that are recognised as successful are subject to accelerated propagation because they can be spread without human interaction.

"Learning" and finding weak points: Language models are increasingly being used to generate programme code in a wide variety of programming languages and thus support programmers in their day-to-day work. If training data for programme code intentionally or unintentionally contains vulnerabilities or bad code, the model will also learn these and can reproduce them in generated code. Under certain circumstances, this can be adopted into new IT products without being reviewed and thus contribute to the multiplication of vulnerabilities.

LLMs can also facilitate searching the internet for existing vulnerabilities in programme code and in corporate networks, as well as finding and creating the necessary exploit for an identified vulnerability. Knowledge of the relevant tools, which was previously required, is then only necessary in a simplified form.

6.2.2 — Code Generated With Errors

AI large language models make mistakes. This is especially dangerous when used in the development of IT products. This applies to both the learned vulnerabilities and bad code mentioned above, as well as, in particular, to the conditions of use of language models. The threat posed by a language model built into a company's infrastructure depends largely on what data and services the model is allowed to access. The outputs that it produces will no longer be able to be tracked in detail by the developers of the model. In effect, they can no longer control what the AI language model will do in the context of a particular use.

Depending on the access rights granted, a model can react very differently to a task or a request. This means that it is virtually impossible for language models to fulfil security-by-design as a basic requirement for the security of IT products. Since there is no specific design for LLMs (the AI design is made by itself through training, for example), there can be no security-by-design. Even specifying generally valid security criteria in connection with AI language models – independent of a concrete use case – is therefore a major challenge.

6.3 — New Threats – AI as an Attack Surface

The range of possible applications for a language model in a company will increase with the amount of company data used and the amount of access rights of the software system in which the language model is integrated.
The more information a model can process about the company and the more access rights the corresponding system has, the better it will be able to support employees in their day-to-day tasks. However, the scope of access rights granted to such a system should be subject to a thorough risk assessment. At the very least, the following risks should be considered.

Reconstruction of training data: Language models can in principle reproduce all learned information from the training data in outputs, even if their training was aimed at avoiding certain outputs. Attackers can circumvent this behaviour to exploit a model for attacks. For example, it has been shown that training data can often be reconstructed in guided dialogue or through the use of targeted queries that suggest a particular context to the model.
For example, hate messages or bomb-making instructions could be elicited from the model in response, if one pretended to need this information as the basis for a cautionary article and thus to do good. Even if it has become more difficult to extract explicit statements by

now due to re-training of the models, abstract descriptions of harmful ideas can still be returned and thus provide for their dissemination or act as idea generators or research aids. If the training data contains sensitive company information, the basic linguistic manipulability of a language model quickly becomes a vulnerability to be exploited for data leaks in this way. Effective rights management that grants different users different access rights and information rights was not possible by the editorial deadline of this report. The entire set of training data is always used.

Collection of corporate information in a single application that is difficult to secure: A system equipped with far-reaching access rights and an AI language model may know more about a company than any or all human employees, and can perform actions in a highly automated manner. Even more than that: the reasons for certain actions or outputs of a model are difficult to understand for employees and even for IT security officers, administrators in companies and sometimes even completely unknown. For this reason, current criteria for effective IT security management, as they apply to other IT products, are only partially applicable to software systems that work with big data and AI language models.

Potential misuse of the model: The usefulness of language models comes essentially from the fact that they can be controlled using natural language. The aim of the current model of development is to no longer need to programme commands and even complex actions, but to delegate them to the model using natural-language work instructions, or prompts. Finding the right instructions is called "prompt engineering". However, this approach also allows for "prompt injections". These are inputs with a manipulative or criminal intent. For example, attackers can use a specific dialogue structure to successively persuade a model to perform a certain malicious action or to hand over data such as identity data.

Furthermore, in certain attack scenarios, these malicious inputs into a language model that does not otherwise act as malware ("adversarial attacks") can also be executed via two-stage attack vectors. Attackers can hide sections of text in web pages that are not visible to humans but contain executable commands for an AI language model, such as to download malicious code. If a harmless information system is given this hidden input, which analyses such pages with an AI language model, and is able to act as an agent due to its technical capabilities and authorisations, malware can then enter the user's system. This type of attack, in which a person other than the user themselves passes an instruction to the language model, is known as an "indirect prompt injection".

Even attackers who have broken into a corporate network in a conventional way can, with the appropriate authorisation, abuse a language model located in the corporate network accordingly.

6.4. — Systemic Threat Shift

In addition to completely new threats to cyber security, AI language models also bring about a change in already known threats. On the one hand, this applies to scaling effects that arise from the enormous performance of AI. However, this also affects the information technology infrastructures as a whole and the AI as an agent, i.e. as an acting actor within these infrastructures. The manipulation of the "human factor" through social engineering is now joined by the manipulation of the "AI factor" through prompt engineering.

6.4.1 — Scaling Effects of Known Threats

Alongside the aforementioned new threats and hazards, AI large language models are likely to have scaling effects on known cyber threats.

Spam, Phishing, Social Engineering

Language models are expected to result in more spam and phishing emails, which will contain fewer spelling and grammatical errors, making them harder to spot. Since LLMs are not only able to write high-quality texts, but can also convincingly imitate corresponding templates in their choice of words and linguistic style, social engineering attacks such as spear phishing and CEO fraud will become customizable and therefore gain further persuasive effect. This development may be further exacerbated by the equally rapid development in the field of AI-generated image, audio and video formats. Methods

that can be used to create fake votes have improved significantly in recent years, both in terms of their quality and their availability and accessibility. For example, it is possible for non-professionals to create fake audio examples of well-known politicians, which are indistinguishable from the original, especially in terms of their timbre (see also chapter *AI for Autonomous Driving and Media Identities*, p. 72). The increasing real-time capability of these manipulations, known as deepfakes, means that in online meetings, for example, it will no longer be possible to be sure that you are talking to a real person, an attacker or even the avatar of a chatbot in the foreseeable future.

Malware

AI large language models that have been trained on examples of code are, in principle, capable of generating programme code. This includes malware. It is true that developers are trying to train AI to not provide assistance for criminal acts. However, prompt engineering can potentially circumvent such qualms of a model. In addition to a faster production of new malware, more rapid changes to existing malware can also be expected in the future, which will make it more difficult to detect it. We can expect attack tools of all kinds to evolve faster and with higher quality: from information stealers to DDoS botnets to the individual modules of a complex ransomware attack. In particular, the opportunities for code generation are likely to significantly lower the entry requirements for cybercriminal activities, such as needing at least some rudimentary programming and system knowledge. The number of people with criminal intent capable of creating malware is likely to increase as a result of these lower technical requirements.

Ransomware and APT

In the context of complex cyber attacks, language models will likely have a direct impact on how attackers spread across an infiltrated corporate network, how they collect data and how they can expand their access rights. While attackers in traditional corporate networks have to work their way from system to system with comparative effort, in future they may encounter an AI language model with extensive knowledge about the company and far-reaching access rights, which can be relatively easily manipulated and misused for attacks. These models are likely to be an attractive means of attack not only for cybercriminals, but also for cyber espionage and cyber sabotage.

Effects

Through the scaling of these basic known threats, new dynamics emerge. The number of potential attackers can increase significantly due to the ease of access, regardless of whether they are state actors, financially motivated attackers, inside perpetrators, *script kiddies* who see it as a game, or even reckless security researchers. Even if the use of AI elements also results in a marked increase in the detection rate on the defender side, a negative balance may emerge. The capacity of law enforcement agencies may be heavily stretched and diverted towards the less knowledgeable AI-enabled attackers in particular, because they are easier to detect. They are then unable to pursue more knowledgeable attackers. It is impossible to predict how the attacker-defender dynamic will develop with both sides using current AI language models. It is reasonable to assume that the side that uses the technology first has greater chances. Considering the current high speed of development, even a smaller lead in time is enough for a substantial advantage.

6.4.2 — Vulnerabilities, Fuzziness and Agent Networks

Due to their black-box nature, AI large language models are a systemic vulnerability of themselves. Prompt engineering used as a tool to exploit the vulnerabilities of a model has no clearly defined limits. It is not a technical failure like a *stack overflow*, which can be checked and prevented. At present, there is also no way to identify a prompt as malicious code, because the input cannot be checked syntactically, but would have to be checked semantically. A natural language prompt injection therefore is fuzzy, making defence unreliable, because the semantic content can be conveyed by many different formulations or contextualised in a different way.

This makes vulnerability management for AI language models a task with fuzzy and undefined target. Not only must a particular text be prevented, but also all semantic equivalents. Vulnerability management therefore shifts from a technical problem to a less tangible one, because it is shifted to a semantic layer. Vulnerabilities of this kind can therefore no longer be unambiguously classified. For example, a prompt that is detected as malicious in one

system may still be effective in another system despite closing the vulnerability in that system, because different systems also have unclear overlaps due to the same training bases. This also blurs the distinction between a zero-day vulnerability and a known public vulnerability, which fundamentally calls into question the procedures for IT security managers.

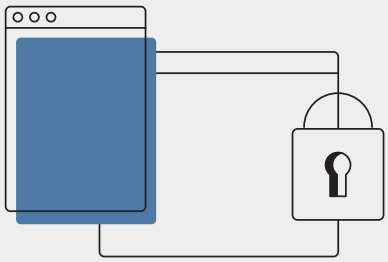
If one takes this fuzziness into account, another development then becomes more relevant. Currently, language models are not just being integrated into IT systems for the output of text that people are supposed to read. Agent systems, in which the outputs of AI language models are translated into (electronic) actions, are of major importance. In this case, the decisive factor is whether people continue to bear responsibility for these actions. In order to do this, these systems must only be able to act under human control. This includes intermediately posed questions such as "Buy/book now for a fee?" or "Do you really want to transfer this personal data to provider XY/ to cloud storage?". However, such security questions run counter to the trend of moving functionalities to the cloud and expanding them into complete agent networks. Combine the fuzziness of individual vulnerabilities with the multitude of external components, that potentially contain AI components with their own vulnerabilities, in future scenarios and the magnitude of the task to protect such structures becomes clear. On this background the BSI is working with national and international partners to develop criteria for the secure operation of AI language models and AI systems in general (see chapter *Artificial Intelligence*, p. 71).

The State if IT Security in Germany in 2023
at a Glance

Ransomware

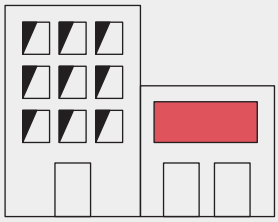
remains the biggest threat.

2 **Ransomware attacks** on local governments or municipal businesses were reported on average per month.



68 successful **ransomware attacks on companies** became known.

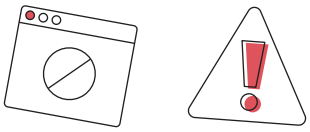
15 of them were directed against **IT service providers**.



More than **2.000** **vulnerabilities** in software products (**15 % of which were critical**) became known on average per month during the reporting period. This is an **increase of 24 %.**

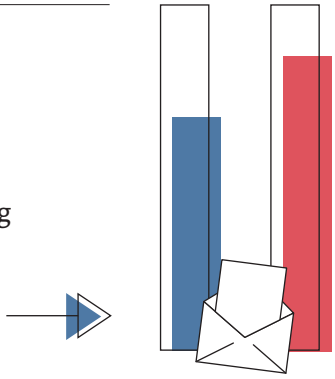
A quarter of a million

new **malware variants** were found on average every day during the reporting period.



66%

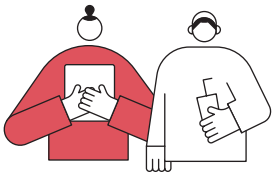
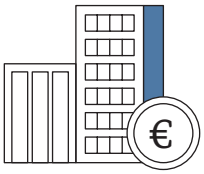
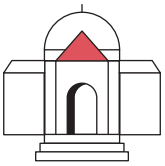
of all **spam** in the reporting period were cyber attacks:
34 % extortion mails
32 % fraud emails

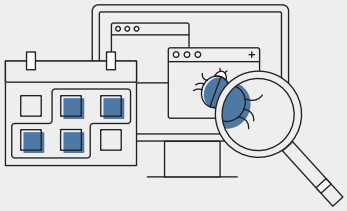


84%

of all fraudulent emails were **phishing emails** to obtain authentication data, mostly from banks and savings banks.

Top 3 Threats per Target Group

Civil Society	Industry	State and Administration
		
Identity theft Sextortion Phishing	***Ransomware*** Dependency within the IT supply chain, Vulnerabilities, open or incorrectly configured online servers	***Ransomware*** APT Vulnerabilities, open or misconfigured online servers



Around **21.000** **infected systems** were detected daily in the reporting period and reported by the BSI to the German Providers.

On average, around **775** **emails with malware** were detected daily in the reporting period and reported by the BSI to the German providers.

370 **websites** were blocked from access from government networks on average each day of the reporting period. **The reason:** the websites contained malware.

6.220
2022

5.100
2021

7.120 participants had joined the **Alliance for Cyber Security** by 2023.

13 Months of Cyber Security at a Glance

June 22

- *Ransomware* attack on all town halls in a district as well as several municipal businesses in a neighbouring city.
- New technical guidelines in security in telecommunication infrastructures, security of digital health applications and for manufacturers of mobile financial applications
- Mututal recognition of IT security certificates between ANSSI and BSI
- Second report on digital consumer protection published.

July 22

- New certification programme for 5G telecommunications network components
- Saarland becomes second pilot region of the Cyber Security Network (CSN).
- First inspection body for *NESAS CCS-GI* programme recognised
- BSI provides tool for telemetry monitoring for Windows 10.

Attacks on Albanian government institutions with the *ransomware* GoneXML and the *wiper* ZeroShred

August 22

- Chambers of Industry and Commerce offline across Germany after cyber attack
- *Ransomware* attacks on higher state institutions in Montenegro
- BSI warns against the use of insecure ABSU brand wireless door locks.
- BSI launches virtual roadshow for municipalities in Saxony-Anhalt.

September 22

- Increased *DDoS attacks* by hacktivist *botnet* project „DDoSia“
- *Ransomware* attacks on senior state institutions in Bosnia and Herzegovina
- 10 years Alliance for Cyber Security (ACS)
- BSI publishes guidance on the use of attack detection systems.

October 22

- Use of the Prestige *ransomware* against companies in Poland, among others
- BSI and Singapore Cyber Security Authority recognize each other's cyber security marks. BSI confirms security features of iPhone and iPad operating systems.
- First regional forum of the Cyber Security Network (CSN) held in the Rhine-Main region

November 22

- CSAF included as an international standard
- Digital Barometer 2022 by BSI and ProPK

December 22

- Shutdown of about 50 websites that offered services for targeted *DDoS attacks*
- BSI and ANSSI publish publication on security certification of IT products.
- BSI and Hesse sign cooperation agreement.
- BSI an ZF develop security check for artificial intelligence in automobiles.

January 23

- Global *ransomware* attack on ESXi servers
- cyber security and digital sovereignty – 5G/6G projects launched

February 23

- Attack campaign against vulnerability in file-sharing software GoAnywhere
- Cyber attacks on IT service providers
- EU Directives NIS 2 and CER come into force.
- BSI releases beta version of TLS test tool "TaSK".

Increased attacks by *DDoS* hacktivists

March 23

- Supply chain attack on several 100,000 business customers as a result of another supply chain attack
- Attack on file-sharing software GoAnywhere
- Critical zero-day vulnerabilities in Exynos modem chips published
- BSI and Rhineland-Palatinate sign cooperation agreement.

April 23

- Recommendations to IT manufacturers together with international partner authorities
- BSI offers certifications according to the latest Common Criteria test rig.
- BSI publishes study on hardware attacks on microcontrollers.
- BSI develops the DIN-SPEC standard security check for SMEs with partners.

May 23

- Assessment of the security situation after the Russian Attack on Ukraine.
- BSI issues first IT security labels for broadband routers.
- Publication of white papers on the auditability of AI systems

June 23

- International cyber security authorities are taking a close look at Ransomware LockBit.
- NEW BSI Standard 200-4 helps to achieve holistic *resilience* with business continuity management .
- BSI and municipal umbrella organisations launch pilot project for better IT security in municipalities.
- BSI publishes new technical guidelines on satellite information security.

Throughout the reporting period:

- 27 *Ransomware* attacks on local government and municipal enterprises
- 23 *Ransomware* attacks in educational and research institutions
- Cyber attacks on 15 IT service providers with effetcs on their customers in public administrations, business, society

Risk Landscape

Part B: Risk Landscape

7. — Insights from the Threat Landscape in Society

German people's lives are more digital than ever before. From online shopping to online banking, from news consumption and information on the internet to spending time on social media: Digitisation has far-reaching effects in many areas of society. The BSI offers services targetet at consumers to fulfil its legal mandate for digital consumer protection and supports people in the safe use of digital services. The focus is on prevention, detection and response. During the reporting period, the BSI paid special attention to the topic of identity data. Alongside measures taken by consumers to protect their personal data from misuse, manufacturers and providers of digital services also have a responsibility.

7.1 — Missuse of Identity Data

For consumers, the issue of data leaks was prominent in the reporting period. In many cases, these were related to ransomware attacks, in which cybercriminals exfiltrated large amounts of data from organisations in order to later threaten to publish it unless a ransom or hush money was paid (see chapter *Ransomware*, page 14). Both companies and public sector institutions, such as local administrations and educational institutions, were affected. A successful ransomware attack entails the potential for enormous damage to the victim of the attack as well as a negative impact on a potentially large number of consumers. While the victims of the attack are concerned with restoring the affected information technology systems, consumers are confronted with the publication of what is sometimes their sensitive data, which often includes address, payment and/or login data. Successful ransomware attacks also mean considerable limitations on the availability or even non-availability of government and business services for customers. The disruption or failure of critical social services such as failure to pay out social benefits or parental allowances has particularly serious consequences.

The identity data captured as a result of a ransomware attack enables the attackers to put additional pressure on the attack victims by threatening to publish captured data on leak sites set up for this purpose on the darknet. Some attackers went a step further and created dedicated websites where consumers affected by a data leak could check whether their data had been stolen. Since these websites are hosted on the clearnet, that is, the public internet, they are indexable by search engines and can be added to search results. In order to limit the negative effects, starting with the victim of the attack and ending with the consumers potentially affected by a data leak, it is therefore essential to act transparently and to provide timely information and assistance.

In addition to ransomware attacks on organisations, consumers were also directly affected by attacks using ransomware. Cybercriminals extorted ransoms, albeit comparatively small sums, with ransomware attacks on private devices such as network-attached storage systems (NAS). As a result, the affected consumers were no longer able to access their private data.

In addition to ransomware attacks, information stealers also posed a threat to the data security of consumers. While ransomware attacks target the victims themselves, demanding a ransom for the decryption of their data, attacks using information stealers focus on trading stolen identity data. Information stealers are a type of malware that allows cybercriminals to obtain various types of personal data, such as login details for various online services, unnoticed on infected devices. The stolen data may also include website cookies and biometric data, such as fingerprints. Stolen credentials are then offered for sale by cybercriminals on darknet marketplaces. On one of the largest underground marketplaces for identity data, cybercriminals offered interested parties a browser plug-in that made it possible to import the stolen credentials directly into the web browser. This allowed another person's digital identity to be assumed with just a few clicks.

Data Leaks from Vulnerabilities

Data leaks also stemmed from a lack of protective measures for login data in online services or vulnerabilities in the IT products used. Among other things, various attackers succeeded in compromising online shops and stealing data such as customer names, billing and delivery addresses, telephone numbers, order details as well as payment data. Vulnerabilities in the software used by online shops pose a major risk to the security of consumers' data. During the reporting period, for example, vulnerabilities were found in online shopping software products that enabled unauthorised database access, allowed access to isolated data by accessing the SQL manager, or could lead to a cross-site scripting attack if exploited. Attackers inject malicious code into web forms or URLs and let the user execute it unnoticed.

As part of a BSI study on the IT security of consumer data in online shopping[5], a vulnerability analysis of ten randomly selected online shopping software products revealed a large number of vulnerabilities, some of which had serious implications for consumer data security. Almost all products tested had inadequate password policies, which meant that customer accounts were not properly protected. Moreover, half of the online shopping software products tested had third-party JavaScript libraries that were vulnerable to known exploits and thus posed an incalculable security risk. These cases illustrate that insufficient IT security measures increase the risk for consumers to become victims of a data leak. A representative survey that was also conducted as part of the study showed that around a quarter of respondents had already been affected by a data leak in online shopping. Furthermore, 68 per cent of respondents said that they have concerns about online shopping in general.

Attacks on the customer databases of online services or the theft of identity data as a result of malware are usually beyond the control of consumers affected by a data leak. Such security incidents involving the subsequent publication of sensitive personal data undermine trust in the use of digital services and in digitisation as a whole. Moreover, the stolen data can be used for further attacks against consumers. Unauthorised access and publication of personal data thus pose a high risk to consumers.

7.2 — Fields of Action: Responsibility of Manufacturers and Suppliers

The findings on the current threat landscape in society make it clear that, in addition to raising awareness and educating consumers, responsible action on the part of manufacturers and providers in particular is crucial for effective digital consumer protection. This is especially clear when it comes to protection against the threat of data leaks (see also chapter *Spam and Phishing*, page 30), as the effects can be both multifaceted and serious for all parties involved. Suitable technical and organisational measures must therefore be implemented for data processing and storage by manufacturers and providers in order to

- protect the privacy and sensitive data of customers,
- avoid financial damage both on the part of consumers (e.g. through stolen online banking access) and on the part of manufacturers and providers (fines, claims for damages),
- protect the reputation of providers,
- promote trust and long-term customer satisfaction.

These measures include, among others, the use of effective encryption technologies, regular checks and stress tests of the IT infrastructure, training employees on how to handle sensitive data, and transparent and fast customer communication in the event of a data leak.

These requirements illustrate the complexity and mechanisms of IT security issues and require a deep organisational understanding of the responsible use of digital technologies in order to find promising answers. Corporate Digital Responsibility (CDR) requires a proactive approach following the "security-by-design" paradigm, among other things. CDR involves considering IT security aspects in all phases of the hardware and software development process, from conception to implementation and operation. By identifying and taking into account security requirements at an early stage, both potential vulnerabilities as well as high (monetary) expenses for later troubleshooting can be minimised.

Another important building block in responsible development of digital everyday technologies is the simple, easy-to-use and intuitive design of security functions (usable security) in devices and online applications. Designing devices, applications and services in an accessible and user-friendly way increases the willingness of consumers to activate them and to use them continuously. Positive user experiences with IT security mechanisms also increase their acceptance. Usable security plays an important role in providing effective protection against spam and phishing in everyday consumer life (see chapter *Spam and Phishing*, page 30).

All of these attempts to improve the IT security features of devices, applications and services should be made more transparent and visible to consumers. Clear labelling such as the BSI's IT security label is an effective instrument for this. The BSI recognises the need to play an even more active role in promoting information security in everyday digital private life.


Volksbanken
Raiffeisenbanken

um die Auswirkungen der gestiegenen Energiepreise für die Verbraucher abzumildern, wird im September ein Pauschalbetrag von 300 Euro an alle Erwerbstätigen ausbezahlt. Dies ist ein Beschluss der Bundesregierung und Inhalt des Entlastungspakets 2022, welches die durch den Ukraine-Krieg entstandene Energiekosten-Explosion etwas abfedern soll.

Wer erhält die Energiepauschale?

- **Steuerpflichtige** mit Einkünften aus Gewinneinkunftsarten (§ 13, § 15 oder § 18 des Einkommensteuergesetzes) und
- **Arbeitnehmerinnen und Arbeitnehmer**, die Arbeitslohn aus einem gegenwärtigen Dienstverhältnis beziehen und in die Steuerklassen I bis V eingereiht sind oder als **geringfügig Beschäftigte** pauschal besteuert werden.

Um Ihre Identät sowie den Anspruch auf eine Auszahlung feststellen zu können, benötigen wir eine Bestätigung Ihrer bereits angegeben Daten bei der Erstellung Ihres Girokontos in einer unserer Filialien.

Geben Sie noch heute Ihre aktuellen Daten auf unserer Homapege an und erhalten Sie innerhalb der nächsten vier Wochen Ihre Auszahlung der Energiepauschale. Dies können Sie ganz bequem von zu Hause aus erledigen, anbei finden Sie einen Direktlink zu den geforderten ...

Zur Homepage

Figure 13: Example of a phishing email made in the name of banks with reference to the energy price flat rate
Source: *Phishing* Radar from 09 September 2022[6]


DHL

Lieber Kunde,
Zur Erinnerung: DHL Express informiert Sie, dass für Ihre Sendung Nr. [redacted] noch Anweisungen von Ihnen ausstehen.

Bestätigen Sie die Zahlung der Heimlieferkosten (1,85 EURO) und den Versand des Pakets, indem Sie auf die folgende Schaltfläche klicken:

Ankunft in der DHL Express Ursprungsanlage: **6.12.2022**

Mein Paket senden

Mit besten Grüßen

Figure 14: Example of a phishing email in the name of a courier service provider
Source: *Phishing* Radar from 02 Dezember 2022[7]

Identity Theft with Phishing-as-a-Service (PhaaS)

Situation

There are now a variety of PhaaS providers offering a diverse range of services for attackers: from creating and sending phishing emails, to managing redirect websites and the final bait pages, to technical support and step-by-step tutorials. Often there are already ready-made phishing sites for well-known websites such as Google, Microsoft, LinkedIn, iCloud, Facebook, Twitter, Yahoo, WordPress and Dropbox, among others. Additionally, there are also services to create individual phishing pages for special attack purposes on request.

Common phishing proxy services include those that act as a man-in-the-middle (MITM) between the victim and a company's login page. They can usually steal credentials and cookies and thus also bypass multifactor authentication, for example.

An example of a phishing proxy service is EvilProxy. What is worrying is that, in addition to the phishing login pages for Google, Microsoft and co, EvilProxy also offers phishing login pages for the Python Package Index (official software directory for the Python programming language), npmjs (JavaScript package manager used by over 11 million developers worldwide) and GitHub (software developer platform). Compromising such sites could lead to supply chain attacks through maliciously modified or cloned code repositories and, for example, infect legitimate software with information stealers that steal credentials.

Assessment

Phishing remains a reliable vector for attackers to gain initial access to IT networks. The aforementioned PhaaS offerings allow less advanced attackers with few resources to carry out phishing attacks, which is expected to have a significant impact on the further development of phishing. Moreover, phishing activities have become more diverse and include attacks via social media, SMS and voice calls.

Response

The BSI has been warning users via its social media channels.

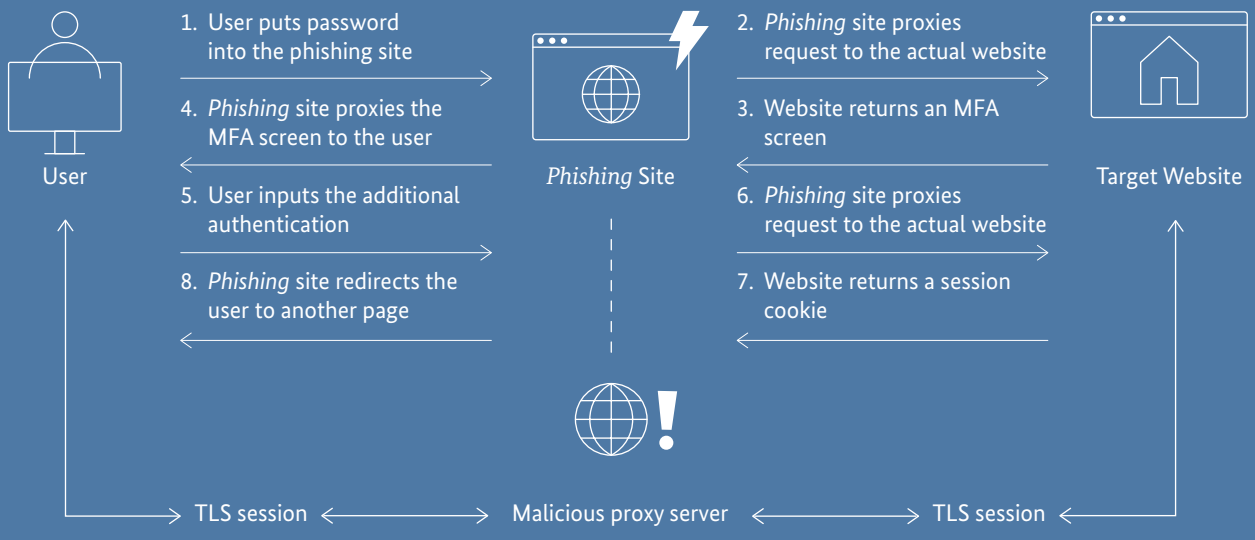


Figure 15: Bypassing multifactor authentication

8. – Insights from the Threat Landscape in the Industry

A look at the state of cyber security in the industry sector shows that a large proportion of German companies have recognised the importance of cyber security. In a survey conducted by the TÜV Association in 2023, 95 per cent of the companies surveyed stated that cyber security is a must for the protection of company data. Similarly, 80 per cent of companies see it as a basic requirement for smooth business operations[8]. This is also reflected in specific measures. Since 2020, corporate spending on IT security budgets has risen steadily. The Federal Statistical Office assumes an annual growth rate of 10.5 per cent[9]. 2022 saw an unprecedented level of investment in cyber security, at around 7.8 billion euros.

Nevertheless, further steps towards more cyber security are urgently needed. According to estimates by the digital association Bitkom, German companies suffered a loss of 203 billion euros[10] from cyber attacks in 2022. Almost every German company has been affected by an attack at some point. Considering these losses, expanding cyber security measures is essential, even if many companies still perceive continuous implementation of cyber security measures in day-to-day operations as an obstacle[11].

Increased Threat Level

The COVID-19 pandemic greatly accelerated digitisation in German companies while expanding the attack surface. In addition, many companies are also confronted with the Russian war of aggression against the Ukraine and the changing global security architecture. Although this uncertainty exists, as already discussed in the chapter *Advanced Persistent Threats and Threats in the Context of the Ukraine War* (page 24), the BSI cannot identify any increased threat in the context of the war in Ukraine on German companies based on the available findings.

The threat posed to companies has become very acute as a result of financially motivated cyber-attacks. The biggest threat to commercial enterprises continues to be ransomware and ransomware as a service (see chapter *Ransomware*, page 14). Progressive professionalisation coupled with an escalating spiral of measures designed to exert pressure on the blackmailed companies can be seen. For a long time, the affected systems have been more than just encrypted. It is now common practice for the perpetrators to threaten the company concerned with the publication of their data in the next step, as well as its customers in the third step (triple extortion). Thus, people who were not involved and whose systems were not affected also become victims.

IT service providers stood out among the known ransomware victims in the current reporting period. Of the total of 68 known victims of ransomware attacks, 15 were IT service providers. For attackers, IT service providers are highly attractive victims, as a large number of other victims can potentially be attacked and blackmailed via their services or customer relationships (see incident *Cyber Attacks on IT Service Providers*, page 57).

Cybercrime Black Market Economy

Attacks on business enterprises are widespread. Large companies with a high turnover are still being attacked. At the same time, ransomware attacks are also becoming a mass business due to the low costs associated with RaaS. Criminals are taking the path of least resistance, so that small and medium-sized enterprises (SMEs), but also municipalities, universities and research institutions are now being affected more and more.

The BSI has observed the development of a cybercrime black market economy as part of this professionalisation (see also chapter *Ransomware*, page 14). Companies do not just face a single attacker, but an efficiently structured attacker industry organised around the division of labour.

At the same time, increasing specialisation has also led to a new level of threat. With well-crafted attacks, it is possible to reach a very high number of corporate networks – now even without the attack vector having been in the affected company. This new threat quality is illustrated, for example, by the security incident at a VoIP software provider in March 2023. In this case, a double supply chain attack potentially threatened around 600,000 companies via an application signed with a valid 3CX certificate (see incident *Cyber Attacks on IT Service Providers*, page 57).

A Strong Shield: Cyber Resilience

In order to position themselves well in this threat landscape, it is necessary for companies to invest in their cyber resilience now. This includes technical and organisational measures such as regular security updates, backups and staff training. While large companies are usually well positioned in this area, SMEs usually still

Known ransomware victims in Germany in the reporting period by type of victim
Amount

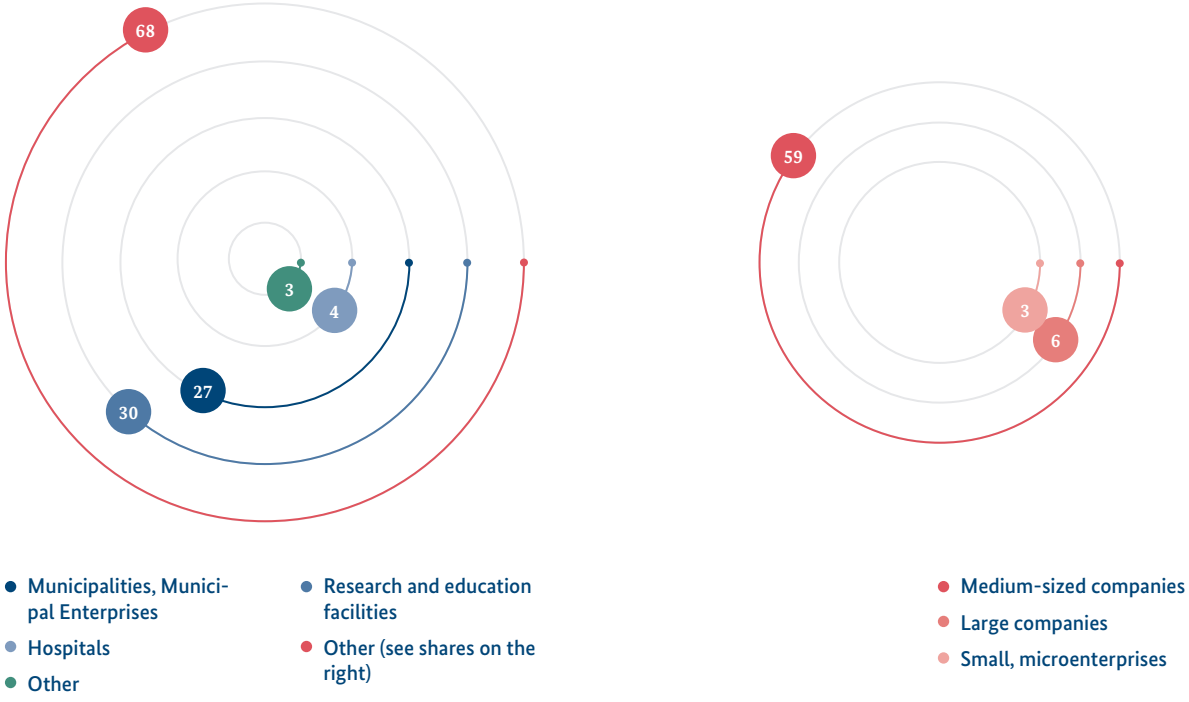


Figure 16: Known ransomware victims in Germany
Source: *Ransomware* victim statistics, BSI

have serious catching up to do. For example, according to a survey by the DIHK, only 61 per cent of microenterprises say they make regular backups (see chapter *Special Situation of SMEs in Germany*, page 64). When it comes to creating emergency plans, both large and small companies still have some catching up to do. Less than one third of the companies have a written emergency plan. The BSI offers an easy introduction to emergency management for the target group of SMEs with the "Catalogue of Measures for Emergency Management" (Maßnahmenkatalog Notfallmanagement in German) and a summary on one page.

Regularly practising the adopted measures is just as important as taking measures to increase resilience. Backups are only helpful if they can be restored. Another essential element is sharing and communicating security incidents. More and more companies are being transparent about incidents and informing the public and their customers. This helps to ensure that potential vulnerabilities can be remedied faster and damage can be averted from affecting more businesses.

The BSI's catalogue of measures for companies can be found here:[h]

Further information for companies can be found here:[i]

The BSI, with its services for the business community and its public-private partnership, the Alliance for Cyber Security,, offers numerous support services to help companies become more resilient and build a strong shield for increased cyber security.

Cyber Attacks on IT Service Providers

Situation

Several ransomware attacks on German IT service providers became known during the reporting period. In addition to the IT service providers themselves, their customers, both in the public administration and in the private sector and society, were often affected. For example, in addition to various local administrations, social institutions and non-profit organisations were also affected.

The ability of the affected IT service providers to operate was restricted by the attacks. Development of software for customers could either not be continued or at least not delivered. Moreover, the ability of the customers of the affected service providers to operate was also severely restricted in some cases.

Assessment

IT service providers are particularly interesting targets for cybercriminals, as attacks on an individual service provider can have damaging effects on numerous victims and the pressure of extortion is thus comparatively high. The BSI generally recommends against paying ransoms or hush money.

Chambers of Industry and Commerce Offline Across Germany after Cyber Attack

Situation

On 3 August 2022, the IT service provider of the Chambers of Industry and Commerce (IHK) discovered conspicuous behaviour in its hosted IT systems. The IHK Cyber Emergency Response Team (IHK-CERT) has investigated these anomalies. In cooperation with external IT security experts, they decided to shut down the systems for security reasons in order to prevent greater damage through the theft of data or the possible encryption of data.

As a result, all 79 Chambers of Industry and Commerce in Germany were disconnected from the internet and their services were no longer available. This resulted in websites being offline and staff not being reachable by phone or email. Internal applications also did not work or functioned only with limitations.

Assessment

The cyber attack was most likely carried out by professional attackers. Their modus operandi suggests the goal was espionage or sabotage, although financial motives on the part of the attackers cannot be ruled out.

Response

In order to reduce the risk of further attacks and possible compromises, all applications and IT systems were only gradually restarted after an intensive check. Individual chambers and various services of the organisation were still affected months later.

8.1 — Threat Landscape of Critical Infrastructure

Critical infrastructure refers to organisations that are of vital importance to the public. The operators of critical infrastructure provide critical services for the population, such as the supply of electricity, water or food. Furthermore, critical services include public transport, cash supply and medical care, among others. Critical infrastructure is a crucial foundation for a functioning society. Nevertheless, their significance is sometimes recognised only when disruptions occur.

"Critical infrastructures (KRITIS) are organisations and facilities of major importance for society whose failure or impairment would cause a sustained shortage of supplies, significant disruptions to public order, safety and security or other dramatic consequences."
KRITIS-definition of the federal government

All critical services are particularly dependent on trouble-free IT. Therefore, the BSI Act (BSIG) provides KRITIS-operators with measures for the prevention (§ 8a BSIG) and management (§ 8b BSIG) of IT security incidents or IT disruptions.

Threats and Response

For operators of critical infrastructure (KRITIS-operators), successful attacks on their IT infrastructure can not only cause damage to the company itself, but also have an impact on the provision of critical services to the population and thus on services of public interest. This makes it all the more important for operators and government agencies to work together to prevent attacks or mitigate their impact.

Operators of critical infrastructure as defined by the BSIG are obliged to report incidents to the BSI. For example, one hospital reported an incident in May 2023 and also worked with the relevant state criminal investigation department to manage the situation. It would, nonetheless, be advisable for operators of critical infrastructure, who do not fall under the regulations of the BSIG (because they do not meet the threshold values according to the BSI KRITIS-Regulation (BSI-KritisV)), to contact government agencies in the event of such incidents. The necessary trust-building for this can take place in particular through the public-private partnership, the UP KRITIS (see chapter *Cooperation Between the State and the KRITIS-Operators: UP KRITIS*, page 60), which offers advantages for all parties involved. The BSI supports operators of critical infrastructure and advises them on contact with government agencies in the context of the prevention of, and the reaction to, cyber incidents. Such a facilitation of mutual trust and cooperation enanbles a coordinated response to a serious IT incident, thereby avoiding as escalation into a full-blown crisis.

Spotlight on the Situation in the Health Sector

The evaluation of incident reports from the health sector shows a high willingness of operators to report their incidents to the BSI. The reports are crucial for the BSI to create a detailed picture of the situation and form the basis for warning and information reports oriented to target groups, which the BSI makes available to the regulated operators of critical infrastructure and the participants in UP KRITIS.

To do this, the reports are sanitised by the BSI, meaning that information requiring protection is removed from a report, while information relevant to other operators remains.

Almost half of the reports received from the health sector indicated a failure or impairment of the critical service provided by the operator. In most cases, technical failure was given as the reason for the disruptions. This correlates with the deficiencies identified in the periodic audits pursuant to § 8a para. 3 BSIG: Most deficiencies in the health sector concern the area of "technical information security".

Attacks played a role in about 20 per cent of the reports from the KRITIS-sector of health. Among these, we can observe an increasing focus on the service providers of the operators as a gateway: Instead of attacking KRITIS-operators and government agencies directly, these supply chain attacks target vendors, suppliers and thus the established supply chains. By compromising products of the manufacturing or third-party suppliers, the potential damage is not limited to the attacked company itself, but affects all companies downstream in the value chain. This knock-on effect makes supply chain attacks particularly lucrative for criminals, which may explain the increased incidence of such attacks. This trend is not limited to the health sector. Operators in other sectors are also fundamentally exposed to supply chain attacks that can circumvent many established prevention measures.

In audits conducted in accordance with § 8a para. 4 BSIG, the BSI has found on several occasions that the relationships between operators and service providers are structured in such a way that the operators cannot sufficiently fulfil their responsibility with regard to adequate IT protection. This is because even when IT services are outsourced, the KRITIS operator is still responsible for their security. There is also often no risk assessment of the relationship with the service provider. Thus, it is sometimes unclear who should assume which part of the operator's responsibility and whether the measures taken are actually sufficient.

Legal Obligation to Use Intrusion Detection Systems

Operators of critical infrastructure are obliged to take appropriate organisational and technical precautions to prevent disruptions to the availability, integrity, authenticity and confidentiality of their information technology systems, components and processes. With the IT Security Act 2.0, the use of intrusion detection systems (IDS) was explicitly prescribed for KRITIS-operators in the BSIG in May 2021 (§ 8a para. 1a BSIG). These systems are an effective measure for detecting cyber attacks and help mitigate the resulting damage. Since 1 May 2023, KRITIS-operators have a legal obligation to submit the evidence of IDS-deployment to the BSI as part of their security audits. This legal obligation affects not only KRITIS-operators who exceed the threshold values of the BSI-KritisV, but also all electricity and gas network operators per § 11 para. 1d Energy Industry Act (EnWG).

An effective IDS offers additional protection against the threat of ransomware in particular. Such systems make it possible to detect ransomware that is already on the network but has not yet started encrypting. Moreover, early detection enables the knowledge gained about the attacker or the attack vector to be shared with other entities and institutions, thus contributing to collective protection.

New EU Directives on the Protection of Critical Infrastructure and Other Critical Facilities

On 16 January 2023, two EU directives came into force:

- the Directive on measures for a high common level of cyber security across the Union with a focus on IT security (NIS-2-Directive, Network Information Security)[12]
- the Critical Entitites Resilience Directive with a focus on physical security (CER-Directive, Critical Entities Resilience)[13]

These directives must be transposed into national law in the Member States by 17 October 2024. Both directives aim, among other things, to ensure that critical facilities are uniformly better protected against cyber attacks, sabotage and natural hazards. In Germany, too, the group of institutions covered by statutory regulation is being considerably expanded. This will not only lead to increased investment in cyber security by the companies concerned, but will also entail numerous additional tasks for the BSI as the supervisory authority.

Number of Regulated Companies Will Rise Sharply

Currently, cyber security requirements for critical infrastructure in Germany are primarily defined by the BSI Act with the associated BSI-KritisV. The two EU directives will expand both the scope of regulated companies and the requirements placed on them in the future. Harmonised requirements for the protection of important, very important and critical entities against cyber and physical threats will become mandatory within the EU. The sectors covered by the directives are largely identical to those of § 2 para. 10 BSIG in conjunction with the BSI-KritisV (see also Table 2, page 60).

NIS-2-Directive – Strengthening the Cyber Security of Important and Very Important Facilities

Because of its focus, the NIS-2-Directive is of particular importance for IT security and its regulatory framework. It is the follow-up to the first NIS-Directive, which came into force in August 2016. Given the increased threat, particularly from cyber attacks, associated with the rapid growth of digitisation in all sectors of the industry and in government institutions, the NIS-2-Directive extends cyber security requirements to more sectors. It sets out security requirements for a significantly larger number of entities than previously covered by the BSI-KritisV and expands the framework for action to enforce the legal requirements. Moreover, with the NIS-2-Directive, corresponding obligations are also imposed on parts of the public administration.

An important feature in the NIS-2-Directive is the distinction between important and very important entities. Very important entities are subject to stricter rules than important entities with regard to the extent of state supervision. The number of the latter is much larger. Critical infrastructure, which is already regulated according to the BSIG, generally belongs to the category of very important entities in the sense of the NIS-2-Directive. Nevertheless, the sectors addressed in the

KRITIS according to nat. KRITIS strategy	KRITIS according to §2 (10) BSIG	NIS-2-Directive	CER-Directive
Energy	Energy	Energy	Energy
Transport and traffic	Transport and traffic	Traffic	Traffic
Finance and insurance	Finance and insurance	Banking and financial market infrastructure	Banking and financial market infrastructure
Health	Health	Health	Health
Water	Water	Water	Water
Information technology and telecommunications	Information technology and telecommunications	Digital infrastructure, ICT services management	Digital Infrastructure
Nutrition	Nutrition	–	Nutrition
Municipal waste management	Municipal waste management	–	–
Media and culture	–	–	–
–	–	Space	Space
State and administration	–	Public administration	Public administration

Table 2: KRITIS sectors according to the national KRITIS strategy, the BSI Act and the current EU directives
Source: Federal Office for Information Security 2023

NIS-2-Directive go beyond the KRITIS-sectors from the BSIG. For important and very important entities, including critical infrastructure operators, changes in obligations and requirements resulting from the transposition of the NIS-2-Directive into national law are therefore to be expected.

8.1.1 — Cooperation between the State and the KRITIS-Operators: UP KRITIS

In UP KRITIS, KRITIS-operators, their professional associations and the respective authorities work together to protect critical infrastructure in Germany. All operators of critical infrastructure can become participants in UP KRITIS. More than 900 organisations participate in UP KRITIS (as of June 2023). Working groups are organized by topic and sector to facilitate the exchange of ideas and information. The self-administration of UP KRITIS takes place via the following bodies

- Council – works at the political level; consists of high-ranking persons fromt the KRITIS-sectors as well as from the authorities of the Federal Ministry of the Interior and Community (BMI), the Federal Office of Civil Protection and Disaster Assistance (BKK) and the BSI,
- Plenum – all sector and thematic working groups send a spokesperson to this body,
- Executive Staff – the working group of the plenum, whose members are determined in the plenum,
- Secretariat – this is located in the BSI and mainly processes registrations and takes care of other administrative tasks..

The BSI participates in most of the working groups, in the plenum, in the executive staff and the council of UP KRITIS (see also Figure 17: Committees of UP KRITIS.

Committees of *UP KRITIS*

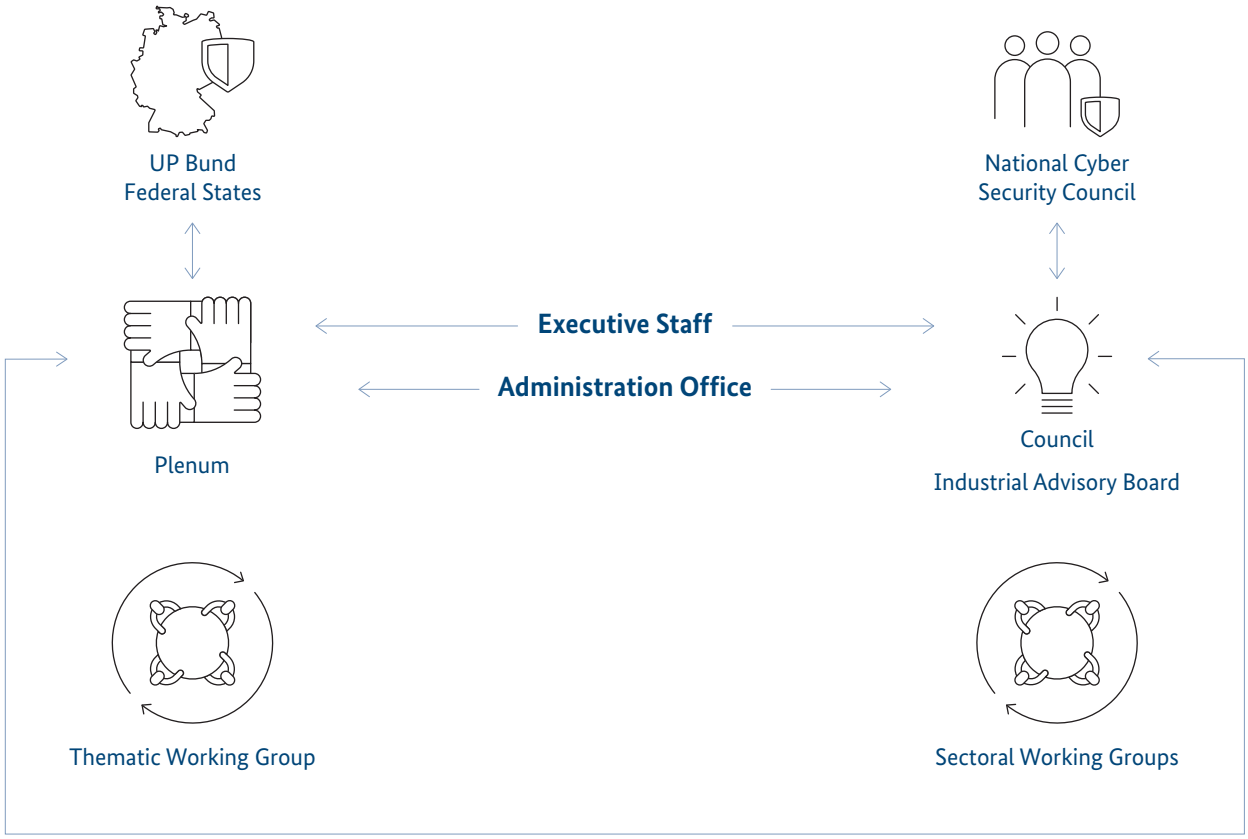


Figure 17: Committees of *UP KRITIS*
Source: Federal Office for Information Security 2023

During the reporting period, developments within the UP KRITIS included the following:

- The thematic working group "Requirements for Suppliers and Manufacturers" published a paper with recommendations on the development and provision of products used in critical infrastructure.
- The thematic working group "Impacts of the Ukraine Crisis" was renamed "Impacts of Current Crises and Events".
- UP KRITIS has accompanied the following legaslative projects: Amending ordinance to the BSI KRITIS Regulation, the NIS-2-Directive, the CER-Directive and the KRITIS Framework Act. Initial steps were taken to reorganize UP KRITIS to accompany the oimplementation of the new legislation.

Further information can be found here:[j]

8.1.2 — Digital Service Provider

The cyber security of digital service providers has also come into sharper focus in the context of the Russian war of aggression in Ukraine. These include online marketplaces, online search engines and cloud computing services. These are regulated according to § 8c BSIG.

As digital service providers have not yet been required to register, it has been difficult in many cases for regulating authorities such as the BSI to identify providers and establish contact so that they can receive BSI products, such as security alerts (analogous to critical infrastructure operators).

The NIS-2-Directive introduced a registration requirement for digital service providers. This is intended to ensure better visibility of security incidents and direct contact with providers in this area.

Moreover, with the NIS-2-Directive, cloud computing services are classified as very important entities and are subject to the same obligations as critical infrastructure operators. In addition, social media platforms have been included as a new category in the scope of digital service providers.

8.1.3 — Statistics

Reports by KRITIS-Sectors (§ 8b para. 4 BSIG)

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

In the reporting period, the BSI received 490 corresponding reports; the distribution among the KRITIS-sectors is shown in Table 3. A high volume of reports is not necessarily indicative of the level of information security in the respective sector. Operators of critical infrastructure sometimes also report incidents that are below the legal reporting threshold and thus contribute to the overall assessment of the situation. The number of reports does not correspond to the number of incidents that have been reported. Incidents that continue over a longer period of time usually include an initial report, one or more intermediate updating reports and a final report.

Maturity Levels of Information Security and Business Continuity Management Systems at KRITIS Operators

Operators of critical infrastructure are legally obliged under § 8a para. 3 BSIG to provide (independent) audits to the BSI every two years that their IT security corresponds to the state of the art. These audits must include the assessment of the auditor on the effectiveness of the Information Security Management System (ISMS) and Business Continuity Management System (BCMS) at the inspected operator. This is done using a maturity model, which makes it possible to document the progress of ISMS and BCMS (with regard to ensuring the delivery of the critical service) in a comprehensible manner across test cycles, without focusing on individual measures.

Sector	Report
Energy	99
Information technology and telecommunications	81
Transport and transit	111
Health	132
Water	16
Food	9
Finance and insurance	61
Municipal waste management	0
Total	490

Table 3: Reporting figures by KRITIS sector in the reporting period
Source: Federal Office for Information Security 2023

The classification into maturity levels is based on classic maturity models. The maturity level is a potential indicator for the management or leadership of the concerned entity.

The guidance on audits pursuant to § 8a para. 3 BSIG describes the following maturity levels for ISMS and BCMS[14]:

ISMS Maturity Level

Maturity Level 1: An ISMS has been planned, but not yet implemented
Maturity Level 2: An ISMS is mostly in place
Maturity Level 3: An ISMS is in place and documented
Maturity Level 4: In addition to maturity level 3, the ISMS has been regularly reviewed for effectiveness
Maturity Level 5: In addition to maturity level 4, the ISMS has been regularly improved.

BCMS Maturity Level

Maturity Level 1: A BCMS has been planned, but not yet implemented
Maturity Level 2: A BCMS is mostly in place
Maturity Level 3: A BCMS is in place and documented.
Maturity Level 4: In addition to maturity level 3, the BCMS has been regularly reviewed and practised.
Maturity Level 5: In addition to maturity level 4, the BCMS has been regularly improved.

Maturity levels vary across the various critical infrastructure sectors, which is also reflected in ISMS- and BCM-deficiencies documented in the audits. The significant differences in, among other things, the size of the entities, the dependence on IT, and the requirements of different supervisory regimes, however, do not admit a cross-sector comparison.

Sector	ISMS maturity level according to the most recent available decent					BCMS maturity level according to the most recent available evidence				
	Maturity level					Maturity level				
	1	2	3	4	5	1	2	3	4	5
Water	0	6	15	27	24	1	13	27	17	14
Energy*	2	7	27	23	25	2	20	34	15	13
Transport and transit	6	13	27	7	7	9	18	16	11	6
Finance and insurance	1	5	33	19	29	1	24	19	23	20
IT and TC**	0	5	6	9	11	3	6	7	7	8
Nutrition	0	8	20	5	9	4	8	20	6	4
Health	14	88	59	26	12	34	79	49	24	13
In total	23	132	187	116	117	54	168	172	103	78

* Excluding energy supply grids and energy plants pursuant to § 11 EnWG
** Excluding public telecommunication networks or publicly available telecommunication services

Table 4: ISMS maturity level and BCMS maturity level by sectors
Source: Federal Office for Information Security 2023

The BSI Continuously Monitors the Security Situation of Critical Infrastructure in Germany.

The state and private sector operators of critical infrastructure bear a high degree of responsibility for safe and trouble-free operation in terms of providing the population with vital services. Due to the Russian war of aggression against Ukraine, the security of critical infrastructure in Germany remains in focus.

The BSI continues to receive audit reports documenting maturity levels 1 and 2 for ISMS and BCM in KRITIS-operators, even in its third audit cycle. By monitoring the elimination of deficiencies on the operator side as part of audit process, the BSI is working towards improving this situation in the short term, towards established management systems. It is also striking that despite various crises, especially the COVID-19 pandemic and the war in Ukraine, BCMS maturity levels are still lagging behind ISMS maturity levels. The BSI considers this to be an area in need of urgent action.

8.2 — The Special Situation of SMEs in Germany

2.6 million small (less than 50 employees) and medium-sized enterprises (50 to 249 employees) in Germany are facing the challenges of digitisation and the associated cyber security. This sub-sector of companies, which accounts for 99.4 per cent of German business enterprises, breaks down as shown in Figure 18.

In particular, micro (less than ten employees) and small enterprises often do not have the necessary staff for operating and securing the company's information technology systems. For example, a small skilled trade business, a medium-sized tax consultancy or law firm, a metalworking company or a care service is often not in a position to hire dedicated IT staff. When deciding between making or buying, the approach is often "we'll manage it ourselves somehow". This stands in contrast to a growing threat situation.

In 2023, many companies still have neither sufficient knowledge about the general state of cyber threats nor about their own risk profile. As a result, it does not occur to them that they should invest more in their security. Even the most basic preventive measures, which can often be implemented free of charge, are often not taken. For example, only 62 per cent of microenterprises regularly install security updates. Even fewer (46%) leave their IT security to an external service provider. And only 18 per cent of microenterprises have an emergency plan[15]. Slightly more than half of the small and medium-sized enterprises (51%) cite the effort and costs involved in ongoing technical operations, adjustments and updates as the main "IT security brake". Only 28 per cent consider the initial effort an obstacle. This is consistent with the feedback from IT service providers to the BSI[16].

On the other hand, those SMEs who have developed an awareness of the problem and want to recruit staff often find that they cannot compete in a competitive market as a potential employer against the salaries at large companies or IT service providers. And those who want to outsource IT/IT security to a service provider often find that there are either too few qualified service providers in their region or only those that do not fit their own company size.

Companies in Germany by size
Share in %

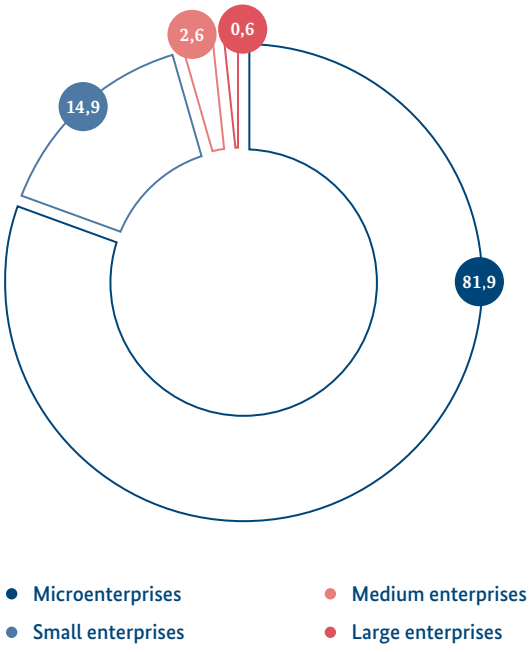


Figure 18: Companies in Germany by size
Source: Federal Statistical Office, as of July 2021

All this means that SMEs often fall victim to cybercriminals – and then they have no idea what to do. A study published on behalf of the Federal Ministry for Economic Affairs and Energy (now the Federal Ministry for Economic Affairs and Climate Action) in 2021 came to the same conclusion: "In the event of an incident, SMEs often don't know where to turn for expert help. In contrast to burglaries in the analogue world, digital damages are not always and not immediately apparent to many SMEs. The reluctance to report incidents and attacks to the police, the state criminal investigation offices or other authorities is high."[17]

Consequently, the issue of cybercrime against SMEs is affected by a large dark field, which makes it difficult to obtain reliable figures. Moreover, the above-mentioned study makes the following recommendation: "The establishment of a nationwide emergency hotline for IT incidents with central accessibility for referral to regional contact points would remedy the situation."

Emergency Hotline

The BSI operates a service centre due to the need for such a hotline. This can be reached free of charge by calling 0800 274 1000. From there, the Cyber Security Network (CSN) will, if necessary, also refer people to regional contact points that can help those affected on site.

Being able to contact an emergency hotline in the event of an emergency is important, but it is more important to take preventive measures to avoid becoming a victim. Yet SMEs often do not know how they can do more for their IT security. Existing standard works on how to set up an Information Security Management System, such as the BSI's IT-Grundschutz compendium or the ISO/IEC 27001 standard, are more suitable for companies that have an independent IT facility. However, this does not apply to the majority of enterprises with less than 50 employees.

Carrying Out CyberRisikoChecks

One service offered to SMEs is the CyberRisikoCheck, which was developed by the BSI together with various partners. This process involves an IT service provider interviewing a company for one to two hours (usually via video conference) about IT security in the company. 27 requirements from six subject areas are checked to see whether the company fulfils them. Points are awarded for the answers in accordance with the DIN SPEC guideline drawn up by a consortium led by the BSI and the German Association of Small and Medium-Sized Enterprises (BVMW). The company receives a report with the score and a recommendation for action for each unfulfilled requirement. The recommendations for action are structured according to urgency and are given indications of which government support measures (at federal, state and municipal level) the respective company can take advantage of. The CyberRisikoCheck is not an IT security certification. But it does enable a company to determine its own IT security level and shows which concrete measures a company should implement or commission from an IT service provider.

Thanks to the anonymised survey data of the CyberRisikoChecks, the National IT Situation Centre will be able to access valid data on the cyber security of SMEs for the first time and include it in the BSI reports on the cyber security situation. The CyberRisikoCheck thus contributes to the continued development of preventive services offered by the federal government, the states and the municipalities.

You can find lots of helpful tips for SMEs here, including a directory of service providers who can help in an emergency and a way to report if you have been affected by a cyber attack to the BSI:[k]

Further information on the CyberRisikoCheck and a list of registered IT service providers that offer the check can be found here:[l]

In addition, companies can become members of the public-private partnership Alliance In addition, companies can become members of the public-private partnership Alliance for Cyber Security founded by BSI and Bitkom e. V. in order to benefit from the numerous information services offered by the members.

For a good overview of the most important IT security measures, see the BSI brochure "Cyber Security for SMEs – The TOP 14 Questions".

9. — Insights from the Threat Landscape in the State and Administration

The state and administration experienced increased exposure to cyber attacks during the reporting period. In particular, the phenomenon of politically motivated hacktivism has been gaining ground in Germany in the context of the Russian war of aggression in Ukraine. With few exceptions (see The State of IT Security in Germany 2022, page 49ff), the pro-Russian hacktivists used DDoS attacks (see incident *DDoS Hacktivism*, page 29). Since this type of cyber attack can only temporarily shut down internet services and does not involve a deeper infiltration of IT systems and networks, attackers can only cause limited damage with it. Therefore, it is safe to assume that DDoS hacktivism is essentially a propaganda phenomenon designed to spread insecurity throughout German society.

In contrast, cyber attacks with ransomware or wipers leave lasting damage. The recovery of affected systems takes a lot of time and the affected agencies are often unable to work properly for months.

9.1 — Federal Administration

Every day, government networks are exposed to predominantly untargeted mass attacks from the internet, but sometimes they are also targeted against the federal administration. To protect government networks from any attacks, the BSI uses a variety of interrelated measures.

Web filters are a preventive component that block access to malicious websites or web servers. For example, they prevent access to malware hiding behind download links that are spread via email, social media or websites as part of social engineering attacks. It also prevents malware from communicating with the corresponding web servers, for example to reload further components or commands. During the current reporting period, an average of 370 malicious websites were blocked every day.

Antivirus protection measures prevent the delivery of malware that is sent directly in email attachments. During the reporting period, this affected an average of around 775 emails per day. Around 82 emails per day were identified as malicious solely on the basis of antivirus signatures specially created by the BSI.

Spam mail index for the federal administration*
2018=100

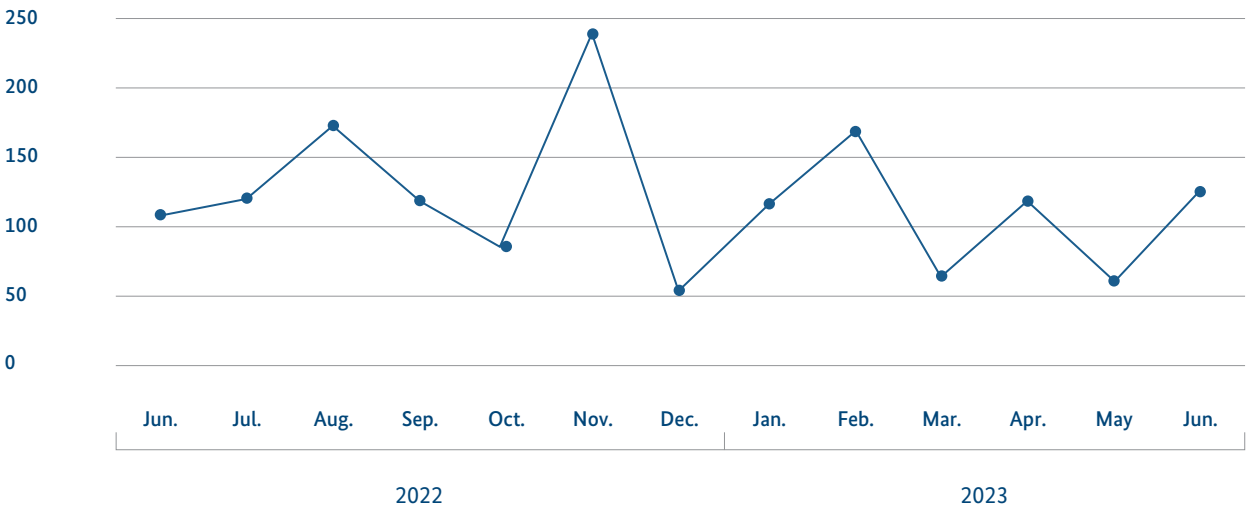


Figure 19: Spam mail index for the federal administration
Source: Survey on email traffic within the federal administration, BSI

*Excluding spam email to authorities that do not participate in the central

In order to be able to detect targeted attacks on the federal administration in particular, the BSI operates a system for detecting malware in the data traffic of government networks in addition to the measures already described. Using a combination of automated testing procedures and manual analysis, the BSI analysts were able to identify an average of at least another 78 attacks per day that were neither detected by a commercial solution nor by one of the automated solutions mentioned above.

In addition, the security of government networks is increased with central protection against spam emails. This measure is not only effective against unsolicited commercial emails. It also detects cyber attacks such as phishing emails. The spam rate, i.e. the percentage of unsolicited emails in all incoming emails, averaged 58 per cent in the reporting period. The volume and development of spam emails in the federal government's networks are measured by the spam mail index. This reached an average of 124 points in the reporting period. This represents an increase of around twelve per cent compared to the previous reporting period (111 points).

There were considerable fluctuations in this. While the volume of spam remained at an average level in the summer of 2022, the index values increased significantly in November 2022. The federal administration's spam filters reliably block such spam waves so that they do not reach the addressed users.

9.2 — State and Local Administration

State and local administrations increasingly fell victim to cybercriminal ransomware attacks during the reporting period.

During the current reporting period, an average of two local administrations or municipal utilities were identified as victims of ransomware attacks each month (see incident *Ransomware Attacks on Local Administrations and Municipal Utilities*, page 69). Thus, they were disproportionately affected by ransomware attacks (see also Fig. 16, page 56).

As is now common practice, not only were servers encrypted, but data from citizens was also leaked and in some cases published on leak sites. Among other things, entire directories containing the files of individuals were affected. The affected administrations were usually unable to provide their administrative services to citizens and businesses for several days to several weeks, and in some cases were still affected months later.

While federal authorities have separately secured government networks with central defences, local authorities design their IT security measures separately. Currently, there are no nationwide uniform requirements regarding IT security or reporting obligations for IT security incidents at the municipal level.

Educational and research institutions were also increasingly targeted by ransomware attackers during the current reporting period (see incident *Ransomware Attacks on Educational and Research Institutions*, page 69).

Ransomware Attacks on Local Administrations and Municipal Utilities

During the reporting period, a total of 27 local administrations and businesses became known as victims of ransomware attacks. Municipalities of all types and sizes were affected: from a rural community with 2,800 inhabitants to a large city with more than 1.8 million inhabitants. In total, the affected municipalities had almost six million inhabitants. Often, city or district administrations were directly affected; however, local transport companies, municipal energy providers or housing associations, city cleaning companies and an education authority with responsibility for 75 schools were also attacked. Even the cemetery service of a major German city was not spared. In June 2022, all the city halls of an entire district as well as several municipal businesses of a neighbouring large city, including the local transportation company, had to be disconnected from the internet after a particularly far-reaching ransomware attack.

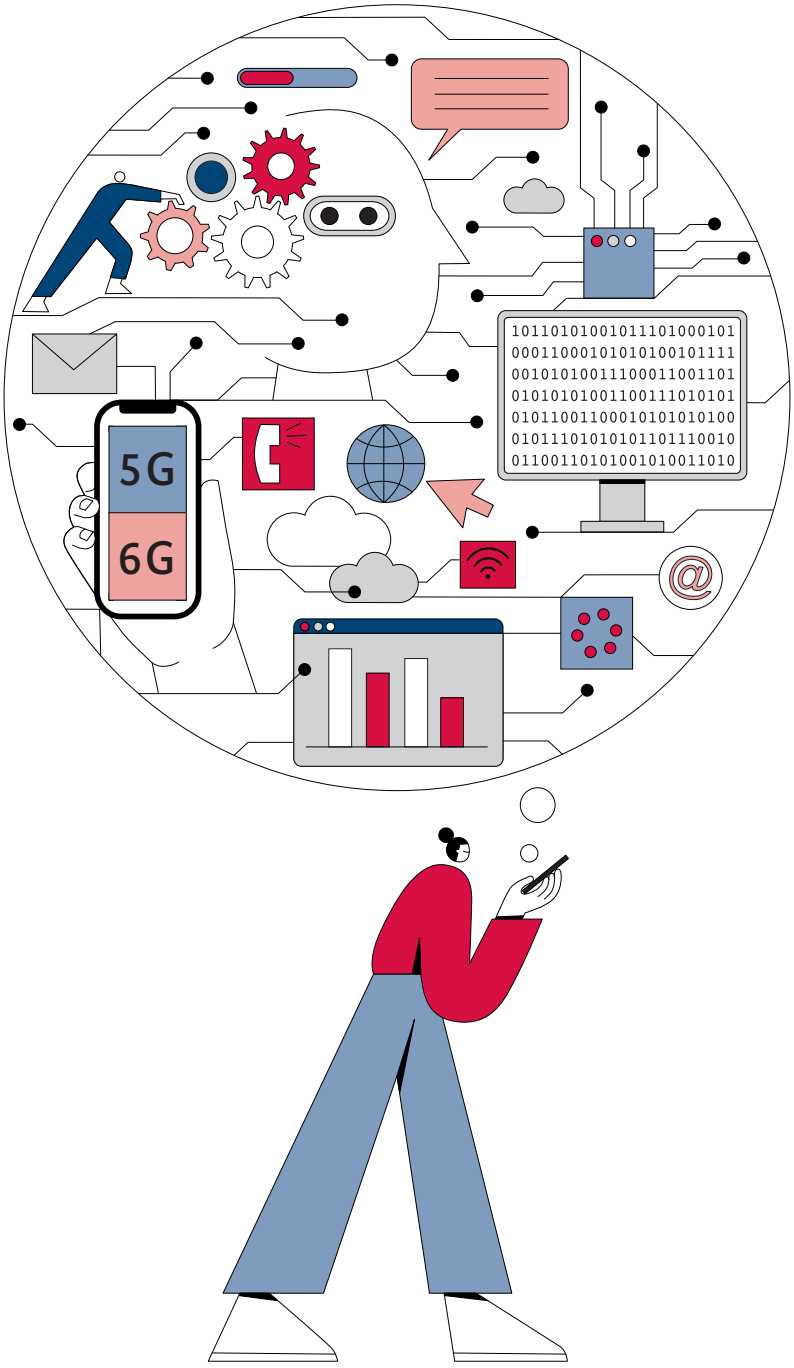
Even though the attacker groups, the vulnerabilities exploited and the RaaS used may have differed from each other, the processes were mostly the same: The initial infection was followed by scanning the infected systems and encrypting data. Afterwards, the victims were confronted with the demand for a ransom. Victims had to completely shut down their systems and disconnect from the internet to prevent further damage and progressive encryption on their networks. Cleaning up the systems and restoring them to full working order often took months.

The BSI recommends that, in addition to the available measures for countering ransomware attacks, the IT-Grundschutz profile "Local Administration Basic Security" (Basis-Absicherung Kommunalverwaltung) be implemented and that the BSI's support services for getting started with information security be used, such as the newly developed checklists for the "Path to Basic Security – WiBA" (Weg in die Basis-Absicherung – WiBA). With the help of the checklists, it is possible to take an initial inventory of information security and to seamlessly implement the above-mentioned profile. The long-term goal should be to reach the level of certifiable standard protection.

Ransomware Attacks on Educational and Research Institutions

*It has been known for some years that universities are attractive victims for cyber attackers (see for example the case of a university hospital, **The State of IT Security in Germany 2022**, page 15). Also during the current reporting period, five universities were again identified as victims of ransomware attacks. In particular, however, criminal cyber attackers targeted universities of applied sciences. Among the 23 known ransomware victims from the education and research sector, 13 were universities and universities of applied sciences alone. Furthermore, several institutions of renowned research associations as well as ten general education schools also became victims.*

Trends


5G
6G
10110101001011101000101
00011000101010100101111
00101010011100011001101
01010101001100111010101
01011001100010101010100
01011101010101101110010
01100110101001010011010

Part C: Highlighted Trends in IT Security

10. — Artificial Intelligence

Artificial Intelligence (AI) is currently on everybody's mind. The topic has found its way into people's everyday lives in no small part due to large language models such as ChatGPT, and is developing at a rapid pace. Be it writing a text or creating an image, artificial intelligence has now reached the point where the result is almost indistinguishable from that of a human – while saving a lot of time.

AI also plays an increasingly important role in other areas, such as AI-supported recommendations when granting loans or deciding on medical treatment methods. Other topics include the use of AI in cryptography and cryptanalysis as well as in the areas of autonomous driving and media identities.

Artificial intelligence is one of the key technologies of digitisation. The BSI aims to shape digitisation securely in all its facets as a thought leader and to become a central body on questions of security and the testing of AI systems in Germany, which is why IT security for AI and by AI are core topics that are actively pursued for this purpose. Together with partners from research and development, business and administration, the BSI is developing the technological foundations and criteria for evaluating and testing AI systems in order to put them into practice. Moreover, the BSI the BSI is actively involved in the development of AI norms and standards and contributes many years of experience and technical expertise to national and international standardisation processes and committees.

The use of AI involves both, risks and challenges (see chapter *AI Large Language Models*, page 40) as well as opportunities and potentials. Through the abovementioned activities, the BSI is committed to support the creation of demonstrably secure, trustworthy and transparent AI systems. This will enable the potential offered by current developments and trends in the field of artificial intelligence to be safely harnessed and implemented for the benefit of the industry and society.

10.1 — Security of AI Large Language Models

Large language models (LLM) are currently the focus of public interest. They are well suited to word processing and text generation and produce high quality text that is difficult to distinguish from human-written text.

Starting in mid-2022, the BSI has been building up expertise on security aspects related to LLMs across departments and locations and has been offering this expertise in the form of advisory services and lectures within the BSI as well as to other authorities and the public. In May 2023, the BSI published a paper highlighting the opportunities and risks of using LLMs in industries and public authorities as well as for consumers.

The BSI publication on Large AI Language Models:[m]

The way LLMs function and are trained creates various weaknesses that can lead to security risks. If the data used to "teach" an LLM is not balanced, but contains a bias or even outdated or discriminatory statements, these can also show up when using the LLM. Moreover, although an LLM delivers a result (output) in response to inputs on topics previously unknown to it, this can be arbitrarily unrealistic ("hallucinating"). Similarly, source code generated by the LLM may be susceptible to vulnerabilities (if they were present in the training data, for example). Another problem is that it is difficult to explain the origin of the outputs of LLMs because of the high complexity of these models.

In addition to the aforementioned risks, LLMs can also be used to generate spam and phishing emails. With the ability to create articulate, persuasive text, the automated generation of hate speech, disinformation and fake reviews is another common scenario of abuse. Furthermore, criminals can use LLMs to generate and regularly modify malicious code, making it more difficult to detect.

These and other scenarios require developers and providers of LLMs or LLM-based applications to take appropriate precautions to prevent or discourage the generation of potentially harmful output as far as possible. Users of these applications should be educated about possible security risks when using LLMs in order to be able to deal with the outputs of such a model in a responsible way.

The integration of LLMs into everyday or office applications can provide a boost to digitisation by offering a wide range of support for text processing and production tasks. At the same time, however, depending on the application, there may be considerable safety risks that should be weighed against the benefits in each individual case.

10.2 — Digital Consumer Protection and AI

Due to their black-box character, decisions made by an AI system are often surprising and not very comprehensible to consumers. Especially in applications with far-reaching effects (e.g. recommendations on medical treatment or granting of credit), the lack of transparency of these systems is a problem. In this context, the BSI is investigating how consumer applications that use AI can be evaluated. The aim is for consumers to identify the use of AI systems in a self-guided way in order to strengthen their resilience in relation to AI systems.

Moreover, the BSI is examining methods to determine the robustness of AI systems and to be able to explain their decisions and make them more transparent. The results of the research will be presented in a consumer-friendly way and disseminated through various communication channels.

10.3 — Use of AI in Cryptography

Artificial intelligence has also been used in various areas of cryptography for a long time. Especially in side channel analysis, machine learning (ML) methods are now firmly established. The best results can be achieved when machine learning is combined with expert knowledge about possible sources of side-channel information, with the use of neural networks being particularly successful. The BSI is therefore addressing this topic both in the context of various projects and within the framework of its own research.

AI techniques can also be used in the field of cryptanalysis, for example in the analysis and evaluation of symmetric cryptographic methods. This is the subject of two BSI projects that build on each other and whose goal is, among other things, the development of AI-supported tools that can contribute to the security assessment of block ciphers.

10.4 — AI-Supported Analysis in the State of IT Security

In a project, the BSI is testing AI methods that can be used to automatically gather and analyse current news about the IT security situation. A knowledge graph (ontology), consisting of terms from the IT security domain, serves as a knowledge base to support this analysis. At the same time, ML is used to improve the knowledge graph in a partially automated way.

The knowledge graph and trained language models are used to identify entities in the text, that is, text passages are recognised as naming an entity – for example, "browser" as software - or even assigned to a concrete object, such as the string "BSI" to the Federal Office. These entities are used for semantic searches as well as for reading support or for targeted statistical evaluation of entire object classes (e.g. malware). Language models also allow text classification and natural language questions to be answered with text passages, which helps to improve the transparency of the results.

10.5 — AI for Autonomous Driving and Media Identities

Since December 2021, the BSI has been conducting projects in which the first concrete criteria and test methods for AI procedures in autonomous driving are being developed based on the consideration of practical use cases. In the first project[18], 50 technically relevant requirements for AI systems were compiled and an expandable test environment for AI systems was developed, among other things. These requirements, methods and tools have been specifically tested and refined in a follow-up project since December 2022. In the medium term, the BSI plans to draft a Technical Guideline based on this preliminary work[19].

Further information on automated driving:[n]

During the last reporting period, a steady increase in the quality of publicly available tools for manipulating identities in audio and video media (deepfakes) was also observed (see also chapter *Scaling Effects of Known Threats*, p. 43). These tools are available partly through open-source software and partly through new cloud services. In some cases, identities can be aligned to a target identity based on just a few seconds of material using "one-shot" processes. This can be used, for example, to deceive speaker recognition systems[20].

The BSI was able to show that identity forgery is now possible in both audio and video with acceptable quality in real time. The project "Securing Media Identities" intends to develop and evaluate countermeasures by 2025.

10.6 — Further Developments in the Field of AI

The topic of AI security continues to be the focus of standardisation bodies and expert groups worldwide, where the BSI contributes its expertise. In a growing number of different application domains, the BSI has been working on the development of test criteria and test methods for AI systems, for example in the automotive, cloud services, medical and agricultural sectors. This will address and implement the core topics and recommendations of the German Standardization Roadmap AI, which the BSI actively helped to create.

In one project, a novel approach to AI-supported static code analysis was successfully implemented and tested. The software is published as open source, which is expected to improve networking with the research community and provide further impetus for research in this direction.

Further information on this and other studies can be found here:[o]



Quantum computers offer a potential that is also of increasing interest in the field of machine learning. Currently, the discussion mainly focusses on approaches that combine classical and quantum algorithms in hybrid methods[21]. In a foundational study[22], the BSI compiled the current state of research on quantum machine learning (QML) and highlighted opportunities and risks with regard to IT security. In a follow-up project, the security properties of and threat scenarios for QML methods and systems will be investigated using practical experiments.

In the area of Explainable AI, the BSI investigated the lack of reproducibility in the training of machine learning models and its impact on the prediction and explainability of the models' outputs. The influence of the dimensionality of data on the quality and reliability of probability-based ML models were also examined.

11. — Quantum Technologies

The progressive development of quantum computers threatens the security of many classic and widely used public key protocols such as RSA and ECC. Therefore, the migration to cryptographic protocols that presumably cannot be broken even with quantum computers (post-quantum cryptography) is highly urgent. The BSI is operating under the working hypothesis, for the high-security sector, that cryptographically significant quantum computers will be available in the early 2030s. It should be emphasised that this statement is not to be understood as a prognosis on the availability of quantum computers, but represents a reference value for the risk assessment.

A detailed analysis, "Status of Quantum Computer Development", was already prepared on behalf of the BSI in 2018 and has been updated twice since then. In another BSI project, a total of three further updates were carried out.

Further information on the study:[p]

In the BSI's Technical Guideline TR-02102-1 the first post-quantum methods, FrodoKEM and Classic McEliece, and the hash-based signature methods, LMS and XMSS, were already recommended in March 2020. An overview the topic is provided in the BSI's guideline "Quantum-safe cryptography".

The BSI guideline "Designing cryptography to be quantum secure" can be found here:[q]

The technical guideline TR-02102 can be found here:[r]

Other European cyber security agencies such as the French ANSSI and the Dutch NCSC have also published initial recommendations on migrating to quantum-safe protocols. The US government has provided particularly comprehensive and concrete measures. Two memoranda, issued in May and November 2022[23], established mandatory migration plans, regular reporting requirements and ambitious migration timetables for public authorities. By 2035, the threat posed by quantum technologies should be minimised as much as possible through the widespread use of post-quantum cryptography. In order to achieve this, the NSA released the Commercial National Security Algorithm Suite (CNSA) 2.0[24] in November 2022. This is binding for operators of National Security Systems and describes schedules for various technical applications. For example, post-quantum cryptography is scheduled to be the standard for web browsers, servers and cloud services as of 2027.

The implications of quantum technologies for cyber security have been considered by the Federal Government of Germany and the BMI. In September 2021, the German government stated in its "Cyber Security Strategy for Germany 2021"[25] that it aims to promote the "development of new encryption solutions, especially in the field of post-quantum cryptography". The BMI set this goal in its cyber security agenda[26] published in April 2022 with the measure of "equipping the federal authorities with advanced IT products and systems for secure communication as well as investment in quantum computing and post-quantum cryptography".

In its "Quantum Technologies Action Plan"[27], the German government set itself the goal of developing a strategy for migration to post-quantum cryptography by 2026.

11.1 — Post-Quantum Cryptography

The standardisation of post-quantum methods has so far mainly taken place through a process initiated by the US National Institute of Standards and Technology (NIST) in 2016 that involved international participation. In July 2022, NIST chose the key encapsulation mechanism CRYSTALS-Kyber and the signature protocols CRYSTALS-Dilithium, Falcon as well as SPHINCS+ for standardisation[28] (see also chapter *Vulnerabilities in Hardware Products*, page 39).

In addition to the standardisation of post-quantum protocols, many concrete activities are currently underway to migrate to post-quantum cryptography. For example, the first products using hybrid key agreement for the high-security sector have already been approved and are in use. At the Internet Engineering Task Force (IETF), numerous working groups are involved in integrating post-quantum cryptography into the IETF's standards. In a BSI project for the continued development of the FOSS cryptographic library Botan, post-quantum protocols and a hybrid key agreement are currently being implemented in TLS 1.3. Another BSI project is aiming to implement quantum secure email encryption and signatures in the Thunderbird email client. A draft standard for post-quantum cryptography in OpenPGP has also been produced as part of this project.

The BSI is also the operator of the root certification authority for the public key infrastructure of public administrations (V-PKI). The cryptographic algorithms currently used in this V-PKI are not secure against quantum attacks. In order to be able to counter the impending threat from cryptographically relevant quantum computers in time, the BSI is currently planning the migration to a quantum-safe V-PKI.

Migration to post-quantum cryptography is also important outside of the high-security sector and public administration. Therefore, awareness of the threat to security posed by quantum computing and possible protective measures must be raised. A survey[29] published in April 2023 shows that companies are not taking adequate measures to address the information security threat posed by quantum computing. Although 97 per cent of the participating companies rated the relevance of quantum computing for the security of today's cryptography as "high" or "rather high"; only 25 per cent of companies are taking this threat into account in their risk management.

NIST selection procedure

Except for SPHINCS+, which is hash-based, the security of these protocols is based on lattice problems in structured lattices. Draft standards for Kyber, Dilithium and SPHINCS+ were published in August 2023. At the end of the fourth round, which is currently underway, another key encapsulation mechanism is expected to be selected for standardisation. In addition, NIST issued a new call for further signature protocols, with submissions being accepted until the beginning of June 2023. FrodoKEM, which is recommended by the BSI, is not being considered further in the NIST process because it is less efficient than Kyber. Classic McEliece, the second BSI recommendation for key encapsulation, could possibly still be standardised at the end of the fourth round. The BSI stands by its recommendation of FrodoKEM and Classic McEliece even after the decision by NIST. These procedures provide a rather conservative alternative to the previous NIST selection and are currently being standardised at ISO.

In recent years, research activity in post-quantum cryptography has been very high, partly due to the high visibility of the NIST selection process. In fact, some of the protocols submitted have proven to be unsafe. For example, the security level of the Rainbow multivariate signature process (a finalist in the 3rd round of the NIST process) has been shown to be insufficient by new attacks in 2022. SIKE, an isogeny-based key transport method, was even completely broken shortly after it was included in the 4th round by NIST. The security of the procedures recommended by the BSI and those selected by NIST for standardisation so far, however, have been based on completely different mathematical problems. Therefore, these procedures are not affected by the new attacks and are still considered secure. Nevertheless, they must also be actively investigated further and the BSI generally recommends the hybrid use of post-quantum cryptography in combination with classic public-key cryptography.

11.2 — Quantum Key Distribution

Quantum key distribution (QKD) is intended to enable quantum-safe key agreement based on principles of quantum mechanical and so it may be a complement to post-quantum cryptography for special use cases. The development of QKD is currently being heavily promoted at the national and European level, for example through the European Commission's EuroQCI project. EuroQCI aims to establish a quantum communication infrastructure in Europe, comprising both a terrestrial and a satellite-based component. Since March 2023, EuroQCI has been part of IRIS2, a project to develop a European satellite-based secure communication system. The BSI is a member of the Security Working Group of EuroQCI.

From the BSI's point of view, essential groundwork is still needed on security issues before QKD is ready for use. In order to contribute to the development of secure QKD systems, the BSI, together with the European Telecommunications Standards Institute (ETSI), has developed an initial Protection Profile (PP)[30] according to Common Criteria for Prepare-and-Measure QKD systems. The first version of this profile was published by ETSI in April 2023. It is currently being certified by the BSI and then an updated version will be made available. However, in order to use the PP for the certification of products, the development of further background documents such as standards and an evaluation methodology is required. QKD standards are currently being developed in several committees.

In order to support the development of an evaluation methodology for QKD, the BSI commissioned a scientific study on side-channel attacks on QKD systems in 2022. The results are expected to be published at the end of 2023.

The Federal Ministry of Education and Research (BMBF) is funding various projects on quantum communication, including the QuNET project. An umbrella project is also

being funded within the framework of the Quantum Communication Innovation Hub, which is intended to bundle and focus the quantum communication expertise available within Germany. This umbrella project, Quantum Communication Germany (SQuaD), is coordinated by the Physikalisch-Technische Bundesanstalt in close cooperation with the BSI.

12. — Security of Modern Telecommunications Infrastructure (5G/6G)

In the future, a particularly important topic for the BSI is a securely designed 5G/6G infrastructure for Germany. With 5G and 6G technologies, application scenarios can be realised that could not previously be realised via mobile telephony. For example, data transmission speeds are increasing while delays are decreasing.

The higher transmission speeds are then improving efficiency in the process. Moreover, the low latency times enable real-time communication of end devices, offering completely new possibilities. As a result, modern mobile technologies are creating an important prerequisite for further digitisation and are becoming critical infrastructure increasingly.

In order to meeting the goal of securely designed 5G/6G infrastructure three pillars are needed:

- Development of specifications for maintaining the safe operation of 5G networks,
- Verification of the specifications through certification and auditing procedures,
- Participation in standardisation organisations for the development and updating of schemas as well as for the implementation of IT security requirements for 5G/6G networks.

12.1 — Specifications and Certification for 5G Networks

The BSI is involved in the development and updating of legal regulations governing 5th generation public mobile telephony networks. The following sub-chapters will provide an overview and highlight different certification schemes that are in use. No legal regulations exist in the field of private 5G networks, also called 5G campus networks. Instead, IT-Grundschutz profiles provide operators and users with standardised tools for the introduction of IT security.

12.1.1 — Co-Design of the IT Security Catalogue and Updating of Technical Guideline TR-03163

The BSI, together with the Federal Commissioner for Data Protection and Freedom of Information and under the auspices of the Federal Network Agency, is designing the catalogue of security requirements in accordance with the Telecommunications Act (TKG), which is currently under revision.

The security catalogue regulates mandatory measures to achieve the security objectives specified in the TKG and is directed at all telecommunications operators and service providers. This sets out increased requirements for 5G network operations to reflect the importance of the 5G mobile network to society. The security catalogue specifies the framework and deadlines for the certification of critical 5G network components and refers to Technical Guideline TR-03163 "Security in Telecommunications Infrastructures" of the BSI, which specifies the schemes and is updated regularly.

The technical guideline TR-03163:[5]

12.1.2 — Implementation of Mandatory Certification for Critical Components in Public 5G Networks

With the publication of TR-03163 and the launch of the National Certification Scheme for 5G Mobile Equipment (NESAS CCS-GI), the BSI has begun to implement the statutory certification obligation under the TKG. The BSI is currently working with interested partners to draw up the requirements for the security certification of various network elements of a 5G network.

The NESAS CCS-GI enables manufacturers to prove that they comply with the security features required by the international standardisation project 3rd Generation Partnership Project (3GPP) with an IT security certificate. The certificate is based on the Network Equipment Security Assurance Scheme (NESAS) of the GSMA, the global interest group of mobile phone providers and manufacturers, and includes a review of the product development and life cycle processes as well as an evaluation of the product manufactured afterwards. During the reporting period, two companies, TÜV Informationstechnik GmbH and atsec information security GmbH, were recognised as testing bodies for NESAS CCS-GI. In January 2023, BSI issued the first NESAS CCS GI certificate for a 5G base station.

Based on the product characteristics and the different approaches to evaluation within the various certification schemes offered by the BSI, TR-03163 lists further certification schemes such as Common Criteria and Beschleunigte Sicherheitszertifizierung (BSZ), a fixed-time evaluation, for defined product classes. This promotes the use of products whose safety properties have already been tested in advance for their intended use.

12.1.3 — Auditing of Public 5G Network Operators

The IT Security Act 2.0 gave the BSI the task of auditing operators of public telecommunications networks and providers of publicly accessible telecommunications services with increased risk potential every two years. Audits in the area of 5G are carried out to determine whether the operators comply with the legal requirements for information security in the TKG. The requirements in the TKG include organisational, technical and operational framework conditions under which the telecommunications networks should be operated and the associated services are provided. For this purpose, the BSI developed a test scheme during the reporting period and, in consultation with the competent authorities, further defined the legal requirements with a basic audit procedure. The first audits will take place in 2023.

12.1.4 — IT-Grundschutz for Secure Private 5G Networks

With the deployment of private 5G networks, new requirements are arising for companies, public authorities, research institutions and other operators.

The BSI is addressing the question of how 5G networks can be operated securely and is using the IT-Grundschutz as a tried and tested, recognised tool for setting up and operating an Information Security Management System.

The "IT-Grundschutz profile for securing 5G campus networks – operation by an external service provider" is a guide that organisations can use to familiarise themselves with the topic of information and IT security in private 5G networks. Its risk analysis provides concrete recommendations for action to protect a 5G campus network. This template can be adapted to each individual company. The experience gained will serve as a basis for future blueprints for security concepts of 5G campus networks.

12.2 — Security in 5G and 6G Standardisation

The BSI is convinced that IT security concerns must be incorporated quite urgently into the development of standards for 6G already now. Moreover, sufficiently implementing IT security requirements as early as the standardisation stage is the basis for successful security certification. For this reason, the BSI is participating in various international standardisation organisations. The most important activities for securing mobile communication standards are listed below.

GlobalPlatform is an international industry standards organisation whose technology enables the technical management of applications on Secure Elements, SIM cards and Trusted Execution Environments.

The basis for NESAS CCS-GI is the NESAS test scheme published by the GSMA. The BSI is involved in the associated expert group and is working on the transition to a certification procedure. Additionally, the BSI is involved in ensuring the harmonisation of NESAS with the requirements for the EU5G certification scheme under the EU Cybersecurity Act.

The 3GPP develops the specifications for the UMTS (3G), LTE (4G) and 5G mobile radio standards, building on GSM (2G). Since 2022, the BSI has been involved with its own contributions on the topic of roaming and in the design of security tests in accordance with Security Assurance Specifications (SCAS). The SCAS define important safety functions that also form the basis for product certification according to NESAS CCS-GI.

So far, SCAS has been implemented with very different levels of accuracy. For this reason, the BSI defined refinements for 59 SCAS test cases. Under NESAS CCS-GI, these must be observed by the testing bodies and promote the comparability and comprehensibility of the results.

In the case of the Open RAN specifications of the O-RAN Alliance, which are intended to make further modularisation in radio access networks (RAN) possible, the BSI has commented on standardisation through both the European Telecommunications Standards Institute (ETSI) as well as through a study commissioned by the BSI that raised points of criticism of earlier O-RAN versions.

Standardisation of the emerging 6G technology has yet to happen. The BSI is already involved with security issues on the 6G Platform, a coordination platform for Germany funded by the BMBF. It allows for continuous communication with important German 6G research projects.

In order to promote standardisation in the organisations, the BSI uses its own test laboratory. With the aim of increasing the security level of mobile networks, the 5G/6G Security Lab TEMIS (Test Environment for Mobile Infrastructure Security) is currently being set up. The focus is on safety investigations of 5G components as well as the development and verification of security tests and specifications for 5G technology. In mid-2023, TEMIS will be in operation with mobile radio components from the first manufacturer.

12.3 — Promoting Cyber Security and Digital Sovereignty in Communication Technologies 5G/6G

Point 45 of the Federal Government's economic stimulus package (KoPa) seeks to address the consequences of the COVID-19 pandemic by promoting investments in future communication technologies (5G/6G). The BSI is implementing number 45 KoPa with its own funding programme "Cyber Security and Digital Sovereignty in 5G/6G Communication Technologies" as well as accompanying studies and procurements. The goals are to promote digital sovereignty and strengthen the innovative power of German companies in the context of IT security. Since the launch of the funding programme in June 2022, 32 projects have been approved.

13. — eID: Amendment of the eIDAS Regulation

One of the biggest threats to consumers in the current reporting period is identity theft and online fraud (see chapter *Insights from the Threat Landscape in Society*, page 51). Digital business processes have become increasingly important, and not just because of the COVID 19 pandemic. This also increased the need for secure electronic identification and secure electronic identities to ensure the integrity of digital processes and a high level of trust between the user and the service provider. This is a major factor in making online fraud and, in particular, identity theft more difficult. The BSI has been working for years to make the online ID function more accessible and to enable more use cases. With the Technical Guideline TR-03128 Part 3, the BSI has established the technical means for citizens to order a new PIN from home or to re-register online at the Registration Office. During the reporting period, the number of users of the PIN reset service increased, and electronic residence registration is currently being implemented as an EfA service of the State of Hamburg and is already being used there.

Under the eIDAS Regulation, EU member states accept mutually notified electronic identification (eID) methods in national applications. For example, it is currently possible to use a service in Germany with an Italian eID. During the reporting period, additional states issued directives notifying electronic identification systems for cross-border recognition, which will be subject to a mutual recognition obligation after a one-year transi-

tional period. The BSI has participated in peer reviews on this. In total, the recognition obligation now concerns 23 electronic identification systems from 18 different states across Europe.

For the use of electronic administrative services in other European countries, citizens can use their German eID card (identity card, electronic residence permit, Union citizen card) together with the online ID function for authentication and identification. The EU member states will be provided with software that translates the German eID system into the European eIDAS system: the eIDAS middleware. Currently, 20 countries and the European Commission are connected to the German eID system. During the reporting period, the European technical guidelines eIDAS Technical Specifications[31] were updated and extended to include additional identity attributes. Moreover, the stability and user-friendliness of the eIDAS middleware have been further improved to minimise downtime and make it easier to use. Furthermore, there are plans to improve the communication between the member states in order to inform them more quickly about changes to the interfaces between the national eID system and the European eIDAS system. This will further increase interconnectivity between member states.

In addition to many minor changes, the new draft regulation published in 2021 as part of the regular revision of the eIDAS Regulation includes a digital wallet, the "EU Digital Identity Wallet" (EUDI Wallet), which is intended to be usable as an electronic means of identification across borders. Apart from conventional identity attributes (first name, surname, etc.), this should be able to provide further attributes (e.g. educational qualification, driving licence) in a verifiable manner for service providers and also offer the option of a qualified electronic signature. During the reporting period, the development of the specifications for this EUDI Wallet made tremendous progress. In early 2023, the first version of the Architecture and Reference Framework (ARF), which is to serve as the basis for future transposition acts, was published by the European Commission. The BSI has been involved in the creation of this document and also in the further development of the ARF, is contributing the existing German infrastructure and is continuing to advocate for secure and user-friendly eID solutions that can be used across borders.

Within the scope of the EUDI Wallet, the Commission would like to demonstrate that the requirements can be implemented using large scale pilots (LSP) and launch one or more wallets on the market as pilots. Moreover, it is designed to give member states the opportunity to test other technologies and ideas not described by the ARF. The findings from the development of these wallets will also be incorporated into the current update and further development of the ARF and future documents.

Unlike the older eIDAS Regulation, which only stipulated the recognition of nationally existing eID schemes in partner states, member states will now be obliged to offer corresponding eID schemes within the framework of a wallet. Furthermore, both public bodies and large private companies that require identification of their users should accept the EUDI Wallet as a means of identification. The LSPs are designed to offer states that do not yet have a recognised eID solution the opportunity to reuse technical know-how.

Basic Structure of the eIDAS revision

Figure 20: Basic Structure of the eIDAS revision
Source: Federal Office for Information Security 2023

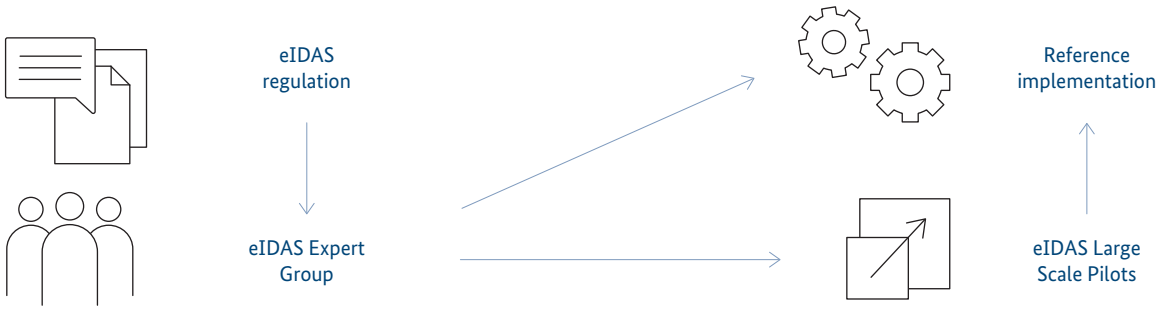
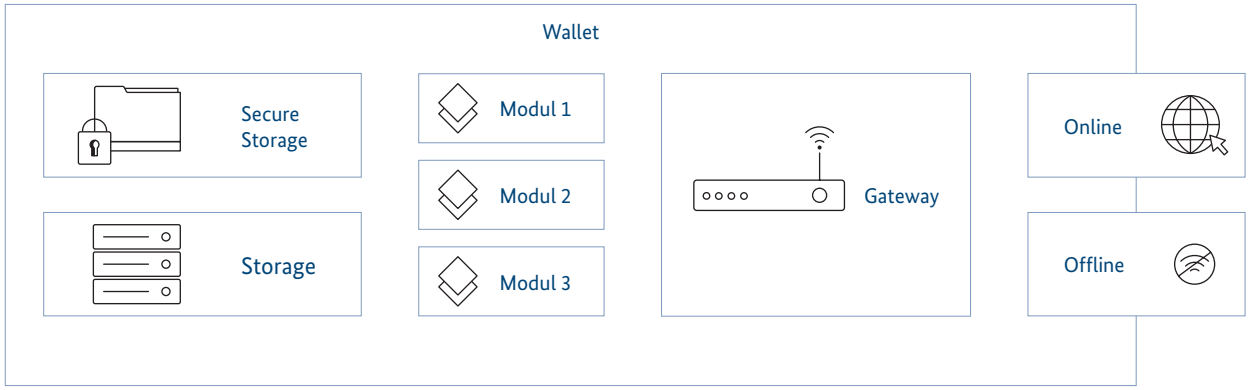


Diagram of module structure

Figure 21: Diagram of module structure
Source: Federal Office for Information Security 2023



The framework conditions under which the eIDAS Expert Group can implement a technical elaboration are defined in the negotiations on the eIDAS Regulation. This technique is being tested in the reference implementation and the eIDAS Large Scale Pilots. This will involve the LSPs using the reference wallet, a wallet implementation by the Commission, and field testing it to provide feedback on both the Expert Group and the development of the reference wallet.

For online identification, the BSI is currently working on implementing the online ID function in a wallet module. This will ensure that the current systems can continue to be used in order to reduce potential investments and to adopt the high level of trust already notified and recognised for the online ID function. By using a modular structure for the wallet, further possible uses can be implemented that do not have to rely on the existing technology, either because there are already internationally used standards or because these use cases do not require a high level of trust. Moreover, a modular approach allows for a technical separation between the standards that are designed to enable online communication and its use in offline use cases, which have to meet a completely different set of requirements without an internet connection. Modules can also be used to map various requirements for data storage, in addition to various requirements for protocols. For example, a smart eID would require storage in its own security chip, such as a Secure Element, while other credentials from the EUDI Wallet do not need these security requirements.

14. — Federal State Cooperation

With the increasing digitisation and networking of the federal government and the states comes an associated increase in attack surfaces (see Findings from the Threat Landscape in the State and Administration, page 67). Ransomware was the greatest threat to municipalities during the reporting period, in particular, as can be seen from the high number of ransomware attacks that were reported. (see incident *Ransomware Attacks on Local Administrations and Municipal Utilities*, page 69). Successfully shaping information security in administrative digitisation requires continued cooperation between the federal government and the states based on trust.

For this reason, the BSI further expanded its cooperation with the states during the reporting period. The goal is to create a uniformly high level of IT security in Germany. To this end, the BSI is actively involved, among other things, in the federal and state committees and shapes cooperation with the states through bilateral cooperation and event forums.

14.1 — National Liaison Office

The BSI has opened a total of five liaison offices since 2017, each of which is responsible for different regions in Germany. Creating direct points of contact makes the BSI more accessible across the country. This enables it to perform its tasks more efficiently and provide additional support in increasing the overall national level of cyber security in Germany. Regional associations, commercial enterprises and also local, state, federal and EU authorities have a short route to the BSI via the liaison offices and are closely supported in their concerns. The aim is to strengthen cooperation and networking and to make an important contribution to regional networking initiatives. An essential element of this is the conclusion of bilateral cooperation agreements between the BSI and interested federal states.

14.2 — Information Security Advisory Service for Federal States and Municipalities

The Information Security Advisory Service for the states and municipalities provides advice to specific target groups at the state and municipal level on all information security issues with a focus on information security management, security concepts and IT-Grundschutz.

Federal States

The advisory services for the federal states were expanded on the basis of the cooperation agreements concluded. In addition to the specific advice, practical approaches to solutions were further developed together with representatives from the federal government, the federal states and the municipalities. The focus was on IT-Grundschutz profiles and scalable instructions for the introduction and implementation of IT-Grundschutz. Particularly noteworthy in this context is the IT-Grundschutz profile "Quick Notifications – Securing Quick Notifications for Nationwide Parliamentary Elections", which was distributed via the Federal Election Commissioner at the beginning of the year.

Municipalities

Efficient cooperation with the almost 11,000 municipalities requires structured approaches that can only be carried out together with facilitators from the municipal umbrella organisations and institutions of the federal states.

Cyber attacks on municipalities can have far-reaching effects on the population, as a large part of administrative services for citizens are provided at this level. This makes it all the more important to support municipalities in the introduction and implementation of information security. This is why the Information Security Advisory Service supports raising awareness at the management level through congresses and conferences and provides information security officers with, among other things, a toolbox and specific assistance on IT-Grundschutz via its internal section for the federal states and municipalities. Moreover, an introductory step into the established methodology of IT-Grundschutz is currently being developed with the "Path to Basic Security – WiBA". WiBA is a bridge to the IT-Grundschutz profile Local Administration Basic Security developed exclusively for municipalities, in order to be able to implement OZG requirements, for example.

During the reporting period, the BSI assisted in the preparation of various handouts for managers in administrations on the initiative of the municipal umbrella organisations. These offer concrete assistance in how to take the first steps towards better information security.

14.3 — Municipal Roadshow

As already reported, the BSI is regularly made aware of successful cyber attacks on municipalities (see chapter *State and Local Administrations*, page 68). Due to the increasing cross-level networking, these attacks also represent a joint challenge for the federal government, the states and the municipalities. The BSI has therefore developed the Municipal Roadshow, a virtual series of events for municipalities, which is carried out together with interested federal states for the target group of municipalities.

The planning and implementation of the event will be carried out with the involvement of the states and municipal umbrella organisations. The BSI will contribute, among other things, presentations on fields such as the Information Security Advisory Service for the states and municipalities, National Liaison Office, CERT-Bund, BSI standards and IT-Grundschutz. Each federal state supplements this with different lectures tailored to the individual state.

The aim of the event is to raise awareness among municipalities regarding the threats in cyberspace and to show options for action to increase the level of cyber security.

During the reporting period, a total of six roadshows were held in the municipalities and reached well over 700 participants from the municipalities. Due to the positive response, the Municipal Roadshow will be continued and the topics will be further developed.

14.4 — Committee Work

The BSI collaborates in an advisory role in various federal and state bodies in the field of cyber and information security, for example in the Information Security Working Group of the IT Planning Council (AG InfoSic) and the State Working Group on Cyber Security (LAG Cybersicherheit) of the Standing Conference of Interior Ministers and Senators of the States (IMK).

Information Security Working Group

The BSI advises the Federal Government and the states on the implementation of the various action points of the IT Planning Council's "Guideline for Information Security in Public Administration", which defines the strategic cross-level goals for information security. The BSI contributes its expertise and actively participates in working groups, for example developing concepts for IT emergency management and a standard for the detection and defence of IT attacks. Moreover, the BSI operates the office of the Information Security Working Group and supports its chair (in the reporting period: Saxony and Saarland) in conducting the meetings.

State Working Group on Cyber Security

The Conference of the Ministers of the Interior (IMK) maintains the State Working Group on Cyber Security (LAG Cybersicherheit) for the purpose of coordinating transnational cooperation in the field of cyber security. The BSI contributed its expertise in various sub-working groups during the reporting period, for example in the Working Group on the Implementation of the Protocol Declaration of the IT Security Act. The aim of this working group is to improve information sharing between the BSI and the states.

14.5 — VerwaltungsCERT-Verbund (VCV)

Operational cooperation with the states is carried out via CERT-Bund within the framework of the VerwaltungsCERT-Verbund (VCV). The exchange of information within the VCV makes it possible to react more effectively and quickly to IT attacks nationwide. The 13 different state CERTs share situational incident information and discuss operational topics such as current vulnerabilities, the general situation and best-practice approaches in confidence. The joint exchange was intensified during the reporting period, partly in view of the increased threat level and was accompanied by bilateral talks, two hybrid working meetings and a visit by several state CERTs to the BSI.

14.6 — Cooperation Agreements between BSI and the Federal States

Bilateral cooperation agreements between the BSI and the federal states form the framework for cooperation and enable mutual support on an equal footing within the currently existing legal framework.

Pursuant to § 3 BSIG, the BSI can advise and warn the states on information security issues and, at their request, support them in securing their information technology and averting threats. Based on this framework, the BSI has developed a catalogue of fields of cooperation. The federal states can then select the cooperation they feel they need.

The states can add to these cooperative services with their own services, which the BSI can in turn use. All parties to this cooperation agreement, including the BSI and the federal states, benefit to the same extent. Each agreement can be tailored to the individual needs of the state and the BSI. During an annual work programme, cooperations, for example consultations on the establishment of a Information Security Management System, are specified and then successively implemented.

At the present time, the BSI has concluded four cooperation agreements with federal states. Further agreements are already planned or in the process of being concluded.

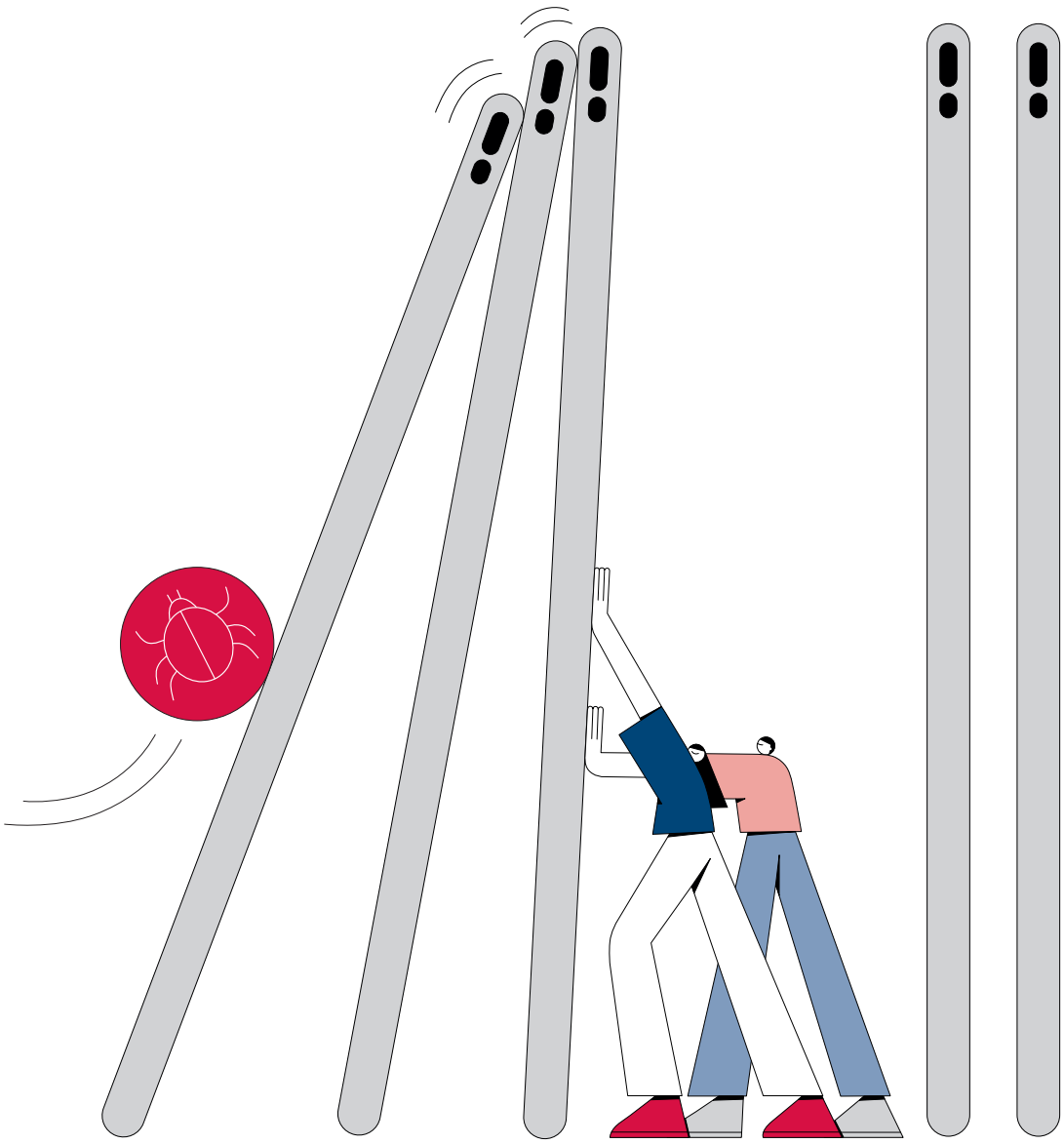
14.7 — Further Development of Cooperation with the Federal States

The cooperation agreements between the BSI and the federal states are an important milestone on the way to establishing binding federal-state cooperation in the area of cyber security. They make full use of the currently existing legal framework of cross-level cooperation.

However, there is a need for closer cooperation to better address current and future threats in cyberspace. For example, the BSI is not currently able to support the federal states in detecting malware in the state networks, for example by providing sensor technology. Meanwhile, it is beneficial to aim for a uniform federal and state overview in order to provide a more comprehensive view of the situation of information security in Germany. A connected picture of the situation makes it possible to identify trends in threats and cross-border phenomena more quickly and in greater detail, in comparison to individual surveys carried out in specific federal states. For this reason, the BMI, the BSI and the states are currently working on a concept for expanding the BSI into a central agency in the federal-state relationship, which will more closely reflect the legal basis for federal-state cooperation in the area of cyber security.

Currently, plans and requirements are being coordinated between the federal government and the federal states. The federal government's goal is to consolidate and deepen cooperation between the federal and state governments in the area of cyber security by amending the Basic Law.

Conclusion



Conclusion

15. — Conclusion

Resilience is More Important than Ever

The threat landscape in the field of cyber security continues to be characterised by high dynamics. The rapid development in the field of artificial intelligence shows how quickly technical innovations can progress. Alongside great opportunities for digitisation, this also poses a significant potential for threats. Once again, ransomware attacks remain the greatest threat to cyber security in Germany. At the same time, cyber attacks on supply chains are becoming more and more common. They can jeopardise the cyber security of entire industries.

In the current reporting period, the development of the threat landscape remains unchanged – it is considered to be tense to critical. Therefore, it is crucial to further enhance the resilience of the Federal Republic of Germany against cyber attacks and IT security incidents.

Ransomware: the Biggest Threat to Cyber Security in Germany

In the case of cyber attacks with ransomware, it can be observed during the reporting period that the previously dominant "Big Game Hunting" approach has declined. Instead of focusing on large, financially strong companies, cybercriminals have once again increasingly targeted small and medium-sized enterprises as well as state institutions and municipalities with ransomware attacks.

Local administrations and municipal businesses have also increasingly been affected by successful cyber attacks. Citizens are often also directly affected. Either because services for citizens are not available for weeks or because personal data ends up in the hands of criminals. This highlights the importance of resilience, which also encompasses the ability to regain the necessary operational capacity and return to normal as quickly as possible after an IT security incident.

Professionalisation of Cybercrime Continues

A steadily advancing division of labour and professionalisation among cybercriminals can be observed in cybercrime, which is increasingly taking on the characteristics of a service-oriented industry. The black market economy of cybercrime is thus mirroring the real economy to a certain extent, which also relies on a strong division of labour and is becoming increasingly connected across national and industry borders.

This expansion of cybercrime-as-a-service is a prominent factor in the evolution of the threat landscape, as specialisation in specific services allows attackers to target and professionalise their services strategically. The only way to counteract this is to professionalise defence. One way of doing this is through qualified security experts – service providers who, for their part, need to be particularly well protected. Through standardisation and centralisation, municipalities and small and medium-sized enterprises can strengthen their cyber resilience. Basic protection in line with the IT-Grundschutz for municipalities or the cyber security check for companies are effective tools for this.

Concerning Levels of Software Vulnerabilities

A worrying development was also observed in the area of vulnerabilities. Significant increases were registered primarily in software product vulnerabilities. Such gaps are often the initial entry point for cybercriminals on their way to compromising systems and networks. Increasing and extensive interconnectivity makes the systems accessible from the outside in the first place and at the same time allows attackers to operate remotely.

During the reporting period, an average of almost 70 new vulnerabilities in software products were reported every day, approximately 25 per cent more than in the previous reporting period. As the number of vulnerabilities found increased, so did their potential harmful effect. 3,784 of the identified gaps were classified as critical (previously: 2,680), constituting 15 per cent of all detected vulnera-

bilities. The development in both quantity and criticality are cause for concern. The BSI is countering this with initiatives for the (partial) automation of corporate and security processes, for example by automatically filtering the reporting of security vulnerabilities for relevance to their own systems. The technical basis for this is the Common Security Advisory Format (CSAF) specified by the BSI, among others, which makes security advisories machine-readable and automatically processable.

Generative AI: Opportunity and Risk for Cyber Security

The emergence of generative artificial intelligence presents to new challenges in the security sector. With the release of ChatGPT and a variety of other tools, AI has also made its way to a broad, less tech-savvy public. AI large language models behind models such as ChatGPT, LLaMA or Bard are partly freely available. The high quality of AI-generated text and images has contributed to their rise, as has the ease of access to these and other tools, including deepfakes. Manipulated images, videos and voices are becoming more and more authentic due to the continuous increase in the quality of publicly available tools, making them harder to expose.

This has many consequences. In addition to already known attacks such as CEO fraud or the grandparent scam, the above tools are also being tested by cyber criminals for further usability in attacks, for example in the generation of malicious code or in social engineering and disinformation campaigns. In addition to the scaling of these well-known threats, new threats are emerging due to new technology and the associated increase in the attack surface. Artificial intelligence itself is vulnerable and can be a weak point. Due in part to the vagueness in the design of AI and LLM, corporate and government vulnerability management is facing unprecedented challenges.

Besides these security risks, the big challenge is keeping pace up with the rapid development in the field of AI. The aim must be to provide information about possible security risks when using AI in order to be handle the capabilities and outputs of these models responsibly. This involves the need for technical measures to identify the output of AI. In addition, manufacturers and providers of LLMs and LLM-based applications must take precautions to prevent or discourage the generation of potentially harmful outputs as far as possible.

Effects of the War in Ukraine on the State of IT Security in Germany

The Russian war of aggression against the Ukraine continued to occupy a central place in public consciousness during the reporting period. The registered DDoS attacks by pro-Russian activists have so far caused little to no lasting damage. Since this is also largely due to the chosen type of attack, DDoS, the attacks so far are more likely to be classified as propaganda – with the aim of creating uncertainty and undermining trust in the state. The past has shown that this can change at any time, for example through collateral damage or attacks on critical infrastructure. This can be successfully countered with a strong cyber resilience and security precautions adapted to the situation.

Successful Digitisation Requires Vigilance and the Ability to Act

Cyber resilience means being able to deal with attacks without collapsing. Cyber resilience also means being able to get back on your feet quickly after falling victim to a cyber attack – and being able to defend yourself if necessary. In order to achieve this, a sustainable cyber security architecture is required.

The BSI sees itself as a central body in Germany's security architecture that offers all stakeholders options for action and support measures. This central position not only enhances efficiency, but is also suitable for the sustainable use of resources. For this reason, the BSI welcomes the federal government's plans to expand the BSI into a central agency in the federal-state relationship.

Cyber security is a joint task of the federal government, the states and the municipalities, which can only be managed by adequate use of resources. However, this

alone is not sufficient. Continuous exchange between policymakers, business, science and society is necessary – in Germany, but also across national borders.

Increase Resilience - Shape Cyber Security - Accelerate Digitisation

The federal government's National Security Strategy emphasises the significantly increased importance of cyber security. And rightly so, as the BSI situation report shows. As the national cyber security authority, the BSI sees its mission in,

- increase resilience as quickly as possible to withstand attacks,
- making cyber security pragmatic in order to stay one step ahead of attackers,
- accelerating digitisation to keep up with current developments.

All this can be achieved if the BSI's positions are heard, its specifications implemented and its products used. The BSI will make its contribution by fulfilling its role as a partner, helper and enabler even more strongly in the future: with standards that can be implemented realistically and solutions that are easy to apply for the state, the industry and society A guiding principle that drives us forward: isolation is not the goal - cooperation is the key to success.

Glossary

Access Broker
Access brokers are cybercriminals who gain access to a victim network through a wide variety of channels and regularly sell this access to other cybercriminals or interested parties.

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

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

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

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

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

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

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

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

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

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

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

Bug Bounty
Monetary rewards (bounty) for finding vulnerabilities (bugs). Software product manufacturers use legitimate bug bounty programmes to reward security researchers for finding and reporting a vulnerability in their product.

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

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

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

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

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

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

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

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

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

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

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

Exploit
An exploit is a method or programme code that can be used to execute unintended commands or functions via a vulnerability in hardware or software components. Depending on the type of vulnerability, exploits can be used, for example, to crash a programme, extend user rights or execute arbitrary programme code.

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

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

Information Stealer
A type of malware that allows cybercriminals to obtain various types of personal data, such as login details for various online services on infected devices without the people affected noticing.

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

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

Legitimate Programmes
Programmes that perform harmless, desired operations.

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

Malicious
Bad, harmful. In IT security, programmes or websites that can perform harmful operations on a computer system are called malicious.

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

Mark-of-the-Web / MOTW
MOTW identifies download files if they are likely to be from an untrusted source. If a user opens a file marked with this, they will be warned accordingly.

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

NESAS
5G Network Equipment Security Assurance Scheme.

NESAS CCS-GI
The National Certification Scheme for 5G Mobile Equipment (NESAS Cybersecurity Certification Scheme – German Implementation).

Network Attached Storage (NAS)
A storage device connected to a network that allows authorised network users and clients to store and retrieve data in a central location.

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

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

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

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

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

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

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

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

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

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

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

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

Script Kiddies
Attackers who, despite a lack of knowledge, attempt to penetrate other people's computer systems or cause damage in general.

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

Security Assurance Specification (SCAS)
Security Assurance Specifications (SCAS) define important safety functions that also form the basis for product certification according to NESAS CCS-GI..

Security by Design
Manufacturers follow the principle of security by design when information security requirements are already taken into account during the development of a product.

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

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

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

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

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

Stack Overflow
A stack overflow or buffer overflow is a frequently occurring and frequently exploited vulnerability. A buffer overflow occurs when more data is successfully written to a memory than the designated buffer can hold. Data is thus also written to adjacent memory areas. This can result in programme crashes, compromising of data, obtaining of extended rights or execution of malicious code.

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

UP KRITIS
The Implementation Plan for Critical Infrastructures (UP KRITIS) is a public-private cooperation between operators of critical infrastructure (KRITIS), their associations and government agencies such as the BSI.

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

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

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

Two and Multi-Factor Authentication (2FA or MFA)
In two- or multi-factor authentication, the authentication of an identity is done using different authentication factors from separate categories (knowledge, possession or biometric characteristics).

Bibliography

1) https://www.heise.de/news/Mehrere-Verhaftungen-Strafverfolger-gehen-gegen-D*DoS*-Booter-Dienste-vor-7396504.html
2) https://www.hertzbleed.com/hertzbleed.pdf
3) https://eprint.iacr.org/2022/975
4) https://samcurry.net/web-hackers-vs-the-auto-industry/
5) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/onlineshopping-plattformen.html
6) https://www.verbraucherzentrale.de/geld-versicherungen/phishingradar-archiv-71872
7) https://www.verbraucherzentrale.de/geld-versicherungen/phishingradar-archiv-71872
8) Studie des TÜV-Verbandes: „2023: Cybersicherheit in deutschen Unternehmen“
9) https://de.statista.com/infografik/26033/ausgaben-fuer-it-sicherheit-in-deutschland
10) https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022
11) https://www.dihk.de/resource/blob/91514/be8371c167a1468d387fdaa075327330/dihk-sonderauswertung-cybersicherheit-2023-data.pdf
12) https://eur-lex.europa.eu/eli/dir/2022/2555/oj
13) https://eur-lex.europa.eu/eli/dir/2022/2557/oj
14) https://www.bsi.bund.de/OHNachweise
15) https://www.dihk.de/resource/blob/91514/be8371c167a1468d387fdaa075327330/dihk-sonderauswertung-cybersicherheit-2023-data.pdf
16) https://www.dihk.de/resource/blob/91516/aac9a26dea81dc7c1bc1e5f28b6105e8/dihk-digitalisierungsumfrage-2022-2023-data.pdf
17) NKMG mbH & BIGS gGmbh im Auftrag des Bundesministeriums für Wirtschaft und Energie: IT-Dienstleister als Akteure zur Stärkung der IT-Sicherheit bei KMU in Deutschland, 2021, S. 5
18) https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/KI/AIMobilityAuditPrep_final_results.pdf
19) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Branchenlagebild/branchenlagebild-automotive.html
20) https://www.vice.com/en/article/dy7axa/how-i-broke-into-a-bank-account-with-an-ai-generated-voice
21) https://iopscience.iop.org/article/10.1088/2058-9565/ab4eb5/pdf
22) https://www.bsi.bund.de/dok/QML
23) https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/, https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf
24) https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.pdf
25) https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf
26) https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/cybersicherheitsagenda-20-legislatur.pdf
27) https://dserver.bundestag.de/btd/20/066/2006610.pdf
28) https://csrc.nist.gov/publications/detail/nistir/8413/final
29) https://www.bsi.bund.de/dok/umfrage-pqc
30) https://www.etsi.org/deliver/etsi_gs/QKD/001_099/016/01.01.01_60/gs_QKD016v010101p.pdf
31) https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eIDAS+eID+Profile

Register of QR Codes Included in the Report

a) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/dvs-bericht_2022.html
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Branchenlagebild/branchenlagebild-automotive-2022-2023.html
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Lagebild_Gesundheit_2022.html
https://www.bsi.bund.de/EN/Service-Navi/Publikationen/publikationen_node.html

b) https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/botnet_node.html

c) https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefaehrdungen/APT/apt_node.html
https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Ransomware-Angriffe/ransomware-angriffe_node.html
https://www.bsi.bund.de/EN/IT-Sicherheitsvorfall/it-sicherheitsvorfall_node.html
https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/cyber-sicherheitsnetzwerk_node.html

d) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister_APT-Response-Liste.pdf

e) https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefaehrdungen/DDoS/ddos_node.html

f) https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html

g) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Branchenlagebild/branchenlagebild-automotive-2022-2023.pdf

h) https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Unternehmen-allgemein/IT-Notfallkarte/Massnahmenkatalog/massnahmenkatalog_node.html

i) https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/Notfallkarte/One-Pager_Einstieg_ins_IT-Notfallmanagement_KMU.pdf

j) https://www.bsi.bund.de/EN/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/kritis_node.html

k) https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/KMU/KMU_node.html

l) https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/KMU/CyberRisikoCheck/CyberRisikoCheck_node.html

m) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KI/Grosse_KI_Sprachmodelle.pdf

n) https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Automotive/Automatisiertes_Fahren/Automatisiertes_Fahren_node.html

o) https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/KI/Security-of-AI-systems_fundamentals_considerations_symbolic_hybrid.pdf
https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Studien/ML-SAST/ml-sast_node.html
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/KI/P464_Provision_use_external_data_trained_models.pdf

p) https://www.bsi.bund.de/qcstudie

q) https://www.bsi.bund.de/PQ-Migration

r) https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html

s) https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03163/tr03163_node.html

Published by
Federal Office for Information Security (BSI)

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

E-Mail
bsi@bsi.bund.de

Telephone
+49 (0) 22899 9582-0

Fax
+49 (0) 22899 9582-5400

Last updated
October 2023

Printed by
Appel & Klinger Druck und Medien GmbH, Schneckenlohe

Concept, editing and design
Faktor 3 AG

Texts and editing
Federal Office for Information Security (BSI)

Illustrations
Anne Albert c/o kombinatrotweiss.de
Instagram: annealbert_illustration | kombinatrotweiss_illustration

Graphics
Federal Office for Information Security (BSI)

Picture credits
Page 2: © BMI; Page 4: © BMI/Henning Schacht

Article number
BSI-LB23/512e