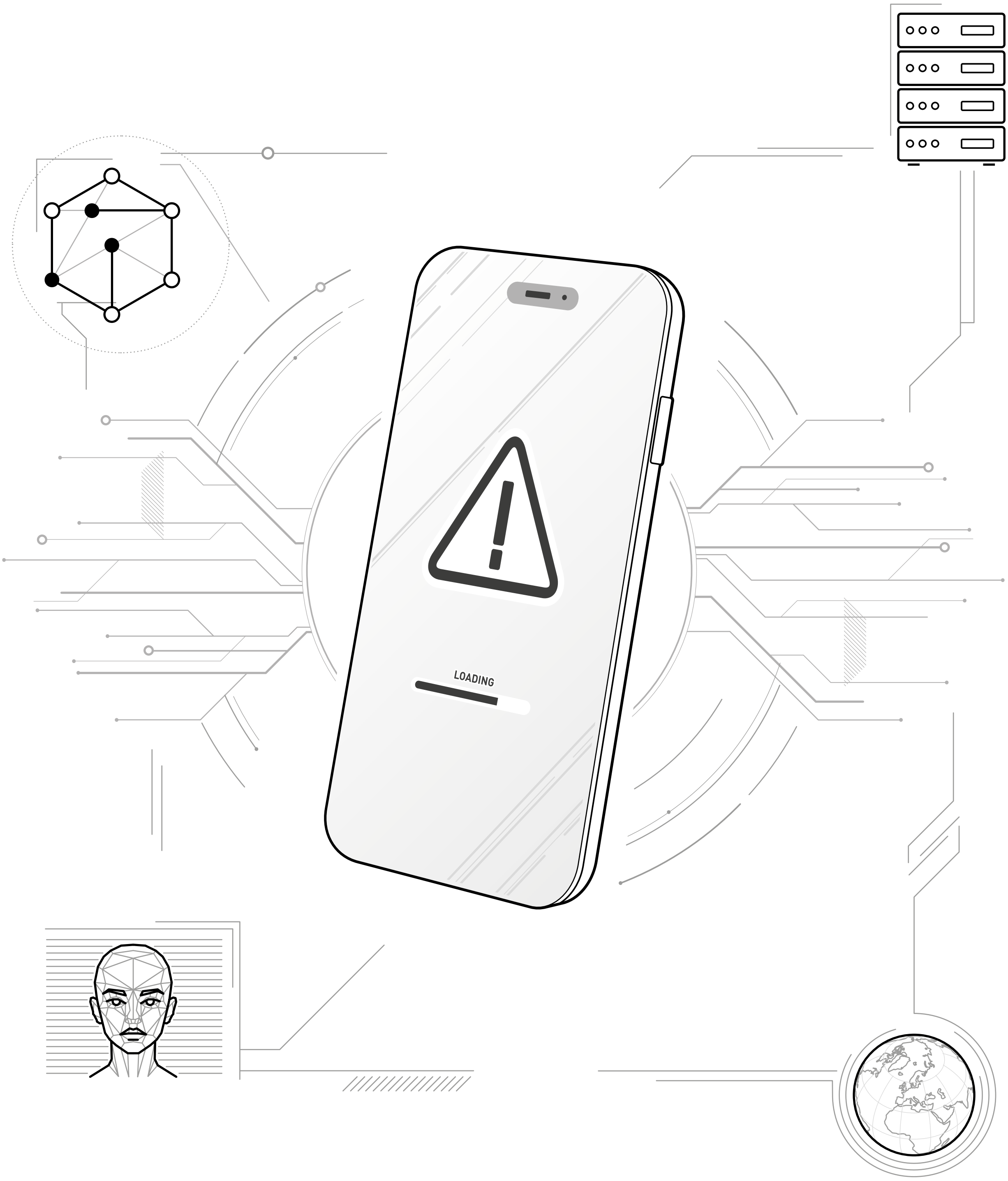
THE STATE OF IT SECURITY IN GERMANY IN 2024



Federal Office
for Information Security

TABLE OF CONTENTS

List of Selected Incidents

List of Figures

FOREWORD

The opportunities opened up by the increasing digitalisation of almost all areas of our lives are manifold. However, the ways in which these digital spaces can be used for hybrid attacks and criminal activities are also manifold. The Russian war of aggression against Ukraine, and its consequences, also mark a turning point for internal security. The threat level in the area of cybersecurity remains high. The Federal Government is therefore acting decisively to further increase Germany's resilience to cyber threats.

In 2024, German IT security legislation was comprehensively modernised and restructured. With the transposition of the second EU Directive on the security of network and information systems (NIS-2) into German law, more companies in more sectors are now obliged to implement cybersecurity measures and report cyber attacks. We are also strengthening the cybersecurity of the federal administration. The Cyber Resilience Act (CRA) implements cybersecurity in additional sectors: in future, manufacturers or importers of networkable products will have to ensure not only operational security, but also information security.

All these new rules create more security. However, they also pose a challenge – for the companies concerned as well as for the Federal Office for Information Security (BSI), which will play a key role in future with new supervisory instruments. The Federal Office for Information Security actively supports companies, and its offerings are already widely used. This is good news, because the damage caused by cyber attacks year after year is immense – for business, administration and society.

In a digitalised world, defence against cyber attacks is important for the resilience of our liberal democracy as a whole. It is therefore worth accepting the challenge. This report on the state of IT security in Germany is an important contribution to greater resilience as it helps us to understand, prevent and recognise threats in cyberspace. I would like to thank everyone who has contributed to this report and wish you an engaging read with lots of interesting information on cybersecurity in Germany.

Nancy Faeser,
Federal Minister of the Interior and Community

FOREWORD

CRA, CSA, RED, NIS 2 and DORA … No, this is not a list of mysterious chemical substances. All these abbreviations refer to laws, regulations and directives on cybersecurity in Europe that recently came into force or are about to do so. These regulations stem from an immense need for action we face with regard to cyberattacks and IT security incidents, and it is obvious that there is a need and urgency to act on a broad scale.

For anyone who would like to see a more "tangible" illustration of the need for action, I would like to remind you of 19 July 2024 – the day on which a faulty update in a security product from the manufacturer CrowdStrike brought IT operations to a standstill worldwide – and with them, operating theatres in hospitals, international flight operations and the production operations of countless businesses. The economic damage is still impossible to quantify, as is the damage to the trust in our digitalised world. And we must always bear in mind that this was not a cyberattack, "only" an operational error.

In an almost textbook manner, this incident has demonstrated how the responsibility for secure digitalisation is shared by multiple stakeholders: by manufacturers for secure and bug-free products; by operators for resilient infrastructures and processes; and by state institutions for protection and prevention as well as a rapid and comprehensive assessment of the situation and appropriate reactive measures. Only when we can confidently assert that we are living up to this responsibility, can and should we begin discussing how each individual citizen can contribute to secure digitalisation.

Unfortunately, the regulatory initiatives mentioned above are not only necessary for the protection of businesses and authorities, but also for all of us as citizens. The Cyber Resilience Act (CRA) will mean that manufacturers have to ensure the cybersecurity of their products in order to obtain the established CE mark for these products. When NIS 2 (Network and Information Security Directive) comes into force, we as the BSI will provide support for around 30,000 businesses and organisations, which will be required to demonstrate IT security measures to us and report IT security incidents in the future. The other regulatory projects also aim to make our digital world more secure, i.e. for cloud products, wireless devices or in the financial sector.

Of course, regulations always entail costs for both businesses and manufacturers – and for supervisory authorities. The BSI will work consistently and in a highly cooperative, advisory and supportive manner to strengthen cybersecurity in Germany and Europe – not just from the sidelines, but directly on the pitch.

One of our key plans for the coming years is to make cybersecurity in Germany measurable – because what can be measured can also be improved. This year's report on the state of IT security in Germany forms the basis for this. It shows us that the threat situation is still worrying and that it is up to us to improve it.

We consider targeted cyberattacks against state and political institutions and AI-boosted disinformation campaigns to be attacks on our democracy, something we are resolutely opposed to. Ransomware attacks, known as encryption Trojans, have once again hit many local authorities, directly affecting citizens. Countless businesses have also fallen victim to cybercriminals. It is essential that we protect ourselves and that local authorities and businesses protect themselves better. The same goes for cyber espionage attacks. Last but not least, DDoS attacks (volumetric flood attacks) continue to be used in particular by supporters of the Russian war of aggression, which violates international law, for the purpose of propaganda.

However, this incomplete list of dangers and threats is no reason for us to bury our heads in the sand. Yes, the attackers are getting better and faster. But so are we – and that's the good news. We are not defenceless against threats from cyberspace! The BSI Situation Report 2024 also confirms that our measures are working.

That is why it is so important to keep up the good work and go the extra mile together. Businesses and manufacturers, researchers, civil society and public institutions must all work together to make the digital world safer today and tomorrow. This is why we at the BSI are vigorously pursuing the goal of making Germany a cybernation. Let's make this vision a reality together.

Claudia Plattner,
President of the Federal Office for Information Security

1 – Introduction

The Federal Office for Information Security (BSI) is the Federal Cyber Security Authority and continuously monitors the IT security threat situation in Germany. The BSI focuses on the detection of cyberattacks on state and public institutions, businesses and private individuals, but also on measures for the prevention and defence of specific threats to the availability, integrity or confidentiality of communications technology. In particular, the BSI implements these measures in co-operation with the police authorities that are responsible for security and law enforcement.

The economic, governmental and social damage caused by threats in cyberspace is immense. This is why the BSI launched the Cybernation Deutschland initiative in January 2024. In addition to increasing cyber resilience, the initiative aims to raise awareness of cybersecurity in general, make cybersecurity pragmatic and measurable, make better use of technological expertise and strengthen the market for cybersecurity products and services in Germany.

This report presents the most important developments for the reporting period from 1 July 2023 to 30 June 2024. The current reporting period again covers twelve months, while the previous reporting period covered a one-off period of 13 months in order to adapt to quarterly formats. Direct comparisons of absolute figures are therefore not possible. This report uses directly comparable daily or monthly averages wherever possible.

1.1 Summary and Assessment

The IT security situation in Germany was tense during the period under review. The cybercriminal black market economy continued to be clearly split between ransomware operators, their affiliates and access brokers. At the same time, it used alternative attack surfaces, such as zero-day vulnerabilities (for which there are no security updates yet), with the aim of exfiltrating data in order to extort high ransoms without ransomware by threatening to publicise the data. In addition to mostly small and medium-sized businesses, the main victims were IT service providers and, once again, local authorities. In the area of cyber espionage and sabotage, however, the trend towards relatively simple attacks on perimeter systems continued. In particular, attackers exaggerated the damaging effects of Distributed Denial of Service (DDoS) hacktivist attacks in the context of geopolitical conflicts on social media in order to fuel general social insecurity.

Along with the increase in threats and hazards, an increase in Germany’s resilience as a cybernation was also noticeable. For instance, international law enforcement agencies were successful in curbing the growth of new malware variants through a series of takedowns.

However, as digitalisation becomes more widespread, there is a need for action, particularly with regards to attack surfaces. Every business, every government agency, every scientific or social organisation, every individual entrepreneur – the whole of Germany is called upon to identify and protect its attack surfaces. This is challenging in historically grown IT landscapes, but necessary as attackers are constantly looking for new ways to attack.

The situation in detail:

(1) Threat:

Ransomware groups: Cybercriminals are professionalising their methods, keeping up with the latest technology and acting aggressively. More and more cybercriminals are delaying the detection of their attacks by disabling endpoint detection and response (EDR) systems on infected networks. This is done using special malware variants, which are increasingly being offered as a service (Malware-as-a-Service, MaaS), making them accessible to many attackers. In addition, access brokers who trade in stolen access data have become an established part of the cybercriminal black market economy. The reporting period also showed that cybercriminal attackers have the necessary resources to track down zero-day vulnerabilities and exploit them for data exfiltration, as was the case with the attackers behind the Clop ransomware. Due to the high ransoms already paid in the past, this risk will continue to exist for the unforeseeable future.

Advanced Persistent Threats (APT): During the reporting period, 22 different APT groups were active in Germany.

Their attacks targeted public authorities and businesses, particularly in the fields of foreign affairs, defence and public safety and order. A number of other developments shaped the APT threat landscape. Once again, it became clear that geopolitical and international conflicts are often accompanied by a whole range of phenomena in cyberspace: disinformation, hacktivism, espionage and sabotage were evident both in the Russian war of aggression against Ukraine and in the aftermath of Hamas' terrorist attack on Israel. A large proportion of cyber activities remain limited to specific regions.

In addition, attackers exaggerate the impact of sabotage or DDoS attacks on social media in order to use this form of "public relations" to create a greater feeling of uncertainty in the targeted regions than would otherwise be justified by the often limited damage.

(2) Attack Surface:

Vulnerabilities: In 2023, an average of 78 new vulnerabilities became known every day. As part of the coordinated vulnerability disclosure process, the BSI also received an average of 18 reports of zero-day vulnerabilities in IT products from German vendors per month.

Vulnerabilities in perimeters: A large number of critical vulnerabilities in perimeter systems such as firewalls and VPNs were also disclosed during the period. Some of these were particularly dangerous zero-day vulnerabilities that were already known to cyberattackers and were exploited before the manufacturers of the affected products were able to provide patches. The trend towards simple and uncomplicated attacks on perimeter systems, which has been observed for a number of years, continued and intensified during the reporting period.

(3) Attack:

DDoS attacks: DDoS attacks were a notable development in the reporting period. The quality and frequency of DDoS attacks increased significantly, particularly in the first half of 2024. The proportion of high-volume DDoS attacks with a bandwidth of over 10,000 megabits per second averaged 13 per cent per month, more than double the long-term average of 6.75 per cent. If the trend continues, this would indicate that attackers have specifically built up botnet capacities and that more high-volume DDoS attacks can be expected in the future.

Ransomware attacks: Cyberattacks, particularly against commercial enterprises, continued to be widespread in the current reporting period. On the one hand, large enterprises with strong sales continued to be attacked. On the other hand, ransomware attacks in particular have also become mass business due to the lower technological effort involved in using Ransomware-as-a-Service (RaaS): small and medium-sized enterprises (SMEs), but also municipalities, universities and research institutions, are increasingly affected. The attackers often continue to take the path of least resistance. Even if targeted attacks on high-revenue businesses continue to be registered, criminals tend to choose the most vulnerable victims. Organisations are more likely to fall victim to cyberattacks the less they protect their vulnerabilities.

Attacks on cloud infrastructures: During the reporting period, there were several successful ransomware attacks on public cloud services, limiting their availability. There have also been several known cases of attacks on the confidentiality of cloud services through identity theft, both of users' identities and of the provider's staff. In September 2023, suspected Chinese state-sponsored cyberattackers gained access to the Microsoft cloud infrastructure using a previously compromised signature key. Due to a validation error, the signature key could be used for both consumer and enterprise accounts, allowing the attackers to impersonate legitimate users.

Attacks on political organisations: During the reporting period, incidents were reported in which the email inboxes of various political organisations were attacked. State-sponsored actors in particular used various methods to access emails. These included attacks with weak or recycled passwords, via zero-day vulnerabilities or phishing attacks. Webmail systems are particularly vulnerable. They can be accessed freely over the internet without multi-factor authentication.

(4) Impact:

IT service providers were the target of attack campaigns in 2023. Cyberattacks on IT service providers have a significant impact on their customers. One such ransomware attack became known in the reporting period, which affected around 20,000 workplaces in 72 municipalities with a total population of around 1.7 million people. The service provider that was attacked shut down most of its systems, resulting in the unavailability of many municipal services, such as social benefits, parental benefits and vehicle registration, as well as the limited operation of public registries and municipal planning authorities. At the time this report was published, the service provider was still in the restart phase, during which certain specialised procedures had been restored or were running in basic mode, while other specialised procedures were still unavailable.

Compared to the previous reporting period, the number of suspected victims of data leaks resulting from ransomware attacks continued to increase. In the second half of 2023, the number of suspected leakage victims even briefly doubled compared to the reference year 2021. The continued high to very high level of activity by the most threatening actors is likely to be the main factor behind this increase. The BSI also noted the presence of several leak pages that were active for a relatively brief period or included a significant number of potential victims through individual campaigns.

Two zero-day vulnerabilities at IT service providers resulted in significant damage in the current reporting period. A ransomware group exploited these vulnerabilities to exfiltrate data without the use of any ransomware. The amount of ransom money extorted continued to rise during the reporting period compared to the previous reporting period. Victims generally had to pay significantly higher ransoms for exfiltrated data than for encrypted data.

Consumer data was also affected by data leaks during the reporting period. Cybercriminals exploited server vulnerabilities and open or incorrectly configured servers, allowing them to extract data and sell it illicitly for further cyberattacks. In the course of data leaks by ransomware groups, some consumers' personal data were also affected. Names and email addresses, postal addresses, dates of birth and telephone numbers were the most frequently leaked consumer data.

(5) Resilience:

Takedowns: During the reporting period, law enforcement officers managed to take down several RaaS in internationally coordinated measures, including the previously very active dropper/loader malware QakBot (August 2023), the RagnarLocker RaaS (October 2023), Alphv (December 2023) and LockBit (February 2024).

Resilience at federal administration level: During the reporting period, the BSI undertook a comprehensive analysis of the federal administration's infrastructure with a view to identifying potential vulnerabilities. On average, 15 vulnerability warnings were issued daily to the relevant authorities. Furthermore, the federal administration has been successful in blocking approximately 368 additional malicious websites from access on average each day, along with an average of 9,212 attempts to access malicious websites. To help safeguard against potential malware risks associated with email communications, an average of around 753,000 emails daily were also reviewed to identify any potentially unwanted content or malicious attachments.

Resilience in cloud infrastructures: Cloud-intrinsic capabilities, such as comprehensive logging and detection options, help to detect and contain any attacks. The high degree of automation inherent in cloud services serves to enhance users' resilience to attacks. This is achieved, for instance, through the prompt installation of security patches and the implementation of preventive measures, detection measures and responsive measures that align with the latest developments in the cyber threat landscape.

Resilience of critical infrastructures: Operators of critical infrastructures (CIs) are obliged to use an information security management system (ISMS) to increase their preventive capabilities and a business continuity management system (BCMS) to increase their coping capabilities. A mandatory biennial maturity assessment provides information on the effectiveness of these systems. According to the survey, 140 out of 671 operators were able to improve the maturity level of their ISMS in the last two years. The BCMSs of 114 operators were improved by at least one maturity level. Overall, the resilience of CI operators subject to reporting requirements was therefore at a medium level on the 5-level maturity scale. Overall, a slightly positive trend is recognisable here.

Electronic identities and security of mobile devices: In accordance with the eIDAS Regulation 2.0, which came into effect on 21 May 2024, the development of a European Digital Identity Wallet (EUDIW) has been authorised, among other things. The EUDI wallet should therefore be capable of functioning as an electronic means of identification across national borders. In addition to the conventional identity attributes, such as first name, surname, etc., it should also be able to provide other attributes, such as educational qualification and driving licence in a verifiable manner for service providers. Furthermore, the EUDI wallet will provide the option of utilising qualified electronic signatures.

European legislation on cyber resilience: The EU is tackling the problems in cyberspace with various legal regulations. In the present reporting period, the incorporation of the NIS 2 Directive into the domestic legal framework was initiated. In particular, the directive introduces new reporting obligations regarding IT security incidents for operators of organisations designated as “important” and “particularly important”. In Germany, this includes several tens of thousands of businesses and other organisations. This will not only result in a notable enhancement of the cybersecurity situation in Germany, but facilitate the implementation of cybersecurity measures in the future, thereby enhancing overall cybersecurity.

While NIS 2 focuses on operators and users, the Cyber Resilience Act (CRA) contains regulations at the product and manufacturer level. The CRA was adopted by the European Parliament in March 2024 and is due to come into force in the autumn. It regulates the access requirements for connected devices (IoT) to the European Single Market – from robotic vacuum cleaners and software to products used in critical sectors. This includes basic product requirements such as security by design, security by default and ensuring the confidentiality and integrity of the processed data. In addition, the CRA includes requirements for manufacturers to deal with vulnerabilities, for example the obligation to provide security updates throughout the entire life cycle of the product and to report and rectify vulnerabilities.

1.2 The Systematics of BSI Situation Monitoring

The BSI monitors the situation in Germany as a cybernation in terms of (1) Threat, (2) Attack Surface, (3) Attack, (4) Impact and (5) Resilience. In the event of a threat such as a malware programme coming into contact with a vulnerability, e.g. a web server, the risk of an adverse event occurring is heightened. Threats are cyberattacks that, depending on your level of preparedness (e.g. security update status), can result in data leakage or other adverse effects. To put it another way, weaknesses (vulnerabilities) are exploited by actors (threats) to cause harm (impact).

(1) Threat

The keyword threat describes phenomena in the cyber world that can pose a risk to cybersecurity. These threats, hereinafter referred to as “cyber threats,”exist independently of specific victims or specific attacks and can potentially manifest themselves in a specific attack at any time. Cyber threats include things such as ransomware groups, botnets, new malware variants, exploits, access brokers and APT groups. The term therefore includes the attackers, their attack infrastructures and their specific means of attack (see mainly part A Threat, page 14).

(2) Attack Surface

Vulnerability includes all IT systems, components and services that an attacker can exploit or misuse for a cyberattack. Attackers find the largest vulnerabilities in cyberspace in the form of IP addresses, domains and URLs as well as email addresses and weak points. As digitalisation increases, so does the vulnerability to cyberattacks. However, if preventive measures such as network segmentation or effective patch management do not keep pace or are lacking, vulnerability will also grow faster than these measures. Incorrectly configured servers or vulnerable applications can be the result (see mainly part B Attack Surface, page 30).

(3) Attack

The term attack refers to specific cyberattacks. Important attacks include ransomware attacks, in which data is encrypted or exfiltrated in order to extort ransom money from victims, or espionage attacks by APT groups that want to steal information or technology in the form of software code. The attack situation may differ depending

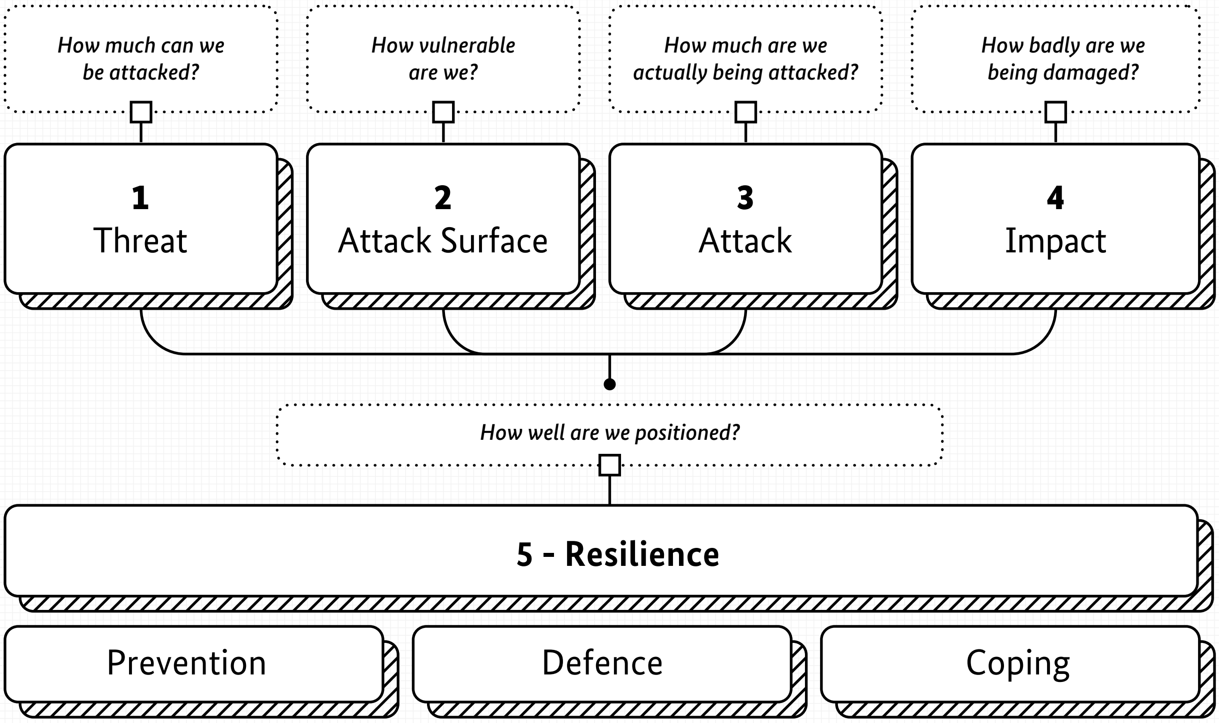

How much can we be attacked?
How vulnerable are we?
How much are we actually being attacked?
How badly are we being damaged?
1 Threat
2 Attack Surface
3 Attack
4 Impact
How well are we positioned?
5 - Resilience
Prevention
Defence
Coping

Figure 1: The systematics of BSI situation monitoring

on the potential target group: While ransomware groups, for example, primarily attack institutional targets in business and public administration, spam and phishing are mainly aimed at private individuals, i.e. consumers (see in particular part C Attack, page 42).

(4) Impact

Successful attacks have damaging impacts. For example, important company data is encrypted or exfiltrated, the company network is compromised or a web service is paralysed. In addition, cyberattacks may have more victims than attacked targets. For example, a ransomware attack on an IT service provider can result in numerous other victims who are indirectly affected as a result of service shutdowns by the targeted IT service provider. The impact of a single attack can multiply and result in a large number of victims. In addition to actual IT damage, there is usually financial damage, such as lost revenue, IT forensic investigation costs, recovery costs, and possibly reputational damage if a successful attack becomes public knowledge.

(5) Resilience

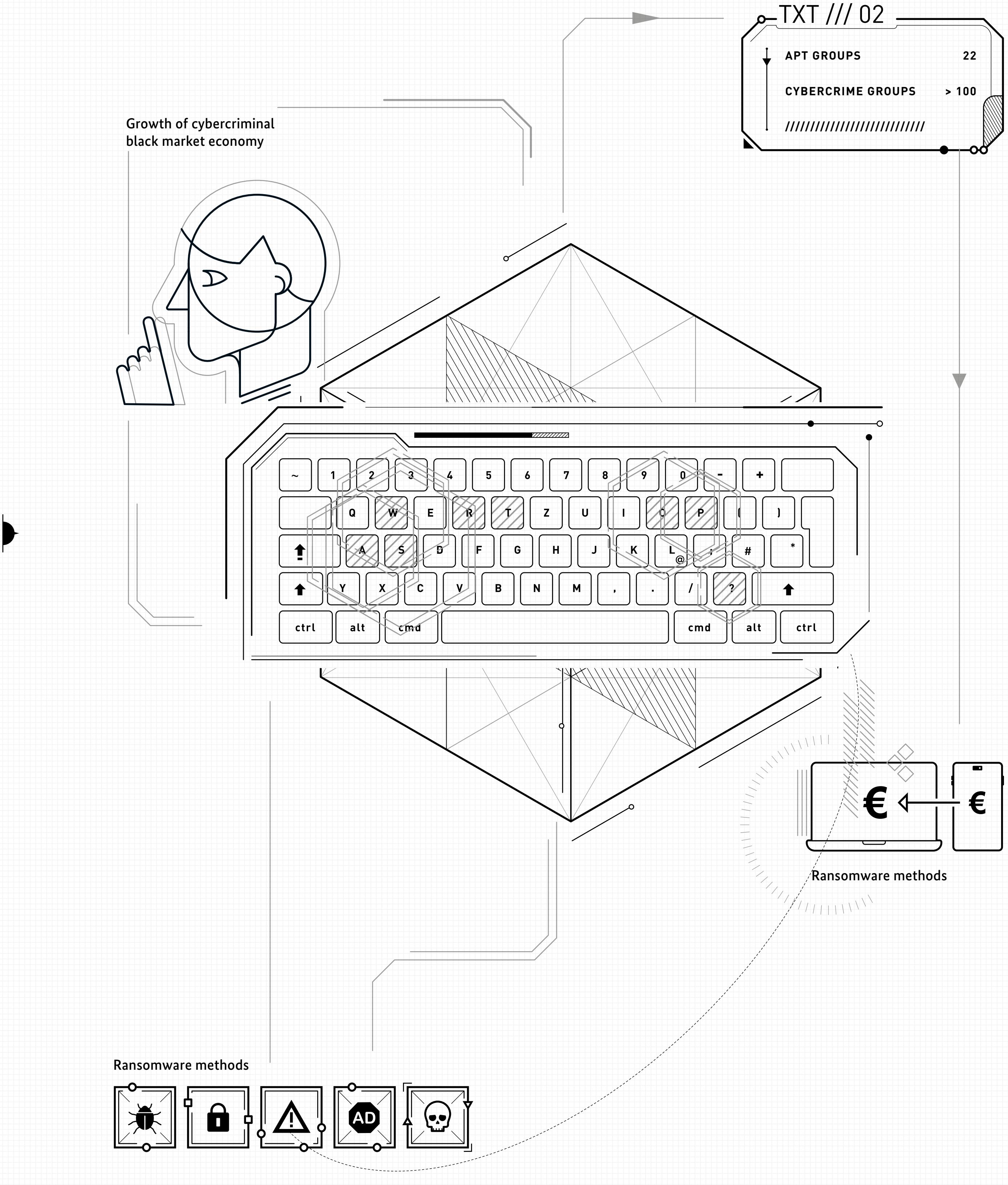
Prevention capabilities: Preventive measures increase the resilience of potential victims to cyber threats. Preventive measures for local networks, such as corporate networks, include an information security management system (ISMS) and patch management, as well as awareness measures and the provision of qualified IT security personnel. The aim of preventive measures is to minimise vulnerability to cyberattacks.

Defence capabilities: Defence measures protect victims in the event of a cyberattack. Traditional defence measures include systems for attack detection, such as antivirus programs, and effective DDoS mitigation. Defence measures are aimed at fending off specific attacks.

Coping capabilities: There is no such thing as 100 per cent security, and cyberattacks can be successful despite preventive and defence measures. Coping capabilities are aimed at minimising the impact and returning the affected systems and processes to normal operation as quickly as possible. A functioning, practised plan for IT emergencies is just as important in state, public and commercial institutions as restorable backups. Digital literacy is becoming increasingly important for consumers in order to be able to recognise a phishing email and act correctly.

Resilience is an important key to secure digitalisation in a successful cybernation like Germany, which is always one step ahead of cyber threats from the internet. The BSI is taking a wide range of measures to increase the resilience of government, business and society. Some of these are highlighted in Part D of this report (see Part D Resilience, page 74).

A THREAT

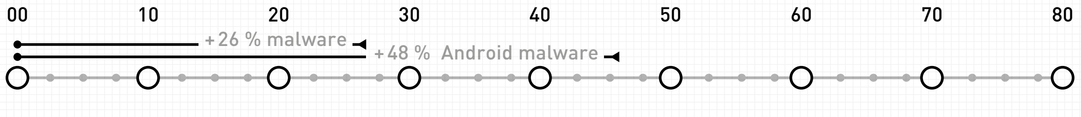


TXT /// 02

APT GROUPS 22

CYBERCRIME GROUPS > 100

New malware variants



2 – Malware

Computer programmes that carry out harmful operations are known as malware. For example, malicious email attachments or links that are clicked on can result in a malicious programme being installed. Manipulated links on websites or manipulated legitimate software that comes into circulation through supply chain attacks, for example, are also typical attack vectors. As a rule, malware exploits existing vulnerabilities in software and hardware to infect computer systems.

2.1 New Malware Variants

If an attacker makes changes to a malware programme, a new malware variant is created. Any variant that is unique in terms of its checksum (hash value) is considered new. While detection methods exist for known malware variants, new variants may not be immediately identified as malware when they first appear and are therefore particularly dangerous.

During the reporting period, an average of 309,000 new malware variants became known every day (see Figure 2, page 16). This was around 26 per cent more than in the previous reporting period, with an average of 250,000 new malware variants every day. The increase was due in particular to a significant rise in new malware variants that exploit vulnerabilities in 64-bit versions of Windows (+256%). In addition, Android variants saw above-average growth in the reporting period (+48%). After the takedown of the Flubot botnet, which was responsible for many infections of mobile systems (see The State of IT Security in 2022, page 25), the emergence of new Android malware initially collapsed in June 2022. The growth in the current reporting period is therefore likely to indicate the renewed development of Android attack infrastructures, although the attackers have not yet returned to the level seen before the takedown.

In addition to regular security updates, protection against malware attacks is provided by antivirus software, which can detect malware, prevent it from running successfully and remove it from the system. However, some attacks also make far-reaching changes to the infected system that cannot simply be undone.

2.2 Botnets

A botnet is the combination of several systems (bots) infected with a malware programme which establish contact with one or more central control systems (command and control servers, C2 servers) of the attackers and are remotely controlled by them. In addition to traditional office computer systems, attackers can also infect all other internet-enabled devices with a malicious programme and integrate them into a botnet. This affects devices such as smartphones, tablets, routers or IoT devices like televisions, set-top boxes, webcams, etc. Such devices can be attacked using malware or directly via the internet. In the first case, attackers inject malicious code into legitimate programmes that users then unknowingly install, for example with system updates or apps. In the second case, attackers use vulnerabilities in the operating systems of the devices to automatically compromise them via the internet without the intervention of the system owner.

Current botnets typically have a modular structure so that attackers can flexibly load and customise the functionalities they need for specific attacks. This means that the infected systems can be used multifunctionally and for different types of attacks. The malicious functionalities can specifically target the users of the system, e.g. for information theft, identity theft, data encryption or cryptomining, or misuse the system to attack third parties, e.g. for DDoS attacks, sending spam, etc.

During the reporting period, botnets were primarily used to steal personal information, to compromise and abuse online banking access and to distribute other malware. In the current reporting period, mobile devices with Android operating systems were once again the focus of attackers. Six of the ten most active botnets known in Germany targeted Android devices. They were responsible for 42.3 per cent of infections (see Figure 4, page 18). Therefore, one of the focal points of the BSI's situation monitoring continued to be this type of botnet.

Smartphones are particularly attractive targets for attackers because they are increasingly multifunctional. From paying at the supermarket checkout, online banking and social networks to controlling smart home devices

Average number of new malware programmes per day

Number in thousands

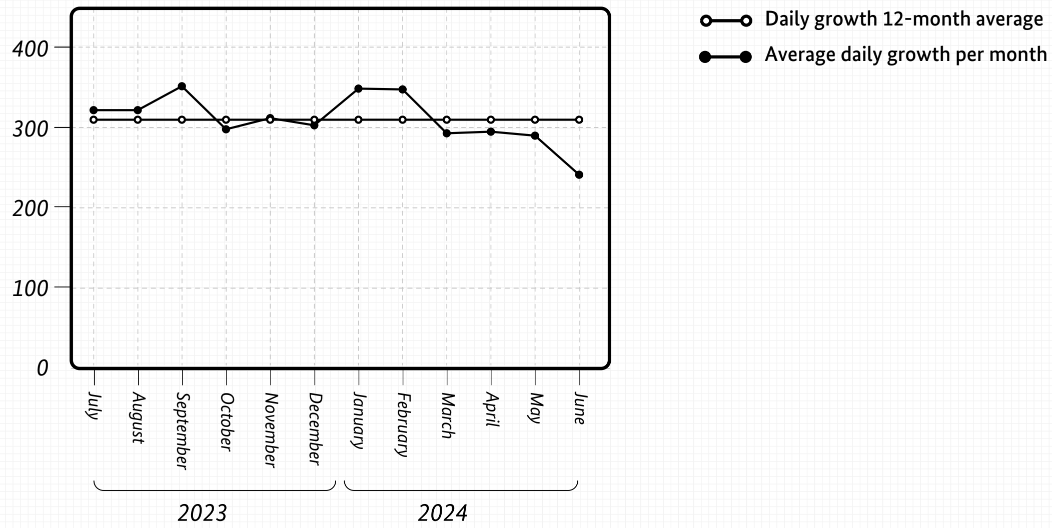


Figure 2: Average number of new malware programmes per day (number in thousands)

Average daily growth of new Android malware variants

Number

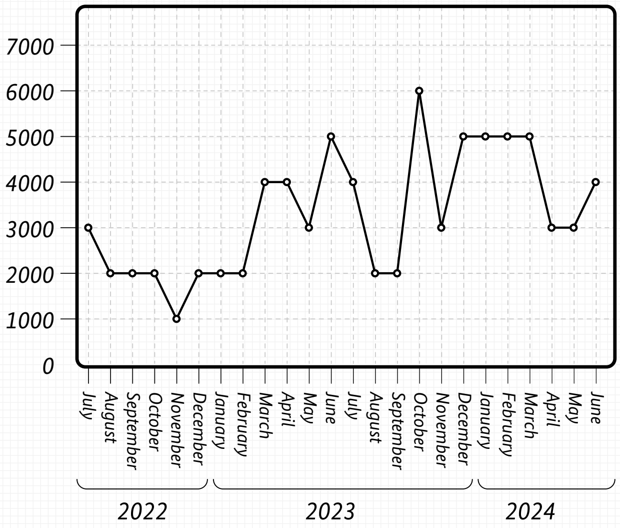


Figure 3: Average daily growth of new Android malware variants per day (number)

Figures 2 & 3 / Malware statistics:

Aim of the statistics: Survey of incoming email traffic with the Federal Administration. Reported monthly. / **Population:** All emails received by the central mail transfer agent. / **Sample:** Complete survey / **Survey design/instruments:** Daily aggregation of spam filter detections on the federal government's networks. / **Scope:** Excludes authorities that do not participate in the BSI's centralised protection measures. General statistical characteristics, spam status and information on e-mail attachments are recorded. / **Quality assessment:** Precise, as a complete survey. Minor inconsistencies due to improving detection and different calculation times and monitoring personal fitness: few devices accumulate as many password-protected functions in apps with sensitive data as smartphones. Botnets such as ArrkiiSDK, the largest of the sinkhole botnets observed in Germany with 12.2 per cent of unique IPs, not only enable abusive user tracking and advertising fraud, but also the silent installation of additional applications without the user's consent. For example, attackers behind botnets such as ArrkiiSDK can install spyware to read users' credentials and then sell them to ransomware groups (for more on access brokers, see the chapter Cybercriminal Black Market Economy, page 19).

The Socks5Systemz botnet, which infects Windows systems and turns them into proxies, also came to light during the reporting period. These are systems that can forward third-party internet traffic so that the real sender can no longer be identified. Botnet operators also rent out such systems to distribute other malware and to circumvent regional restrictions, e.g. on streaming services. However, they are particularly useful in the context of cyber espionage attacks for concealing the sender addresses of malicious internet traffic (see also APT Groups, page 22).

The BSI records infected systems via so-called sinkholes. These are servers that receive and log the communication from bots on behalf of the attackers' control systems. During the reporting period, an average of around 20,650 infected systems were recorded and reported to the German providers every day. The providers use the data provided to identify the customers affected and notify them. A description of sinkholing and profiles of commonly reported botnets can be found on the BSI website.

Read more about botnets:

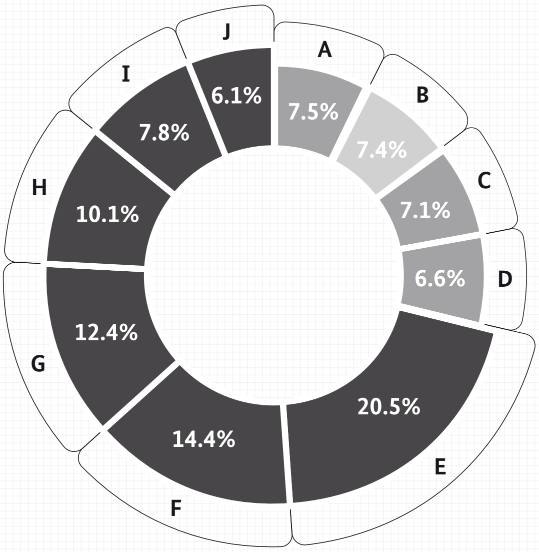
Also based on the empirical values from takedowns (see e.g. incident box Takedowns, page 50), it can be assumed that the total number of infected systems is significantly higher. This is because many cases involve multiple infections. Also, only some of the globally active botnets can be detected by traditional sinkholing techniques. The attackers behind prominent botnet families take measures against sinkholing, such as the use of fixed IP addresses, tunnelled DNS connections (DNS over HTTPS, DoH) or blockchain techniques to conceal communication between control servers and bots. The trend in recent years also indicates an increasing professionalisation of attackers.

As in previous years, the threat level from botnets is high. For the reasons given above, the infection figures obtained through sinkholing represent only a minimum threshold. The increasing number of internet-enabled devices creates increased vulnerability as inexpensive mass-produced IoT devices in particular often only have short support cycles from the manufacturers and serious vulnerabilities are not closed promptly, if at all. Vulnerable devices can be easily found by attackers on the internet and compromised using suitable tools.

This makes it possible for attackers with comparatively few technical resources to infect systems in order to set up their own botnets.

Unique IP by the top 10 botnets

Shares in %



	Operating system	Botnet
A	*Windows*	*socks5systemz*
B	*Linux*	*qsnatch*
C	*Windows*	*zeus*
D	*Windows*	*nymaim*
E	*Android*	*arrkiisdk*
F	*Android*	*pushiran*
G	*Android*	*flubot*
H	*Android*	*triada*
I	*Android*	*flubot-doh*
J	*Android*	*mobidash*

Figure 4: Infected systems (unique IP) July 2023 to June 2024 by the top 10 botnets (shares)

Figure 4 / Botnet structure statistics:

Aim of the statistics: Structural survey of known botnets worldwide. Reported monthly. / **Population:** All botnets worldwide that can be picked up by sinkhole servers. / **Sample:** Deliberate selection of around 300 of the most threatening botnets for BSI sinkholing. / **Survey design/instruments:** Monthly aggregation of an ongoing survey of IP addresses contacting BSI sinkholing servers. / **Coverage:** Infected systems (bots) worldwide, including Germany. Technically, only a portion of the globally active botnets can be recorded via sinkholing. / **Quality assessment:** Due to technical capacity limits, the BSI can only monitor a small proportion of infected systems (bots). It is therefore not possible to make statements about the number of infected systems.

3 – Ransomware Groups

Ransomware refers to malware that denies the victim access to an attacked system unless a ransom payment is paid. The first forms of ransomware relied on just locking the screen. Nowadays, ransomware is mainly used to encrypt data that is relevant to the victim. This can be any form of digital asset, from simple documents and patient files to entire databases and system backups. Ransomware attackers extort money by first taking control of a victim's data and systems and then demanding a ransom in return for restoring the availability of the data and systems. Such an approach is called a ransomware attack.

However, there is no guarantee that the attackers will actually release the encrypted data or actually delete the stolen data, even if a ransom has been paid. There is also the possibility that the decryption tool provided by the attacker is faulty. In addition, data that has already been transferred must always be regarded as compromised. The BSI therefore advises against paying a ransom as a matter of principle.

Potential victims are institutions of all types and sizes – from micro-businesses to public authorities and CI companies to international corporations, from local authorities and hospitals to scientific institutions, schools and universities. In addition, the BSI occasionally becomes aware of mass campaigns that also directly affect consumers.

Ransomware attacks are mainly carried out by criminal attackers for financial reasons. However, APT groups can also use ransomware to disguise or divert attention from other attacks (see chapter APT Groups, page 22). Ransomware can also be used purely for sabotage. In this case, the ransomware is used in a similar way to a so-called wiper malware programme, which deletes data: data is encrypted in such a way that it cannot be technically restored.

The BSI provides recommendations and measures against ransomware.[1] Countermeasures were also summarised by attack phase in the BSI's The State of IT Security 2023 (page 22 f.). These are still valid.

3.1 Cybercriminal Black Market Economy

Financially motivated attacks are accompanied by an entire black market economy of criminal services related to cyberattacks. This is also known as Cybercrime-as-a-Service (CCaaS). These CCaaS can support a cybercriminal in almost every aspect of a cyberattack. For example, CCaaS offer malware or provide support for other criminal activities such as extortion or money laundering (see The State of IT Security in Germany in 2023, page 16 f.). Sooner or later, new methods will be adopted in CCaaS and thus made accessible to many attackers. In the current reporting period, this related in particular to so-called EDR killers and the exploitation of zero-day vulnerabilities by ransomware groups.

3.1.1 Malware-as-a-Service EDR Killers

In addition to antivirus software, software called Endpoint Detection and Response (EDR) is increasingly being used to protect systems. While antivirus software scans files when a virus scan is carried out or when a file arrives on a system by email, EDR programmes run permanently. The aim of such software is to use signatures and behavioural heuristics to detect anomalies during system operation, for example whether an executed programme is behaving maliciously. Attackers try to evade detection by antivirus or EDR software in various ways. EDR killers are tools that are used to terminate and, if possible, remove the EDR software installed on a compromised system.

Many EDR killers abuse legitimate but vulnerable antivirus and EDR software drivers. This procedure is also known as Bring Your Own Vulnerable Driver (BYOVD). Antivirus and EDR software often requires other antivirus and EDR software to be uninstalled to ensure smooth operation, as such software intervenes comparatively deeply in process sequences to detect suspicious behaviour. Several EDR programmes running in parallel would tend to lead to errors, as they would interfere with each other. The drivers therefore uninstall competing EDR software. Attackers exploit these and similar functionalities in vulnerable drivers.

The aim of the attackers is to delay the detection of their activities and leave as few traces as possible. During the reporting period, the BSI observed that several EDR killers were offered as malware-as-a-service (MaaS). This is probably a reaction of the attackers to the increasing use of EDR software for attack detection and management.

3.1.2 Exploitation of Zero-Day Vulnerabilities by Ransomware Attackers

Once exploits have been published, i.e. malware designed to exploit a specific vulnerability, they are quickly adapted by other attackers. During the reporting period, the BSI also observed the exploitation of zero-day vulnerabilities by ransomware attackers. For example, the attackers behind the ransomware and leak site Clop have repeatedly exploited targeted zero-day vulnerabilities in file-sharing servers for large-scale attack campaigns. In the incidents observed by the BSI, there are indications that the attackers prepared an infrastructure for the attack several days or weeks in advance. The attackers therefore set themselves up for a race to steal as much data as possible with the aim of blackmailing before the vulnerable servers can be taken offline and cleaned up if necessary.

It can be assumed that ransomware attackers will continue to exploit zero-day vulnerabilities in the future. The attacker group in question does not need to have the technical expertise to identify the vulnerability and develop an exploit. Due to the millions of ransoms that have already been stolen in recent years, attackers have sufficient funds at their disposal to do things such as commission criminal service providers to search for an exploitable zero-day vulnerability or to buy an exploit or proof of concept.

3.2 *Ransomware Groups Relevant for Germany*

The BSI monitors more than 100 cybercriminal groups active in Germany. The five most active groups are regularly responsible for around half of the alleged victims named by attackers on their leak pages (see Figure 5, page 21).

The ransomware group behind the LockBit ransomware-as-a-service was the most active in the current reporting period, both in Germany and worldwide. Law enforcement officials have reported more than 2,500 ransomware victims from this group worldwide in recent years. In Germany alone, the group published 40 alleged leak victims on its leak page during the reporting period. Worldwide, there are said to have been 944 leak victims in the same period. After the takedown in February 2024, the group remained active, but was still far from its previous level of activity at the time this report went to press.

The group behind the Black Basta ransomware-as-a-service, which has been known since 2022, also continued to dominate in Germany during the reporting period. The group repeatedly exploited vulnerabilities, some of which have been known for several years. In the current reporting period, the group named 21 alleged victims from Germany on its leak page.

The ransomware group behind the 8Base RaaS, which previously focussed its activities on North and South America, has also been among the top 5 RaaS in Germany since mid-2023. 8Base attacks victims from all sectors and named at least 15 alleged leak victims from Germany on its leak page during the reporting period. The attackers repeatedly used access brokers for the initial infection.

The ransomware group behind the Play RaaS attracted attention for its activity against German organisations back in 2023. In the process, 13 alleged victims were published on the group's leak page. The group repeatedly exploited vulnerabilities in exposed services such as VPNs or mail servers for the initial infection. Like other groups, the attackers also purchase access from access brokers.

Access brokers are gaining in importance overall. The ransomware group behind Cloak also bought compromised credentials of legitimate accounts to initially infect networks during the reporting period. Germany is a particular focus of the group. During the reporting period, the attackers named 12 suspected victims from Germany on their leak page, making them one of the top five leak pages in Germany, whereas the group is not in the top 25 worldwide.

Top 5 leak pages July 2023 to June 2024

By number of leak victims

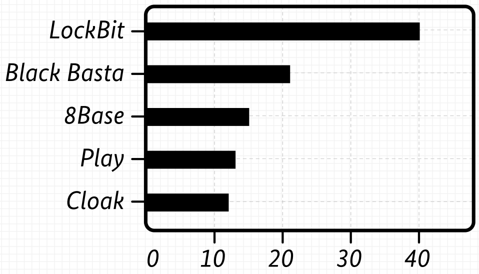


Figure 5: Top 5 leak pages July 2023 to June 2024 by number of leak victims (number)

Figure 5: Top 5 leak pages July 2023 to June 2024 by number of leak victims

Aim of the statistics: To identify the victims of data leaks who have not paid a ransom after a ransomware attack and whose data has therefore been published on a leak website of an attacker group in order to increase the blackmail pressure. Reported quarterly. / **Population:** All dedicated leak sites on which the data of victims of data leaks resulting from targeted cybercrime attacks (ransomware attacks and attacks against new vulnerabilities) were published. / **Sample:** Full survey of known leak victims. / **Survey design/instruments:** Detection of data service providers, reports from victims and public sources. / **Coverage:** No statement on the number of underlying attacks, but on the number of victims unwilling to pay whose data was published on a leak page. No differentiation between ransomware victims and victims of data exfiltration through vulnerability exploitation. / **Quality assessment:** High global coverage with comparison of different data sources.

4 – APT Groups

While malware is usually distributed by criminal attackers en masse and in an untargeted manner (see chapter Ransomware Groups, page 19), APT attacks are often long-term attacks on individually selected, prominent targets that are planned with great effort. APT attacks are therefore generally not used for criminal gain, but to obtain confidential information from the target and possibly for sabotage.

To the BSI's knowledge, 22 different APT groups were active in Germany in the current reporting period, targeting authorities and companies, particularly in foreign affairs, defence, public security and order. In addition, there were a number of developments that shaped the APT threat landscape.

4.1 Cyber Activities within the Context of Geopolitical Tensions and Conflicts

The current reporting period also showed that geopolitical and interstate conflicts are often accompanied by a whole range of phenomena in cyberspace. Disinformation, hacktivism, espionage and sabotage were evident both in the Russian war of aggression against Ukraine and in the aftermath of Hamas' terrorist attack on Israel in October 2023. A large proportion of cyber activities in these conflicts remained limited to specific regions. However, collateral damage to third countries can never be ruled out, especially if there are technical or organisational relationships with a party to the conflict.

The cyber sabotage attacks observed in the aforementioned conflicts were technically simple in the vast majority of cases. Instead of complex attacks on industrial control systems (see, for example, Industroyer, The State of IT Security 2022, page 51), simple wipers were mostly used in office networks. So far, geopolitical tensions have not led to attackers using previously developed, advanced cyber sabotage tools. However, this observation does not necessarily apply to other actors in future conflicts.

The simple sabotage attacks observed, which usually caused little lasting damage, were often accompanied by disinformation and propaganda to exaggerate the damage. The same phenomenon has been observed in hacktivist DDoS attacks (see also The State of IT Security in 2023, page 30). These usually only last for a short time and also cause hardly any lasting damage. In social networks, however, the disruptions are presented by the attackers as massive and relevant in order to maximise their impact on the population and public opinion. In the reporting period, hacktivism and cyber sabotage were therefore primarily aimed at creating diffuse insecurity in the public perception. In this sense, incident management in times of geopolitical tension also means public relations work in order to be able to place and assess attacks in a technically correct context.

The conflict between Israel and Hamas is another example of the use of cyber means in an escalated situation. However, it has also been shown that different conflicts lead to different phenomena in cyberspace. For example, according to media reports, the Israeli armed forces were able to seize servers that they attributed to Hamas during their operation in the Gaza Strip. Evidence had been found that surveillance cameras in Israeli cities on the border with the Gaza Strip had been compromised in the run-up to the Hamas attack in October 2023. Data was also stolen from compromised smartphones belonging to Israeli military personnel. The data collected in these espionage operations was suitable for supporting the attack on the Israeli border regions. However, there are currently no indications that the attack itself was accompanied by cyber sabotage. This is in contrast to the invasion of Ukraine by Russian forces in February 2022, at the beginning of which cyber sabotage against military communication systems was observed, among other things. Another difference is that in the context of the Gaza conflict, significantly more hacktivist groups, whose members claim to come from different countries, have claimed responsibility for attacks on Israeli targets as a result of Hamas' attack on Israel than is the case in the context of Russia's war against Ukraine.

In addition, hacktivists or strategically motivated actors who only pretended to be hacktivists repeatedly attributed incidents to themselves in which they claimed to have carried out attacks on ICS systems. For example, a group called CyberAv3ngers accessed Unitronics systems used for water treatment in the US. The attack vectors were technically simple and took advantage of weak passwords and other inadequate security precautions such as accessibility from the internet.

Given the massive damage and costs caused by ransomware worldwide, the BSI is concerned about the possibility of strategically motivated actors posing as ransomware criminals in the context of geopolitical conflicts in order to actually carry out cyber sabotage against critical infrastructure. This camouflage allows strategically motivated actors to plausibly deny their involvement without having to reckon with diplomatic or economic consequences.

In another strategic environment outside the regions affected by the Ukraine and Gaza wars, international authorities are publicising evidence of so-called prepositioning. According to the report, groups such as Volt Typhoon collected access to target networks for a possible conflict in order to have these accesses available for cyber sabotage in the event of an escalation and to be able to use them at short notice. According to the BSI, however, these are very early phases of prepositioning: it has not been reported that process control environments (OT/ICS networks) have already been extensively and systematically exposed or that backdoors with destructive capabilities have been observed. It also remains unclear whether these activities are regionally limited.

4.2 Information Operations

The term “information operations” covers disinformation as well as propaganda and similar activities that are designed to influence public opinion or the opinion of decision-makers by means of narratives. The BSI generally considers the phenomena of APT and information operations separately, but during the reporting period it became evident that the boundaries are becoming blurred. For example, the BSI has made political and pre-political organisations aware of the possibility of hack-and-leak campaigns in view of the 2024 elections. This involves compromising the accounts or devices of politically relevant people, stealing data and publishing it with a narrative. APT groups, whose core business is stealing information, can opportunistically decide whether the captured data is suitable for hack-and-leak operations and should be published accordingly. However, no such publications in Germany or concerning German victims were observed during the reporting period.

The effects of cyber sabotage are now also being amplified in public perception by accompanying information operations, for example in social media. The actual damage and consequences of attacks are exaggerated, apparently in order to sow uncertainty among the population and discredit the responsible authorities or governments. As described above, this was observed above all in the context of attacks by Hamas on Israel and the subsequent Gaza war, in which the attackers, for example, presented their technically comparatively simple attacks on Unitronics systems in the social media as more spectacular than they actually were.

These two phenomena – hack-and-leak operations and information operations in the context of cyber sabotage – indicate that the actors define cyberspace more broadly than IT devices and the associated infrastructure. Instead, the information space, i.e. the space in which the media and the public negotiate opinions and interpretations of the world, is also becoming the focus of attackers. A purely technical focus by security professionals on IT devices therefore falls short and must be supplemented by education and awareness-raising in the information space.

4.3 Technical Trends

APT groups are active worldwide and demonstrate a wide range of attack techniques. The trends presented here are therefore only a selection of the most important observations. In principle, APT groups use all attack paths and vulnerabilities that they need for their objectives.

Obfuscation nets: Trends already observed in the previous reporting period continued. The BSI has identified an increasing number of obfuscation networks. These are compromised routers, IoT devices and VPS servers that are interconnected to form a botnet. Attackers can use this botnet to disguise their traffic via several intermediate stations (see also chapter Botnets, page 15). This makes both the detection of attacks and the assignment to known groups more difficult. These networks are now operated in a professionalised manner in order to guarantee customers, i.e. APT groups, the greatest possible convenience when using them.

EDR killers: The constant race between attackers and defenders is illustrated by the phenomenon of undercutting endpoint detection and response (EDR) products. EDRs have now become established as a security component in many companies and authorities, and represent a further hurdle for attackers (see chapter Malware-as-a-Service EDR Killers, page 19). Attackers are responding to this and are now increasingly using techniques to undermine these EDR products. This is done partly via vulnerable drivers that allow EDR products to be deactivated, or by suppressing notifications from the systems used to detect attacks.

Cloud applications: Attackers are also adapting to new developments and user habits. For example, they are now targeting data stored in the cloud. In many cases, the attack vector is not specific to the cloud. For example, attackers steal access data via phishing sites or information stealers, which are then also used to log in to cloud applications (see also The State of IT Security in 2023, page 17). When exploits are used, they often affect vulnerabilities in web applications or server software that are used both in cloud environments and on in-house systems. Only when the attackers have access to the cloud do they start using cloud-specific techniques. Many groups are now very adept at using cloud configurations and APIs to spread or persist their access within cloud environments. For instance, configurations are often changed in such a way that databases or interfaces become directly accessible to the attackers from the internet.

Zero-day vulnerabilities: The trend towards exploiting vulnerabilities in server applications and VPN products continued in the area of zero-day exploits, i.e. malware designed to exploit vulnerabilities for which no security updates are yet available. Zero-days in end-user products such as smartphones or browsers, on the other hand, were often associated with commercial exploit brokers. Their customers typically target individuals such as dissidents or journalists – unlike APT groups, which usually attack corporate or government networks.

Despite these technically advanced methods, many APT groups continue to use classic phishing to collect credentials. As usual, the login pages of corporate webmail portals or commercial email providers are imitated and the victims are lured there by emails so that they enter their access data. This approach remains attractive to attackers because it can be used against a large number of victims with little effort.

4.4 Diplomatic, Legal and Political Measures

The interdependence of developments between attackers and defenders can also be seen at the strategic level, which is characterised by diplomatic, legal and political measures. In response to the use of obfuscation botnets from compromised routers and IoT devices, US authorities in particular have implemented several coordinated countermeasures. For example, they carried out takedowns against an APT28 botnet consisting of compromised Ubiquiti Edge routers and a botnet of compromised routers and IP cameras used by the Volt Typhoon APT group. The US authorities also accessed compromised devices in the USA to remove malware and make temporary configuration changes to prevent the perpetrators from gaining access to the devices again. These technical measures were accompanied by notifications to the owners of the compromised devices so that they could finalise the clean-up and security measures.

In addition, US authorities imposed sanctions on individuals and companies allegedly linked to the APT group APT31 and the Doppelganger campaign disinformation network, among others. European and German authorities have also established a framework for formal sanctions against attackers in cyberspace within the EU and through the national attribution process. This complements the technical measures to increase cybersecurity in conjunction with diplomatic and legal measures.

4.5 APT Groups Relevant for Germany

On the basis of its own incident findings and dialogue with partners, the BSI considers at least the following APT groups to be relevant for Germany. As a rule, the groups are mainly active against targets in the specified sectors. The typical attack techniques listed should not be considered exhaustive, as some of the groups are very versatile. For reasons of space, only the attack techniques from the first phase of an attack are listed.

In addition, the groups APT30 (Naikon) and APT31 (Judgment Panda), as well as the Gallium group (Softcell/Phantom Panda/Alloy Taurus/Granite Typhoon), are under observation at the BSI due to incidents in neighbouring EU countries.

APT Groups in Germany

Threat actor and alias	Sectors, according to German WZ 2008	Characteristics
APT15 / Vixen Panda / Mirage / Ke3chang / Nylon Typhoon	• Administration of the State and the economic and social policy of the community	The threat actor uses its own relay network of compromised routers and VPN servers.
APT28 / Fancy Bear / Sofacy / Forest Blizzard	• Provision of services to the community as a whole • Administration of the State and the economic and social policy of the community • Computer programming, consultancy and related activities • Service activities incidental to air transportation	APT28 uses a variety of attack vectors, e. g. Outlook vulnerability CVE-2023-23397 (via email) WinRAR vulnerability CVE-2023-38831 (via email-attachment) Bruteforcing and password-spraying against internet-facing servers email)
APT29 / Cozy Bear / Nobelium / Midnight Blizzard	• Provision of services to the community as a whole • Administration of the State and the economic and social policy of the community • Activities of political organisations • Computer programming, consultancy and related activities	The threat actor engages in social engineering and initially sends several emails without malicious code until the recipient has built up trust. Only then will malicious code or a phishing link be delivered.
APT43 / Velvet Chollima / Kimsuky / Emerald Sleet	• Research and experimental development on social sciences and humanities • Administration of the State and the economic and social policy of the community • Higher education • Manufacture of weapons and ammunition • Manufacture of air and spacecraft and related machinery	The threat actor engages in social engineering and initially sends several emails without malicious code until the recipient has built up trust. Only then will malicious code or a phishing link be delivered.
Bitter / Hazy Tiger	• Provision of services to the community as a whole	Attack vectors are usually CHM or RAR attachments.
Cosmic Wolf / Sea Turtle / Marbled Dust	• Computer programming, consultancy and related activities	The threat actor may compromise a supply-chain entity first, in order to gather information for follow-up attacks on the intended targets.
DarkHotel	• Administration of the State and the economic and social policy of the community	
Earth Estries	• Unknown	

Threat actor and alias	Sectors, according to German WZ 2008	Characteristics
Gamaredon / Primitive Bear / Aqua Blizzard	• Provision of services to the community as a whole	The threat actor continually registers a large number of phishing-domains and sets up new servers.
Ghostwriter / UNC1151 / Storm-0257	• Unspecific	The threat actor targets private email accounts at commercial webmail providers via spear phishing.
Labyrinth Chollima / Lazarus / Diamond Sleet	• Computer programming, consultancy and related activities	The threat actor often uses emails with malicious documents about supposed job offers as an attack vector.
Mirage Tiger	• Administration of the State and the economic and social policy of the community	
Mustang Panda	• Administration of the State and the economic and social policy of the community	
Outrider Tiger / Fishing Elephant	• Administration of the State and the economic and social policy of the community	
Red Dev 61 / UTA0178 / UNC5221	• Administration of the State and the economic and social policy of the community	The attacks are usually targeted against VPN and other internet-facing systems.
RomCom / Storm-0978	• Administration of the State and the economic and social policy of the community	
Salted Earth / Sturgeon Fisher / Yoro Trooper	• Unknown	
Sharp Panda	• Administration of the State and the economic and social policy of the community	
Sidewinder / Razor Tiger	• Administration of the State and the economic and social policy of the community	
Snake / Venomous Bear / Turla / Secret Blizzard	• Administration of the State and the economic and social policy of the community	
Storm-0558	• Research and experimental development on social sciences and humanities	The threat actor uses their own VPN networks in order to obfuscate their attack traffic.
Viceroy Tiger / Donot	• Provision of services to the community as a whole • Administration of the State and the economic and social policy of the community	

Figure 6: APT groups relevant for Germany

5 – Phishing

The phishing methods used by cybercriminals against consumers changed in the current reporting period. In addition to already known phishing campaigns in the name of banks and financial institutions, an increase was registered in campaigns abusing the brand names of prominent streaming services. Thematically, these campaigns referenced measures to prevent unauthorised account sharing, changes to the terms of use for family accounts and changes to prices and payment terms. These were issues that were widely known in society and the media. This successfully contributed to the increase in phishing campaigns.

In connection with streaming accounts, cybercriminals particularly target the sensitive information stored in the profile. The data on payment methods such as credit cards, other information from payment service providers and personal data of account holders are then misused for other activities, such as data trading via access brokers.

Another increasing attack technique that has been observed in the context of payment services is the deliberate delay of follow-up actions after a successful phishing attack. This has already been reported in a previous study[2]: Attackers remained inactive for an average of five days until they carried out an abusive transaction with the previously obtained data. The total number of these transactions increased steadily over a period of 14 days after the respective phishing attacks.

Frequency of registered phishing URLs from the gaming, social networking and streaming sectors

Number of URLs and IPs

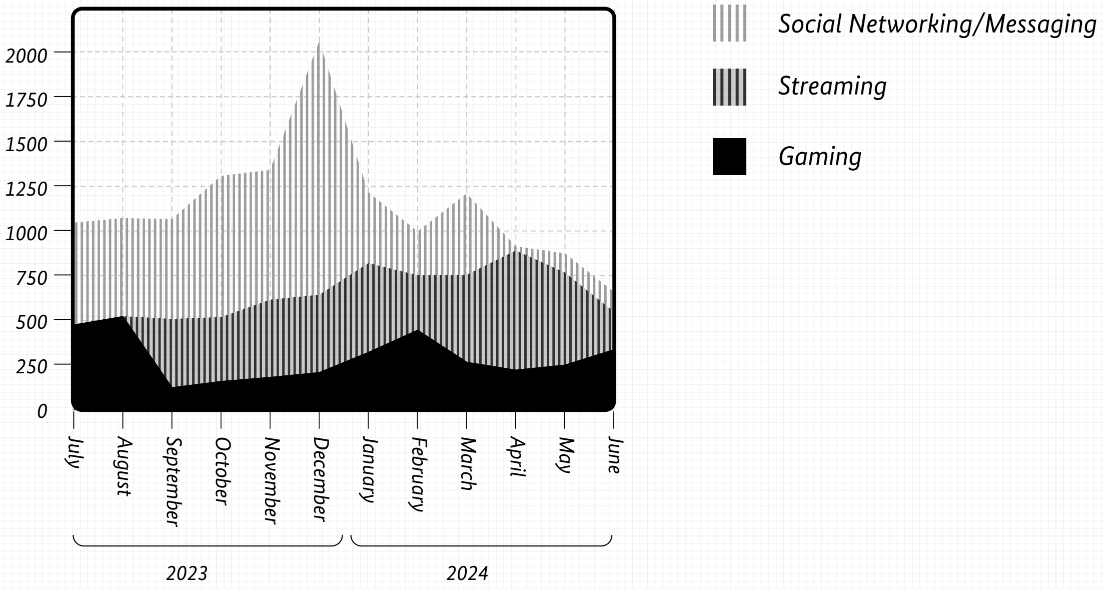


Figure 7: Frequency of registered phishing URLs from the gaming, social networking and streaming sectors compared over time (openphish, absolute figures)

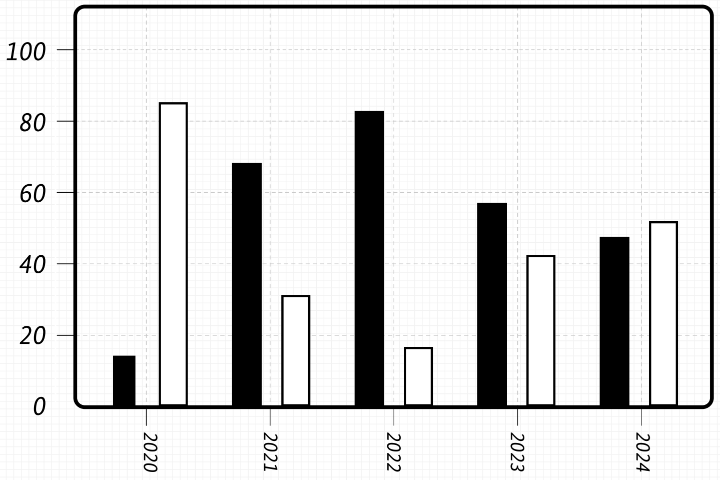
Figure 7 / Statistics:

Aim of the statistics: To collect data on suspected malicious web addresses; generic and brand-specific phishing addresses are collected. Reported monthly. / **Population:** all websites available on the internet / **Sample:** All suspected malicious websites known to the openphish.com platform. / **Survey design/instruments:** Daily aggregation of an ongoing survey using a scanner. / **Coverage:** worldwide / **Quality assessment:** Bright-field statistics. Automated industry categorisation requires certain characteristics on a website. These cannot always be determined precisely, resulting in an indeterminable number of unreported cases.

The time delay can be caused by the trading of information on underground platforms such as darknet forums, but it can also be used as a tool to disguise the connection between the exfiltration of data and the exploitation of that information. Such phishing attacks are particularly damaging for consumers, as they are usually unaware of the acute security incident and therefore oblivious to the danger. It also makes it more difficult to associate subsequent damage, such as loss of account and money, with the acute incident, to seek help and to file a complaint.

Reported phishing emails relating to financial brands

Share in %



Year	Financial sector	Other figures
2020	14.24	85.76
2021	68.56	31.44
2022	83.21	16.79
2023	57.32	42.68
2024	47.77	52.23

Figure 8: Share of reported phishing emails relating to financial brands in the total volume of reported phishing emails compared over time (Phishing Radar 2020 to 2024, NRW consumer advice centre, in per cent)

Figure 8 / Statistics:

Aim of the statistics: Survey of malicious emails in the mailboxes of German consumers. Reported monthly. / **Population:** All malicious emails that reach consumers' mailboxes bypassing the providers' protective measures. / **Sample:** Reports of suspected malicious emails, especially from German consumers, to the phishing radar of the NRW Consumer Advice Centre. / **Survey design/instruments:** Monthly aggregation of ongoing consumer reports. / **Scope:** Reporting parties must know the reporting channel. This requires knowledge of the NRW Consumer Advice Centre's phishing radar. / **Quality assessment:** Categorisation is based on individual case assessment by experts from the NRW Consumer Advice Centre.Annual average of around 30,000 emails with brand names (rounded to the nearest 10,000).

B ATTACK SURFACE

Vulnerabilities

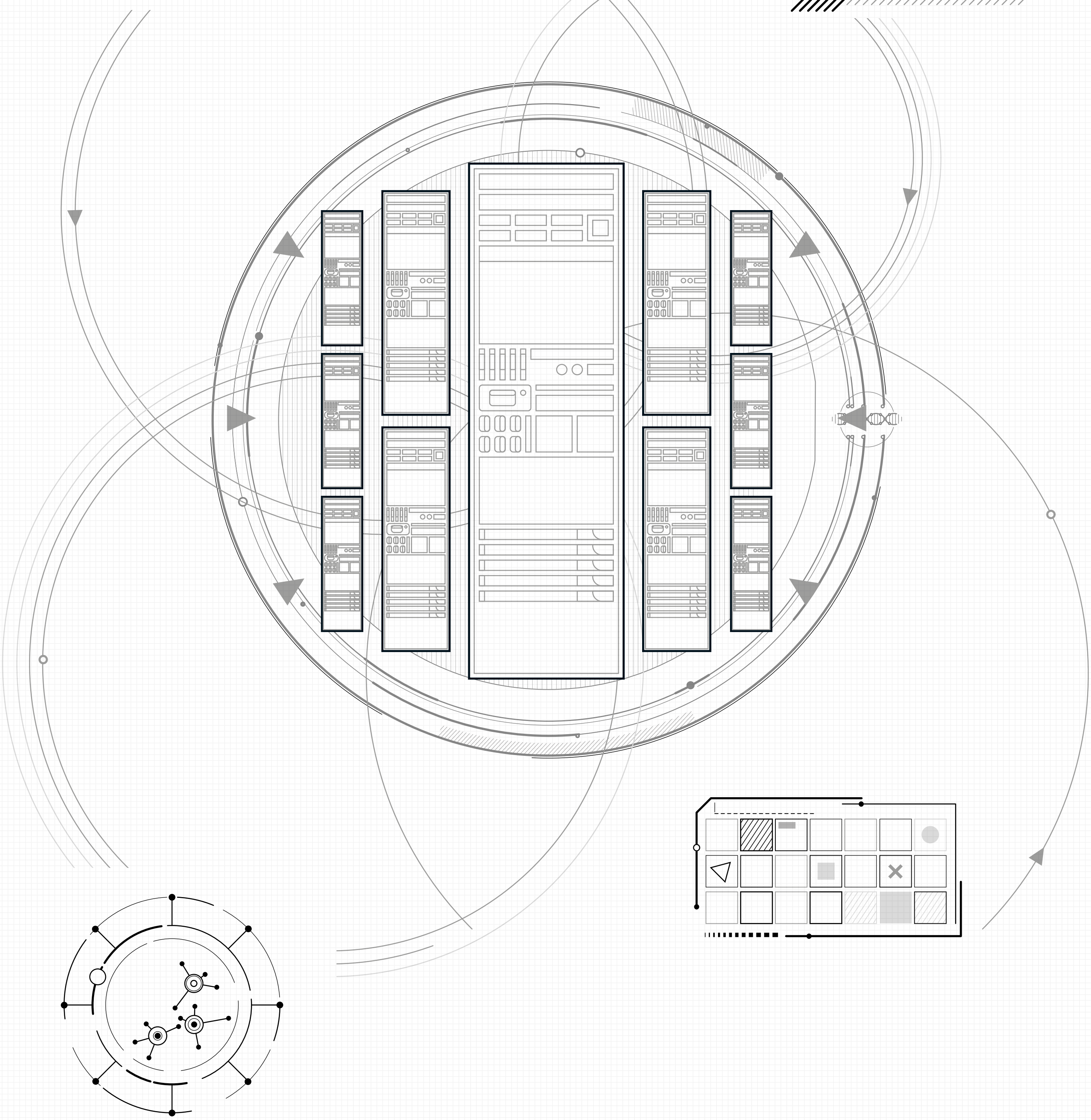
78 NEW VULNERABILITIES PER DAY IN 2023

14 PER CENT INCREASE COMPARED TO 2022

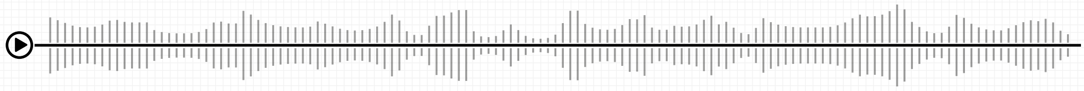
4,500/639,000

reachable IP addresses / active email addresses

attack surface federal administration



Millions of DDoS attacks



6 – Vulnerabilities

Attackers often exploit vulnerabilities in the IT infrastructure to infiltrate computer systems. Vulnerabilities therefore represent a significant part of the attack surface for cyberattacks. Malicious code that uses a vulnerability to carry out a cyberattack is known as an exploit. Exploits are used by cybercriminals, for example, to infect systems for the first time and to prepare a ransomware attack.

Vulnerabilities usually arise due to programming errors, weak default settings of IT products in productive operation or misconfigured security settings. IT systems are becoming increasingly complex and production conditions are becoming more and more modular and based on the division of labour, making vulnerabilities very common. If a vulnerability is discovered in an IT product, manufacturers usually provide security updates (patches) to remove the vulnerability and prevent it from being exploited for cyberattacks. Structured patch management is therefore one of the most important preventive measures for organisations of all types and sizes.

6.1 Vulnerabilities in Software Products

Vulnerabilities in software products often serve as the first gateway for compromising systems and entire networks – after all, they can often be exploited via the internet and thus allow attackers maximum anonymity and flexibility from a distance.

In 2023, an average of 78 new vulnerabilities became known every day, an increase of 14 per cent compared to 2022. All types of software products were affected, from specialised applications to complex server infrastructures and smartphone apps. As in previous years, the increasing modularisation and division of labour in software production also had an impact on the threat landscape in the current reporting period. If a vulnerability becomes known in a software component that is used in a large number of different applications, then such a single vulnerability can be exploited for cyberattacks against all of these applications. Not every vulnerability is easy to exploit for attacks from the internet. For example, a vulnerability in a local application without a connection to the internet can only be exploited by a local attacker. On the other hand, vulnerabilities in software products that are directly accessible from the internet can be exploited more easily and by a greater number of cybercriminals for attacks.

In addition to reports of publicly known vulnerabilities in software products, the BSI also receives special vulnerability reports from security researchers who have uncovered vulnerable components in IT systems. Typically, the focus is on vulnerabilities that have not yet been made public or have not yet become known to the manufacturer, so-called zero-day vulnerabilities. As part of a coordinated vulnerability disclosure (CVD), the BSI then has the opportunity to take the lead or act as an intermediary between security researchers and product owners or manufacturers to work towards eliminating these zero-day vulnerabilities (see chapter NIS 2 Directive, page 82).

During the reporting period, the BSI received an average of 41 reports per month from security researchers about vulnerable software products and classified them according to the Open Web Application Security Project (OWASP) system. While CWE (Common Weakness Enumeration) and CVSS (Common Vulnerability Scoring System) describe the vulnerabilities themselves, OWASP allows a description of the vulnerable product. Around 61 per cent of the reports related to vulnerabilities that made the affected products susceptible to injection cyberattacks. Attackers can use the vulnerability to inject malicious code into the software product, setting the stage for further cyberattacks such as data exfiltration.

In addition to reports of products with vulnerabilities, an average of six reports of incorrectly configured servers or missing patches for previously publicised vulnerabilities were received each month during the reporting period.

Exploitation of Zero-Day Vulnerabilities at IT Service Providers in Germany

Situation

As in the 2023 reporting period, incidents at IT service providers continue to be relevant. In 2023, the BSI identified an attack campaign against German IT service providers and other German organisations that had been ongoing since 2022. The attackers exploited zero-day vulnerabilities on Confluence systems, which are often exposed on the internet. The attackers disguised their malware as a plug-in and used, among other things, captured access data to spread throughout the organisation's entire network.

The IT service providers concerned also worked for federal authorities, among others.

Assessment

Dangers from the exploitation of zero-day vulnerabilities affect all IT products. Products that can be accessed directly from the internet are at high risk.

The cyberattacks mentioned here were carried out by a professionally operating cyber espionage group at great expense. The attackers developed specific attack methods tailored to the victim, exploited the vulnerability in some cases months before it was known, and used techniques to disguise the infection of the affected systems and hide within the affected systems. The attackers were therefore difficult to detect and were sometimes able to spy on the affected systems for months. This and other similar attacker groups pose a high potential threat to IT service providers, the federal administration and politically relevant organisations.

IT service providers are a particularly valuable target, as they are highly networked and can therefore provide access to their customers' infrastructures and information. In addition, they often have extensive administration rights to at least some of the systems.

For those affected, the consequences are particularly serious and challenging, for example in terms of crisis communication or the clean-up effort. The functional failures of the IT infrastructure during the clean-up are sometimes massive and long-lasting. Establishing emergency operations during incident handling and IT reorganisation also poses immense problems for many of those affected.

Response

The primary goal is to ensure that a zero-day exploit on an exposed system does not lead to the compromise of other critical systems or the internal network. Effective attack surface management is therefore one of the most important prevention capabilities. This includes the following aspects:

1. Only those systems and services whose functionality requires internet access should be publicly accessible.
2. Internal networks should be highly segmented to limit the spread of attackers across the network if breached.
3. General prevention measures should be implemented, such as limiting access rights to the necessary minimum, using strong and individual passwords, multi-factor authentication, etc.

This development justifies the BSI's increased activities in this area. With the provision of a vulnerability reporting form, the publication of a CVD guideline and the first incentives to report discoveries to the federal agency, such as the Hall of Fame for vulnerability researchers, the BSI's CVD process has become much more relevant and visible in recent months.

Find more information for security researchers:

Notifications of products with vulnerabilities July 2023 to June 2024 by potential harmful impact

Share in %

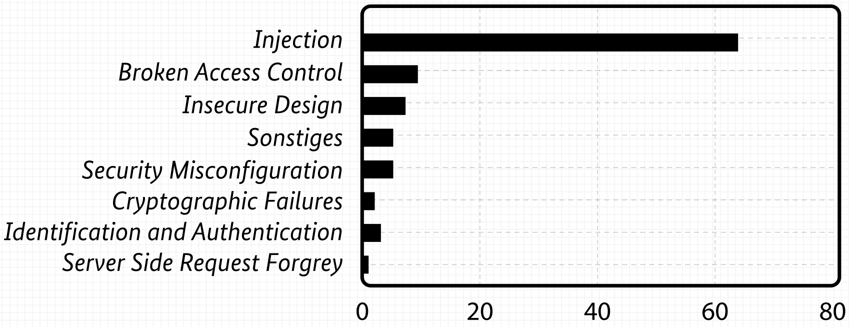


Figure 9: Notifications of products with vulnerabilities July 2023 to June 2024 by potential harmful impact (percentages)

Figure 9 / Statistics:

Aim of the statistics: Reports of vulnerable products from security researchers to the BSI as part of the Coordinated Vulnerability Disclosure (CVD), focussing on vulnerabilities that are not known to the manufacturer. / **Reports are submitted annually.** / **Population:** Vulnerabilities in IT products from German manufacturers reported to the BSI via CVD. / **Sample:** Complete survey. Reports on products with vulnerabilities are counted, not the vulnerabilities themselves. / **Survey design/instruments:** Online reporting form; reports are analysed by BSI employees using the CVD guideline. / **Coverage:** Germany-wide / **Quality assessment:** Full survey of CVD reports.It is not possible to make statements about vulnerabilities, zero-day vulnerabilities or the spread of vulnerable products.

6.2 *Vulnerabilities in Hardware Products*

Hardware vulnerabilities allow attacks on the physical structure and material properties of products or the microarchitecture of processors. These vulnerabilities can be exploited either by hardware-based attacks or through software attacks that target hardware weaknesses. Unlike software vulnerabilities, hardware vulnerabilities in products that have already been manufactured are difficult to rectify, which attracts the interest of attackers. Depending on the type of attack, exploiting these vulnerabilities can be simple or require considerable technical expertise and expensive equipment. Despite the relatively greater effort required, hardware vulnerabilities are increasingly being exploited in practice, especially in targeted attacks.

Microarchitectural attacks, such as Spectre or Meltdown, are software-based techniques that exploit flaws in the implementation of the architecture. Although executed purely by software, they leverage hardware-level vulnerabilities. Several new variants of these attacks were also published during the reporting period. For example, GhostRace exploits speculative execution and other architectural features to enable the reading of arbitrary memory areas. Similarly, the Inception attack against AMD processors combines two attack techniques to trigger speculative executions and access protected memory areas. Fuzzing, an established technique for recognising errors in software, is increasingly being used to detect CPU weaknesses. This involves feeding a programme with random or invalid input data in order to detect errors and security vulnerabilities. Zenbleed was discovered using this technique, which also exploits speculative execution to bypass memory protection mechanisms in the AMD Zen 2 microarchitecture. Another novel attack, GoFetch, abuses an optimisation feature in Apple ARM CPUs to infer sensitive information, even reconstructing protected key material.

Beyond attacks against CPUs, other hardware components were also targeted. The ZenHammer attack targets DDR5 memory, demonstrating that, despite error correction, memory can still be manipulated. GPU.zip and so-called drive-by GPU cache attacks make it possible to read sensitive data via vulnerabilities in graphics processing units (GPUs).

Attacks that require external hardware can also be of interest to attackers, despite being typically more complex and expensive to execute than purely software-based attack methods. Hardware-based attacks can compromise systems to which no software access is available. For instance, voltage glitching was used to induce errors in an attack against the Tesla Autopilot hardware to access the system's firmware. In a study commissioned by the BSI, the Fraunhofer Institute AISEC also describes a laser fault attack on signature procedures, altering the programme sequences of a chip and gaining access to sensitive data.

Particular attention is needed for hardware and chip products where security functions were not considered from the outset in development. Independent safety testing and certification, for example in accordance with ISO standard 15408, is a strong indicator of strong safety functionality. With the increasing practical relevance of hardware and chip attacks, hardware-based security features are playing an increasingly critical role in the overall security of products and systems.

6.3 Path-related Vulnerabilities

Path-related vulnerabilities have attracted a great deal of attention in the field of web applications for many years. Ignorance and carelessness on the part of programmers have allowed countless path traversal attacks, where files and directories can be accessed outside of the intended areas. It was often even possible to access passwords and other sensitive data.

But path-related vulnerabilities are also a favourite target of attackers outside of web applications. Several privilege escalation vulnerabilities in recent years were based on file or device redirection, such as symlinks, or the ability to place executable files directly in certain paths – on Windows often in conjunction with a default setting that allows normal users to create directories in the root directory (C:\).

The associated risks are often underestimated or not realised by programmers and administrators. As a result, on the one hand, programmers do not secure actions based on path specifications, or do not secure them sufficiently, so that ordinary users can influence the path specification or the destination of the path. This is particularly problematic if the code created by the programmers is intended to be executed later with elevated rights. On the other hand, Windows administrators fail to, for example, remove the permission to create folders in the root directory (C:\) for the group of authenticated users. Freely available tools can help programmers and administrators identify and fix privilege escalation vulnerabilities such as DDL, EXE or COM hijacking.

Another type of path-related vulnerability is based on the application incorrectly attempting to determine whether the target addressed by the path points to a local file or an external source on the internet, based on a path that can be controlled by attackers. If the checking function incorrectly concludes that the path points to a local file and security functions for retrieving or handling this file are not activated as a result, this can lead to a variety of damage patterns. The existence of such vulnerabilities regularly enables successful attacks and reopens already blocked attack paths.

6.4 Vulnerabilities in Networked Devices

Digitalisation also increases the attack surface for cyberattacks on networked devices. The digitalisation of cars and automobile traffic is one of the fastest growing areas of networking.

As the electrification of road transport continues to progress, the issue of cybersecurity for electric vehicles and the charging infrastructure is also coming under increased scrutiny. In March 2024, 114,565 publicly accessible charging points were in operation nationwide.[3] The number of public charging points increased by around 36 per cent in 2023 compared to the previous year.

Charging stations or charging points are highly networked devices. In addition to the actual charging interface to the electric vehicle, these typically have further interfaces for the necessary exchange of data. This includes mobile phone-based connections via the internet to the operator's backend systems or to other parties, such as energy providers, payment service providers or e-roaming providers. WLAN or Bluetooth access can be provided at the charging station for maintenance purposes. Customers can register at the charging point using RFID cards or a smartphone, also via WLAN, Bluetooth or NFC.

The large number of interfaces and data connections results in a potentially large attack surface from an IT security perspective. The classic security objectives of confidentiality, integrity, authenticity and availability are also important in the context of charging infrastructure. When charging processes are invoiced, personal data is transmitted which must be treated confidentially. The data received or sent by the charging station must be authentic and of integrity in order to prevent unauthorised charging processes or unauthorised discharging processes from the vehicle to the grid (vehicle-to-grid) or unauthorised access to maintenance functions, for example. After all, the charging points need to be reliably available to users. If no IT security measures are implemented, attackers could paralyse charging stations through denial-of-service attacks, for example, and in extreme cases potentially jeopardise the stability of the electricity grids or physically damage the infrastructure.

During the reporting period, several vulnerabilities were discovered in control units for charging points. In the course of an automotive hacker competition in January 2024, charging hardware from six different manufacturers that are also represented on the German market was analysed. Vulnerabilities were found in all six cases. Not all details of the gaps discovered were available at the time of reporting. However, high CVSS base scores of over 8 out of 10 points were achieved in some cases. The problems found with one model of charging hardware included a lack of authentication, unencrypted transmission of sensitive data and inadequate validation of input data.[4] The vulnerabilities would have allowed an attacker to remotely execute arbitrary code and take control of the control unit. The gaps in this model have since been closed by a firmware update from the manufacturer.

6.5 Vulnerabilities in Perimeter Systems

The emergence of new vulnerabilities and patching of affected products is daily business of every IT organisation. For some years now, attackers have been increasingly exploiting critical vulnerabilities in perimeter systems such as firewalls, VPN or application gateways (see The State of IT Security in Germany in 2022, page 38). These systems are attractive targets for cyberattacks due to their exposed position as a protection or perimeter system at the boundary between an internal network, such as a corporate network, and the internet. Compromising these systems offers attackers numerous options for spreading further in internal networks or on server and client systems, bypassing authentication or manipulating data traffic. In addition, methods for logging and attack detection on perimeter systems are limited and common, so that attacks are not as easily detectable as on client systems, for example.

In the current reporting period, a large number of critical vulnerabilities in perimeter systems became known, for example a zero-day vulnerability in Ivanti Connect Secure and other Ivanti products, critical vulnerabilities in FortiGate products from Fortinet and critical vulnerabilities in Citrix NetScaler. These vulnerabilities in widespread perimeter systems were exploited as zero-day vulnerabilities by cybercriminals or APT groups before or shortly after they were disclosed by the manufacturer. In general, the great interest in exploiting such vulnerabilities is regularly visible by internet-wide scans, through which attacker groups attempt to identify and compromise vulnerable devices en masse.

The exploitation of vulnerabilities in perimeter systems is also accompanied by changes in attacker behaviour. Whilst client attacks, such as spear phishing, typically involve the installation of malware that actively establishes a connection from the network to a command and control server operated by the attackers, this is not usually the case with perimeter attacks. Instead, so-called webshells are typically installed. These wait passively for the attackers to establish a connection from outside. This is possible because perimeter systems are by definition accessible from the internet.

This approach also has the advantage for attackers that they can access the compromised perimeter systems from any system or via obfuscation networks. From a detection standpoint, this has the disadvantage that indicators of compromise, such as IP addresses of command and control servers, are not applicable in this case. This development is linked to the establishment of so-called obfuscation networks, which attackers use to disguise or dynamically redirect their access (see chapter Technical Trends, page 23).

The BSI Situation Centre sent out alerts to its constituency about the vulnerabilities that became known during the reporting period in order to inform them about the vulnerabilities, the risk, measures, security updates and workarounds.

The critical vulnerabilities show that IT organisations also need to focus on the need to secure perimeter systems beyond the established protection of client systems. In some cases, however, patching alone is not enough. Instead, devices must also be analysed for compromise before they can continue to operate safely after a security update has been installed.

6.6 *Vulnerabilities in Cryptographic Processes*

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

Read more about the Technical Guideline TR-02102:

On the other hand, the following aspects may reduce the theoretical security level in practice:

- Weaknesses in cryptographic mechanisms or protocols
- Implementation errors
- Insufficiently secured side channels
- Weaknesses in random number and key generation

The classic application of cryptography is to protect the confidentiality and integrity of data, for example when it is transmitted via open networks such as the internet. Various cryptographic mechanisms and protocols are available for this purpose, and it is generally assumed that an attacker with access to the network traffic cannot discover the secret keys or decrypt the exchanged data or manipulate it without being detected. To ensure the effectiveness of cryptographic mechanisms and protocols, suitable procedures must be selected and implemented correctly. The info box “Attacks on SSH and its Implementation” (page 37) describes two vulnerabilities from the reporting period, one relating to the security of the SSH (Secure Shell) protocol itself and the other to an implementation of the protocol.

Side-channel attacks are currently one of the most successful methods of attacking IT products and pose a serious threat to the security of cryptographic implementations. In side-channel attacks, knowledge is gained from observable physical effects, including runtime behaviour, energy consumption, electromagnetic radiation and cache behaviour, when processing sensitive data. Even if a completely side-channel-free implementation is not possible, suitable measures can be taken to ensure that a side-channel attack is practically impossible. In 2024, the BSI published updated and expanded guidelines on this topic, which contain recommendations on how to proceed when evaluating implementations with regard to their side-channel resistance.

Read more about side-channel resistance:

An essential prerequisite for the secure use of cryptography is the generation of genuine random numbers which must fulfil certain quality criteria. Among other things, random numbers are needed for key generation. For cryptographic applications, random numbers must not be predictable and must not have any exploitable statistical defects. To prevent attacks using weak random numbers, the BSI defines functionality classes of random number generators for different purposes in the "Notes on Application and Interpretation" AIS 20 and AIS 31. In June 2023, a workshop was held at the BSI to present a new draft of the mathematical-technical annex to AIS 20/31.

Read more about random number generators:

Attacks on SSH and Its Implementation

The SSH protocol is used to establish a secure channel in an insecure network. The most common use of the SSH protocol is for administrators to log on to a remote server with their client computer in order to execute commands on it. Part 3 of Technical Guideline TR-02102 provides recommendations for the cryptographic algorithms and key lengths to be used.

In December 2023, security researchers at Ruhr University Bochum presented the so-called Terrapin attack on SSH (CVE-2023-48795).[5] Under certain conditions, it is possible for an attacker to block encrypted and integrity-protected messages from the server to the client without being noticed. Since such messages can also be used to exchange information about algorithms yet to be negotiated, an attacker can force certain security services not to be used for the connection by blocking these messages. The website https://terrapin-attack.com lists measures to prevent this attack.

In April 2024, security researchers at Ruhr University Bochum also published a vulnerability in versions 0.68 to 0.80 of the SSH client PuTTY (CVE-2024-31497).[6] This implementation error affects the ECDSA (Elliptic Curve Digital Signature Algorithm) signature scheme when using the NIST P-521 elliptic curve, and has the effect that the ephemeral keys generated by the ECDSA signature always have nine leading zeros, even though they must be randomly and equally distributed. This enables an attacker to calculate the private signature key from around 60 valid signatures using a mathematical procedure. The vulnerability was fixed in PuTTY 0.81.

7 – AI Large Language Models

Artificial intelligence (AI) is a hot topic in public debate. Large AI Language Models (LLMs), such as those used in ChatGPT, CoPilot, Claude and Luminous, have become highly influential across all industries due to their broad applicability. In contrast to classic IT systems, language models are complex architectures of neural networks with the following properties:

Vector processing: While classical programming formulates rules explicitly, neural networks consist of models of predefined functions whose parameters are trained, i.e. the model parameters are gradually adjusted until training data is reproduced as well as possible.

Error tolerance: Neural networks, and therefore language models, are very flexible by the nature of their architecture and produce results for any input without explicitly indicating error situations. The language models are trained in such a way that the results often correspond to the user's expectations. This can lead to them appearing correct at first glance, but being incorrect in terms of content. Errors therefore only become visible at a semantic level, i.e. at the level of meaning in a specific context. For example, it is possible for an LLM to "invent" an incorrect quotation. This is referred to as hallucinating.

Fuzziness: The LLM must provide an output for each input. For this, it receives a possibly large, but definitely limited amount of training data. It therefore derives outputs from the available data for inputs that do not appear in the training data. As a result, fuzziness occurs in such a way that two LLMs trained using the same data can provide different outputs for the same input. The fuzziness can vary greatly between different inputs and can include both true and false statements (hallucinations) that were not part of the training data.

Data-based functionality: The main functionalities of a language model are determined by the data used for training. A language model that has been trained exclusively with poetry will probably be able to generate poems, but will not be able to reproduce the logic and structures of a legal text.

7.1 Vulnerabilities of Language Models and Their Causes

LLMs are achieving great success, not least because of the apparent "omniscience" that for every input there is an output. However, the associated challenges and weaknesses should also be recognised and taken into account. Three challenges are considered below:

- Lack of explainability
- Dependence on training data
- Dynamic development favoured by flexible infrastructures

7.1.1 Explainability

It would be useful to be able to understand why an LLM has generated a certain output, especially due to the fuzziness of an LLM's answers described above. However, this is inherently impossible due to the system. It is therefore unclear which inputs were used by the LLM to generate the output and how. This means that the output cannot be "explained" retrospectively.

Language models can flexibly combine texts from the smallest components. To this end, they learn fine language structures such as sentence structure and grammar, but also semantic connections via statistical correlations. These are statistically occurring dependencies, for example, the phrase "cars drive" is more likely to be completed by "on the road" than by "on the water". In principle, the following applies: the more parameters the models contain, the better they can map all these correlations.

Larger models also require increasing amounts of data for training in order to mathematically determine the associated larger number of parameters. However, a larger parameter set also means more potential for unintended results. This could, for example, be used by attackers to obtain information from the LLM that it should not have released, such as instructions on how to build weapons.

A larger parameter set in the language models is therefore not only associated with increased capabilities, but also with larger, unknown attack surfaces that can only be reduced, not eliminated.

7.1.2 Dependence on Training Data

While the functionality of classic software systems was defined by the programme logic of computer programmes that work schematically (accounting software for bookkeeping, graphics programmes, etc.), in many LLM-based applications it consists primarily of the functionality of the language models they contain. However, if such systems with LLM-based applications control relevant actions such as administrative processes or financial transactions, vulnerabilities in the LLMs can then become vulnerabilities in the overall system. Since the functionality of the LLMs comes from the training data used, their control is of increased importance. The following aspects play a special role here:

Data selection: The immense size of the models only makes sense if correspondingly large amounts of training data are used. The manufacturers of base models therefore also control the quality and variety of possible outputs by selecting the data. This means that they have a great deal of responsibility to bear.

Public availability: The need for more and more training data also necessitates the use of publicly available data. Knowing which public data, such as Wikipedia articles, is used to train large language models can lead to this public data being manipulated (data poisoning). In addition, the public forums for models and developers offer further opportunities for manipulation.[7]

Therefore, if you can manipulate public data that is used as training data, you can manipulate the functionality of LLMs. Manufacturers can counteract this by making the extraction of training data less predictable for attackers. A possible counteraction would be the collection of training data at varying intervals. Moreover, the risk can be mitigated by employing appropriate criteria for the selection of training data.

Fine-tuning: To start with, large LLMs are trained using non-specific tasks. These are known as the foundation models or original models. In order to operate a certain type of application, they are fine-tuned with a more detailed level of training. This should increase the likelihood of desirable text outputs, such as friendliness and expertise, and reduce the likelihood of undesirable text outputs, such as hate speech and weapon building instructions. If fine-tuning is applied in different steps for various purposes, the success of one step can be reduced by subsequent steps, as these influence each other.

Patching: If an attacker can find a text input that leads to an unwanted output, this is called an adversarial example. For example, a chatbot can be “persuaded” to make unwanted statements by a longer prompt, i.e. a specific context description.

Errors in the programmed framework of an AI application can be patched in the traditional sense by a software update. This is not possible in the case of factual errors in the language model. Instead, two main approaches are currently being used to counter this. The first is appropriately adapted fine-tuning (see also above), known as alignment, which is intended to prevent the output of malicious content. The second is Retrieval Augmented Generation (RAG). Prior to utilising the LLM, the software extracts texts from a text corpus, ideally one that has been verified, to which the output is to be referenced. This means that the generated text is closely linked to the content of the extracted texts. For example, if a question is asked about the managing director of a particular company, a description page of the company could be searched for in Wikipedia, for example, and the language model could be instructed to answer the question from the text provided.

Neither approach offers complete protection against unwanted output. However, RAG appears to be more successful and robust in this area.

Filters can also restrict the input and output options. When implementing filters, there is generally an interaction between the broad utility of the models and the security of the filters.

To summarise, code-based patching of LLMs is not suitable for completely suppressing or modifying unwanted output generated from the language model. It is therefore essential to conduct comprehensive testing of the finalised model.

7.1.3 Influence of Infrastructure

The simplicity and ready availability of cloud soulutions and prepared containers may lead to a lack of consideration of the potential risks and uncertainties associated with this technology.

With the introduction of various cloud and container technologies, easy-to-use, scalable software platforms have created an ideal infrastructure for the development, exchange and commercialised use of language models. Language models also only require a very simple universal interface for text input and output, via which the entire complexity of the functionality is transported. Together, these two factors mean that even technically inexperienced users are able to create and operate their own applications.

As language models are frequently introduced as cloud services, with straightforward interfaces, the number of services utilising the capabilities of large commercial language models, self-trained or fine-tuned public models and linked traditionally programmed systems in virtual supply chains is growing rapidly. This gives rise to a large number of services, e.g. for creative writing, translation, text recognition (OCR), dictation (speech-to-text), speech synthesis (text-to-speech), sentiment and speech analysis, etc. These services can entice users to use them by offering interesting free services without them being aware of the risks, such as fuzziness.

The lack of transparency regarding the models, as well as a lack of information about models from the supply chain, makes it challenging to conduct a comprehensive safety assessment. The possibility of using adversarial examples, text inputs that lead to unwanted statements, is less linked to the specific software product than to the training data in the case of modified models in supply chains. However, due to the vector architecture of the models, these can only be identified at the overall model level, but not effectively analysed.

The widespread use of language models, the associated commercial dynamics and the fundamental vagueness of the models can pose a high IT security risk, depending on the criticality of their use. The impact of associated threats should be assessed by means of testing, for example pen testing, and by considering worst-case scenarios as part of a risk analysis.

7.2 *Misuse of Language Models*

The opportunities for misuse of language models are similar to those during the previous reporting period. Nevertheless, the BSI is noting a growing awareness and prevalence of these models in everyday life. Public awareness of both the opportunities and the risks has increased and their use has become part of day-to-day life for many people. Important risks are:

Phishing: Attackers use LLMs to generate texts for phishing messages and websites with deceptive intent, as well as to create disinformation that can have a direct and short-term impact, especially before elections. More powerful AI chatbots can now also be used for phishing and spreading disinformation.[8] There is no doubt that the various offers for such services indicate lively usage. High-quality, improved and personalised voice and image generation (deepfakes) support both blackmail attempts, such as sextortion, and the compromising of publicly active persons.

Technical attack support: Language models are used to generate and refine executable malicious code. However, their application is difficult to prove. In principle, malware attacks still require extensive expertise. However, individual procedures for breaking into software systems have already been implemented autonomously.[9] Language models can also help overcome password protection or captchas.

Cyber espionage: Language models are also a useful tool for attackers in targeted attacks. For example, a company chatbot trained with too much internal data can reveal internal information. In addition, internal company language models equipped with far-reaching rights can be useful for exfiltrating or manipulating data after initial compromise.

7.3 *Developments*

Task decomposition: In order to reduce the black box character of language models, there are approaches to break down the solution of a task into smaller steps, which can then be completed individually by language models. This line of research could lead to more transparency and greater regulability in the long term. Such research is known as XAI (Explainable AI).

Localisation/specialisation: Larger language models also mean more effort and costs for creation, operation and utilisation. However, the high performance of these larger models is not necessary for many applications. Smaller local systems could be customised to the specific environment, tasks and users.

Regional and cultural differences in the evaluation of statements support the development of localised language models, for example in European countries. Here, too, the selection of training data is of course the essential step towards achieving this goal.

As such, LLMs will undoubtedly be localised in the future.

Self-referentiality: There is already a vast number of generated texts on the web today. Because language models are trained with data that contains generated statements itself (see The State of IT Security in 2023, page 42), the problem of self-referentiality is increasing. It is impossible to predict the consequences of the interplay of this feedback loop with deliberately disseminated disinformation and unintentionally falsified information. It is therefore crucial to perform manual checks. However, it cannot be guaranteed that they will always meet the required standard, particularly given the increasing pressure on time and resources.

7.4 Conclusion

The use of language models leads to a far-reaching change in dealing with unwanted output (errors). While such errors in traditional applications can usually be clearly identified and eliminated by a patch, the undesirable behaviour in LLMs is often in the learned language models, i.e. not in the programme code, but in the data that describes the model. As such, the undesirable behaviour of LLMs is transmitted fuzzily at the semantic level.

A sustainable correction is not easily possible due to the fuzziness.

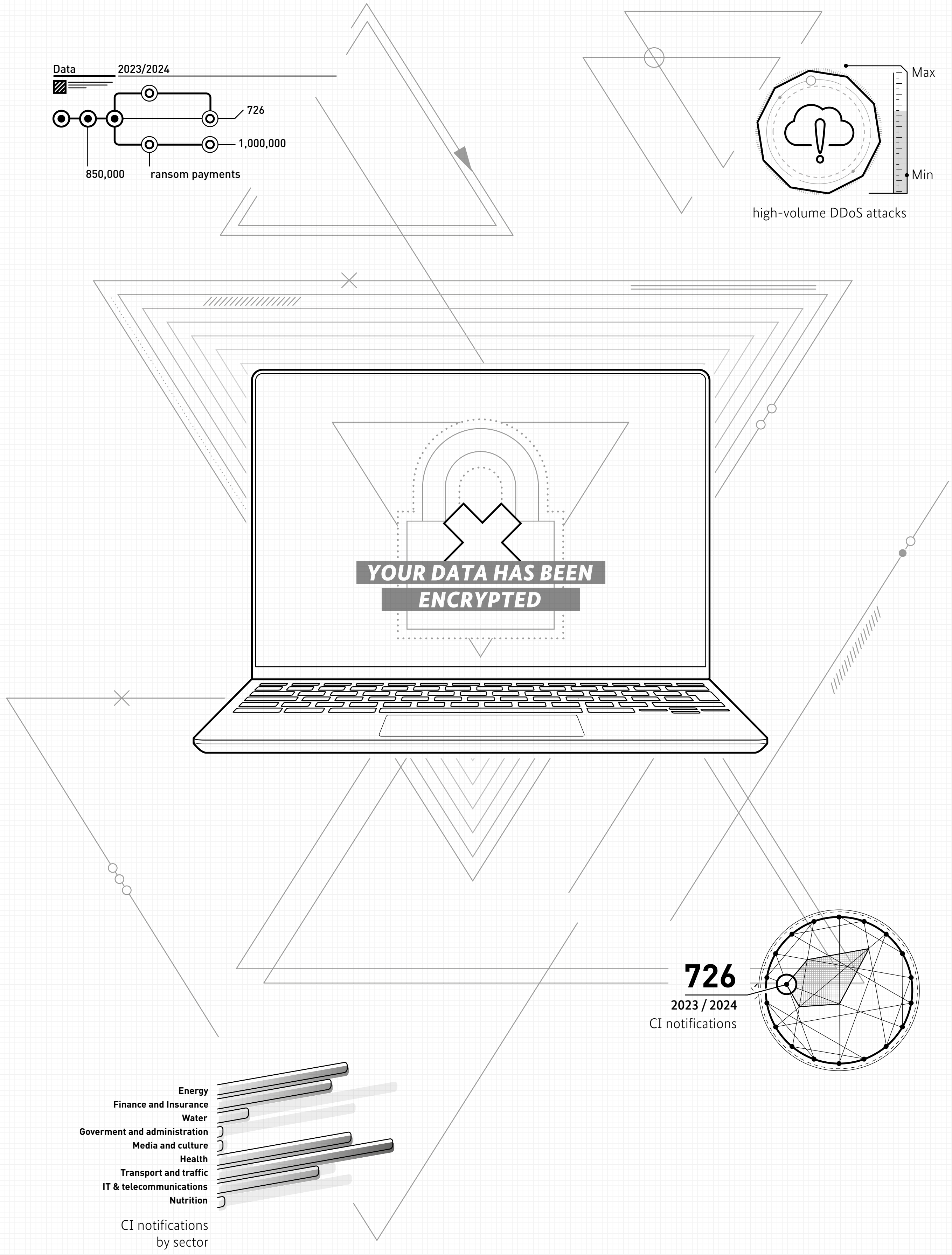
This lack of clarity has an impact on the security objective of confidentiality, e.g. because applications could output confidential information despite appropriate countermeasures and user input cannot be encapsulated in the organisation if cloud services are involved. If language models are used to obtain information, correct information that is available to the model as input, such as training data, can be falsified by the inherent fuzziness of the system. The security objective of integrity is therefore also fundamentally jeopardised. If the fuzziness of an LLM jeopardises the security objectives of the environment in which it is used, this blurring therefore represents a vulnerability.

The interpretation of the output of an LLM can either be carried out by humans or technically in order to connect automatic actions. Without human review, automated systems inevitably contain errors that are difficult to identify. Furthermore, they may also contain vulnerabilities that cannot be eliminated with absolute certainty. This represents something fundamentally new in cybersecurity and adds to the classic vulnerabilities in programme code that continue to cause problems.

Further measures must be taken for critical applications, such as human review of the results and access restrictions (least privilege), in line with the dual control principle.

The development and technical environment of language models is highly dynamic, and the new, inherent uncertainty means that security measures must be constantly scrutinised and updated. The introduction of new possibilities and feedback effects has resulted in a notable increase in complexity. For this reason, all those responsible for deployment should inform themselves comprehensively on the topics mentioned, critically scrutinise areas of application and weigh up and consider the opportunities and risks in solutions. Increased watchfulness at all levels must go hand in hand with the ability to react quickly, for example through prepared fallback mechanisms or filter modifications. The BSI aims to provide guidance on how to deal with this situation through its publications.

C ATTACK



high-volume DDoS attacks

CI notifications

CI notifications by sector

8 – Selected Common Types of Attacks

Various attacks against the state, the industry and society were observed during the reporting period. Specialised botnets are set up for DDoS attacks, for example. These bots then flood web servers with requests until they are no longer accessible.

Another example is ransomware attacks. Attackers get into the systems of those affected, encrypt data and demand money to get it back. These attacks are usually accompanied by a data leak. If the victims do not pay, the attackers threaten to publish the stolen data.

Attackers are also increasingly focussing on public cloud services. Malware, for example, restricts availability or encrypts customer data, including backups. During the reporting period, there were also known cases of attacks on the confidentiality of cloud services through identity theft.

8.1 Distributed Denial of Service

Attacks on the availability of internet services are carried out using specialised botnets (see chapter Botnets, page 15) and are referred to as distributed denial-of-service attacks (DDoS attacks). Flooding web servers with requests, for example, means that websites are no longer accessible. The aim of the attackers is to overload the attacked services to such an extent that they are paralysed.

The consequences of a DDoS attack include financial losses for service providers or online shops if they are unavailable. On the other hand, damage to image and possible unease among the population can result (see The State of IT Security in Germany in 2023, page 30).

The number of known DDoS attacks in Germany is measured by an index (see Figure 8, page 44), which averaged 101 points in the reporting period and was therefore almost exactly the same as the average value for the reference year 2021.

This was characterised by strong fluctuations. There was a notable surge in the number of attacks in the initial six-month period of 2024. In April 2024, the index peaked at almost 160 points. There was also a notable rise in the quality of attacks.

In the first half of 2023, the hacktivist groups NoName057 caused a media stir with their botnets DDoSia and Killnet by paralysing several websites of state governments and police forces, among other things, without causing any lasting damage. As a result, the attackers apparently felt compelled to further upgrade their botnets for higher-bandwidth DDoS attacks.

The proportion of high-bandwidth attacks, which reached maximum bandwidths of over 10,000 megabits per second, averaged 13 per cent per month and was therefore almost twice as high as the long-term average of 6.75 per cent. In April 2024, up to 28 per cent of DDoS attacks were identified as belonging to the particularly high-bandwidth category. Should this trend persist, it would suggest that the attackers' infrastructure is becoming increasingly sophisticated over time.

Please refer to the BSI website for detailed information on DDoS prevention and mitigation, as well as a comprehensive list of qualified mitigation service providers.

Read more about DDoS prevention and mitigation (German):

8.2 Leak Victims

Since 2021, there has been a notable trend of ransomware attacks being accompanied by data leaks. This is probably also due to the increasing resilience of potential targets to ransomware attacks.

The latest figures from IT security service provider Coveware show a temporary spike in the average ransoms paid, reaching over USD 850,000 in the third quarter of 2023[10] (see Figure 10, page 44). This is attributable to the leak attack campaign by the attackers behind Clop against MoveIT file-sharing servers (see chapter Exploitation of Zero-Day Vulnerabilities by Ransomware Attackers,

Known DDoS attacks in Germany

Measurement number

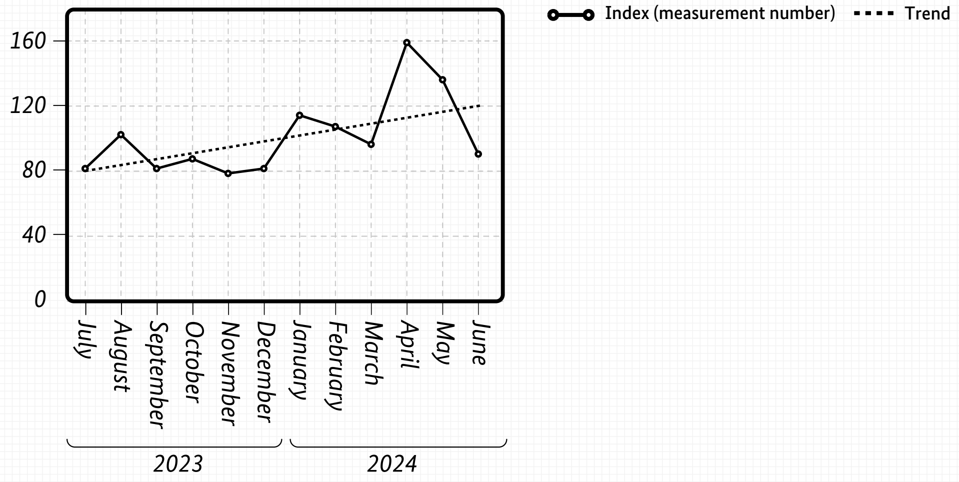


Figure 10: Known DDoS attacks in Germany (measurement number)

High-volume attacks DDoS attacks in Germany

Share of high-volume attacks in all known DDoS attacks in Germany

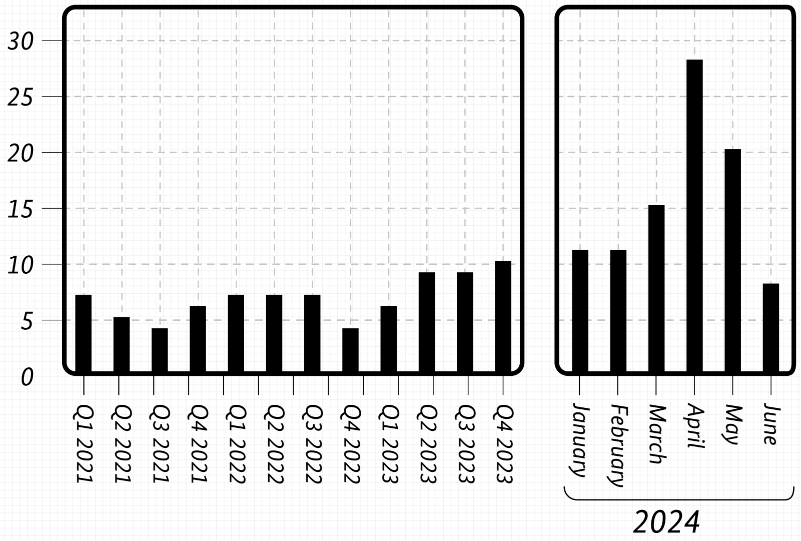


Figure 11: Share of high-volume attacks in all known DDoS attacks in Germany, source: DDoS attack statistics

Figures 10 & 11 / DDoS attack statistics:

Aim of the statistics: Structural survey of distributed denial-of-service attacks (DDoS attacks) against targets in Germany. Reported on a monthly basis. / **Population:** All DDoS attacks against targets in Germany. / **Sample:** All DDoS attacks against targets in AS 3320 (Deutsche Telekom). / **Survey design/instruments:** Monthly aggregation of an ongoing survey from Deutsche Telekom’s DDoS mitigation. / **Coverage:** Deutsche Telekom’s AS 3320 covers around 98% of targets in Germany. / **Quality assessment:** Regular comparisons with the DDoS mitigation findings of other service providers regularly confirm the structures identified in the DDoS attack statistics.It is therefore not possible to make any statements about the incidence of DDoS attacks in Germany as a whole.

page 20, and The State of IT Security in Germany in 2023, page 38). In this wave of breaches, the attackers demanded significantly more money for the stolen data than is usually the case with ransomware attacks and for encrypted data. Even though fewer companies responded to these demands, the payments made are significantly higher than before.

In the context of the campaign against MoveIT servers, over 250 individuals identified as potential victims were listed on the leak page of the attackers behind Clop in June and July 2023. This is an extraordinarily high number of suspected victims for a single attack campaign. The attackers stole data from vulnerable servers on a large scale. It would appear that the average hush money paid per case for the exfiltrated data was almost three times as high as might have been expected for pure ransom extortion (see Figure 10, page 44). In the first quarter of 2024, however, the average amount of ransoms paid fell back to the level seen at the end of 2022.[11]

Those who have taken precautions, for example by creating a functioning, restorable backup, are not obliged to enter into any ransom negotiations with the attackers regarding encrypted data. It is also worth noting that a significant proportion of victims of ransomware attacks still choose to pay the ransom, despite the risks involved. According to reports, this has fallen from 56 per cent at the beginning of 2021 to 36 per cent today (see Figure 11, page 44).[12]

If victims refuse to pay the ransom to retrieve their encrypted data, it is only a matter of time before the attackers publish the exfiltrated data. This is their next step in maintaining blackmail pressure and persuading victims to pay up.

This procedure is known as double extortion. Exfiltrated data also appears to be worth considerably more than encrypted data (see also the extortion campaign by the ransomware group Clop, which was made possible by exploiting vulnerabilities in file-sharing systems). The BSI's leak victim statistics provide information about the victims of hush money extortion. To this end, the BSI monitors so-called leak pages on which attackers publish the names and captured data of victims of their ransomware attacks if they do not pay a ransom (see also The State of IT Security in Germany in 2023, page 19 ff.).

These leak pages can therefore be used to identify suspected victims who have been threatened with the publication of their data. In this respect, the leak victim statistics are not statistics on ransomware attacks, but on victims of hush money extortion. This is why the term "alleged victims" is also used, since being named on a leak page that is under the control of an attacker does not necessarily mean that an attack actually took place. In some cases, attackers explicitly name victims with the sole intention of extorting money from them, even if no actual attack has taken place.

Average ransom payments by quarter

In US dollars

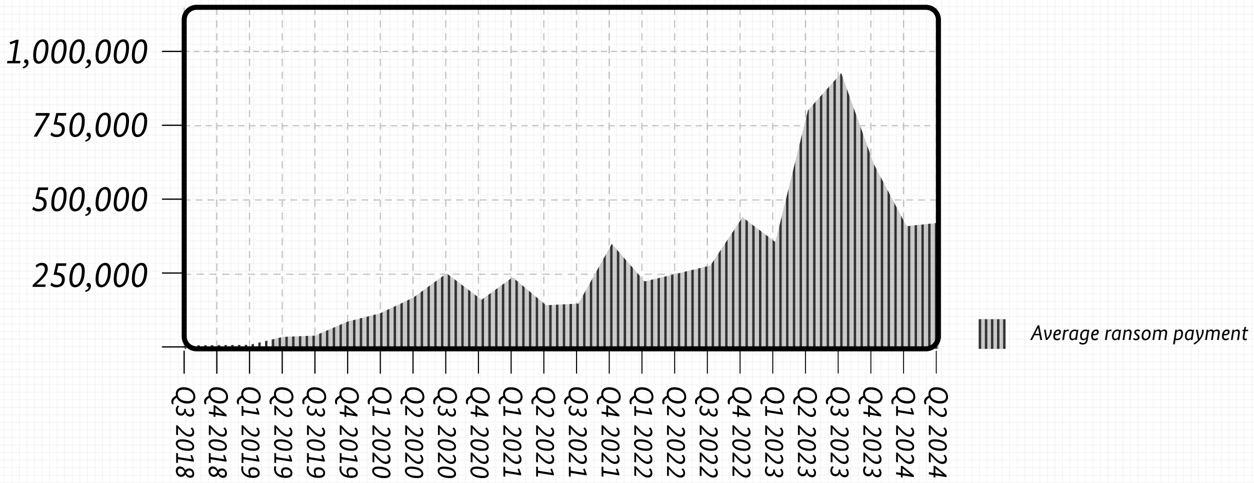


Figure 12: Average ransom payments by quarter (dollars), (Source: Coveware)

The number of suspected victims increased significantly in 2023 compared to previous years (see Figure 12, page 45). In 2023, the global average was almost 1.7 times higher than in the reference year 2021. Germany was no exception. This corresponds to an increase of almost 50 per cent worldwide and almost 30 per cent in Germany within a year. The preliminary peak of the timeline was reached in the second quarter of 2023 with 1,395 recorded suspected victims worldwide and 65 suspected victims from Germany (see Figure 13, page 47).

The main factors behind this increase were probably the sustained high to very high level of activity by the most threatening actors (see chapter Ransomware Groups, page 19).

The BSI also noted the presence of several leak pages that were active for a relatively brief period or included a significant number of potential victims through individual campaigns. In addition, the BSI recorded an increase in activity across the board on all leak sites monitored.

The five most active leak sites are regularly responsible for around 40 per cent of alleged victims. They are briefly presented below. More information can be found on the BSI website.[13]

The ransomware group behind the LockBit RaaS was the most active ransomware, both in Germany (see Figure 14, page 48) and worldwide (see Figure 15, page 48). The LockBit leak site named a total of over 944 alleged leak victims worldwide during the reporting period. The Alphv ransomware group (also known as BlackCat) was first observed in November 2021. Alphv, together with LockBit, was one of the most threatening ransomware families during the reporting period.

The Alphv ransomware-as-a-service (also known as BlackCat) was first observed in November 2021. In March 2024, the operating group ended the Alphv ransomware-as-a-service with an exit scam against its affiliates. The operators therefore retained the ransom paid for the exit scam, did not share it with affiliates and could no longer be reached by affiliates or those affected. Alphv, together with LockBit, was one of the most threatening ransomware families during the reporting period.

The Play ransomware has been active since at least June 2022. In addition to ransomware, the attackers also rely on a leak site for double extortion identified in November 2022. According to current knowledge, the Play ransomware is reserved for an exclusive group of affiliates (RaaS partners) and is therefore classified as a closed ransomware group.

The attacker group behind the Clop ransomware generated the majority of the suspected victims observed for this attacker with two major attack campaigns in 2023. As far as the BSI is aware, the attackers did not use ransomware in either attack campaign, but stole data from vulnerable file-sharing servers.

The 8Base ransomware group has probably been active since 2022. The leak site for this ransomware group became known in May 2023. The 8Base ransomware is based on Phobos ransomware. Unlike other RaaS, Phobos offers a model that allows individual branding. Accordingly, many ransomware families are known that are effectively Phobos by another name. Phobos ransomware also does not have its own leak site.

The Black Basta ransomware group first appeared in April 2022. It is believed that Black Basta is connected to the Conti group, as evidenced by recent public reports. Conti fragmented in May 2022 and has been inactive since June 2022. The BSI considers the Black Basta ransomware group to be a separate threat, independent of Conti.

Ransomware attacks are occasionally flanked by other blackmail methods to increase the pressure on the victim to pay. For example, some attackers actively approach customers of victims and inform them that sensitive data about them has been exfiltrated due to an unpaid ransom. Various attacker groups also threaten to resell the captured data so that it can be misused for further cyberattacks. In addition, individual attacker groups use DDoS attacks during the negotiation phase to emphasise their ransom demands (see The State of IT Security in Germany in 2023, page 21 f.). In the current reporting period, one case became known in which attackers from the Alphv ransomware group allegedly attempted to report a victim to the US Securities and Exchange Commission (SEC). The BSI can confirm that this is the first publicly known case in which attackers have carried out their threat to report a victim to a regulatory authority.

At the end of 2022, the BSI observed a trend among cybercriminal groups to dispense with encryption and simply steal the data instead. This trend did not continue within the reporting period. Although the BSI is still aware of groups that probably only rely on blackmail with stolen data, this approach has not become widespread. However, it can be assumed that pure data theft will continue to be used as a means of blackmail in the future – alongside data encryption or double extortion.

Ransomware victims who paid a ransom

Share in % of all ransomware victims

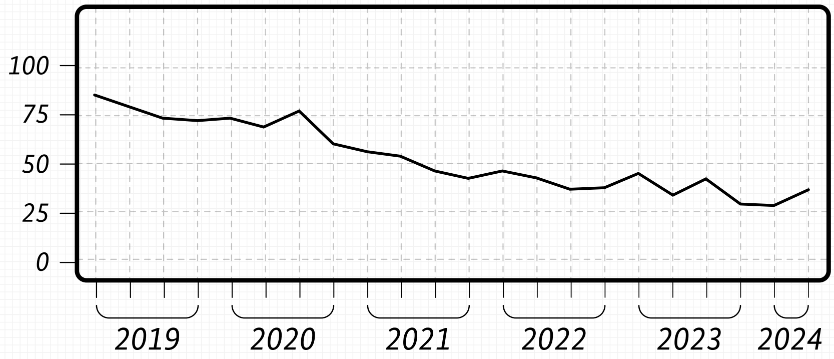


Figure 13: Ransomware victims by payment behaviour (per cent), (Source: Coveware)

Alleged victims on leak sites from Germany and around the world

Number

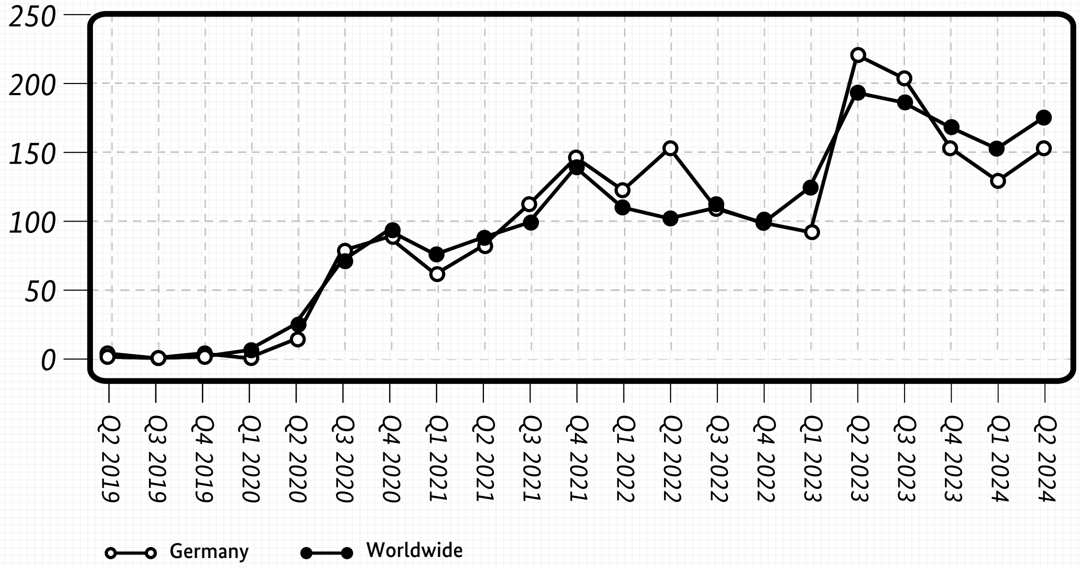


Figure 14: A comparison of alleged victims on leak sites from Germany and around the world (2021 = 100)

Alleged victims from Germany on leak sites

Number

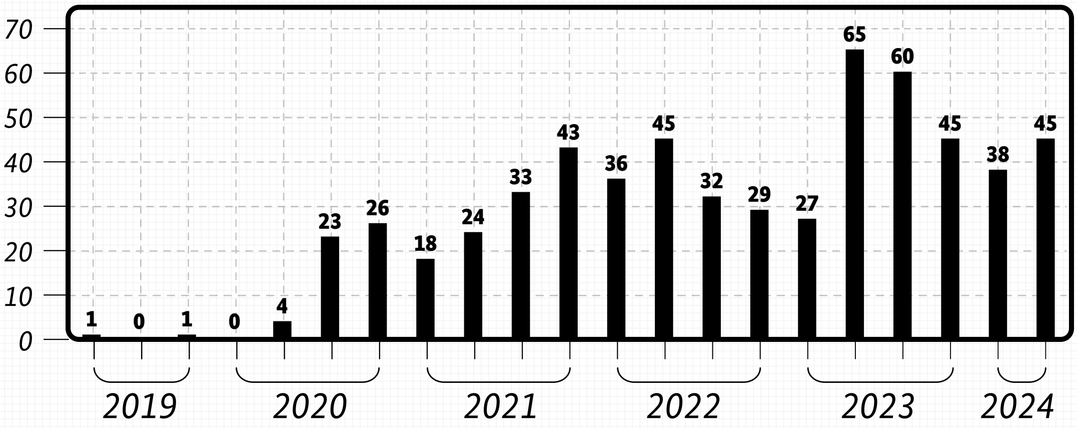


Figure 15: Alleged victims from Germany on leak sites (number)

Alleged victims from Germany according to leak sites

Shares

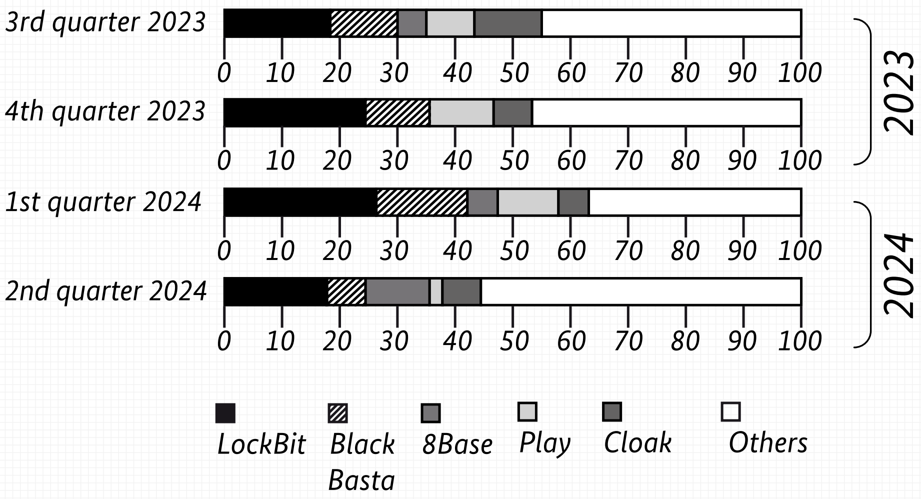


Figure 16: Alleged victims from Germany on leak sites (per cent)

Alleged victims worldwide according to leak sites

Shares

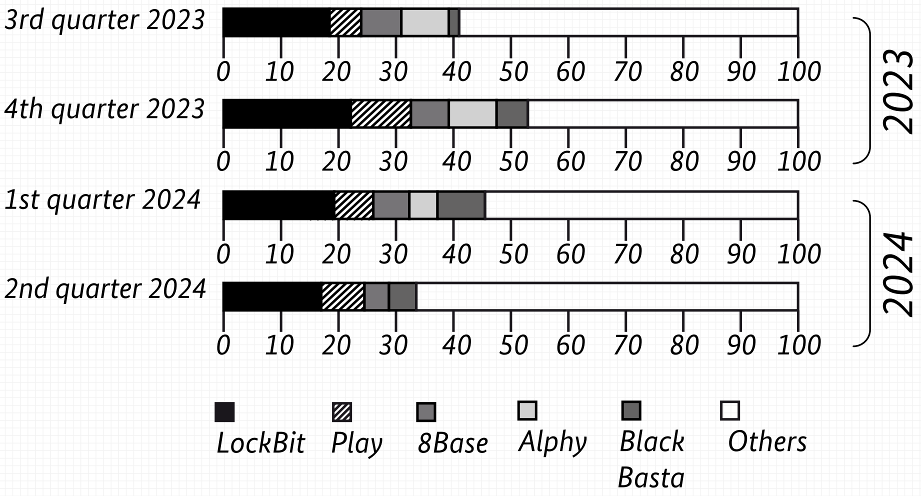


Figure 17: Alleged victims worldwide according to leak sites (per cent)

Figures 14, 15, 16 & 17 / Leak victim statistics:

Aim of the statistics: To identify the victims of data leaks who have not paid a ransom after a ransomware attack and whose data has therefore been published on a leak website of an attacker group in order to increase the blackmail pressure. / **Reported quarterly. / Population:** All dedicated leak sites on which the data of victims of data leaks resulting from targeted cybercrime attacks (ransomware attacks and attacks against new vulnerabilities) were published. / **Sample:** Full survey of known leak victims. / **Survey design/instruments:** Detection of data service providers, reports from victims and public sources. / **Coverage:** No statement on the number of underlying attacks, but on the number of victims unwilling to pay whose data was published on a leak page. No differentiation between ransomware victims and victims of data exfiltration through vulnerability exploitation. / **Quality assessment:** High global coverage with comparison of different data sources.

Takedowns

During the reporting period, law enforcement officers managed several takedowns against ransomware-as-a-service in internationally coordinated measures. These achievements illustrate the mounting pressure to prosecute cyber criminals.

In an internationally coordinated operation between 16 and 20 October 2023, law enforcement officers seized the leak site, crypto wallets and server infrastructure of the RagnarLocker RaaS. At least one main suspect was also arrested. Due to the arrest of a suspected developer of the ransomware and the seizure of several servers, RagnarLocker is not expected to return. There is no evidence of the group having rebranded under a different name.

On 19 December 2023, law enforcement officials announced an internationally coordinated operation against Alphv RaaS. Parts of the server infrastructure were confiscated and some key material was seized. A few days after the measures, the operators of Alphv RaaS set up a new infrastructure and tried to keep their affiliates at the RaaS. Attacks with Alphv continued to be observed. On 3 March 2024, the operators of Alphv RaaS were subjected to an exit scam and the operators' infrastructure was no longer available from 4 March 2024.

On 19 February 2024, law enforcement authorities carried out a comprehensive takedown against the LockBit RaaS. Between 24 and 26 February 2024, a new leak site for the LockBit RaaS was observed, on which new suspected victims were also named. In March 2024, a large number of suspected victims were published on the leak site. According to the BSI, a large number of the suspected victims named on the leak site since March 2024 are incidents that took place before the takedown and in which a ransom was probably also paid. However, actual attacks with the LockBit RaaS can still be observed.

After takedowns against cybercriminal services, the BSI often observes a temporary decrease in activity in the field in which the service was active. However, it has so far only been a matter of several weeks or months before existing or new cybercriminal services have filled the resulting gap. Attackers also learn from the countermeasures taken by law enforcement officers in order to evade them in the future.

8.3 *Attacks on the Cloud*

During the reporting period, there were several successful ransomware attacks on public cloud services that restricted their availability, for example in summer 2023. During the relocation of a cloud provider to a new data centre, the servers to be migrated were connected to the provider's internal network. Malware that had previously been on one of the servers was able to spread to the other servers. As a result, the majority of the provider's systems and customer data, including their backups, were encrypted. The provider's IT department was able to restore the provider's own systems. In most cases, however, customer data was irretrievably lost if it had no further backup.

In addition, several cases of attacks on the confidentiality of cloud services through identity theft, both of users' identities and of the provider's staff, have been reported. For example, attackers managed to carry out token forgery at a major cloud provider by stealing a signature key and imitating the identities of legitimate users of the cloud service. This made it possible for the attackers to access their data. After the attack became known, the signature key and the tokens signed by it were blocked by the provider to prevent further exploitation by the attackers.

At another cloud provider, the compromise of a service account allowed attackers to access the customer support system and exfiltrate customer support requests. The requests also contained confidential data, which the attackers used in some cases for session hijacking attacks against the affected customers. After the compromise was detected, the affected service account was deactivated and sessions associated with it were terminated.

Public clouds are attacked continuously, sometimes successfully. However, the greatest risks when using the cloud lie with the users themselves: there have been many incidents resulting in data loss due to misconfigurations in ID management. The Thales Group's "2023 Cloud Security Study" report also concludes that 55 per cent of all cloud-related data leaks in the companies surveyed were due to human error.

Compromise of the Microsoft Cloud Infrastructure

Situation

On 11 July 2023 (and subsequently on 14 July 2023, 6 September 2023 and 12 March 2024), Microsoft wrote a blog post to report a successful attack on OWA (Outlook Web Access) and Outlook.com accounts by a suspected Chinese state-sponsored attacker group known as Storm-0558. In the course of this attack, the attackers managed to gain unauthorised access to the email accounts of around 25 organisations worldwide, including government institutions.

The attack vector was the compromise of a Microsoft signature key. Signature keys are used to prove the authenticity of access tokens employed to authenticate users. By accessing the signature key, the attackers themselves were able to create valid access tokens (token forgery).

The compromised signature key was only authorised to sign access tokens for Microsoft consumer accounts. However, a regression in the identity validation logic provided by Microsoft and used by the affected email services extended the scope of the signature key to Microsoft consumer accounts and enterprise accounts.

It is not yet known how the attackers obtained the key.

Assessment

According to Microsoft, the access gained by the attackers was only utilised for OWA and Outlook.com, but other services could presumably have been affected. Furthermore, according to Microsoft, the affected group was limited to around 25 organisations that were actually impacted. As a result, the actual extent of the damage was significantly less than the potential damage.

The incident shows that public clouds can also be successfully attacked. However, cloud-inherent capabilities, such as sophisticated logging and detection options, made it possible to detect, comprehensively analyse (including a reliable assessment of the blast radius) and contain the attack.

Response

The attack was initially detected by one of the affected Microsoft customers, who notified Microsoft on 16 June 2023 that an analysis of its log data had revealed abnormal Exchange Online data access. Microsoft then implemented mitigation measures until 3 July 2023, which, according to its own information, prevented the continuation of the attack with the compromised key – customer intervention was therefore not necessary. In particular, these mitigation measures include blocking the signature key and the access tokens signed by it. Furthermore, according to Microsoft, the affected group could be precisely determined by analysing the existing log data, and subsequently informed.

As a result of the incident, the US Department of Homeland Security's Cyber Safety Review Board (CSRB) announced in August 2023 that it would look into the case. The resulting report was published on 2 April 2024 and criticises Microsoft: according to the report, the incident could have been avoided and Microsoft's security culture was inadequate. In addition to presenting the findings of the investigation, the report also contains a list of recommended security measures and technical improvements aimed at Microsoft and other cloud providers.

The BSI also looked intensively into the technical background of the incident and possible defence measures in view of the attack techniques used and was in direct contact with Microsoft from the outset.

As a result of this mutual exchange, Microsoft published a technical whitepaper on the correct use of Double Key Encryption (DKE). For the first time, customers will be able to assess the protective effect of DKE and any residual risks depending on their deployment configuration and correctly use it accordingly. Under these conditions, DKE represents a possible mitigation measure against the attack techniques used here.

9 – Threats to Society

Various approaches are needed to strengthen consumers' resilience to online threats such as phishing. On the one hand, the focus is on raising awareness, educating and informing consumer about risks and safety measures. This also includes topics of emergency preparedness and crisis management for when consumers need to deal with IT security incidents in the private sphere. On the other hand, cybersecurity through active technical protective measures on the part of the provider as well as the promotion of secure and user-friendly products (usable security) are of great importance. This includes establishing practicable security standards in the development of digital products and services (security by design, security by default) as well as a transparency obligation on the part of manufacturers and providers with regard to their IT and data security measures. Effective digital consumer protection is a task for society as a whole. Cooperation, networking and exchange between IT security stakeholders from civil society, academia, business and the public sector should be further promoted in order to strengthen the resilience of consumers in the digital space.

The BSI plays a central role in preventing, detecting and responding to IT security risks. Evidence-based work such as surveys or studies in the consumer market form an important basis for continuously improving IT security for consumers in dialogue with manufacturers and providers.

Study

At the beginning of 2024, the BSI published the study "IT security in the digital consumer market: focus on tax declaration apps". Across the nine apps examined, 97 security flaws, including 75 vulnerabilities, were discovered and subsequently rectified in dialogue with the manufacturers. A lack of security updates, inadequate password guidelines and the absence of an option for two-factor authentication are some of the shortcomings that have been reported to the manufacturers.

Read more about the study on tax declaration apps (German):

9.1 Threats on the Digital Consumer Market

In the 2024 Cybersecurity Monitor (CyMon), the extent to which consumers are affected by cybercrime is at a similarly high level as in the previous year's survey. Around a quarter of respondents have already been affected by cybercrime (24%; 2023: 27%). Compared to the previous year, the damage suffered in terms of loss of trust (30%; 2023: 33%), time lost (24%; 2023: 26%) or emotional damage (23%; 2023: 23%) has barely changed. The loss of trust in online services continues to be the most frequently mentioned form of damage. However, the number of people who suffered a financial loss in the last 12 months has increased (26%; 2023: 18%).

The survey also shows that the proportion of consumers affected by cybercrime remains constant. As in 2023, 15 per cent of respondents stated that they had been the victim of a phishing attack in the last 12 months.

For more information about the current citizen survey on cybersecurity in cooperation with the Police Crime Prevention of the Federal States and the Federal Government (ProPK) and the BSI, go to:

During the reporting period, the BSI Service Centre received 8,244 enquiries from consumers. That is an average of 687 calls per month that the BSI receives and answers regarding consumer concerns. More than a third of enquiries (39%) related to specific IT security incidents. Here too, phishing, including the vishing and smishing variations, was the most frequently mentioned concern among enquirers (35.3% of all reported IT security incidents).

Data Leaks of Consumer Data

Since the beginning of 2024, the BSI's market observation has been recording data leaks of consumer data in a structured manner. From this, findings are derived about the extent and progression of the impact on consumers in Germany. The collected data shows that names (83%) and email addresses (53%) were the most frequently leaked information. In more than a third of all cases other personal information, such as address and date of birth/age and telephone numbers, are also affected. Around a quarter of the data leaks involved sensitive information, such as payment data or national insurance numbers.

In 14 per cent of the registered cases of data leaks consumers in Germany were directly affected. In 46 per cent of the cases, it can be assumed that no consumers from Germany have been affected. In 40 per cent of cases, the person affected is unknown or cannot be clearly determined. It is clear that data leaks are not limited to national borders.

Case Study of a Data Leak

On 23 September 2023, a cloud PC gaming service provider was allegedly the victim of a data leak incident in which consumer data was exfiltrated. According to the company's information, the attack first became known through a blackmail message. After forensic examination of the IT systems, it became known that the data leak was caused by stolen session cookies and subsequent misuse of one of the company's accounts. All in all, data of 500,000 customers was exfiltrated, which could be traced back to around 60,000 affected consumers in Germany. The leaked data included names, email addresses, dates of birth, billing addresses and credit card expiration dates. In dialogue with the company it was revealed that the company had informed customers about the incident and warned them about the possibility of phishing emails based on the data obtained, as well as potential risks of account takeovers.

The BSI is in favour of dealing transparently with data leaks and communicating appropriate assistance to consumers so that they can protect themselves from further potential damage.

Share in % of affected consumers

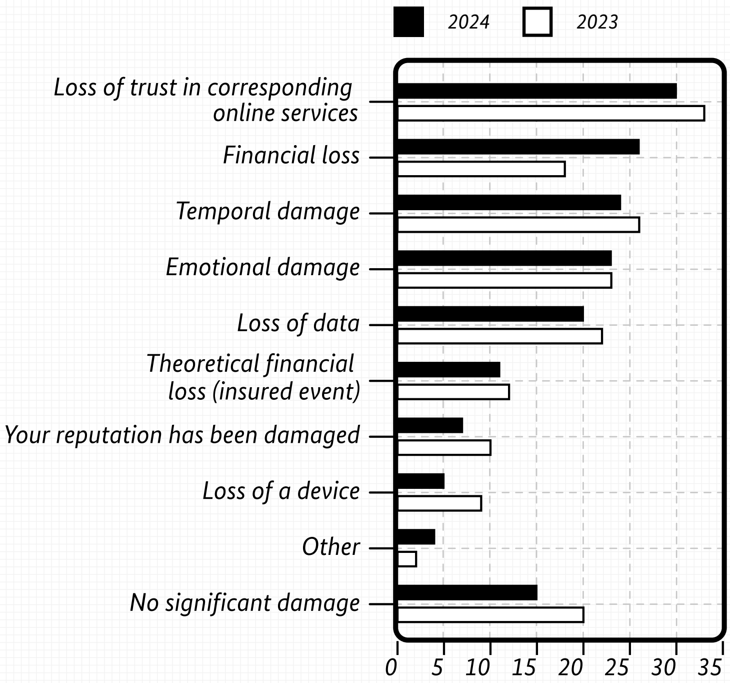


Figure 18: Damages of consumers affected by cybercrime (CyMon 2023 and 2024, multiple answers possible, in %, n = 3,012 (2023) / 3,047 (2024)

Enquiries from consumers to the BSI Service Centre

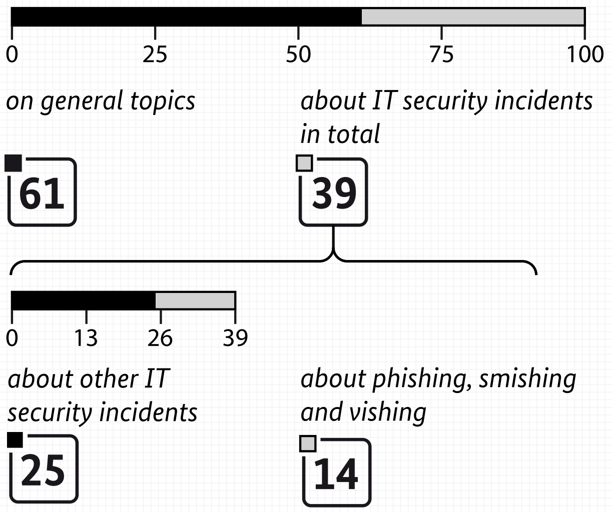


Figure 19: Enquiries from consumers to the BSI Service Centre

Type of leaked information by frequency

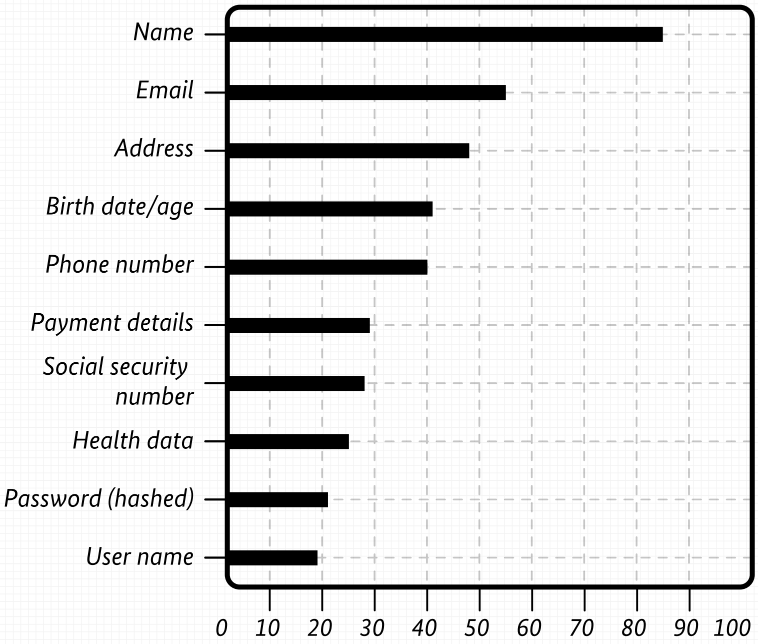


Figure 20: Type of leaked information by frequency (cases involving consumers, multiple items possible, in %, n = 98)

Affectedness of consumers from Germany

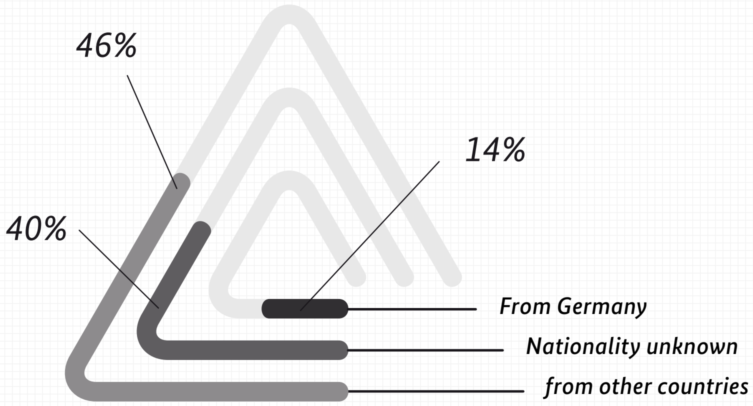


Figure 21: Affectedness of consumers from Germany in registered data leaks (in %, n = 141)

Which of the following channels do you use to search for information about cybersecurity?

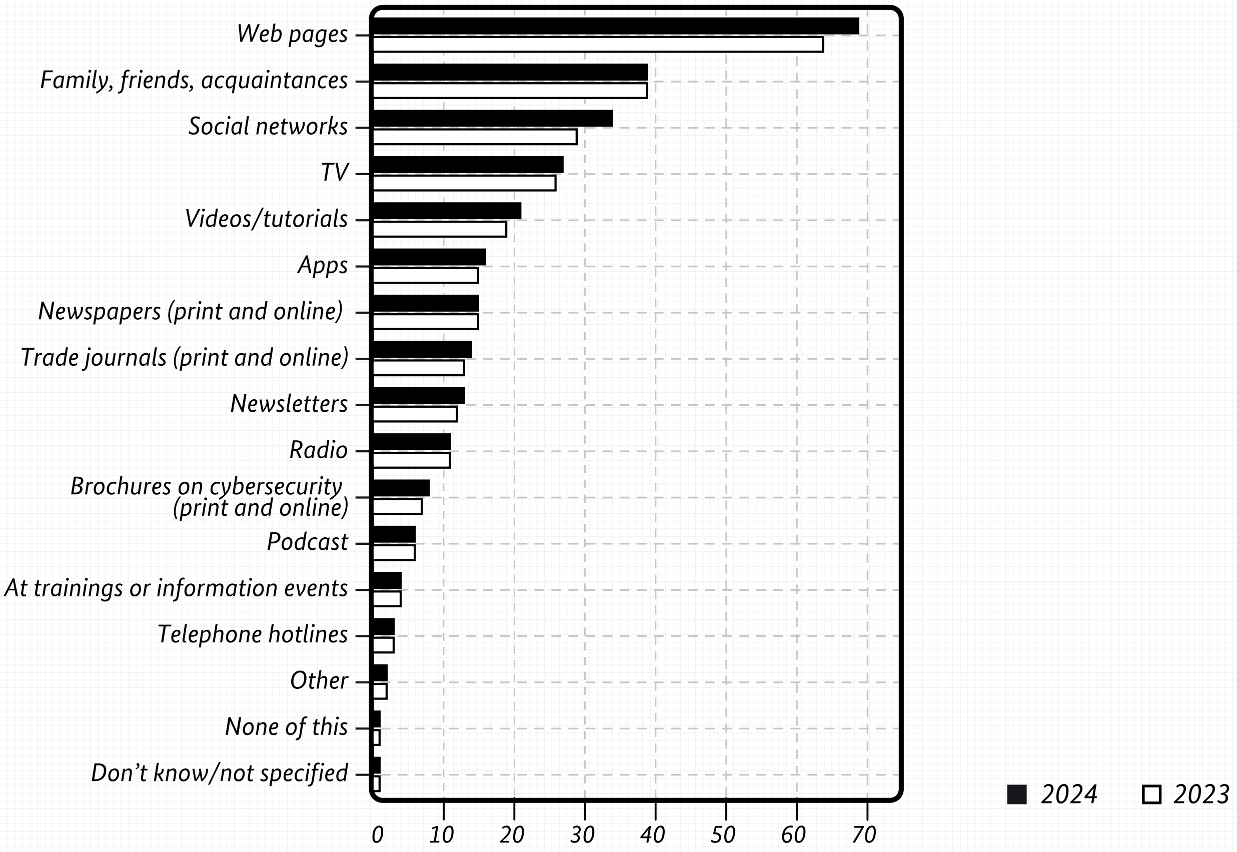


Figure 22: Which of the following channels do you use to search for information about cybersecurity?
Source: Cybersecurity Monitor 2024

9.2 *Threats in Social Media and Networks*

The term social media stands for many different digital communication and dissemination channels. What is new is that texts, images and videos are no longer just of human origin, but are generated in part by applications based on artificial intelligence. The threat situation in social networks has been exacerbated by AI-generated disinformation. This is because untruths spread more quickly thanks to the technical possibilities, especially if they are not recognisable as having been manipulated. Disinformation campaigns can be played out to specific target groups and based on algorithms with comparatively little effort.

At the same time, it must be noted that people include social networks in their information and search behaviour, in this case in their search for information regarding cybersecurity (see Figure 20, page 56). More than one-third of respondents use social networks to search for information – and the trend is increasing.

Respondents in the 16 to 39 age group in particular are increasingly using social media as a source of information (see Figure 21, page 56). This raises the question of whether users can recognise what is fact and what is fake.

This reveals cautious interventions by the controlling network operators. Technical restrictions and a desired balance between freedom of expression and the protection of other users are key challenges here.

Focus: Social Bots, Disinformation and Artificial Intelligence

Automated accounts can be used to influence and manipulate users in a targeted manner. These social bots can behave similarly to humans. Through targeted likes, sharing and commenting on certain content, they can simulate supposed interest and thus influence the recommendation algorithms of the platforms so that they suggest desired content more frequently. In this way, manipulated and falsified content can be distributed automatically and on a large scale. Increasing politicisation and attempts at instrumentalisation are the order of the day, especially in the context of geopolitical situations or upcoming elections. The platforms record a significant increase in such activities, particularly in the run-up to elections.

Under the EU’s Digital Services Directive, the operators of very large online platforms are obliged to moderate or remove content based on certain criteria with regard to systemic risks. However, these requirements have not yet been sufficiently implemented in practice. One reason for this is that new and faster obfuscation tactics make it more difficult to distinguish fake content (disinformation) from serious information. The spread of disinformation is often supported by AI-based social bots.

The platforms themselves are now increasingly using AI-based methods to recognise dubious content and accounts. The aim here is to permanently strengthen the mechanisms used for detection.

Cybersecurity information sources used

Information sources by age in %

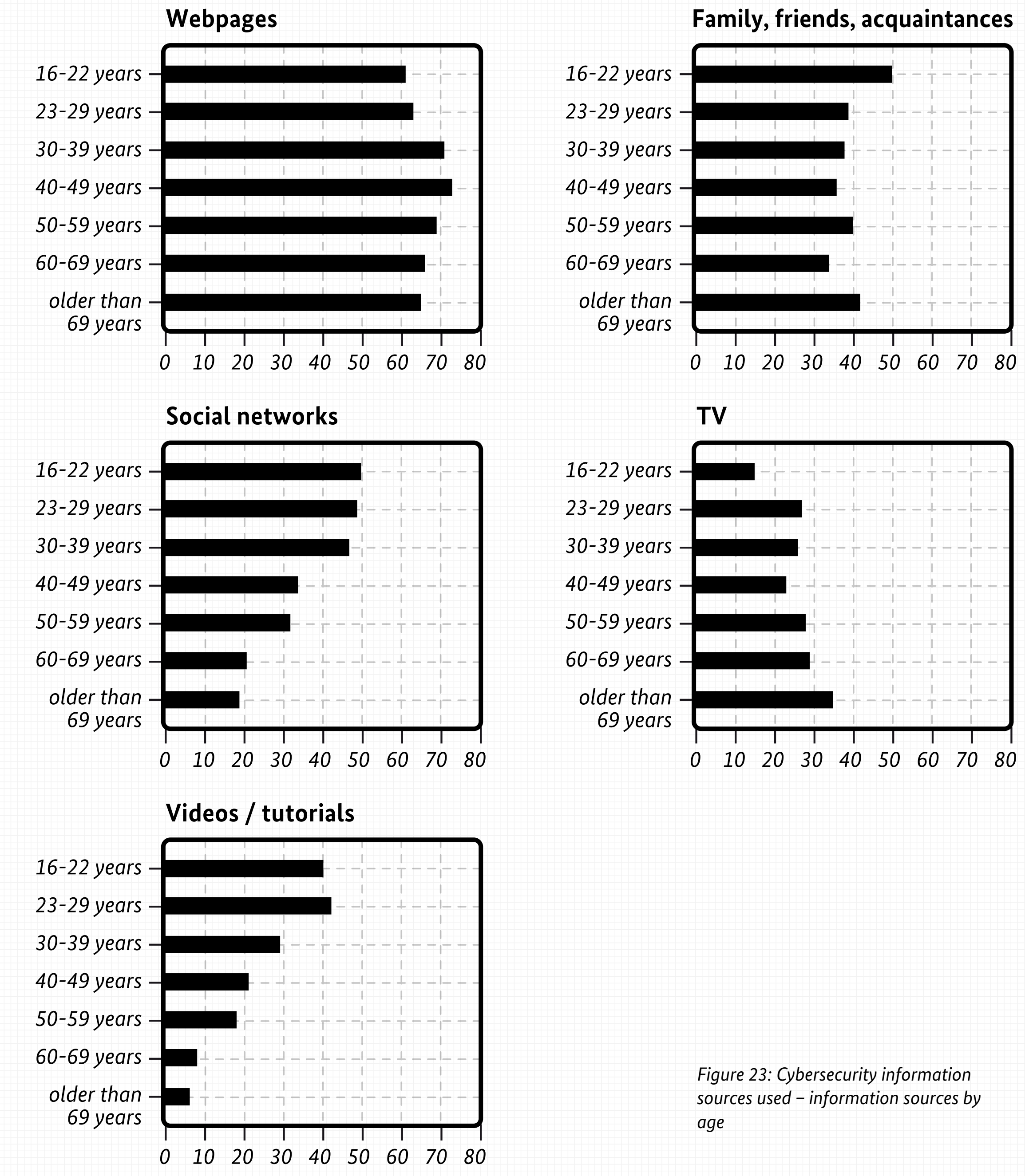


Figure 23: Cybersecurity information sources used – information sources by age

10 – Threats to the Industry

As in previous years, cyber risks will continue to be one of the top 10 threats for companies worldwide in 2023.[14] Cybersecurity must be put on the agenda by company management and viewed as a company-wide risk. According to a recent study by Pricewaterhouse Coopers, awareness at management level has increased. For example, 42 per cent of the managers surveyed stated that they felt threatened by cyber risks.[15] Those responsible perceive cybersecurity as a decisive factor for corporate security, but also as a competitive advantage. This is reflected in concrete measures. Companies are investing more in IT security. Spending on IT security budgets in companies has risen continuously since 2020. The Federal Statistical Office assumes an annual growth rate of 10.5 per cent for the period between 2020 and 2025.[16] In 2023, around 8.5 billion euros was invested in cybersecurity, more than ever before. The BSI welcomes this development and has long recommended fixed minimum expenditure for in-house cybersecurity measures.

Strong Threat

At the same time, companies are increasingly exposed to cyberattacks. According to estimates by the digital association Bitkom, German companies suffered losses of around 206 billion euros in 2023 due to digital attacks, industrial espionage and sabotage.[17] According to Bitkom, 148 billion euros of this – i.e. three quarters of the total loss – is attributable to cyberattacks, the biggest threat. The attacks on commercial enterprises are widespread. On the one hand, large companies with strong sales continue to be attacked. At the same time, ransomware attacks in particular are also becoming a mass business due to the lower technological effort involved in using ransomware-as-a-service. As already described, criminals often take the path of least resistance, so that not only small and medium-sized companies (SMEs), but also municipalities, universities and research institutions are increasingly affected. SMEs in particular often have a lower budget for cybersecurity or the topic is generally not high enough on the agenda (see chapter Threats to SMEs in Germany, p. 66). The BSI believes that this professionalisation is helping to create a cybercrime black market economy (see chapter on Ramsomware Groups, page 19). Companies do not face a single attacker, but an efficiently organised attacker industry based on the division of labour. In the international environment, cybercriminals supported or tolerated by some states find safe havens for their activities.

The BSI continues to see ransomware as the greatest threat to commercial enterprises (see chapter Cybercriminal Black Market Economy, page 19). Other frequent damage is caused by phishing, malware and password theft.[18] The damage caused by such attacks is often accompanied by a feeling of insecurity regarding successful digitalisation – with sometimes serious consequences for the innovative capacity and digital transformation of affected businesses.

Businesses are also challenged by the changing global security architecture. Businesses and research institutions are concerned about becoming the target of politically motivated espionage, industrial espionage or politically motivated cyberattacks[19] – (see chapter Cyber Activities within the Context of Geopolitical Tensions and Conflicts, page 22).

Future Challenges

Companies are already increasingly relying on the use of artificial intelligence. The influence of AI on the industry will undoubtedly continue to increase in the future. In a recent study, 70 per cent of the companies surveyed stated that the use of AI will significantly change the way companies develop and work.[20] At the same time, however, 64 per cent also see an increased IT security risk here, thus expressing their current uncertainty regarding this new technology. The BSI is in favour of a pragmatic use of AI and provides assistance for the use of AI in companies. Companies that want to benefit from the productivity gains of using AI must invest in cybersecurity in order to be able to master this technology securely.

Read more about the use of AI in companies (German):

Resilience and Cooperation

The increased awareness of cyber risks should be reflected, first and foremost, in appropriate protective measures. Taking concrete steps to protect one's business is essential. Businesses need to continue to invest in their resilience in order to position themselves well in this threat landscape. This includes technical and organisational measures such as regular security updates, backups and employee training, certifications in accordance with ISO 27001 and IT Grundschutz. While large companies are generally well positioned in this respect, SMEs urgently need to catch up (see chapter Threats to SMEs in Germany, page 66). The BSI provides numerous services for SMEs. When it comes to drawing up emergency plans, businesses of all sizes can intensify their measures. Less than a third of all businesses have a written emergency plan. The BSI offers an easy introduction to emergency management with its "Catalogue of measures for emergency management"[21] and an overview document for the SME target group.[22] Just as important as the implementation of resilience measures is the regular practice of these measures. A backup is only useful if it can be restored. Another important tool for greater resilience is the BSI standard 200-4 for holistic business continuity management (BCM). The practical guide helps to minimise the interruption of operations after a specific IT security incident.[23]

Another key factor is exchange and communication on security incidents. More and more companies are handling incidents transparently and informing the public and their customers. This helps to close potential security gaps more quickly and prevent damage to other companies, but also to publicise examples of how companies have successfully improved their cybersecurity using best practices. The BSI offers the opportunity to report an incident via the reporting and information portal and thus contribute to the situation.[24]

Cybersecurity is a team effort. Cooperation creates resilient, sustainable structures. The BSI contributes to this with its services for industry, such as the publication series "Management Blitzlicht" (Management Spotlight) and the Alliance for Cyber Security network.

10.1 *Threats to Critical Infrastructures*

Critical infrastructures (CI) are organisations or facilities that are important for the state community, the failure or impairment of which would result in lasting supply bottlenecks, significant disruptions to public safety or other dramatic consequences. CIs form a crucial basis for the functioning of our society. However, their importance is sometimes only recognised when there is a disruption. All critical services are particularly dependent on smoothly functioning IT.

Ongoing Heightened Threat

The threat situation for companies remains tense and the number of cyber incidents is increasing. This also applies to the subset of companies that belong to the critical infrastructures (CIs). Successful attacks on CI operators can not only lead to economic damage, but can also have an impact on the supply of critical services to the population. To meet these challenges, operators must achieve and maintain a high level of cybersecurity.

Reporting Improves the Situation

Section 8b (4) of the Act on the Federal Office for Information Security (BSI Act - BSIG) stipulates a reporting obligation for CI operators. The reporting obligation applies to disruptions that have led or could lead to a failure or to a significant impairment of the functionality of the CI. However, the National IT Situation Centre also accepts voluntary reports. During the reporting period, the BSI received 726 reports (2023: 490).

Management Systems for Information Security and Business Continuity

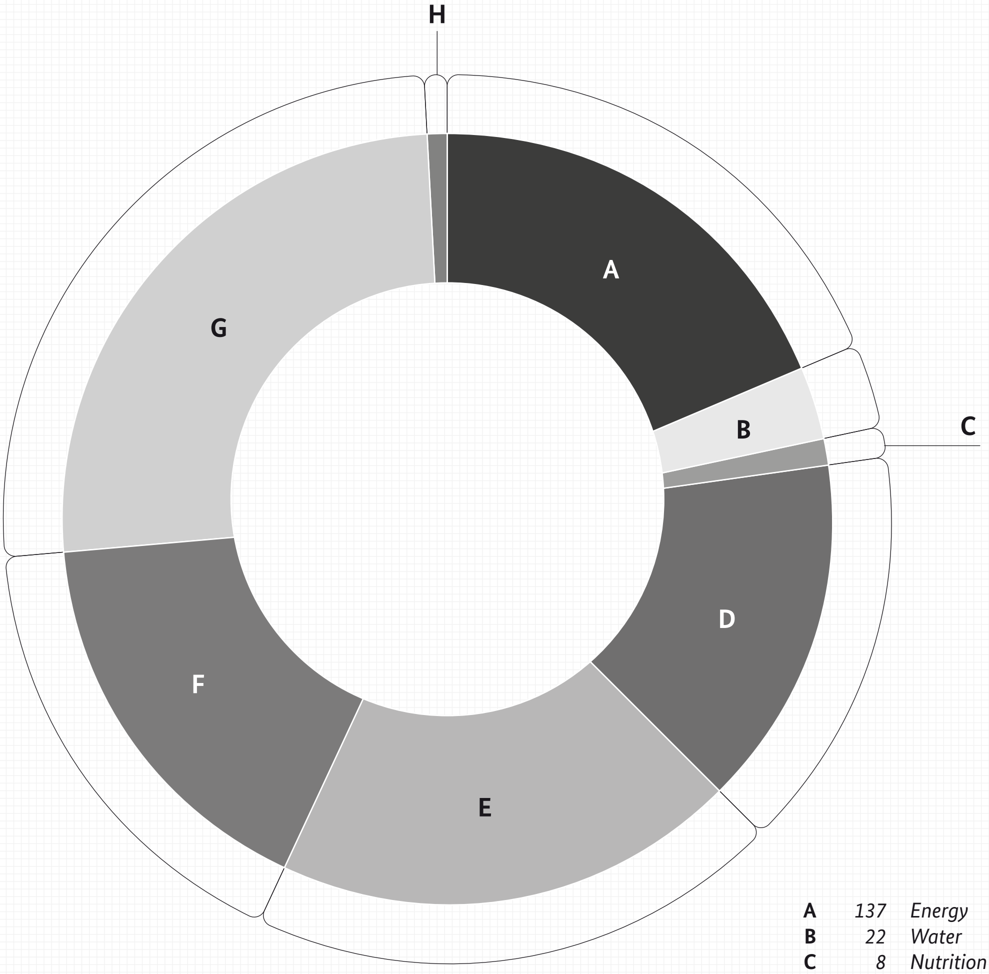
The regular audit reports of CI operators contain an assessment of the effectiveness of the information security management system (ISMS) and business continuity management system (BCMS). The auditing body uses a maturity model to assess the level of the management systems implemented by the operator. The BSI's guidance on audit reports in accordance with Section 8a (3) BSIG describes the maturity levels for ISMS and BCMS on page 62.

Regular determination of the maturity level in the course of providing audit reports enables the documentation of ISMS and BCMS maturity across audit cycles. The determination of maturity levels has proven to be a practical method to give the BSI an initial impression of the degree of implementation of the management systems.

Intrusion Detection Systems

With the IT Security Act 2.0, the use of intrusion detection systems (IDS) was expressly prescribed for CI operators

Notifications by CI sector



A	*137*	*Energy*
B	*22*	*Water*
C	*8*	*Nutrition*
D	*107*	*Information Technology and Telecommunication*
E	*141*	*Health*
F	*120*	*Finance and Insurance Industries*
G	*185*	*Transportation and Traffic*
H	*6*	*Municipal Waste Disposal*
	726	***Total***

Figure 24: Notifications by CI sector during the reporting period, source: BSI

in the BSIG in May 2021 (Section 8a (1a) BSIG). This legal obligation not only applies to CI operators that exceed the thresholds of the BSI Critical Infrastructure Ordinance (BSI-CIV), but also to all electricity and gas network operators via Section 11 (1d) of the German Electricity and Gas Supply Act (Energy Sector Ordinance - EnWG). The quality of the systems used in accordance with Section 8a (1a) BSIG and Section 11 (1e) EnWG can be assessed using an implementation level model. Auditors and inspectors can use this to assess how advanced the organisational and technical measures in the audited critical infrastructure are.

The aim of using an implementation level model is to increase the quality of intrusion detection systems. Regular analyses can be used to check which sub-areas are still insufficiently controlled. A low degree of implementation justifies a particular need for action. Degree of implementation models can therefore help to prioritise the further development of intrusion detection systems.

IDS Implementation Rate According to the Latest Available Audit Report

The number of audit reports does not correspond to the number of operators. Some energy industry operators are required to provide audit reports in accordance with Section 11 (1f) EnWG. These audit reports contain implementation levels of the systems for intrusion detection, but no ISMS/

ISMS maturity level

according to the latest available audit report

	Maturity Level				
Sector	**1**	**2**	**3**	**4**	**5**
Energy	1	20	40	28	28
Water	0	8	13	28	30
Nutrition	0	11	20	8	10
Information Technology and Telecommunications	0	2	9	10	18
Health	3	78	64	43	23
Finance and Insurance	0	8	35	20	42
Transport and Traffic	3	24	30	6	8

BCMS maturity level

according to the latest available audit report

	Maturity Level				
Sector	**1**	**2**	**3**	**4**	**5**
Energy	2	28	51	23	13
Water	3	13	21	21	21
Nutrition	4	10	22	9	4
Information Technology and Telecommunications	2	8	11	6	12
Health	15	104	52	26	14
Finance and Insurance	0	28	22	29	26
Transport and Traffic	7	28	21	6	9

ISMS and BCMS Maturity Levels

1: is planned but not yet established / **2:** is largely established / **3:** is established and documented / **4:** in addition to maturity level 3, regularly reviewed for effectiveness (ISMS) resp. regularly reviewed and practised (BCMS) / **5:** in addition to maturity level 4, regularly improved

Figure 25: ISMS maturity levels and BCMS maturity levels by sector according to the latest available audit report, source: BSI

BCMS maturity levels. There are also operators who are not required to provide audit reports in accordance with Section 8d (2) BSIG. Finally, there are recently registered operators, for example in the municipal waste disposal sector, who only have to submit audit reports two years after registration.

Cooperation Wins – even with CI

For many years, Germany has had an independent partnership for critical infrastructure (Unabhängige Partnerschaft KRITIS, UP KRITIS) where CI operators, their professional associations and the responsible authorities work together to protect critical infrastructures in Germany. All CI operators can become participants in the UP KRITIS, including smaller operators that remain below the threshold values of the BSI-CIV and are therefore not covered by the statutory registration and audit reporting obligation. There are currently 960 organisations registered as participants in the UP KRITIS (as of 30 June 2024). Professional dialogue takes place in particular in thematic and sector working groups. In 2024, the UP KRITIS will expand to include working groups that focus on the physical protection of criticial infrastructures as part of an organisational update. Thanks to this closer integration, the UP KRITIS is geared towards the increasingly complex threat landscape, which is countered with an integrated, comprehensive approach.

IDS implementation rate

according to the latest available audit report

	Maturity Level					
Sector	**0**	**1**	**2**	**3**	**4**	**5**
Energy	2	7	39	28	3	2
Water	1	8	8	11	5	0
Nutrition	0	2	7	10	3	1
Information Technology and Telecommunications	0	0	3	12	2	3
Health	1	44	87	35	13	0
Finance and Insurance	0	2	22	23	17	4
Transport and Traffic	0	19	24	9	1	0

The guidance on the use of intrusion detection systems describes the following levels of implementation:

0: No measures to fulfil the requirements have been implemented to date and there are no plans to implement any measures. / **1:** There are plans to implement measures to fulfil the requirements, but for at least one area no concrete implementation yet. / **2:** Implementation of measures to fulfil the requirements has begun in all areas. Not all MUST requirements have been fulfilled yet. / **3:** All MUST requirements were met for all areas. Ideally, the necessity and feasibility of the SHOULD requirements have been checked. A continuous improvement process has been established or is being planned. / **4:** All MUST requirements were met for all areas. All SHOULD requirements have been fulfilled, unless they were excluded with sound and comprehensible reasons. A continuous improvement process has been established. / **5:** All MUST requirements have been fulfilled for all areas. All SHOULD requirements and CAN requirements have been fulfilled for all areas, unless they were excluded with sound and comprehensible reasons. Sensible additional measures were identified and implemented for all areas in accordance with the risk analysis/assessment of protection requirements. A continuous improvement process has been established.

Figure 26: IDS implementation rates according to the latest available audit report

The security of critical infrastructures is the foundation of Germany as a cybernation. This includes strengthening resilience against cyberattacks, which is primarily achieved through close cooperation between the state, business and society. The UP KRITIS and its working groups play an important role here.

10.1.1 Threats to Critical Infrastructure – Energy

The threat level in the energy sector remains high. Operators of critical infrastructures in the energy sector are confronted with a wide variety of attack scenarios.

The example of a software company that provides services to the energy sector shows that ransomware attacks continue to pose a threat to suppliers and service providers. In February 2024, it became known that the company had been the victim of a cyberattack. According to the internationally active company, it employs 2,200 people at 13 locations in Germany and 16 international locations. In addition to control systems, it also develops process control and information systems, especially for energy operators. The company's products are also used in industry and logistics as well as by transport infrastructure operators.

The attackers gained unauthorised access to the software company's IT infrastructure and then encrypted parts of the IT systems and data. The company then deactivated all external connections to customers. CI operators from the energy, transport and traffic sectors informed the BSI that restrictions could be possible with regard to critical services. In all cases, the acute impact on operators was limited to maintenance access systems. Critical services were not impaired in the further course of the project. The BSI was in contact with many CI operators and sent out regular updates using its cybersecurity warning messages (CSW).

Another victim of a ransomware attack was an electrical engineering company. The attackers were able to capture several terabytes of data and threatened to publish it if no ransom was paid. The company is a well-known manufacturer of industrial control and automation systems (ICS), including for the petroleum industry in Germany.

The ransomware incidents observed show that cybercriminal groups are increasingly targeting victims with high ransom expectations. Ransomware actors focus on supposedly solvent targets who are presumably willing to pay a high ransom. The focus is therefore shifting to companies from the CI sectors, where the need to maintain critical services could favour a high willingness to pay.

Phishing, DDoS and Human Error

In addition to ransomware, phishing can also be observed in the energy sector. For example, several phishing campaigns attributed to a suspected pro-Russian group have been uncovered since November 2023. The aim of these campaigns was to persuade victims to download malware designed to steal information.

The Federal Network Agency (BNetzA) also reported an ongoing phishing campaign in which phishing emails were sent in the name of the BNetzA. Potential victims were asked to enter sensitive data on a fake website that resembled the BNetzA website.

DDoS attacks were also observed in the reporting period. As a result of a DDoS attack on an energy operator, there was a temporary partial outage of the critical infrastructure. The operator stated that the cyberattack caused the firewall to be overloaded. The DDoS attack was directed against a processing system for the sale of fuel and heating oil. For around 2.5 hours, the availability of the critical service was restricted at several locations across Germany. The scope of the attack was reduced by switching off systems and thus reducing the attack surface.

The various attack scenarios include technical and/or human errors that resulted in the impairment of critical services. For example, a pipeline operator reported that both main data connections were inadvertently interrupted at the same time. Originally, these were to be gradually replaced by fibre optic connections. Due to the simultaneous interruption of the data connections, both routers were no longer accessible. The cause of the malfunction was a human error in which copper data connections were accidentally and irreparably removed. As a safety measure, the oil transport through the pipeline was stopped. Customers were informed by the operator at an early stage. The outage lasted several days. A prolonged outage would have had an impact on the critical supply service of crude oil (products). In cooperation with a service provider, an alternative data connection was set up and the accessibility of the routers was restored.

10.1.2 Threats to Network Infrastructure (Focus on Mobile Communications/5G)

In modern society, the exchange of information has become a very important economic factor and part of everyday life. An important part of the German industry is heavily dependent on uninterrupted voice and data transmission. A failure of the basic ICT infrastructure can lead to a standstill in production companies after a short time, as production and logistics cannot communicate with each other. The mobile communications sector in particular has gained considerably in importance due to the introduction of new mobile communications standards and ever-increasing networking. The BSI continuously monitors and evaluates the security situation in national telecommunications networks based on reports of incidents and vulnerabilities.

National Situation

With the introduction and integration of new mobile communication standards and modern technology concepts, the complexity of network structures is also increasing. The resulting functional dependencies increase the attack surface for public and private mobile networks. In particular, the parallel operation of different generations of mobile communication technology leads to highly complex networks with the need for a holistic approach to security. Intensive monitoring and analysis of cyberattacks and vulnerabilities in the context of mobile communications is therefore essential to ensure the resilience of national mobile networks. The outages that occurred were often caused by maintenance work or upgrades in the complex network structures. However, the BSI has also detected an increasing number of physical attacks on individual base stations. Vandalism or sabotage led to longer, but regionally limited outages, which could usually only be rectified by replacing the defective infrastructure. The BSI also observed several impairments in the area of emergency call technology in wired networks. Furthermore, maintenance work or failed updates as well as damage to infrastructure also led to outages and disruptions in these networks.

International Situation

During the reporting period, the BSI also observed an increasing threat from state actors in the international arena. Due to a cyberattack on Ukraine's largest mobile phone provider Kyivstar, its mobile network was largely unavailable for several days. In addition to the failure of mobile communication, numerous networked applications such as payment terminals, alarm systems and even street lighting were also impacted. In another incident, the entire mobile phone network of the Australian network operator Optus went down for several hours. Around half of the Australian population, numerous hospitals, payment terminals and underground railway services were affected by the outage, which was presumably caused by a failed update. These two large-scale incidents once again highlight the importance of mobile networks for digitalised applications.

Weaknesses in Mobile Communications

During the reporting period, numerous vulnerabilities were also discovered in commercially available 5G modems from two chip manufacturers for mobile communication technology. Using fake base stations in the mobile network, it is possible to exploit implementation errors in unpatched modems and carry out a denial-of-service attack. The BSI was able to simulate the attack on these vulnerabilities in its own 5G/6G security lab and estimates that it is unlikely to be widely implemented in the public mobile network due to the necessary technical requirements. In addition, certain security mechanisms of the new mobile communications standards can be circumvented by downgrade attacks on older generations of mobile devices. Older, vulnerable signalling infrastructures will continue to be necessary for roaming between different countries, network operators and mobile phone generations and can be exploited to locate and monitor people if they are successfully compromised. In this context, the BSI has observed that signalling protocols such as SS7 remain the focus of attackers and regularly result in mobile network operators having to adapt their detection mechanisms. Signalling protocols are used to transmit information for controlling communication connections in telecommunications networks.

Overall, the BSI sees an increasing threat to private and public telecommunication networks at both national and international levels. Mobile networks in particular are increasingly susceptible to infrastructure-related vulnerabilities in their hardware and software platforms due to virtualisation and cloudification. With the help of sophisticated detection and response measures by network operators, cyberattacks on telecommunication networks can usually be detected and mitigated at an early stage in order to minimise damage and impact for end users. In order to further increase the security of the networks, the BSI is involved in the creation of new security requirements as part of the updating of the catalogue of security requirements in accordance with Section 167 TKG for which the Federal Network Agency is responsible. The BSI is also involved in the standardisation of 5G/6G and Open RAN as well as the future signalling and roaming infrastructure between mobile network providers. In addition, critical 5G components in public mobile networks are subject to mandatory certification to ensure that the specified security features are in place. This will come into force after a transitional period in 2026. As a qualified independent body, the BSI checks compliance with security requirements in public networks in the event of increased risk potential, as required by the Telecommunications Act.

10.1.3 Threats to Satellite Communications

Today, satellite-based services are playing an increasingly important role for society, the industry and the state. The dependency of users of modern IT systems and satellite-based services is therefore constantly increasing. Above all, satellite communication in any form, for example satellite-based internet access for independent communication by emergency services, is becoming increasingly important. Modern satellite constellations such as Starlink or OneWeb offer increasingly comprehensive, suitable services to provide internet access in remote locations without terrestrial broadband access. Earth remote sensing and navigation are also inconceivable without space-based systems and services. As a result, these systems are becoming increasingly attractive to attackers. The cost of an attack is moderate due to the signalling structure, but the potential damage caused and the unforeseeable collateral damage are quite serious.

In the case of satellite systems, in addition to the classic attack vectors on terrestrial infrastructures, the possible attack paths on the satellites themselves must also be explicitly considered. There are already tried and tested concepts for securing terrestrial systems. Satellites, on the other hand, are a vulnerable element due to their global availability and require special protective measures.

NIS 2 Directive with Extended Requirements for Satellite Communication

The aim must be to develop a good level of security requirements for satellites that are as standardised as possible. Satellite systems cannot be regulated and secured on a purely national basis. Cooperation with other countries and international organisations, such as ESA or the EU, is essential here. The NIS 2 Directive, in which space is presented as a separate sector, recognises this to a certain extent. It represents an important step towards European security for satellite systems. Nevertheless, it remains relevant to establish such minimum requirements in a global context. The BSI sees itself in a pioneering role here and will work on this with international partners. Find out more about the NIS 2 Directive in chapter NIS 2 Directive, p. 82.

10.2 ***Threats to SMEs in Germany***

More than three million small and medium-sized enterprises in Germany are facing the challenges of digitalisation and the cybersecurity it entails. This sub-sector of companies, which accounts for 99.4 per cent of all German commercial businesses, is broken down as seen in Figure 27 on page 67.

Micro (< 10 employees) and small (< 50 employees) businesses in particular often do not have the necessary staff to take care of the operation and security of the company's information technology. For example, it is simply not worthwhile for these companies to employ their own IT staff. As part of the classic "make or buy" decision-making process, the "we can somehow manage it ourselves" approach is often chosen. This contrasts with the growing threat landscape.

In 2024, the BSI's experience is that many companies will still not have sufficient knowledge of the general cyber threat landscape or their own risk profile. They do not even realise that they need to invest more in their security. Even basic preventive measures, which can often be implemented free of charge, are therefore often not taken.

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

Fortunately, the number of small and medium-sized businesses (SMEs) that would like to do more for their IT security is increasing. However, they often do not know how best to proceed. Existing standard works for setting 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 independent IT operations. However, this does not apply to the majority of companies with fewer than 50 employees.

Consortium for the Development of a DIN SPEC

In order to support such companies, a consortium was founded in cooperation with the German Association of Small and Medium-Sized Enterprises (BVMW) under the leadership of the BSI to develop a DIN SPEC. A total of almost 20 partners were involved, including the German Institute for Standardisation (DIN), business development agencies, a subsidiary of the German Insurance Association, IT Grundschutz experts, data protection specialists and IT service providers. The project was funded by the Federal Ministry for Economic Affairs and Climate Protection as part of the "Mittelstand Digital" programme.

The results of the consortium's eight months of work are the "DIN SPEC 27076 IT Security Consulting for Small and Micro Enterprises" published in May 2023 and the Cyber-RisikoCheck (CyberRiskCheck) based on it. This enables SMEs to obtain standardised advice from IT service providers that is specifically tailored to their needs. The recommendations for action for SMEs were also standardised in the DIN SPEC. This means that both the client and the contractor know what service is to be expected and provided.

Performing CyberRisikoCheck

In the CyberRisikoCheck, an IT service provider asks a company about its IT security in a one- to two-hour interview, usually via video conference. In it, 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 specifications. As a result, the company receives a report that includes the score and a recommendation for action for each unfulfilled requirement. The recommendations for action are ranked according to urgency and include information on what federal, state and local government support is available to the business. CyberRisikoCheck is not an IT security certification. However, it enables a company to determine its own IT security level and shows which specific measures the company should implement or commission from an IT service provider.

At the federal level, the check and subsequent recommendations for action are already being subsidised by 50 per cent via the "go-digital"[26] programme, and in North Rhine-Westphalia (NRW) by as much as 70 per cent via the "Mittelstand Innovativ & Digital (MID)"[27] programme. Several other states have also signalled their willingness to provide funding. From March to June 2024, the BSI trained 351 IT service providers in the implementation of the CyberRisikoCheck. Since May 2024, the BSI has also provided them with web-based software to carry out the CyberRisikoCheck at their customers' premises and receives the anonymised survey data from the checks. This allows the National IT Situation Centre to access valid data on the cybersecurity of SMEs for the first time and include it in the BSI reports on the cybersecurity situation. The Situation Report 2025 will therefore provide a comprehensive presentation of the situation of SMEs for the first time.

The CyberRisikoCheck thus contributes to the further development of preventive services offered by the federal, state and local authorities. Further information on the CyberRisikoCheck as well as a list of registered IT service providers offering the check and other useful information for SMEs can be found on the BSI website.

CyberRisiko Check

nach DIN SPEC 27076

Read more about CyberRisikoCheck:

More information for SMEs (German):

To the brochure "Cybersecurity for SMEs - The Top 14 Questions" (German)

Breakdown of companies in Germany

In 2019

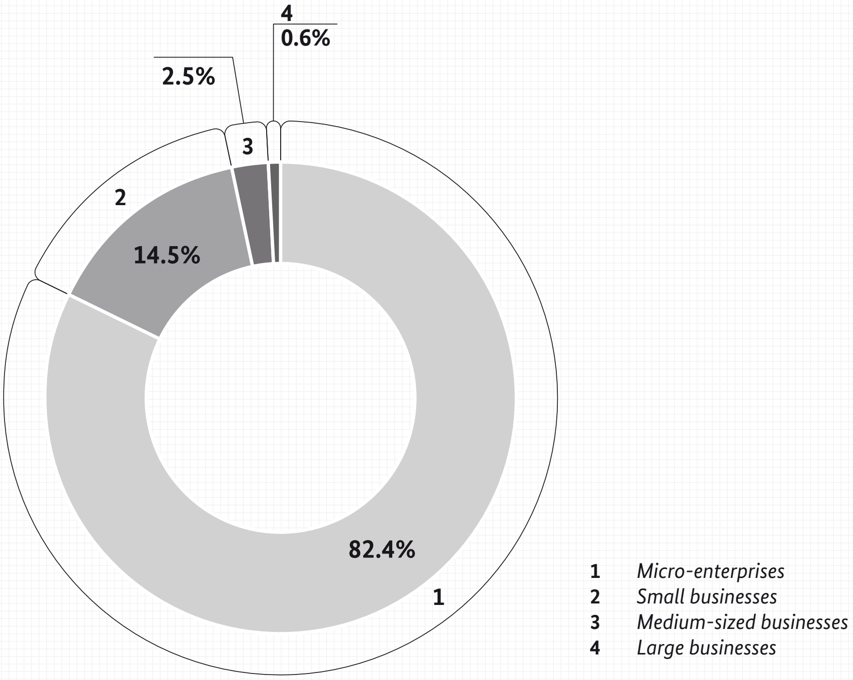


Figure 27: Breakdown of companies in Germany in 2019, source: Federal Statistical Office, Status: 6 May 2024[25]

Cybersecurity Incident at a Remote Screen Sharing Provider

Situation

In February 2024, the manufacturer of widely used software for remote access and screen sharing published a press release on a successful cyberattack that resulted in the compromise of internal systems.

Public sources report that source code and certificates for signing the software were also leaked in the course of this compromise. The manufacturer carried out the clean-up and restoration directly with a service provider. As a result, certificates have been withdrawn and updates have been provided to replace end-user certificates.

The affected manufacturer told the BSI that the company currently has no knowledge of any compromise of user data, but has forced a reset of its customer portal passwords as a precaution.

Assessment

According to the BSI, there is a risk that this information could be used for further attacks on the provider's customers due to the possible leakage of the source code and certificates. Man-in-the-middle and supply chain attacks are conceivable in this context. In particular, certificates that may have been leaked could have gone unnoticed or, in the worst case, attacks that have already taken place could have remained undetected. The measures implemented by the manufacturer concerned have considerably reduced the hazard potential. Nevertheless, it cannot be ruled out that malicious versions of the software that are signed with a compromised certificate may be offered by attackers on third-party websites or sent specifically to customers.

In the corporate context, the application is often used with privileged rights, which opens up a particular risk potential.

Response

The BSI is in contact with the company concerned, can confirm the incident and also issued an incident warning at the beginning of February.

The BSI generally recommends following the recommendations of software manufacturers and installing the latest version with the new certificate. Updates should only be obtained via the update function within the software or via the manufacturer's website. In addition, employees should be made aware that software should never be obtained from insecure sources.

CrowdStrike Falcon Causes Worldwide IT Outages

Situation

On 19 July 2024, an IT security solution from CrowdStrike caused global IT outages in numerous industries. Many IT failures were reported in Germany, including at CI operators and organisations subject to reporting requirements. The IT failures occurred in connection with an update of the EDR software Falcon. Falcon is an enterprise tool that is only used in companies, so private individuals were not affected. CrowdStrike had rolled out a content update to the software, which led to a system crash with a final “blue screen of death” (BSOD) on Windows-based installations. The error only occurred when the Falcon EDR sensor had been installed. The cause was a programming error in the IT security solution programmed in C++. CrowdStrike immediately communicated a workaround to solve the problem on 19 July 2024. According to Microsoft, a total of around 8.5 million Windows systems were affected. Cyber criminals have exploited the IT failures for various forms of phishing, scams or fake websites. By 21 July 2024, the situation had returned to normal.

Assessment

This was not a cyberattack, but a lack of quality assurance on the part of the manufacturer. The IT outages caused by CrowdStrike have resulted in enormous, as yet unquantified, costs to those affected. According to initial estimates, the costs are likely to be in the billions.

Response

CrowdStrike provided mitigation measures for various systems on its support portal on 19 July 2024. On 19 July 2024, the BSI also published management information on the facts of the case and the possible mitigation measures for its target groups. On 21 July 2024, Microsoft published a recovery tool for the systems affected by the CrowdStrike outage.

Together with CrowdStrike and Microsoft, the BSI has developed initial measures to prevent similar incidents in the future. In addition, the BSI will agree measures with CrowdStrike to ensure the operational stability of customer systems, even when installing software updates required at short notice. The measures include short, medium and long-term steps until the end of 2024 as well as further measures until 2025. The BSI will review the effectiveness of implemented measures.

11 – Threats to Federal Administration

Every day, government networks are exposed to predominantly untargeted mass attacks from the internet. In some cases, however, attacks are also directed specifically at the federal administration. The BSI uses a range of complementary measures to protect government networks from these attacks.

Web filters, which block access to malicious websites and web servers, are a preventive component. This, for example, prevents access to malicious programmes hidden behind download links. These links are distributed as part of social engineering attacks via email, social media or websites. This protective measure also prevents malware that is already active from communicating with web servers that are under the attackers' control. This prevents the malware from receiving new components and commands from the attackers. In addition, it is then no longer possible for the malware to send the victim's data to these web servers. In the current reporting period, an average of 375 new malicious websites were blocked every day. The index of new blocks of malicious websites averaged 278 points, more than two and a half times higher than at the start of recording in 2018 (see Figure 23, page 58).

In addition, a centralised protection against spam emails increases the security of government networks. This measure is not only effective against unsolicited emails. It also recognises cyberattacks such as phishing emails. The spam rate, i.e. the proportion of unwanted emails in all emails received, averaged 53 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 (see Figure 24, page 61). This averaged 88 points in the reporting period (-30% compared to the previous reporting period). There were slight fluctuations due to various waves of spam. The federal administration's spam filters reliably fend off such spam waves so that they do not reach the intended users.

Index of new blocks of malicious websites

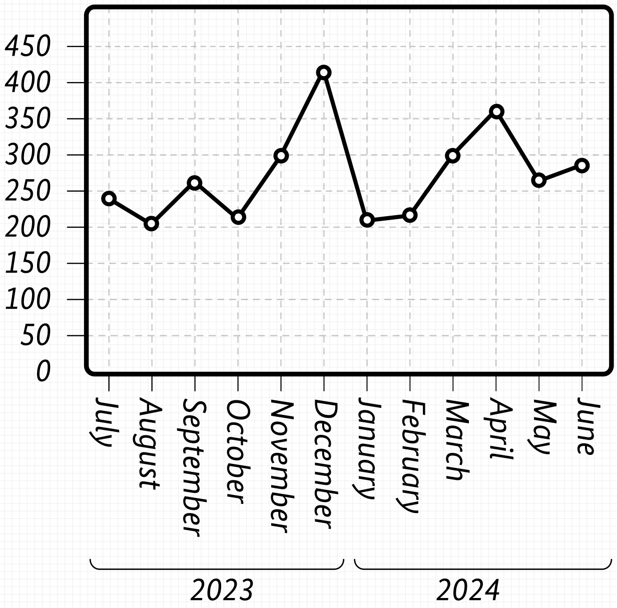


Figure 28: Index of new blocks of malicious websites (2018 = 100)

Figure 28 / Web filter measurement in federal networks
Aim of the statistics: The number of new blocks that have become necessary on the web filter of the federal government's networks, which block access from the federal administration to malicious websites. / **Reported monthly. / Population:** All new blocks of malicious websites that appear necessary to the BSI based on current knowledge of the situation. / **Sample:** All new blocks, i.e. detection and filtering rules on the web filter of the federal government's networks. / **Survey design/instruments:** Monthly aggregation of an ongoing survey on the web filter of the federal government's networks. / **Scope:** Authorities that do not participate in the BSI's centralised protection measures are excluded. Blocking of malicious websites is reported, not attempts to access malicious websites / **Quality assessment:** The situation assessment on which the blocking is based applies to the federal government's networks; federal government networks are one of the largest networks in Germany and can therefore be regarded as a blueprint for the internet as a whole.

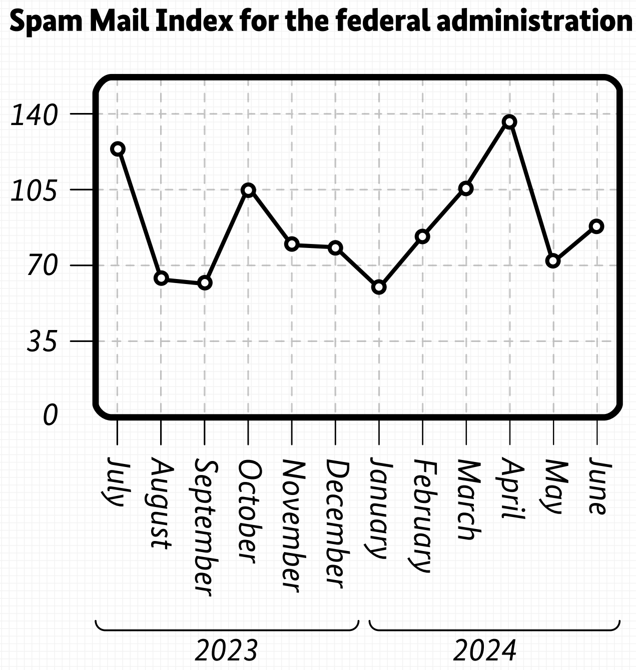


Figure 29 / Survey on email traffic with the Federal Administration

Aim of the statistics: Survey of incoming email traffic with the Federal Administration. / **Reported monthly. / Population:** All emails received by the central mail transfer agent. / **Sample:** Complete survey / **Survey design/instruments:** Daily aggregation of spam filter detections on the federal government's networks. / **Scope:** Excludes authorities that do not participate in the BSI's centralised protection measures. General statistical characteristics, spam status and information on email attachments are recorded. / **Quality assessment:** Precise, as a complete survey. Minor inconsistencies due to improving detection and different calculation times.

Figure 29: Spam Mail Index for the federal administration (2018 = 100)

Attacks on the Email Inboxes of Various Organisations

Situation

Last year, the BSI became increasingly aware of incidents in which the email inboxes of various relevant organisations, some of which are politically connected, were attacked. State-sponsored actors in particular used various methods to access emails. These included attacks with weak or recycled passwords, attacks via zero-day vulnerabilities or phishing attacks. Webmail systems are particularly vulnerable. They can still often be accessed freely over the internet without multi-factor authentication.

Assessment

Such attacks may have leaked data that could be used by state actors as part of hybrid threats. This poses an increased risk, particularly due to the current geopolitical circumstances and the elections in 2024. In addition to pure data leaks, there is also the risk of targeted spear phishing attacks, either based on the leaked information or through the active use of compromised mailboxes.

Response

In several incidents, the BSI has supported the affected organisations with forensic investigations and advice, sometimes in cooperation with other federal authorities. Better implementation of password policies, the use of multi-factor authentication and restricting the accessibility of the internal network from webmail systems could have prevented attacks of this kind and the use of stolen credentials in some cases. This emphasises the need to implement basic safety measures.

Ransomware Attack on a Municipal IT Service Provider

Situation

A municipal IT service provider fell victim to a cyberattack at the end of October 2023. According to a press release from the responsible police headquarters, the attack took place on the night of 30 October 2023. On 31 October 2023, the IT service provider announced that encrypted data had been discovered on servers. Due to the cyberattack, the IT service provider had shut down the majority of its IT systems as a precautionary measure.

A large number of municipal administrations, specialised procedures and websites were affected by the attack.

According to its own information, the IT service provider is responsible for the support of 20,000 municipal workstations. According to the media reports, the IT service provider has 72 municipal customers with at least 1.7 million inhabitants who were affected by the attack.

In January 2024, the IT service provider published a forensics report that identified the Akira ransomware group as the attacker. According to the report, initial access to the company was gained via a VPN solution, by means of previously captured or guessed access data or by exploiting a vulnerability.

At the time this report was published, the service provider was still in the restart phase, during which certain specialised procedures are being restored or are running in basic mode, while other specialised procedures are still unavailable.

Assessment

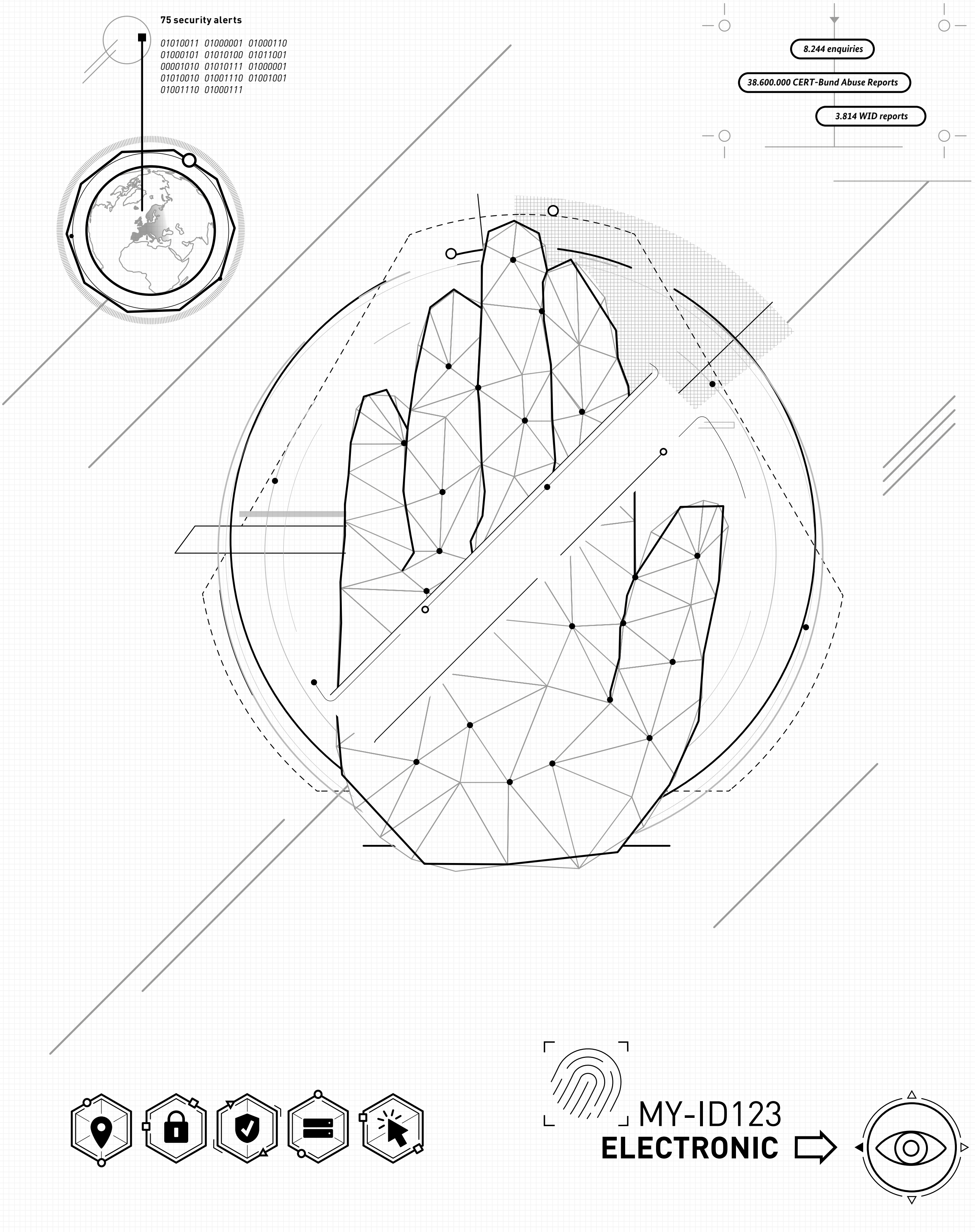
While federal authorities are secured centrally via government networks, local authorities organise their IT security measures differently. The IT service providers of the municipalities are independently responsible for the established defence measures. The failure of a central IT service provider has a serious impact on a large number of municipal services and therefore on the general population.

The Akira ransomware is based on the source code of the Conti ransomware that became public in 2022. Attackers usually rely on a combination of encryption and the publication of stolen data on a leak site.

Response

The IT service provider under attack had shut down the majority of its IT systems as a precautionary measure and was in contact with the State Office of Criminal Investigation, external security service providers and the BSI. In response to the cyberattack, an extended crisis team was formed on 31 October 2023, which included the victim, external IT forensic experts and the IT managers of all the district administrations in the association area.

D RESILIENCE



12 – Cyber Resilience in the Context of Major Social and Political Events

Security concepts for mass events must also encompass the digital space. Before the European Football Championships in summer 2024, for example, entire infrastructures as well as individual sports clubs were threatened by phishing campaigns, DDoS attacks and ransomware infections.

Democracy is under attack in the digital space as well. Cyberattacks on political parties paralyse servers or steal emails and documents. Foreign states exert illegitimate influence on political events in Germany. Russia, for example, has stepped up its activities since the war of aggression against Ukraine. Targeted disinformation makes it difficult for the public to distinguish between serious and dubious sources of information on the internet. Artificial intelligence is used to manipulate images, audio and video files in a deceptively realistic way. Disinformation and political influence before elections manipulate the political decision-making process.

12.1 Cybersecurity in the Context of Elections in the Year 2024

In 2024, more than 70 elections are scheduled or have already taken place worldwide, including presidential elections in the USA, India and Russia, for example. For German citizens, not only the European elections took place, but also three state elections in Saxony, Thuringia and Brandenburg as well as nine local elections. Both the electoral process and communication by the authorities and the media, as well as the formation of opinion and will in the context of elections, are now highly dependent upon information technology and are therefore at the centre of information security.

Threats and Types of Illegitimate Influence and Attacks in the Context of Elections

The BSI makes a fundamental distinction between direct influence (on the electoral process) and indirect influence (on public opinion). The legitimacy of elections is deliberately called into question in order to weaken citizens' trust in democratic processes and institutions. These include so-called hack-and-leak campaigns against political parties, in which emails and documents are stolen and then published, sometimes in a manipulated form. In addition, there are repeated attempts to attack websites and servers that contain voter data or provide information about the election.

Examples of illegitimate influence include:

- spreading false information in order to deliberately pit social groups against each other and incite them, for example by means of inflammatory topics
- falsification and illegitimate takeover of social media accounts, websites of individuals (defacement), political parties, media companies or authorities
- use of artificial intelligence to manipulate images as well as audio and video files (deepfakes)[28]
- delegitimisation of democratic institutions and individuals, which undermines trust in the state and democracy in general
- targeted disinformation in the name of a real person, combined with considerable reputational damage

What does the BSI actually do to protect parliamentary elections?

The BSI takes a broad, cross-society approach to the protection of parliamentary elections. Among other things, it supports federal and state electoral administrations, candidates and political parties in matters of information security with various information, assistance and advisory services.

In the course of elections, the measures are particularly aimed at:

- strengthening the core election process
- increasing resilience to technical manipulation attempts
- raising awareness among candidates and mandate holders as well as digital privacy protection

To **strengthen the core selection process,** a federal-state working group has created an IT Grundschutz profile for rapid notifications together with the BSI. This is to facilitate the adaptation of the security process in line with IT Grundschutz for rapid reporting in national parliamentary elections down to the district electoral administrations.

In addition, through the National IT Situation Centre, the BSI exchanges and evaluates information on emergency planning and IT crisis management with the participating electoral authorities and relevant stakeholders. The BSI also offers assistance in finding suitable DDoS mitigation service providers.

To **increase resilience to technical manipulation attempts in elections,** the BSI offers web checks, pen tests, cybersecurity checks for exposed persons (CYBEX checks) and incident support, including the use of Mobile Incident Response Teams (MIRT). In the event of incidents, the responsible national Computer Emergency Response Team Bund (CERT-Bund) at the BSI plays a central role.

Prevention and, above all, **raising awareness among target groups,** such as electoral authorities, political parties, candidates and elected officials, are particularly important to the BSI in the political arena. The BSI provides regular information through webinars, handouts, leaflets and presentations, and continually adapts its offerings to meet the needs of its target audiences.

Support for the Federal States

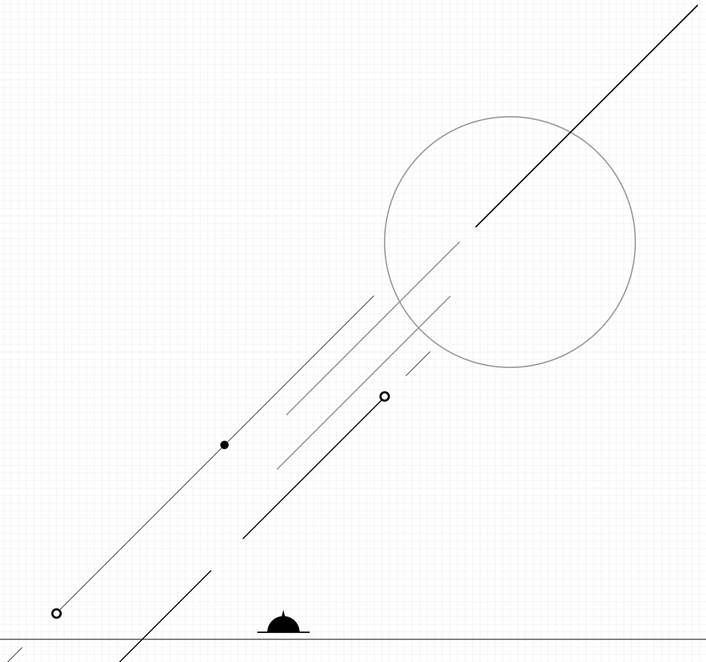
The BSI uses the knowledge and experience gained from elections at various levels to offer the federal states support for the information-secure organisation of the respective state elections.

For upcoming Bundestag or European Parliamentary elections, support for the federal states is mainly provided by addressing them via multipliers such as the Federal Election Management.

12.2 ***Cybersecurity in the Context of Sporting Events***

Due to the increasing digitalisation of the event industry, the current general threat landscape and its social and sometimes political relevance, major events are increasingly affected directly or indirectly by cyberattacks. Recent years have seen an increase in event-related incidents, from phishing campaigns[30] to data leaks[31], DDoS attacks[32] and ransomware infections of individual infrastructures[33] and sports clubs[34], to the targeted use of malware such as the 2021 Olympic Wiper[35]. Continuous monitoring of the situation, possible threat scenarios and appropriate response measures should therefore be integrated into event security concepts and reporting and escalation channels should be practised.

For these reasons, the BSI was involved in the security planning for this year's European Football Championship in Germany at an early stage. In close cooperation with Euro 2024 GmbH, other German security authorities and the UEFA cybersecurity team, the BSI monitored the threat landscape in cyberspace, raised awareness among the host cities and other relevant stakeholders and sent a liaison officer to the International Police Coordination Centre (IPCC 2024) in Neuss, which was set up specifically for the games.



13 – Cloud Resilience

High flexibility, performance and availability – due to its numerous advantages, cloud computing is the method of choice for many applications, sometimes even the only possible method. According to KPMG's Cloud Monitor 2023, more than 9 out of 10 organisations are already using cloud computing. More than half pursue a cloud-first strategy, just under a fifth a cloud-only strategy.

Attacks are Shifting to the Cloud

This high usage makes cloud providers targets for attacks (see chapter Attacks on the Cloud, page 51). The complexity of clouds can also make them difficult to manage, thus leading to, in some cases major, incidents. This generally affects a large number of institutions that use cloud services (hereinafter "users"), and in some cases even entire sectors of the industry.

Responsibility of Cloud Providers

Cloud providers bear a very high level of responsibility and must therefore have an equally high level of information security – for their own protection and for the protection of their users. The BSI is active here in a variety of ways.

The BSI's Cloud Computing Compliance Criteria Catalogue (BSI C5) describes the minimum level of information security for the provision of cloud services. Well over 50 cloud providers have secured a total of several hundred cloud services in accordance with BSI C5 and verified this in a certificate. The BSI C5 is also one of the most important foundations for the upcoming EU Cloud Security Certificate (EUCS).

In addition, the BSI has been in extensive, trusting communication with many cloud providers for a long time. These include cooperation agreements that emphasise the importance of the BSI for cloud providers. This gives the BSI in-depth insights and allows it to contribute its expertise and advice directly.

Following the successful attack on the Microsoft Azure Cloud by Storm-0558 (see Incident Compromise of the Microsoft Cloud Infrastructure, page 52), the BSI issued a request for information pursuant to Section 7a (2) sentence 1 BSIG on the subject of double-key encryption (DKE) in January 2024 and asked Microsoft to answer the questions raised in this context. These questions were answered fusing the established means of trusting communication. One result of this is a white paper from Microsoft[36] that for the first time enables M365 users to assess the protective effect of DKE and any residual risks depending on their deployment configuration and to correctly use it accordingly.

Responsibility of Cloud Users

Even though the cloud provider is responsible for much of the information security, a significant part of the responsibility remains with the cloud user. In fact, attacks on users or misconfigurations implemented by users are among the most common causes of cloud incidents.

Users must therefore have a suitable security architecture, for example in accordance with IT-Grundschutz, as well as a strategy and procedure for cloud use. The IT-Grundschutz module for cloud usage and the BSI minimum standard for the use and shared use of external cloud services provide valuable guidance here.

Cloud services often offer additional security measures that can be easily utilised by users, such as identity and access management based on the "least privilege"/"need to know" principle, multi-factor authentication or the use of hardened servers. The very extensive monitoring within the cloud makes all activities transparent and enables services such as intrusion detection or DDoS mitigation. The cloud offers ideal conditions for automated security certificates (Compliance as Code), which are also used in basic IT protection and BSI C5.

The BSI is working on the provision of secure services using infrastructure as code (provision, configuration, update and deletion of cloud services by code).

Encryption is a very important means of ensuring the confidentiality of data. Within the cloud, encryption is used as standard for all data in transit and at rest. It is crucial that the degree of control the user has over key management corresponds to the protection requirements of the data to be encrypted. The spectrum of options ranges from the use of provider-generated and -managed keys to procedures such as DKE, in which the user generates and manages keys themselves.

Confidential computing, i.e. further encryption during processing (in use), is possible with many cloud providers and offers additional security.

BSI Cloud Strategy

Cloud computing offers many opportunities in terms of functionality, security and resilience, making it the backbone of digitalisation. The BSI has developed a cloud strategy to enable the secure use of cloud services in the federal administration and to take into account the risks associated with cloud computing in doing so.

Goal 1: Active and secure use of hyperscalers' public clouds in Germany. To this end, the BSI carries out risk and threat analyses.

Goal 2: Process classified information up to VS-NfD in clouds. The BSI is analysing, including through the RED-Cloud-Study, which security requirements and measures can ensure adequate protection in specific use cases. The approval of cloud infrastructure components also plays a role in this.

Goal 3: Design competitive sovereign usage scenarios for European and national clouds. To this end, the BSI is involved in many projects aimed at implementing sovereignty.

Goal 4: Advancing the resilience of digitalisation through secure cloud use. The BSI plans to provide and support tools for scaling secure cloud use. Such tools can be code examples for the implementation of Infrastructure as Code or Compliance as Code, facilitating the secure and compliant use of cloud services and contributing to the regulation of digitalisation.

Cloud Use in Public Administration

The BSI supports public administration organisations in the resilient and sovereign use of cloud services. Based on specific use cases from federal agencies, the BSI analyses and evaluates their cloud security and sets guidelines for secure use. It also supports large-scale cloud projects for the federal administration, such as the Deutsche Verwaltungscloud and the Delos Cloud.

In addition, the BSI is engaged in intensive discussions with national and international cloud providers on the use of cloud services in public administration, including as part of the project "Cloud-Reallabor: Sichere Verarbeitung in der Cloud" ("Cloud-Reallabor: Secure processing in the cloud") by the Deutsche Rentenversicherung Bund (German Federal Pension Insurance Association) at GovTech Campus Germany.

GovTech Campus Germany is a non-profit organisation founded by the BMI and other representatives from government, the tech scene, companies, science and civil society. The BSI joined the organisation at the beginning of 2024. GovTech Campus offers collaborative discourse on the modernisation and digitalisation of the state and administration.

The BSI is contributing its expertise to the Cloud-Reallabor project. This project aims to investigate the secure use of public cloud services – including for processing sensitive data – for public administration and KRITIS (CI) operators.

In summary, there are opportunities and risks associated with the use of cloud services. Users must weigh up the risks carefully and individually for each application – this also includes planning suitable risk minimisation measures. The BSI cloud products mentioned above can help users with this.

The opportunities for information security are obvious. Cloud computing increases resilience against attackers and will play an increasingly important role in this function in the everchanging cyber threat landscape of the future.

The BSI observes and anticipates developments in cloud security – it already has extensive technical expertise thanks to its deep insight into public clouds and is able to assess their security features. The BSI uses this expertise to support federal authorities in migrating to the cloud and using the cloud securely. The BSI is thus paving the way for the resilient digitalisation of German public administration – with cloud computing as the backbone and driver.

14 – Electronic Identities

Electronic identities form the basis for secure digitalisation. With the electronic identification function, Germany has already had a highly secure and data-saving electronic identity (eID) for more than ten years. It is also recognised throughout Europe for security and data minimisation and is notified under eIDAS. However, the development and utilisation of digital services based on the eID has so far fallen short of expectations. Nevertheless, a significant and steady increase in services and user numbers was observed in the reporting period.

14.1 Fit for the Future: EUDI Wallet

The new eIDAS regulation has come into force and sets out the legal framework for the European identity ecosystem with EUDI Wallet. The EUDI wallet should therefore be usable across borders as an electronic means of identification and be able to provide other attributes (e.g. educational qualifications, driving licence) in addition to the traditional identity attributes (first name, surname, etc.) in a verifiable manner for service providers. It should also offer the option of a qualified electronic signature.

eIDAS Large Scale Pilots (LSP)

In connection with the EUDI wallet, the Commission wants to prove that the requirements can be implemented in four Large Scale Pilots (LSPs). Germany is in charge of the "POTENTIAL" LSP[36] together with France.

The associated technical sub-working groups are to define and implement an interoperable European wallet infrastructure and try functionalities in cross-border usage scenarios. The BSI is actively involved in these endeavours.

eIDAS national – the Consultation Process

The consultation process of the BMI aims to achieve a national identity ecosystem in a transparent manner, which has a German wallet as a core component and fulfils the requirements of the eIDAS Regulation. In the context of this process, work is also underway in streams on the architecture for a German EUDI wallet. The BSI is closely involved in many streams of the process.

First Iteration of a National EUDI Wallet

As the first iteration of a national EUDI wallet, the "evolution solution," which is also aimed at bringing eID use to the masses at the instigation of the BSI, is intended to be a quickly available eID that can be used on most mobile devices and is purely mobile.

However, secure hardware in mobile devices is not yet available and usable to a sufficient extent, so it will initially be necessary to rely on backend systems to secure the processes.

For a purely mobile, fully decentralised eID that is widely used and meets a high level of assurance, widely available (certified) secure hardware elements, such as Secure Element (SE), eSIM etc., are required on users' end devices. The foundations for this still need to be laid in standardisation, regulation, etc. This is a process in which the BSI is actively involved.

CSP

New generations of Secure Elements (SEs) such as eSE and eUICC appear regularly with constantly updated hardware and software. In order to be able to make reliable security statements despite these dynamics, the BSI has developed the concept of the Cryptographic Service Provider (CSP). The CSP[37] makes it possible to certify eID applications with high protection requirements according to Common Criteria, regardless of the hardware. The CSP is currently being standardised at GlobalPlatform[38] and should be available as an international standard for SEs from 2025. The CSP has also been recognised by ENISA as a component for the certification of third-party applications for eUICC.

14.2 Recognition of eIDs in Europe

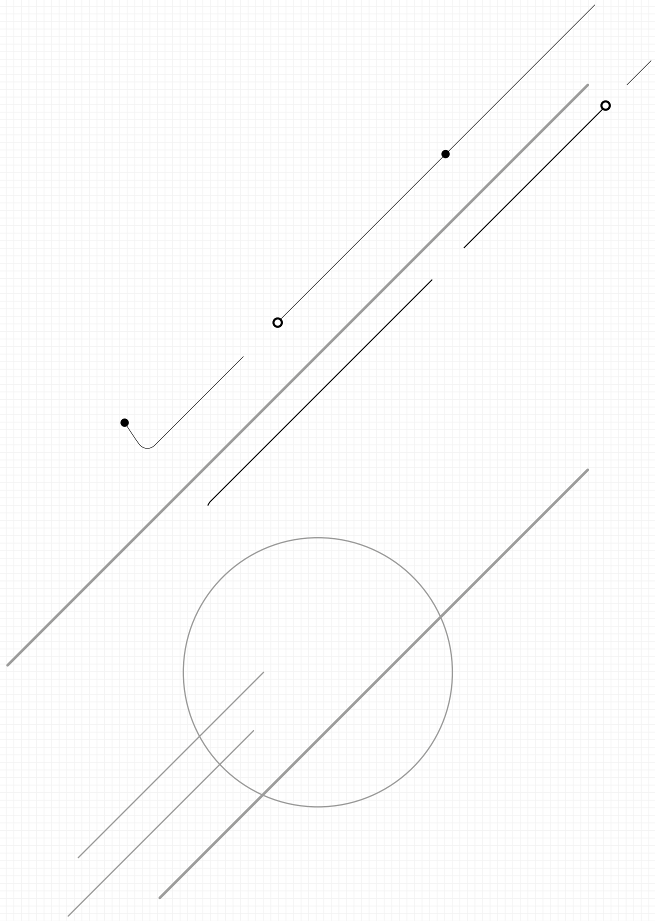
Under the current eIDAS Regulation, EU member states accept mutually notified eIDs. Over the course of the last year, the BSI has participated in peer reviews to check the conformity of new eIDs from other EU countries with the eIDAS Regulation. Last year, eIDs from Bulgaria and Cyprus were among those notified with the participation of the BSI.

The final decision on notification takes place in eIDAS Cooperation Network Meetings, in which general challenges and solutions for European eID systems are also discussed. In February 2024, the BSI hosted such a meeting of the Cooperation Network, where demonstrations included vulnerabilities in biometrics and countermeasures.

14.3 *AusweisApp*

With the AusweisApp[40] provided by the BSI, holders of an ID card, an electronic residence permit or an eID card for citizens of the EU and the European Economic Area (EEA) can identify themselves securely online.

The AusweisApp was given a new, more modern design during the reporting period. At the same time, the name AusweisApp2 was changed to AusweisApp[40].



15 – Europeanisation of Cybersecurity

Cybersecurity requires cross-border cooperation. This is why Europe is ensuring a common level of safety through legal requirements. These requirements help to increase resilience in the member states.

15.1 Cyber Resilience Act (CRA)

The Cyber Resilience Act (CRA) was adopted by the European Parliament in March 2024. This EU regulation aims to introduce horizontal cybersecurity requirements to protect digital products throughout their entire lifecycle, regardless of product category. Manufacturers need to take responsibility for the IT security of their products beyond the point at which they are purchased. The law was adopted by the EU Parliament in March 2024 and approved by the Council after the end of the reporting period in October 2024.

An Upgrade for Information Security

With a few exceptions, the new regulation will apply to all connected or network enabled products: from vacuum robots and software to products used in critical sectors.

The CRA is defining access requirements for the EU internal market and is extending the scope of the CE mark. Manufacturers will have to extend their guarantees from operational safety to cybersecurity. This is not only mandatory at the time the product is placed on the market, but also over the expected lifetime of a product.

The CRA is putting requirements both on the manufacturers of the products and on the products themselves – right from the design stage of a product.

- Products will have to account for security by design, security by default as well as the confidentiality and integrity of processed data.
- For example, to deal with vulnerabilities, manufacturers are obliged to provide security updates throughout the entire life cycle of the product, as well as to report and rectify vulnerabilities and to maintain a Software Bill of Materials (SBOM).
- This includes providing users with clear information about known vulnerabilities, available updates and how to use the product in a safe manner.

This applies not only to manufacturers, but also to importers or distributors who are placing such products on the EU internal market. Market surveillance authorities will be appointed in the individual member states, which are able to withdraw affected products from the market if the requirements are not met. Furthermore, if the affected parties do not comply, they will be penalised by the market surveillance authorities.

Different Product Classes – Graduated Testing

Even if the essential cybersecurity requirements are the same for all products, they differ in the type of verification obligation and depth of testing. As a minimum, manufacturer self-assessment is required for non-critical products. “Important products” in Class I, such as password managers or routers, may be self-assessed in accordance with harmonised European standards (hEN). If there is no harmonised standard for a product in this particular class, the product has to undergo a conformity assessment by a notified third-party body. For “important products” in class II, such as firewalls, a conformity assessment is mandatory. For products in the “Critical” risk class III, certification in accordance with a certification scheme of the Cybersecurity Act (CSA) is mandatory. This class includes items such as smart meters.

BSI Support – Implementing CRA Requirements

As an EU regulation, the CRA does not require any national implementing legislation. The transition period will be 36 months from entry into force. The obligation to report exploited vulnerabilities and serious cybersecurity incidents will be effective after 21 months. It is advisable for manufacturers to prepare for the new market access requirements at an early stage. Future requirements should be considered as early as possible, especially for new product developments with a longer-term horizon, in order to ensure compliance at the time of market launch.

To make these requirements more tangible in advance, the Federal Office for Information Security is in the process of developing guidelines for affected manufacturers of all shapes and sizes, as well as for developers.

- TR-03183 specifically and clearly describes the cyber resilience requirements for manufacturers and products. A part with specifications on the scope, content and format of a Software Bill of Materials (SBOM) was already made available in August 2023.
- Quality assurance and secure development processes are covered by further guidelines and recommendations.

The EU Commission draws on the expertise of the European standardisation bodies for many of the more specific requirements within the framework of the CRA. The experts of the Federal Office for Information Security are involved with standardisation in order to provide a basis for a secure design of products.

15.2 ***NIS 2 Directive***

NIS 2 Directive, the European cybersecurity directive, is to be transposed into national law by October 2024. Among other things, it specifies criteria for the operation of critical systems and defines minimum standards for their information security. In addition, member states are obliged to set up a Computer Security Incident Response Team (CSIRT), a centre for the coordinated disclosure of vulnerabilities. The BSI already fulfils this task as the Federal Cyber Security Authority.

In the European context, the implementation of the NIS 2 Directive into national law is currently resulting in significant fields of action for the BSI. In accordance with Art. 31 Para. 4 of the NIS 2 Directive, the BSI will be responsible for national supervision of the implementation of IT security measures defined in the Directive. The directive also obliges member states to set up a Computer Security Incident Response Team (CSIRT), which is to serve as a central point of contact for coordinated vulnerability disclosure (CVD). This function is already performed by the BSI, as it acts as the national authority for IT security and is heavily involved in the implementation of the directive. The NIS 2 Directive harbours many innovations and challenges for the industry, but also for the Federal Republic of Germany. As one of the pioneers of European cybersecurity, Germany is well prepared for many of these challenges or is already implementing some of the requirements of the EU directive.

As “operators of critical facilities,” the operators of critical infrastructures (CI), whose maintenance of essential social functions is of central importance, are a subset of the “essential facilities” addressed in the NIS 2 Directive. In Germany, the first IT Security Act (IT-SiG) has provided a standardised legal framework for greater cybersecurity for CI since July 2015.

With the transposition of the NIS 2 Directive into national law, there will be an amendment to the BSI Act. This will significantly increase the number of companies falling under the supervision of the BSI. For the existing CIs, little is expected to change, but for around 29,000 “particularly important” and “important” facilities as defined by the Act, registration, verification and reporting obligations will arise for the first time. The BSI is currently preparing for these additional tasks by adapting existing processes for registration, notification and receipt of evidence.

The reporting of security incidents enables a rapid and coordinated response to threats and the creation of a detailed picture of the situation, which leads to a cooperative exchange to improve resilience and the level of cybersecurity in Germany and the EU.

As part of the preparations for the national implementation law for the NIS 2 Directive, the BSI has worked intensively to ensure that basic security requirements for an information security management system (ISMS) are declared binding for the federal administration. This serves to strengthen the federal administration’s own security and to guarantee a minimum level of necessary information security in Germany. The requirements are based on Section 8 (1) of the BSIG, which already stipulates minimum standards. These binding minimum standards aim to achieve a standardised and appropriate level of security in order to effectively counter the growing threats in cyberspace.

Basic IT protection provides a reliable framework for implementing an ISMS. Risk analyses to identify and assess security risks and the implementation of suitable security measures are planned within this framework. An ISMS that has been implemented in accordance with basic IT protection already covers most of the risk management measures required by the NIS 2 Directive, or at least provides a solid foundation on which organisations can build.

The implementation of the NIS 2 Directive is a significant step forward for cybersecurity in Europe and in Germany as a cybernation. The BSI is one of the key players and drivers of this development and is committed to ensuring that the new requirements are effectively transposed into national law and implemented in practice.

The BSI is already providing active support with assistance on the BSI website:

- The NIS 2 impact assessment is the central tool for checking whether a company is likely to be affected by the national implementation of the NIS 2 Directive in Germany.
- The NIS 2 FAQs provide a collection of answers to the most frequently asked questions about the NIS 2 Directive.
- The page "NIS 2 – What to do?" contains numerous tips on what important and particularly important organisations can already do.

In addition, the BSI's communication on the implementation of the NIS 2 Directive will also continue via other channels and formats. The BSI will update existing guidance in the coming months and create new guidance as soon as new information becomes available.

Read more about the NIS 2 Directive on the BSI website (German):

15.3 *Cybersecurity Act (CSA)*

The European Cybersecurity Act (CSA) came into force on 27 June 2019. For the first time, the European Union Agency for Cybersecurity (ENISA) has been given an open-ended mandate with expanded tasks and additional resources, especially in the operational area. Requirements for European cybersecurity certification have also been introduced.

This new system increases the resilience of information and communication technology (ICT) products, services and processes to cyberattacks throughout the EU and sets high standards for protection and trustworthiness in the digital infrastructure. The CSA ensures that Europe is well equipped to meet the challenges of the digital future.

BSI's Role in Certifying Cybersecurity

In the reporting year, the European Common Criteria (EUCC) scheme came into force as the CSA's first certification scheme. A number of other schemes are currently being prepared at the European level.

The BSI is the German National Cybersecurity Certification Authority (NCCA). The NCCA supervision ensures that the infrastructure required for certification is available by authorising conformity assessment bodies. It is also responsible for the market surveillance of certified products. The certifying NCCA assesses the trustworthiness of ICT products, services and processes.

Being put to the Test: The First Comprehensive Evaluation of the CSA

The first comprehensive evaluation of the CSA was due in 2024, and will be repeated every five years. As part of this evaluation, extensive interviews and workshops were organised in which various stakeholders contributed their perspectives and experiences.

As a result, the European Commission will prepare an impact assessment and present various options for the future direction of the CSA. The results of the evaluation and the resulting recommendations will play a key role in shaping the EU's future cybersecurity strategy to adequately address the ongoing changes of the digital age.

How BSI is Helping to Shape the Future of the CSA

The BSI was a key contributor within the process of evaluation of the CSA. This active participation has enabled the European Union Agency for Cybersecurity (ENISA) to sharpen and strengthen its role. The BSI has been actively involved in ENISA for many years through its contributions on the Management Board and the Executive Board. Last year, the head of BSI's section Liaison Office and Legal Affairs was elected Chairwoman of ENISA's Management Board. BSI colleagues participate in ENISA working groups and provide support by contributing to studies, conferences and technical publications. Personnel is also regularly seconded to ENISA. Colleagues are currently working in the ENISA staff and within the operations division. This promotes trust and fosters dialogue.

The BSI is constructively involved in the further development of the certification framework. In future, the BSI aims to continue contributing its expertise to the further development of European cybersecurity.

15.4 *Status Report on European Standardisation*

The main objective of the BSI's current standardisation work is to significantly raise the security level of products and infrastructures through high-quality and implementable standards on the European internal market, so that the state, society and the industry are all better protected against attacks and outages.

In the area of cybersecurity standardisation, the BSI is involved at European level in the creation and updating of standards, in particular European standards (EN) within the three European Standardisation Organisations (ESOs). These are CEN, CENELEC and ETSI. The BSI represents the interests of the German Federal Government in the ESO's standardisation activities.

In its standardisation activities, the BSI particularly pursues the approach of harmonising national specifications through the adoption of proven methods and approaches (best practices) in the area of cybersecurity in European standards. In addition to cybersecurity aspects, the BSI also pays attention to the economic and technical feasibility as well as the verifiability of the standards.

From the BSI's point of view, European standardisation has become much more important, as there has been a significant increase in European regulation in the area of cybersecurity, and as a result, new standards are being developed by the ESOs. The development of harmonised European standards (hEN) plays a key role here. These hENs are developed by the ESOs on the basis of official standardisation mandates from the European Commission and, if adopted by the Commission, are published in the Official Journal of the European Union. They are of particular importance when it comes to declarations of conformity of the regulated market, recognisable by the CE mark.

In the reporting period, the BSI therefore focused on participating in the development of harmonised standards for the Artificial Intelligence Act (AI Act), the Cyber Resilience Act (CRA) and the Radio Equipment Directive (RED). Of particular note here is the creation of the European draft standards FprEN 18031-1 to -3 in CEN/CENELEC in response to the cybersecurity requirements from the RED, which were finalised in good time thanks to the BSI's extensive use of resources. These have already been adopted by the national standardisation organisations of the member states. With the start of standardisation activities within the framework of the CRA, there are still many opportunities for participation and cooperation.

16 – Approval of VS Products

The BSI issues approvals for IT security products on the basis of the General Administrative Provision on Material Security (classified information directive, VSA). The approval confirms that these products can be used in an appropriately secure manner to protect classified information in IT systems. Evaluated VS products minimise the impact of malicious cyber incidents and protect the confidentiality of the classified information in the event of attacks.

The number of approvals granted is at a consistently high level. The majority of the approval statements are re-evaluations of already approved IT security products. With the amendment of the VSA on 1 April 2023, the previous release recommendation was replaced by the approval recommendation (see Figure 25, page 62).

In addition to issuing approval statements for the protection of national classified information, the BSI also issues approvals for the protection of NATO and EU classified information (see Figure 26, page 63). In most cases, this is done in a joint approval procedure so that the corresponding international approval is also available once the national approval has been granted or the necessary second part evaluation can be initiated.

Read more about classified information authorisation:

Developer Qualification

The dynamic and constantly growing threat landscape leads to a mandatory increase in cyber resilience in the field of electronic classified information (CI). Thus, one goal is to carry out approvals of IT security products even more effectively and efficiently. The Developer Qualification is a well-established method to achieve this goal.

A successfully completed Developer Qualification is mandatory and a prerequisite for developers of IT security products to allow their IT security products to undergo the "BSI qualified procedure for VS-NfD approvals". After a successful evaluation of its development processes, the BSI issues a "Developer Qualification" to the developer. This means that the BSI is confident that the developer is able to design and develop IT security products in compliance with corresponding BSI requirements.

If products have been developed in accordance with audited and trustworthy development processes, approval procedures can be carried out with a significantly reduced evaluation scope while ensuring the evaluation assurance level. This enables a "Qualified Developer" to obtain product approvals much faster than would be the case with the conventional approval procedure. A large number of successfully completed qualified procedures for VS-NfD approvals, in which product approval was granted within four to eight weeks, demonstrates the efficiency of the Developer Qualification method.

Currently, six developers have successfully completed a Developer Qualification. Additionally, three developers are undergoing the initial qualification process now. In the reporting period, the BSI carried out 14 procedures for the continuous maintenance of the Developer Qualification.

On top of that, the BSI developed a process model and a set of evaluation criteria in order to maintain previously issued Developer Qualifications continuously. The process model supports the transparent and reproducible execution of various re-qualifications. The set of evaluation criteria is currently in validation. They enable both the developers and the BSI to produce and review the necessary evidence of the development processes.

Classified Information Requirements Profile

In general, Classified Information (CI) Requirements Profiles are further instruments used to increase cyber resilience. A CI Requirements Profile describes IT security requirements for IT security products that shall be approved. Users, operators, developers and the BSI create the Requirements Profiles within a cooperative joint process. This ensures that security requirements are defined in a harmonised, needs-based and efficient manner. Consequently, this allows all previous mentioned stakeholders to react more quickly to new trends and changes in the IT security threat landscape, which also leads to an increased cyber resilience. Thus, CI Requirements Profiles are a critical and controlling element of the BSI approval scheme.

As of today, the BSI has already successfully published a total number of 22 CI Requirements Profiles. They cover a wide range of product types and are often used by product

BSI authorisation procedure for classified information products

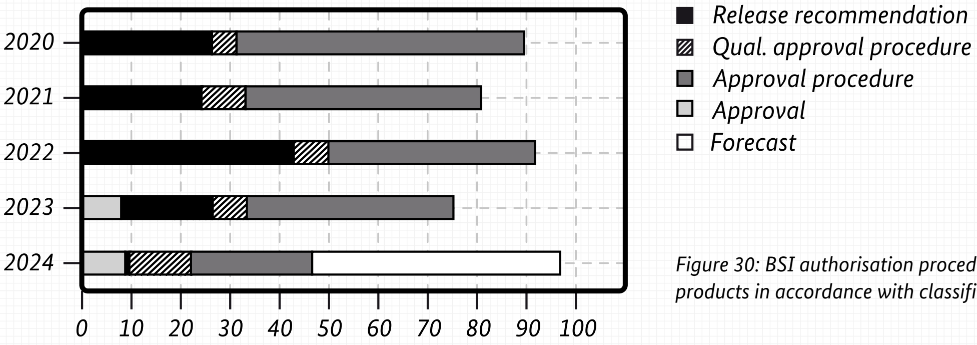


Figure 30: BSI authorisation procedure for classified information products in accordance with classified information directive (VSA)

National and international BSI approvals for classified information products

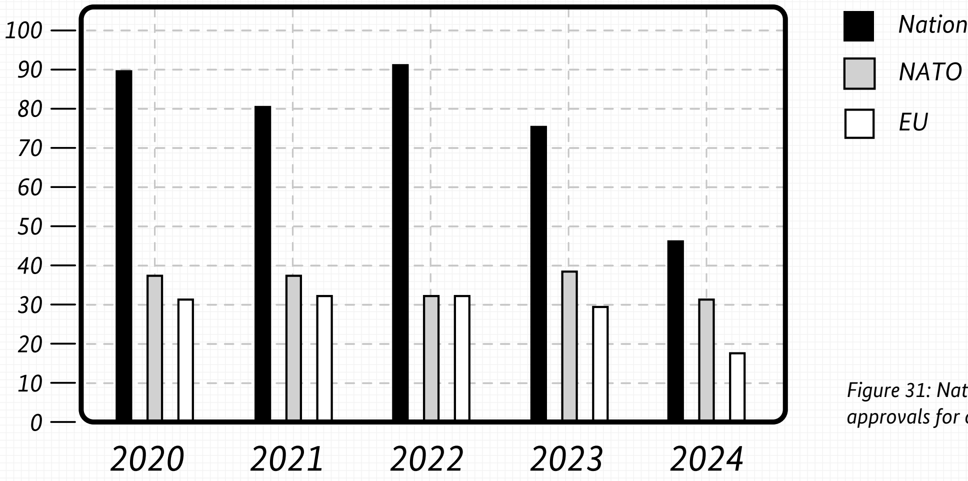


Figure 31: National and international BSI approvals for classified information products

Total numbers of the BSI Classified Information Requirements Profiles

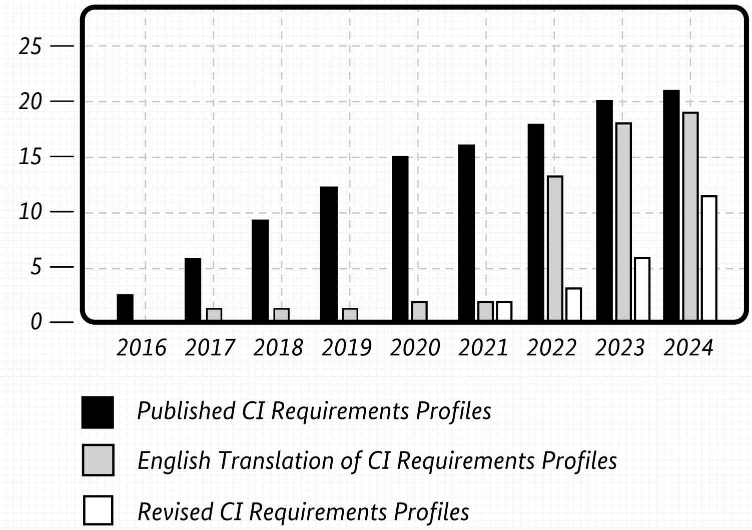


Figure 32: Total numbers of CI Requirements Profiles

developers as can seen by a large number of IT security products that have been developed and approved in accordance with corresponding CI Requirements Profiles. A complete list and a detailed description of already published CI Requirements Profiles and those currently under development is available on the BSI website.

Read more about CI-Requirements Profiles:

During the reporting period, both CI Requirements Profiles "CI-Registry System" and "Data Diode" were initially developed and published. They describe requirements for IT security products for the processing of classified information up to the classification level "VS GEHEIM". Additionally, the CI Requirements Profile "Firewall" has been successfully revised. This profile describes requirements for processing of classified information up to the classification level "VS NfD". Further, English translations are also available for a significant majority of the published CI Requirements Profiles. As all existing Requirements Profiles represent a standard, which is continuously adapted to the current state of the art, they will be revised continuously in the future.

In the recent years, the interest of national and international developers in both, the creation and revision of CI Requirements Profiles has grown significantly. Among other things, an increased number of stakeholders, which are involved in the creation process, shows this increasing high interest. Further, surveys have also shown that manufacturers of IT security products and users are in favour of the CI Requirements Profiles.

17 – Conclusion

The IT security situation in Germany was and still is a cause for concern. The threat landscape continues to develop rapidly. The digital attack surface is constantly increasing, vulnerabilities all too often offer serious opportunities for intrusion and attackers are finding ever faster and more skilful ways to exploit them. But nobody is defenceless. The order of the day is to drastically increase Germany's resilience to cyber threats and incidents. As part of Cybernation Germany, the BSI has taken many concrete steps to better prepare companies, authorities and citizens for IT security incidents and to protect them against cyberattacks. This is based on monitoring the situation in terms of threats, attack surface, attacks, damage and resilience, with resilience having a positive impact on the other four dimensions.

Cybersecurity Dimensions

Threats have come from a variety of attacker groups over the past reporting period. For example, cyber espionage attacks by APT groups have targeted public authorities, particularly in the areas of foreign affairs, defence, public security and public order, as well as companies and organisations operating in these areas. The cybercriminal black market economy based on the division of labour has also become more professionalised: while some groups increasingly traded in stolen access data (access brokers), other cybercrime groups used zero-day vulnerabilities to steal data. Increasingly, this data has been used for extortion without first using ransomware known as encryption trojans. Human error can also pose a threat; the CrowdStrike incident in July 2024 was caused by a mistake in the software.

The number of attack surfaces has continued to expand during the period under review, as the number of complex and vulnerable systems is also growing with increasing digitalisation. In addition to the daily increase in known vulnerabilities, a large number of critical vulnerabilities have been identified in perimeter systems such as firewalls and VPNs. At the same time, attacks on perimeter systems continued to increase significantly. Android systems were also noticeably vulnerable – especially if they were running outdated versions of the software, some of which were no longer updated.

Threats that were reported included many types of attacks. The huge increase in the number of high-volume DDoS attacks, particularly in the first half of 2024, was alarming and protection measures had to be adapted. Ransomware attacks are being launched on a massive scale against easy targets such as small and medium-sized businesses and municipalities, which are often still inadequately protected. The attack on a municipal IT service provider at the end of October 2023 alone affected 72 municipal customers with around 20,000 municipal workplaces. Public cloud infrastructures were also attacked. The suspected Chinese and state-sponsored attack group Storm-0558 compromised the encryption of email accounts. This meant that the identity data of millions of people was potentially at risk.

The damaging impact in the reporting period was considerable. This includes e.g. the downtime of local authorities, sometimes for months, due to ransomware attacks. Ransomware attacks also resulted in $1.1 billion USD in ransom being captured worldwide, although the number of unreported cases is likely to be much higher. It is worth noting that on average, almost three times as much was paid for captured exfiltrated data as for captured encrypted data. The number of suspected victims of data breaches also continued to rise during the period. In the second half of 2023, the number of suspected leakage victims even briefly doubled compared to the reference year 2021.

The Decisive Factor: Resilience

Although the effects in the four dimensions of threats, attack surface, attacks and impact are serious, Germany is not defenceless against this backdrop. During the reporting period, the BSI, with the broad expertise of its staff, made a significant contribution to detecting threats at an early stage, issuing warnings and providing assistance and solutions. With the help of its sensor technology, the BSI was e.g. able to detect botnets through sinkholes and has thus contributed to criminal prosecutions. Authorities around the world were able to carry out numerous takedowns against botnets operated by cybercriminal attacker groups. As a result, the emergence of new malware variants was kept at a stable level compared to the strong upward fluctuations in previous years. To prevent long downtimes following cyberattacks, institutions improve their ability to respond by setting up business continuity management systems (BCM systems) which are described in detail by the BSI in Standard 200-4 and are explicitly required by CI operators.

Resilience is a Shared Effort

Germany has already come a long way on the road to becoming a resilient cybernation. However, resilience cannot be achieved in a sprint. The BSI and all other players need long-distance qualities in order to achieve this objective. To strengthen resilience to cybercrime and IT security incidents, all stakeholders are called upon to play their part. From the BSI's point of view, it is essential that manufacturers provide secure products that are developed and maintained in accordance with the principles of security by design and security by default. Operators are required to implement the principles of cybersecurity, ideally in a structured information security management system (ISMS). The BSI and other government agencies will continue to provide support and guidance, for example through the cooperative and effective implementation of the NIS 2 Directive. Consumers should develop cybersecurity skills, for example by keeping up to date with possible attack vectors or scams.

The BSI as a Partner and Helper for Greater Cybersecurity

Reducing harmful effects is also the aim of all resilience efforts. The BSI is already making a significant contribution to achieving this. For example, the BSI Situation Centre has been expanded and modernised in order to better monitor the IT security situation in Germany 24 hours a day, 7 days a week, 365 days a year, and to become the National IT Crisis Response Centre in particularly serious cases.

The number of individual cooperation agreements between the BSI and federal states for closer collaboration was increased to seven in the reporting period. In addition, the BSI is working with other German authorities in the Digital Cluster Bonn to ensure a common and coordinated approach to current EU directives and to reduce bureaucracy. In order to improve the German communications infrastructure, the 5G/6G Security Lab has been established at the BSI site in Freital, Germany. In the cloud domain, BSI has developed the highly regarded BSI Cloud Strategy, which provides leading technological and ready-to-deploy solutions across the entire cloud operating spectrum. Last but not least, this year's European Football Championship and European Elections in Germany went off without any significant cybersecurity incidents because Germany was well prepared – also with the support of the BSI.

European and international cyberspace is also part of the BSI's commitment to increasing resilience. The BSI, which is responsible for cybersecurity in Germany, is introducing reporting requirements for many new companies and businesses in accordance with the German law implementing the EU's NIS 2 Directive. This will also help to provide a more comprehensive picture of the situation. In addition, two new EU directives came into force with the Cyber Resilience Act (CRA) and the Cybersecurity Act (CSA). As part of the CRA, the BSI is preparing to take on a market surveillance function. The first Cybersecurity Certification Scheme EUCC for the security certification of IT products came into force under the CSA with the involvement of the BSI.

A Vision for Cybersecurity

Increasing Germany's resilience as a cybernation with its many stakeholders is a challenging task. In addition to the Cyber Resilience Act or NIS 2, further regulatory innovations will increase cybersecurity in Germany and Europe. At the same time, however, the associated requirements must also be implemented. Businesses and institutions are particularly challenged in this respect. Numerous framework conditions are also changing for supervisory authorities such as the BSI. Not only does market surveillance for the CE label under the Cyber Resilience Act need to be expanded, but tens of thousands of companies and businesses also need to be supported under the NIS 2 Directive. These challenges can only be met if government, business, science and society work closely together. In the spirit of Germany as a cybernation, the BSI will work together with all stakeholders to achieve the common goal of a secure digital everyday life.

The impact of the global IT disruption in July 2024 was a powerful reminder of how dependent our digitalised world is on functioning IT systems. This incident was inadvertent proof that, because of the networks and interdependencies in place, only intensive co-operation between all parties involved can be effective. In a very short space of time, the cause of the problem had been identified, a solution was in place and information was provided to stakeholders and the public. Users, vendors, operators, associations and the BSI worked hand-in-hand to overcome this crisis as quickly as possible. Prevention is crucial to ensure that such crises occur less frequently in future. For this reason, the BSI is working closely with all stakeholders, including the scientific community, to develop and implement the right measures, also after the acute crisis.

The example of CrowdStrike demonstrates that Germany's major goal as a cybernation can only be achieved by joining forces. Germany's high level of technological expertise is an asset in the development of solutions. Together with industry, research and government, these solutions are being implemented in a vibrant ecosystem of cybersecurity products and services. Together, we are increasing the security and speed of digitalisation. Now and in the future, the motto has to be: "Cooperation wins".

18 – Glossary

Access Broker

Access brokers are cybercriminals who gain access to a victim network in a variety of ways and regularly sell this access to other cybercriminals or interested parties.

Advanced Persistent Threats

Advanced Persistent Threats (APT) are targeted cyberattacks on selected institutions and facilities in which an attacker gains persistent (permanent) access to a network and subsequently extends this access 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 manufacturers to IT security managers in companies and other organisations on how to deal with vulnerabilities found.

Affiliates

With cybercrime-as-a-service, the cybercriminal using the service is usually referred to as an affiliate. The term is derived from affiliate marketing, in which a commercial provider makes advertising material available to its sales partners (affiliates) and offers a commission. In the context of cybercrime, for example, ransomware is provided instead of advertising material and the affiliate is promised a share of the ransom.

Attack vector

An attack vector is the combination of attack path and technique used by an attacker to gain access to IT systems.

Authentication

Authentication is the process of verifying the identity of a person or a computer system on the basis of a specific characteristic. This can be done by entering a password, chip card or biometrics.

Backdoor

A backdoor is a programme, usually installed by viruses, worms or Trojan horses, which gives third parties unauthorised access to the computer, but in a hidden manner and bypassing the usual security measures.

Backup

Backup is the copying of files or databases on physical or virtual systems to a secondary storage location in order to use them for recovery in the event of a device failure or disaster and to keep them safe until then.

Bitcoin

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

Blockchain

Blockchain describes distributed, synchronised, decentralised and consensual data storage in a peer-to-peer network. A hash-linked list of data blocks is kept redundantly in all network nodes, which is updated using a consensus procedure. Blockchain is the technological basis for cryptocurrencies such as Bitcoin.

Bot/botnet

A botnet is a network of computers (systems) that are infected by a remotely controllable malicious programme (bot). The affected systems are monitored and controlled by the botnet operator using a command and control server (C&C server).

Brute forcing

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

Bug bounty

Monetary rewards (bounty) for finding vulnerabilities (bugs). Manufacturers of software products 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 or similar and to 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 defend against cyberattacks, respond to IT security incidents and implement preventive measures.

CERT-Bund

The German Federal Government's Computer Emergency Response Team (CERT) is based at the BSI and acts as a central point of contact for federal authorities for preventive and reactive measures in the event of security-related incidents in computer systems.

Cloud/cloud computing

Cloud computing refers to the dynamic provision, utilisation and billing of IT services via a network in line with demand. These services are offered and utilised exclusively via defined technical interfaces and protocols. The services offered as part of cloud computing cover the entire spectrum of information technology and include infrastructure (computing power, storage space), platforms and software.

Command and control server (C&C server)

Server infrastructure used by attackers to control the infected computer systems (bots) integrated into a botnet. Bots (infected systems) usually report to the attacker's C&C server after infection in order to receive the attacker's commands.

Confidential computing

Confidential computing uses hardware-based, certified Trusted Execution Environments (TEE) to protect the confidentiality and integrity of data while it is being processed ("in use"). A TEE is an isolated part within a system that provides a specially protected runtime environment. The TEE can, for example, be a component of the main processor (CPU) or part of the system on chip (SoC) of a smartphone. Only authorised bodies are permitted to add or change applications in the TEE. The attestation of the TEE and the application running in the TEE serves to validate the trustworthiness of the processing.

CVSS score

Industry standard used to assess the criticality of vulnerabilities on an internationally comparable basis.

Cybercrime-as-a-Service (CCaaS)

Cybercrime-as-a-Service (CCaaS) describes an area of cybercrime in which offences are committed by cybercriminals by commission or facilitated as a service. For example, in the case of Malware-as-a-Service (MaaS), which is a subset of CCaaS, a hacker is provided with the malware to commit a crime for a fee by a third party or a group of hackers, and can also be provided with updates and similar services, just as in the legal software industry. One type of MaaS is Ransomware-as-a-Service (RaaS), where the malware for encrypting an infected system, updating this malware, handling the ransom negotiations and payments, and other extortion methods are often provided for a fee. The dissection of a cyberattack into individual services associated with CCaaS enables even less IT-savvy attackers to carry out technically sophisticated cyberattacks.

Deepfake

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

Defacement

The word "defacement" means "to disfigure" or "to distort". In a defacement, a website is wilfully modified by an attacker by exploiting vulnerabilities or using spied out or guessed access data.

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 in parallel using several systems, it is referred to as 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 ransom money for encrypted data, but also hush money for exfiltrated data.

Downgrade attack

A mobile downgrade attack is an attack where the attacker attempts to downgrade the communication between a mobile device (e.g. a smartphone) and the mobile network to a less secure protocol version (e.g. from a 5G connection to a 2G connection) in order to exploit its security vulnerabilities.

Drive-by download/drive-by exploits

Drive-by exploits refer to the automated exploitation of vulnerabilities on a PC. When a website is viewed without further user interaction, vulnerabilities in the web browser, additional browser programmes (plug-ins) or the operating system are exploited to install malware on the PC covertly.

eUICC

The embedded Universal Integrated Circuit Card (eUICC) is a SIM card with an overwritable profile that allows the mobile operator to be changed without physically replacing the SIM card. This SIM profile can be overwritten remotely via the air interface (Over the Air, OTA). To enable SIM profiles to be changed, an eUICC requires a minimum memory of 512 KB.

Exit scam

The term exit scam describes a form of fraud in which a person accepts transactions, including cryptocurrency, for services without providing the agreed consideration and absconds with the proceeds.

Exploit

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

Hacktivism

Hacktivism is a combination of the terms hacking and activism. These are ideologically motivated hacking activities aimed at spreading ideological, political and/or social statements in the digital space. The preferred criminal offences used by hacktivists to carry out protests and/or propaganda in the digital space are web defacement, DDoS attacks and the spying on and manipulation of data.

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 makes it possible to map large amounts of data (e.g. a malicious programme) exactly in comparatively few characters. The hash function is a mathematical function for converting data. Subsequent recalculation of the hash value into the original data is virtually impossible or only possible with extremely high computing effort.

Hybrid threats

Hybrid threats are characterised as coordinated actions by state actors to achieve their own goals to the (system-relevant) detriment of another state, and which remain outside the framework of a conventional military conflict. Cyberattacks or disinformation campaigns can also be used in this context, for example.

Information stealer

Malicious programmes that enable cyber criminals to access various types of personal data, such as login data for various online services, on infected devices without the affected person noticing.

Internet of Things/IoT

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

ITSEF

According to Implementing Regulation 2024/482, an Information Technology Security Evaluation Facility (ITSEF) is an IT security evaluation facility that is a conformity assessment body within the meaning of Article 2(13) of Regulation (EC) No 765/2008 and carries out evaluation activities.

IT Security Act 2.0

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

Crypto wallet

A crypto wallet is a digital wallet for cryptocurrencies that serves as a storage location for private and public keys that are used to carry out transactions with the respective cryptocurrency.

Legitimate programmes

Programmes that perform harmless, desired operations.

MaaS

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

Malicious

In IT security, programmes or websites that can carry out harmful operations on a computer system are referred to as malicious or harmful.

Malware

The terms malicious function, malicious programme, malware and malicious software are often used synonymously. Malware is an artificial word, derived from malicious software, and refers to software that has been developed with the aim of executing unwanted and usually harmful functions. Examples are computer viruses, worms and Trojan horses. Malware is usually designed for a specific operating system variant and is therefore usually written for popular systems and applications.

Man-in-the-middle attack

In a man-in-the-middle attack, the attacker infiltrates a private communication between two or more communication partners in order to spy out information or manipulate the connection.

Mark-of-the-Web/MOTW

An MOTW flags download files if they probably originate from an untrustworthy source. If a user opens a file marked in this way, he or she will be warned accordingly.

Monero

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

NCCA

The BSI is the National Cybersecurity Certification Authority (NCCA for short) within the meaning of Article 58 (1) of Regulation (EU) 2019/881 (Cybersecurity Act, CSA for short) in conjunction with Section 9a BSIG. In compliance with Article 58 (4) CSA, the BSI as NCCA carries out supervision and certification strictly separately and independently of each other.

NESAS

Certification programme for 5G mobile communications equipment (Network Equipment Security Assurance Scheme).

NESAS CCS-GI

The national certification programme for 5G mobile communications equipment (NESAS Cybersecurity Certification Scheme – German Implementation).

Network attached storage (NAS)

A storage device connected to a network that enables authorised network users 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

A patch is a software package with which software manufacturers close vulnerabilities in their programmes or integrate other improvements. Many programmes make it easier to install these updates with automatic update functions. Patch management refers to processes and procedures that help to obtain, manage and apply available patches for the IT environment as quickly as possible.

Peer review

As part of peer reviews, a selected group of experts from various EU states check new eIDs from other EU states for their conformity with the eIDAS Regulation.

Phishing

The word is made up of the words password and fishing, which means fishing for passwords. The attacker attempts to gain access to an internet user's personal data via fake websites, emails or text messages and to misuse this data for their own purposes, usually to the detriment of the victim.

Plug-in

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

Proliferation

The term originally comes from military defence and refers to the transfer of weapons of mass destruction, including the technical know-how required for them and the materials needed to manufacture them. In IT security, the term is used to describe the sharing of cyber weapons (software and methods) between attackers. Through proliferation, the means and methods of attack can spread very quickly among different attacker groups without them having to develop specific technical expertise.

Proof of concept

Proof that a project developed in theory can also be implemented in practice.

Provider

Service providers with different focuses, for example network providers who provide the infrastructure for data and voice transport as mobile communications providers, internet service providers or carriers, or service providers who provide services that go beyond network provision, such as the network operation of an organisation or the provision of social media.

Public key cryptography

In public-key cryptography, i.e. asymmetric encryption, there are always two complementary keys. One key, the public key, is used to encrypt a message, another, the private key, is used to decrypt it. Both keys together form a key pair.

Source code

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

Ransomware

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

RaaS

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

Resilience

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

RSA

The term refers to a method of public key cryptography 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 modulus "n," a natural number that is the product of two secret prime numbers "p" and "q". The security of RSA is based in particular on the difficulty of factorising the RSA module n, i.e. calculating the two prime factors "p" and "q" from knowledge of "n" only.

Scam mail or fraud mail

Category of spam mails with which attackers pretend to collect donations, for example.

Rapid reports

Rapid reports are regulated for German Bundestag elections in Section 71 of the Federal Election Ordinance (BWO), for example. The election results of each electoral district are aggregated and forwarded by telephone, electronically or in another way from the electoral board via the municipality, district electoral management, state electoral management to the federal electoral management. Once the results of all constituencies are available, the provisional official final result is published. This is typically the case on election night.

Script kiddies

Attackers who try to penetrate other people's computer systems or generally cause damage despite a lack of knowledge.

Security advisory

Recommendations for IT security managers on how to deal with vulnerabilities found.

Security Assurance Specification (SCAS)

Security Assurance Specifications (SCAS) define important security functions that also form the basis for product certification in accordance with NESAS CCS-GI.

Security by default

A product that is delivered according to security by default is already in a securely preconfigured delivery state without any additional measures required.

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 (e.g. energy consumption, electromagnetic radiation, time consumption of an operation) in order 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.

Smishing

Smishing (phishing via SMS) is characterised by the sending of countless SMS or short messages via messenger to a large number of phone numbers, for example with alleged delivery notifications or instructions for downloading a voice message. The aim of this method is usually to trick the recipient into clicking on a link containing malicious apps or malicious websites.

Social engineering

In cyberattacks using social engineering, criminals try to trick their victims into disclosing data, bypassing protective measures or installing malware on their systems themselves. Both in the area of cybercrime and espionage, attackers use skilful methods to exploit supposed human weaknesses such as curiosity or fear in order to gain access to sensitive data and information.

Spam

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

Spear phishing attack

Spear phishing is a targeted cyberattack that is carried out using emails that have been specially prepared for a specific group or individual in order to obtain personal data or infect the target with malware.

Speculative execution

Speculative execution is a microarchitectural optimisation to increase the efficiency of processors. It attempts to predict the next commands to be executed and process them ahead of time (speculatively). If the prediction does not materialise, the intermediate results are discarded, the executed commands have no effect and become volatile.

Stack overflow

A stack overflow or buffer overflow is a frequently occurring and frequently exploited vulnerability. A buffer overflow occurs when more data can be written to a memory than the buffer intended for this purpose can hold. This also writes data to neighbouring memory areas. This can result in programme crashes, compromised data, the acquisition of extended rights or the execution of malicious code.

Supply chain attack

In a supply chain attack, cyber criminals gain indirect access to the attack target by successfully attacking manufacturers, service providers or suppliers (i.e. the supply chain) and using the trust relationships established with them to attack the actual target (e.g. by using established VPN connections, existing maintenance access or manipulating patches).

Symlink

A symlink – also known as a symbolic link – is a file system object that references a file or directory using a path specification.

Trusted Execution Environment (TEE)

A Trusted Execution Environment (TEE) is an isolated part within a system that provides a specially protected runtime environment. For example, the TEE can be part of the main processor (CPU) or part of the system on chip (SoC) of a smartphone. The TEE protects the integrity and confidentiality of the data and key material it contains from unauthorised third parties, including the user of a device, for example. Only authorised bodies are permitted to add or change applications in the TEE.

Implementation Plan for Critical Infrastructure (IPCI)

IPCI is a public-private cooperation between CI operators, their associations and government agencies such as the BSI.

Voltage glitching

Voltage glitching is a method of manipulating the programme sequence of chips by switching off the supply voltage for a short time (in the millisecond range). For example, critical authentication routines can be “skipped” in order to gain access to otherwise protected data. In December 2023, a successful attack on Tesla Autopilot hardware using voltage glitching was published. This attack made it possible to extract programme code, user data and cryptographic keys from the system.

Virtual Private Network (VPN)

A virtual private network (VPN) is a network that is physically operated within another network (often the internet), but is logically separated from this network. In VPNs, cryptographic processes can be used to protect the integrity and confidentiality of data and securely authenticate communication partners, 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.

Vishing

With vishing (voice phishing), the target person is contacted by telephone and tricked into disclosing information or making a payment with the help of a conversation script. The widespread and still current content of the phone calls is fake calls from alleged IT support or authorities, in which the victims are suggested that they have to make a payment or release personal data for verification.

Webshell

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

Wiper

Malware that destroys data. In contrast to ransomware, wipers are not aimed at encryption with subsequent blackmail, but at sabotage through the final destruction of data.

Two-factor or multi-factor authentication (2FA or MFA)

With two-factor or multi-factor authentication, an identity is authenticated using different authentication factors from separate categories (knowledge, possession or biometric features).

19 – Bibliography

1 https://www.bsi.bund.de/dok/ransomware-links

2 https://www.usenix.org/system/files/sec20-oest-sunrise.pdf, P. 21

3 https://nationale-leitstelle.de/verstehen/o-LIS-Report_der_Nationalen_Leitstelle_Ladeinfrastruktur/

4 https://cert.vde.com/en/advisories/VDE-2024-011

5 https://terrapin-attack.com/

6 https://www.openwall.com/lists/oss-security/2024/04/15/6

7 https://www.vice.com/en/article/xgwgn4/researchers-demonstrate-ai-supply-chain-disinfo-attack-with-poisongpt

8 The State of Phishing 2023, https://slashnext.com/wp-content/uploads/2023/10/SlashNext-The-State-of-Phishing-Report-2023.pdf

9 https://www.medianama.com/2024/04/223-anthropic-writes-paper-jailbreak-claude-trick-answering-harmful-questions, https://www-cdn.anthropic.com/af5633c94ed2beb282f6a53c595eb437e8e7b630/Many_Shot_Jailbreaking__2024_04_02_0936.pdf

10 https://www.coveware.com/blog/2023/7/21/ransom-monetization-rates-fall-to-record-low-despite-jump-in-average-ransom-payment, https://www.coveware.com/blog/2023/10/27/scattered-ransomware-attribution-blurs-focus-on-ir-fundamentals

11 https://www.coveware.com/blog/2024/4/17/raas-devs-hurt-their-credibility-by-cheating-affiliates-in-q1-2024

12 https://www.coveware.com/blog/2024/4/17/raas-devs-hurt-their-credibility-by-cheating-affiliates-in-q1-2024

13 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Aktive-Crime-Gruppen/aktive-crime-gruppen_node.html

14 https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf

15 https://www.pwc.de/de/cyber-security/ceosurvey.html

16 https://de.statista.com/infografik/26033/ausgaben-fuer-it-sicherheit-in-deutschland/

17 https://www.bitkom.org/Bitkom/Publikationen/Studie-Wirtschaftsschutz

18 https://www.bitkom.org/Bitkom/Publikationen/Studie-Wirtschaftsschutz

19 https://www.bitkom.org/Bitkom/Publikationen/Studie-Wirtschaftsschutz

20 https://www.pwc.de/de/cyber-security/ceosurvey.html

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

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

23 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/bsi-standard-200-4_Business_Continuity_Management_node.html

24 https://mip2.bsi.bund.de/meldungen/meldung-ohne-registrierung-erstellen

25 https://www.destatis.de/DE/Themen/Branchen-Unternehmen/Unternehmen/Kleine-Unternehmen-Mittlere-Unternehmen/Tabellen/wirtschaftsabschnitte-insgesamt.html

26 https://www.bmwk.de/Redaktion/DE/Artikel/Digitale-Welt/foerderprogramm-go-digital.html

27 https://www.mittelstand-innovativ-digital.nrw/

28 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html

29 https://www.gesetze-im-internet.de/bwo_1985/__71.html

30 https://www.theguardian.com/money/2016/jul/28/last-minute-olympics-tickets-scam-warning

31 https://www.reuters.com/article/us-twitter-olympics-idUSKBN2090SA/, https://www.spiegel.de/sport/fussball/football-leaks-informant-rui-pinto-ich-habe-getan-was-ich-tun-musste-a-a586ab53-3bd7-4c72-9843-307b423f9c84

32 https://www.theverge.com/2022/12/14/23509674/fubo-tv-down-france-morocco-world-cup-semifinal

33 https://www.bleepingcomputer.com/news/security/ransomware-hits-garage-of-canadian-domain-registration-authority/

34 https://www.bild.de/sport/fussball/fussball-international/premier-league-cyber-angriff-hacker-erpressen-manchester-united-74168850.bild.html

35 https://www.fortinet.com/blog/threat-research/wiper-malware-riding-tokyo-olympic-games

36 https://news.microsoft.com/de-de/richtiger-einsatz-von-double-key-encryption/

37 https://www.digital-identity-wallet.eu

38 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Cryptographic-Service-Provider/csp.html

39 https://globalplatform.org

40 https://www.ausweisapp.bund.de/home

Overview of cybersecurity in Germany 2024

1 BSI cybersecurity warning 26.03.2024

2 BSI cybersecurity warning 01.03.2024

20 – List of Abbreviations

Abbreviation	Long form
5G/6G	5th/6th generation
AI	Artificial Intelligence
AISEC	Fraunhofer Institute for Applied and Integrated Security
AMD	Advanced Micro Devices, Inc. (Incorporated)
API	Application Programming Interface
APT	Advanced Persistent Threat
ARM	Advanced RISC (Reduced Instruction Set Computer) Machines
BCMS	Business-Continuity-Management-System
BNetzA	Bundesnetzagentur
BSI	Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik)
BSI C5	Cloud Computing Compliance Criteria Catalogue of the BSI
BSIG	BSI Act (BSI-Gesetz)
BSI-KritisV	BSI KRITIS Regulation (BSI-Kritisverordnung)
BSOD	“Blue Screen of Death”
BVMW	Federal Association of Small and Medium-Sized Enterprises (Bundesverband mittelständische Wirtschaft)
BYOVD	Bring Your Own Vulnerable Driver
C2-Server	Command-and-Control-Server
CCaaS	Cybercrime-as-a-Service
CE	Conformité Européenne
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CERT	Computer Emergency Response Team
ChatGPT	Chat Generative Pretrained Transformer
CPU	Central Processing Unit
CRA	Cyber Resilience Act
CSA	Cyber Security Act
CSIRT	Computer Security Incident Response Teams
CSRB	Cyber Safety Review Board (USA)
CSW	Cyber Security Warning (of the BSI)
CVD	Coordinated Vulnerability Disclosure
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System

Abbreviation	Long form
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
DDL	Data Definition Language
DDoS	Distributed Denial of Service
DDR	Double Data Rate
DIN	Deutsches Institut für Normung
DIN SPEC	DIN Specification
DKE	Double Key Encryption
DNS	Domain Name System
DoH	DNS over HTTPS
DORA	Digital Operational Resilience Act
ECDSA	Elliptic Curve Digital Signature Algorithm
EDR	Endpoint Detection and Response
eID	Electronic Identification
eIDAS	Electronic Identification, Authentication and Trust Services
Email	Electronic Mail
EN	European standards
EnWG	Energy Industry Act (Energiewirtschaftsgesetz)
ESA	European Space Agency
eSe	Embedded Secure Element
eSIM	Embedded SIM
ETSI	European Telecommunications Standards Institute
EU	European Union
EUCC	EU cybersecurity certification scheme on Common Criteria
EUCS	EU Cloud Certification Scheme
EUDIW	European Digital Identity Wallet
eUICC	Embedded Universal Integrated Circuit Card
GPU	Graphics Processing Unit
hEN	Harmonised European Standards
HTTPS	Hypertext Transfer Protocol Secure
ICS	Industrial Control System
ID	Indentification
IDS	Intrusion Detection System

Abbreviation	Long form
IEC	International Electrotechnical Commission
IKT	Information and Communication Technology
IoT	Internet of Things
IP	Internet protocol
IPCC	International Police Coordination Center
ISMS	Management System for Information Security (Informationssicherheitsmanagementsystem)
ISO	International Organization for Standardization
IT	Information Technology
KMU	Small and medium-sized enterprises
KRITIS	Critical infrastructures
LLM	Large Language Model (KI)
LSP	Large Scale Pilot
MaaS	Malware-as-a-Service
MID	Mittelstand Innovativ & Digital Programme
MIRT	Mobile Incident Response Team
NCCA	National Cybersecurity Certification Authority
NFC	Near Field Communication
NIS	Network and Information Security
NIST	National Institute of Standards and Technology (USA)
NRW	North Rhine-Westfalia
OCR	Optical Character Recognition
OP	Operation
OT	Operational Technology
OWA	Outlook Web Access
OWASP	Open Web Application Security Project
ProPK	Police Crime Prevention of the Federal States and the Federal Government (Programm Polizeiliche Kriminalprävention)
RaaS	Ransomware-as-a-Service
RAG	Retrieval Augmented Generation (AI)
RAN	Radio Access Network
RED	Radio Equipment Directive
RFID	Radio-Frequency Identification
SBOM	Software Bill of Materials
SE	Secure Element

Abbreviation	Long form
SEC	Securities and Exchange Commission
SS7	Signalling System 7
SSH	Secure Shell (Netzwerkprotokoll)
TKG	Telecommunications Act (Telekommunikationsgesetz)
TR	Technical Guideline (Technische Richtlinie)
URL	Uniform Resource Locator
US(A)	United States (of America)
VPN	Virtual Private Network
VPS	Virtual Private Server
VS	Classified information (Verschlusssachen)
VSA	Classified information directive (Verschlusssachenanweisung)
VS-NfD	Classified information - for official use only (Verschlusssachen - nur für den Dienstgebrauch)
WLAN	Wireless Local Area Network
XAI	Explainable AI

Legal Notice

Published by
Federal Offce for Information Security (BSI)

Source
Federal Offce for Information Security
Godesberger Allee 87, 53175 Bonn
Email: bsi@bsi.bund.de
Phone: +49 (0) 22899 9582-0
Fax: +49 (0) 22899 9582-5400

Last updated
October 2024

Printed by
Appel & Klinger Druck und Medien GmbH, Schneckenlohe

Design

KOMPAKTMEDIEN – Agentur für Kommunikation
GmbH, Berlin

Content and editing
Federal Offce for Information Security

Infographics
Federal Offce for Information Security

Image credits
Page 5: © Bundesfoto/Christina Czybik;
Page 7: © BMI/Henning Schacht

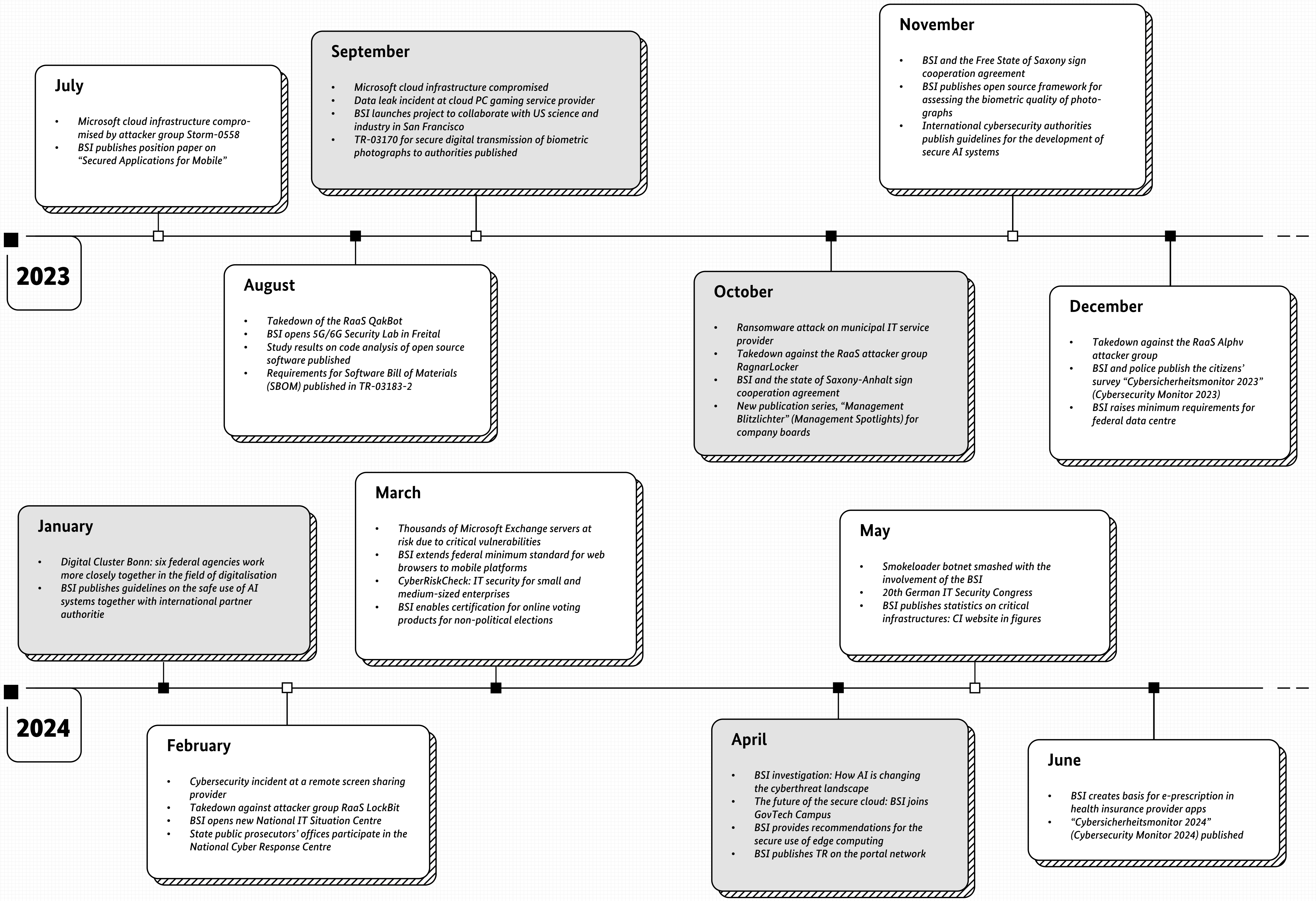
Item number
BSI-LB24/513e

This publication is part of the Federal Offce for Information Security's public relations work. It is distributed free of charge and is not intended for sale.

www.bsi.bund.de

Timeline 2024

topics



2023

July

- Microsoft cloud infrastructure compromised by attacker group Storm-0558
- BSI publishes position paper on "Secured Applications for Mobile"

August

- Takedown of the RaaS QakBot
- BSI opens 5G/6G Security Lab in Freital
- Study results on code analysis of open source software published
- Requirements for Software Bill of Materials (SBOM) published in TR-03183-2

September

- Microsoft cloud infrastructure compromised
- Data leak incident at cloud PC gaming service provider
- BSI launches project to collaborate with US science and industry in San Francisco
- TR-03170 for secure digital transmission of biometric photographs to authorities published

October

- Ransomware attack on municipal IT service provider
- Takedown against the RaaS attacker group RagnarLocker
- BSI and the state of Saxony-Anhalt sign cooperation agreement
- New publication series, "Management Blitzlichter" (Management Spotlights) for company boards

November

- BSI and the Free State of Saxony sign cooperation agreement
- BSI publishes open source framework for assessing the biometric quality of photographs
- International cybersecurity authorities publish guidelines for the development of secure AI systems

December

- Takedown against the RaaS Alphv attacker group
- BSI and police publish the citizens' survey "Cybersicherheitsmonitor 2023" (Cybersecurity Monitor 2023)
- BSI raises minimum requirements for federal data centre

2024

January

- Digital Cluster Bonn: six federal agencies work more closely together in the field of digitalisation
- BSI publishes guidelines on the safe use of AI systems together with international partner authoritie

February

- Cybersecurity incident at a remote screen sharing provider
- Takedown against attacker group RaaS LockBit
- BSI opens new National IT Situation Centre
- State public prosecutors' offices participate in the National Cyber Response Centre

March

- Thousands of Microsoft Exchange servers at risk due to critical vulnerabilities
- BSI extends federal minimum standard for web browsers to mobile platforms
- CyberRiskCheck: IT security for small and medium-sized enterprises
- BSI enables certification for online voting products for non-political elections

April

- BSI investigation: How AI is changing the cyberthreat landscape
- The future of the secure cloud: BSI joins GovTech Campus
- BSI provides recommendations for the secure use of edge computing
- BSI publishes TR on the portal network

May

- Smokeloader botnet smashed with the involvement of the BSI
- 20th German IT Security Congress
- BSI publishes statistics on critical infrastructures: CI website in figures

June

- BSI creates basis for e-prescription in health insurance provider apps
- "Cybersicherheitsmonitor 2024" (Cybersecurity Monitor 2024) published

TENSE SITUATION, DETERMINED RESPONSES: CYBERSECURITY IN GERMANY 2024

Threats

on available

Threat actors

Attack quality

APT groups active in Germany: **22** (of approx. 140 worldwide)

Cybercrime groups known in Germany: more than **100**

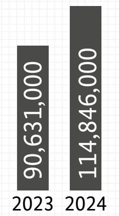
Occurrence

APT groups (advanced persistent threat) are highly trained, often state-controlled **attackers who target** networks and systems **for the purpose of sabotage and espionage. Cybercrime groups** are financially motivated, categorised by type of crime and often offer **malware-as-a-service** (ransomware-as-a-service).

Malware & Phishing

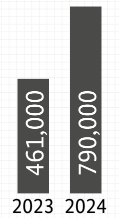
New malware variants:

+ 26 %



Among them: New Android malware

+ 48 %



Phishing: gateway for malware

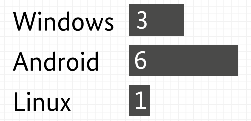
Worldwide **phishing URLs** and IPs detected worldwide:
approx. 1000/day
Lifetime of a page: a few days

Infrastructures

Botnets regularly active in Germany:

more than **200**

Top 10 botnets by target system:



Botnets: Grouping of several systems (bots) infected with a malware programme that attackers can control remotely to carry out cyberattacks.

- APT groups in Germany - including the most dangerous ones - remain active
- Android is gaining importance as a target system for malware

Attack Surface

become

Attack surface

An **attack surface** consists of **accessible IT systems** such as **active IP addresses and email addresses.** Software on these systems may have **vulnerabilities** that can be exploited for attacks. Especially dangerous: **zero-day vulnerabilities** that need to be fixed immediately.

Example: attack surface of the federal administration:

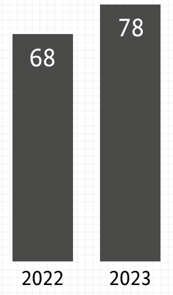
IP addresses accessible from the internet: **4,500**

Active **email addresses: 639,000**

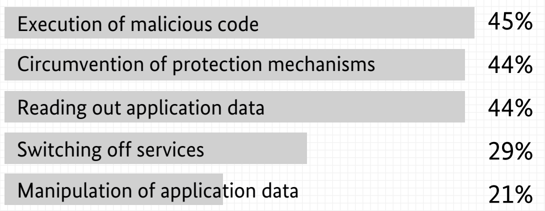
Vulnerabilities

Globally publicised **vulnerabilities per day:**

+ 14 %



Globally publicised **vulnerabilities in 2023** by possible **type of attack** (multiple answers possible)



One system, many affected parties:
- at least 37% of the 45,000 exchange servers in Germany vulnerable[1]
- Zero-day vulnerabilities exploited in various Ivanti products[2]

Examples

Android devices in Germany

25 % of devices no longer receive security updates and are definitely vulnerable.

Theft of access data to
- Multifactor authentication
- Password management
- Online banking
- Company network

- Vulnerabilities have been steadily increasing for years
- Diverse attack techniques target digitalised everyday life – anyone can be attacked

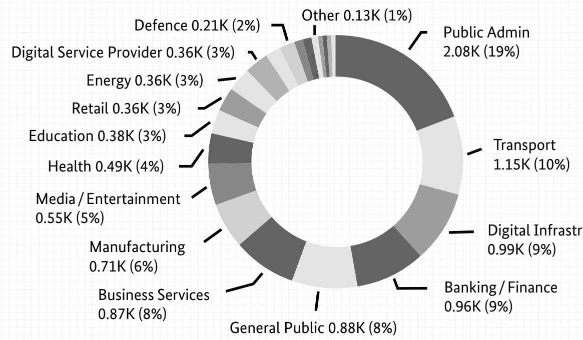
Attacks

with resulting

Cyberattacks & phishing

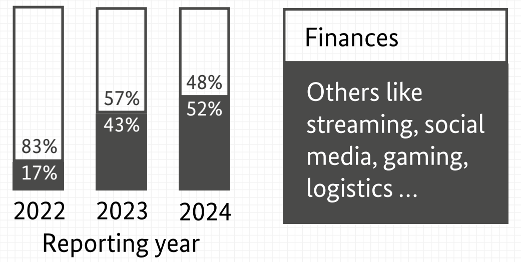
Public administration most affected of all sectors in the EU.

IT security incidents in the EU by sector



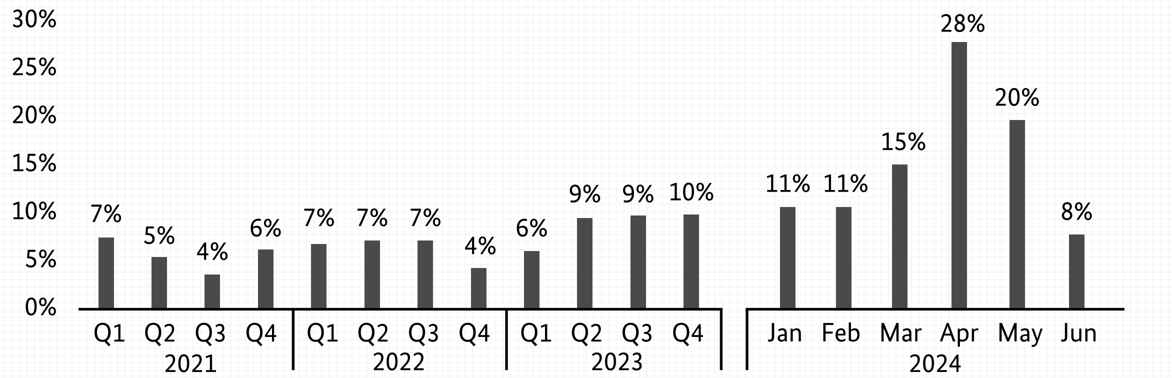
Phishing permeates all market segments

Phishing emails reported by consumers by type of market sector exploited (shares in %)



DDoS attacks

High-volume DDoS attacks in Germany (shares in %)

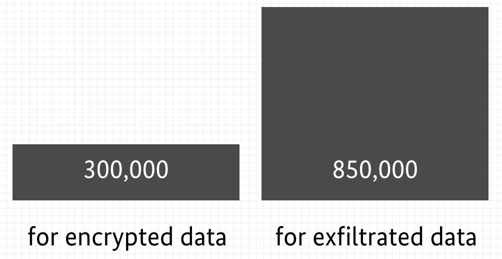


- Proportion of high-bandwidth DDoS attacks has doubled compared to the long-term average.
- Phishing attacks are no longer limited to the misuse of bank names.

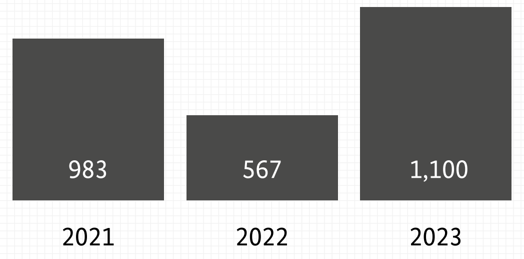
Impact

Ransomware

Ransom per case (in USD, average):



Ransoms captured by ransomware groups worldwide (in million USD):



CI

Disruptions for CI operators 490

Examples

Ransomware attack on municipal IT service provider in October 2023

Municipalities affected:	72
Workplaces affected:	around 20,000
Citizens affected:	around 1.7 Mio.

Estimated damage due to system failures caused by a **faulty update** in CrowdStrike software Falcon:
> 8.5 million devices > 5 billion USD

Consumers

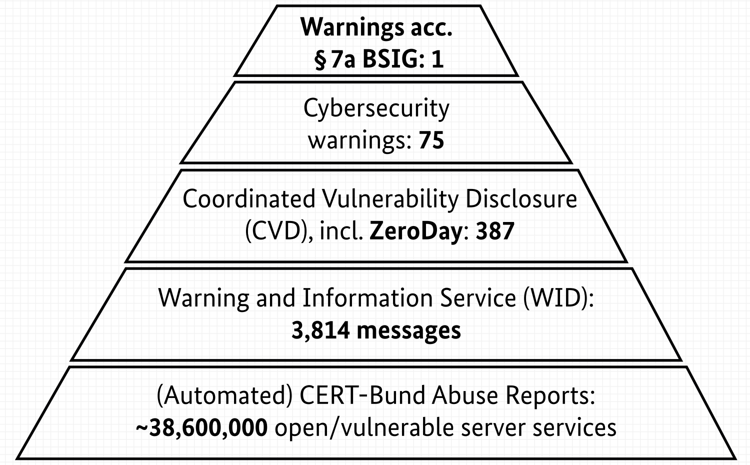
Top 3 damages to consumers from IT security incidents and cybercrime (%)

Loss of trust in the online service	30
Financial loss	26
Time lost	24

- Exfiltrated data much more valuable than encrypted data → Prevention capability must be strengthened
- Losses in the billions, unforeseen events, human error → Incident management capability must be strengthened

Resilience — Prevention

Prevention for the state, economy and society – BSI reporting systems



Warnings acc. § 7a BSIG: 1

Cybersecurity warnings: **75**

Coordinated Vulnerability Disclosure (CVD), incl. **ZeroDay: 387**

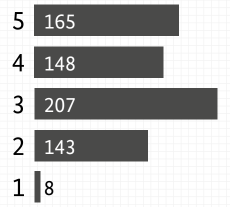
Warning and Information Service (WID): **3,814 messages**

(Automated) CERT-Bund Abuse Reports: **~38,600,000** open/vulnerable server services

BSI warning systems range from **technical warnings** (CERT-Bund Abuse Reports, WID) and **exceptional individual cases** (CVD) to **serious threats** (Section 7a warnings).

Focus on CI: ISMS maturity levels - Information Security Management System

140 ISMS have improved within 2 years

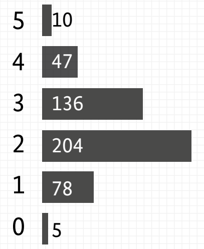


Maturity levels: system is
5 - regularly reviewed and improved
4 - regularly reviewed and practised
3 - established and documented
2 - largely established
1 - planned, not established

BSI supervises **IT security systems** (ISMS, SZA, BCMS) for operators of critical infrastructures **(CI).**

Resilience — Defence

Focus on CI: Maturity levels of Intrusion Detection Systems Initial recording 2023



Degree of implementation: Measures
5 – MUST, SHOULD, CAN completed
4 – MUST and SHOULD completed
3 – MUST completed
2 – Implementation started
1 – In planning
0 – Not available

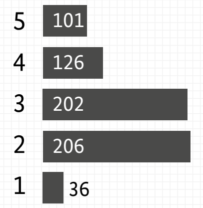
The **federal government** has its own detection, warning and blocking systems, e.g. malicious websites are blocked within the federal government's networks.

Warning - closure, lockdowns

BSI vulnerability warnings to affected authorities	Ø 15/day
Vulnerabilities closed after BSI warning in the reporting period	>500
New blockings of malicious websites	Ø 368/day
Blocked attempts to access malicious websites	Ø 9,212/day
Total emails checked Of which: Spam mails Spam rate Of which: Malware mails Share of malware mails	Ø around 753,000/day Ø around 405,000/day Ø 53% Ø 772/day 0.1%

Resilience — Coping

Focus on CI: BCMS maturity levels - Business Continuity Management System



114 BCMS have improved within 2 years

Expertise for emergencies:

Registered experts in the cybersecurity network CSN (digital first responders, incident practitioners, incident experts):	566
Qualified APT service providers	51
Qualified service providers for DDoS mitigation	19

Strengthen consumer competencies:

Advice for consumers on general IT security topics from the BSI:	5,111
Enquiries about IT security incidents and cybercrime from consumers to the BSI:	3,198