Federal Office
for Information Security

# The State of IT Security in Germany in 2019

# Foreword

A number of cyber incidents in recent months and years have shown us once again that cyber security is a key precondition for the success of the digital transformation. If we want to fully exploit the opportunities that digitalisation offers us, we must ensure that we can master its associated risks. German citizens rightly expect that the government will adopt policies to counter the inherent dangers of digitalisation. Here, the German Federal Office for Information Security (BSI) has an increasingly important role to play.

Consumer protection is a matter of particular concern to me. With the First Amendment to the German IT Security Act, we have expanded the BSI's mandate to include consumer protection.

The BSI is itself part of a robust network: to ensure effective protection for citizens, the economy and the state, all public authorities cooperate as part of the National Cyber Response Centre (Cyber-AZ). At the end of June 2019, we decided to develop the Cyber-AZ into a centralised information, cooperation and coordination platform for public authorities. The next step will be to further optimise the cyber situation map and risk assessment for cyber threats. The resulting improvements in the sharing of information will ensure our ability to deliver even more coordinated and rapid responses to cyber attacks in the future.

No matter how well they are run, however, public authorities cannot ensure IT security on their own: this must be seen as a challenge to be met by society as a whole. We will be successful here only if citizens, businesses, researchers and politicians work together on coordinated solutions. In fulfilment of our obligations under the Coalition Agreement, we have therefore launched the National Cyber Security Pact. This brings together all the socially relevant groups, manufacturers, providers, end users and public authorities at every level to share the responsibility for achieving better cyber security.

Special attention is paid here to critical infrastructure – our electricity, water and heating utilities, for example. At all levels of our society, we are dependent on critical infrastructure being available on a continuous basis. Without this infrastructure's systems and services, public life as we know it would cease to exist. Critical infrastructure is in turn dependent on information technology working smoothly and without disruption. To guarantee this, critical infrastructure operators, their member associations and our agencies work together in a secure public-private partnership known as the CIP Implementation Plan (UP KRITIS). Within this partnership, stakeholders can discuss recent incidents, evaluate the cyber security situation, set up crisis management structures and coordinate crisis response teams. This approach is complemented by the duties of operators of critical infrastructure as set out in the BSI Act: these duties also ensure that operators' IT systems meet the very highest security standards.

Alongside critical infrastructure, other parts of the economy also have particular significance for security. We will regulate the requirements for these areas in the First Amendment to the German IT Security Act.

In our networked world, we derive immediate benefits from our European and international partners providing a corresponding level of security. We will therefore be supporting steps taken by the EU to improve IT security, as well as an increased level of global dialogue.

The State of IT Security in Germany Report for 2019 clearly shows how the assistance the BSI provides to numerous digitalisation projects – not least the rollout of the 5G mobile network standard – ensures that IT security is accounted for and implemented in these projects from the outset. This is essential for digitalisation projects conducted on this scale.

The report clearly underlines the diversity and complexity of the challenges faced in IT security. I will do everything in my power to ensure that we are able to meet these challenges together. At every level of government, digitalisation is being pursued in a way that offers security for us all. This is precisely what the BSI stands for.

**Horst Seehofer**
Federal Minister of the Interior, Building and Community

# Foreword

As our society becomes increasingly interconnected, the digital transformation is now affecting almost every area of our lives. We're becoming faster, smarter and more mobile. At the same time, potential risks and dangers are also on the rise. To ensure the digitalisation of our society is both future-proof and secure, we need to contribute to the design of information security from the outset – whether for the digital transformation of our day-to-day lives or for processes in government administration or business.

This 2019 Report analyses the current IT security landscape while looking at a number of actual incidents, including a description of the methods and resources used by the attackers. Specific approaches for improving IT security in Germany are presented, as are a number of strategies and services offered by the BSI. The various entities addressed – the Federal Government, the world of business, society and international partners – will be discussed in detail below.

During the reporting period, the BSI again identified a wide range of critical vulnerabilities, especially in recent chip hardware. The importance of high-quality software and hardware was once again underlined, as was the importance that must be given to security-by-design and security-by-default: both of these basic principles are a sensible and necessary condition to protect consumers and ensure the necessary degree of both security and reliability.

In a related area, the BSI also established that trends that had already been described and forecast in last year's report came to pass in this reporting period. These included the frequency and impact of ransomware attacks, as well as the scope and significance of cases of identity theft.

Meanwhile, the ongoing process of digital transformation is strengthening digital dependencies: ultimately, attacks that are capable of rapid, automated propagation can cause widespread economic damage on a global scale or even endanger human health – if they were to occur in the context of self-driving cars or medical systems, to name just two examples. The structured implementation of IT security in businesses and organisations has never been more important. Our Alliance for Cyber Security (ACS) is the right point of contact here for companies and organisations of any size.

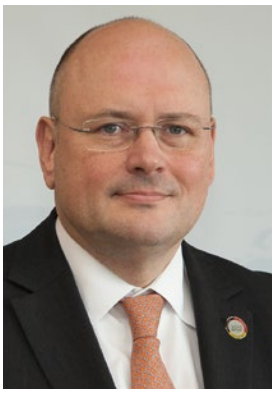
As Germany‘s national cyber security authority, the BSI implements prevention, detection and response measures to ensure digital information security for the Federal Government, businesses and civil society. Our well-qualified and highly motivated employees in Bonn, Germany – who will soon be joined by a second office in Saxony – work on analysing the current IT security situation, countering threats and increasing the general level of cyber security throughout our society. The BSI not only provides IT security services to the German government; it is also a centre of excellence for questions of cyber security at the national and international levels.

The relentless advance of digitalisation is also reflected in questions of cyber security. The BSI's remit has therefore expanded to include topics such as the new 5G network infrastructure, artificial intelligence, Digital Consumer Protection, a wider scope for consulting services provided to municipal and state actors, and the BSI as a central certification and standardisation body. In taking on a new organisational structure and expanding to include new units and departments with concomitant responsibilities, the BSI has been successful not only in managing the new level of staffing required, but also in meeting its many new challenges.

These cyber security challenges must be addressed at all levels and as a task tackled jointly by the relevant actors – whether with our peers in the EU and NATO or at the German federal, state and municipal level; with operators of critical infrastructure or small or mid-sized enterprises (SMEs); or with long-standing partners in the responsible federal departments and their subordinate public authorities.

To pursue the integrated nationwide approach necessary, the BSI works closely with all public authorities involved in the Cyber Response Centre, which is subject to ongoing developments.

Cyber security is a task that must be tackled by society as a whole, and the process starts by improving awareness regarding secure and self-reliant usage of the Internet. The BSI is a service provider and point of contact that makes its wealth of information and advisory services (including a toll-free hotline) available to each and every citizen.



With its integrated, nationwide and manufacturer-neutral approach, the BSI serves as a centre of excellence that considers itself as a framer and thought leader for the digital era.

Arne Schönbohm

**Arne Schönbohm**
President of the Federal Office for Information Security

# Table of Contents

# 1 Threat Landscape

# 1 Threat Landscape

The BSI monitors the IT security threat landscape in Germany on a continuous basis. In this report, it presents its findings from the period 1 June 2018 to 31 May 2019. After a summary of the threat landscape, the methods and resources used by attackers are described in detail, as are the general circumstances and causes. Numerous examples are also used to illustrate how attacks on IT security can adversely affect life in a digitalised society.

## 1.1 Summary and Assessment of the Threat Landscape

Recent cyber attacks have occurred primarily in the area of cyber crime. One typical example of this was another wave of ransomware attacks at the end of 2018 and the beginning of 2019. A particularly severe incident involved a cyber attack on a Norwegian supplier of aluminium. On 19 March 2019, this supplier suffered a wide-ranging attack utilising the LockerGoga ransomware. Most of the company's business segments were affected, and automated production was largely halted throughout the group. Even this single incident shows that ransomware continues to pose a serious threat and can cause immense damage.

As in previous years, malware infections continue to be one of the biggest IT-related threats to private users, businesses and public authorities. Evidence for this has been provided by the cyber security surveys conducted in 2017 and 2018 by the Alliance for Cyber Security, among others. In 2018, 53% of reported attacks were malware infections (a slight decrease from 57% in 2017).

One piece of malware of note in the reporting period is Emotet. First identified in 2010, this malware has been spreading again since November 2018 with the help of infected Office documents and an increasingly sophisticated set of mechanisms. The fact that Emotet is an evolving piece of code is shown in particular by its new capabilities, such as 'Outlook harvesting' – which involves the analysis of the infected computer's e-mail history – the downloading of other pieces of malware in the context of cooperative and distributed cyber crime and the use of techniques previously deployed only by Advanced Persistent Threats (APTs).

Incidents of identity theft that involve large volumes of personal data being misused by third parties are also becoming more common. Cases of identity theft utilising smaller volumes of data can nonetheless become critical if perpetrators are able to disclose the victim's personal data to the wider public. Alongside technical solutions, efforts to raise awareness and ensure that users take responsibility for their digital lives are necessary responses to the rise in the misuse of digital identities.

In terms of botnets (clusters of computers or systems that have been infected by a remotely controllable malware program, or ‚bot'), the long-term threat landscape remains serious. As recent developments have shown, the risk of becoming part of a botnet is high, especially for mobile end-user devices and Internet of Things (IoT) systems, whose increased deployment and use in almost all areas of our day-to-day lives is offering botnets an ever-expanding set of targets. The comparatively low rate of infection of IoT devices in Germany can be attributed primarily to the typical kinds of Internet connection utilised by German end customers, which are regularly established through a router and do not normally allow external access from the Internet.

Server-based botnets (clusters of servers infected by a remotely controllable malware program) offer a huge pool of resources for the execution of distributed denial of service (DDoS) attacks. DDoS attack bandwidths regularly exceed the 150 Gbps mark, and may even achieve up to 300 Gbps. In general terms, constant specialisation based on the use of new attack vectors, targeted aggregation of DDoS attacks (multi-vector attacks), the deployment of new attack tools (DDoS from the cloud) and DDoS booter services (see DDoS in Section 1.2.4) is providing for a consistently tense threat landscape.

One interesting development involves malware spam: while the absolute volume of this kind of e-mail is in sharp decline, spam still represents a serious potential threat. The quality – and thus the effectiveness – of malware spam continues to rise. The factors at play here include innovations, technical expertise and considerable personal effort on the part of attackers.

A number of phenomena can be identified as trends for APTs (attacks neither opportunistic nor motivated by financial gain, but which follow strategic or tactical goals): a wide range of publicly available APT tools, a growing number of international 'APT service providers', the use of legitimate services as cover for illicit activities, hindrances to malware analyses and the integration of APT techniques into criminal operations. While these trends make the detection of APT attacks more difficult, a coherent set of systematically implemented IT security precautions can prevent many such incidents.

## 1.2 Attack Methods and Resources

The ability to counter attacks lies at the very heart of a successful cyber security strategy. That said, effective protection is possible only if at least the key aspects of both the general and concrete threat landscape are known. Since the cyber security situation is extremely volatile, regular and targeted evaluation of existing risks is essential in selecting a suitable range of preventive and responsive measures.

Time and again, the publication of new information about hardware or software vulnerabilities is quickly followed by real-world exploits. The large number of discrete attack targets and potential attack methods enables the identification of trends and tendencies, however, which can then be utilised in mounting a successful defence.

### 1.2.1 Identity Theft

In the context of information security, an 'identity' is understood to mean a set of attributes that represents the real nature of a person or thing. Accordingly, the identity of a person or thing can be defined by a single unique attribute or by a combination of several discrete attributes. In the online world, the identity of a person is typically deduced from identification and authentication data, such as the combination of a user name and password. The concept of 'identity theft' is therefore defined as the unlawful acquisition of such data.

One prominent type of identity theft is known as ‚phishing'. In this kind of attack, a set of sophisticated ‚social engineering' techniques are used to encourage the victim to disclose sensitive information. Another potential attack vector for acquiring identity data is the use of specialised malware. Identity data can also be acquired even without the direct involvement of the actual victim. A data leak suffered by the victim's service provider is one such example.

Frequent reports of data leaks of customer information were observed in the reporting period. The service providers affected included a number of prestigious companies, such as the Marriott hotel chain and the social media platform Facebook. Judging by the response in the media and from those affected by the leaks, the publication of dossiers compiled about German politicians was a major talking point and raised the profile of this practice, which is known as 'doxing' (see Case Study: Doxing).

The BSI learns of data leaks through its situation monitoring activities or from direct reports submitted by law enforcement agencies, for example. Viewed in isolation, these reports are not sufficient to identify whether the data involved is of a high quality (in terms of its validity, currency, etc). In many cases, even an extended analysis of the datasets disseminated or offered for sale is unable to definitively establish their quality. If an affected service provider does not confirm a given data leak, it is also questionable whether the allegedly leaked data actually stems from this provider. With such incidents, it may actually be the case that the data has simply been generated or aggregated from public domain sources with the intent of selling it. Past experience also tells us that several years may actually pass before a data leak is publicly announced. Currently, a number of large datasets are circulating that are more impressive in terms of their sheer size than their quality. This fact is underlined by the data collection analysis performed by the BSI at the start of the year (see Box: Analysis of the Data Collections bigDB, Collection#1 to Collection#5, Zabagur and Anti Public).

As the BSI has observed, identity theft need not involve any major effort on the part of perpetrators thanks to the use of unprotected public cloud storage or misconfigured software. Systems that lack important patches or are open to zero-day exploits also offer attackers a range of data access options. Publicly available tools (such as 'sqlmap', a program for detecting and exploiting database vulnerabilities) can also be used for automated attacks designed to obtain, copy or tamper with databases. Since many online shops also use the same software, ready-to-use scripts make it easy for attackers to target a wide range of specific platforms. In this context, scripts are also used that identify vulnerable targets automatically with web crawlers or search engines (e.g. 'Google Dorker'). This gives attackers a never-ending source of new datasets, which are enriched with existing sets of leaked data in order to generate the largest possible aggregated dataset – with a lucrative sale being the ultimate aim. In combination with the problematic reuse of passwords for multiple services, the enormous volume of disclosed sets of identity data consequently offers the option of executing direct attacks on an ever-increasing number of online accounts: the practice of ‚credential stuffing' involves automated attempts to match linked combinations of user names and passwords to service providers.

## Doxing

**Situation**

The probable perpetrator, using the pseudonyms @_0rbit and @_0rbiter, published links to downloads containing large collections of data on the short message service Twitter. The publications were formatted rather like an Advent calendar. Up until 24 December, the perpetrator opened a new 'door' every day and disclosed sets of private data on Twitter while also referring to the affected person by name. Along with well-known persons in the public eye, German politicians at all levels of government were affected by the material published. The sets of data offered online included both information in the public domain – a politician's official party e-mail address, for example – as well as private, unpublished data. In isolated cases, private communications such as content from family chats and images were also offered as downloads.

**Response**

The BSI set up a special unit to respond to the incident. The National Cyber Response Centre took over the central coordination of casework at the federal agencies involved. The head offices of the political parties of affected politicians were notified by the BSI. From that point on, the BSI was then in constant contact with the parties and MdBs, and also offered private consultations upon request where possible. The perpetrator stored copies of the data packages on a large number of download portals. The BSI contacted 50 of these hosts, some of which were based abroad, in order to secure deletion of the data and thereby make further distribution of the packages more difficult. The Twitter accounts used were also shut down.

For those affected, the incident created a lot of uncertainty in many areas: apart from the actual publication of private information itself, many of those affected were left wondering how the perpetrator had acquired the data – and whether confidential information had been published.

**Recommendation**

The case described illustrates two key points. First, it shows how a wide range of motives can result in an incident of this kind. Headline-grabbing cyber attacks are not necessarily the work of foreign governments. Perpetrators can also cause considerable damage when working alone. The case also points to the sheer volume of personal data that is now in the public (online) domain.

BSI for Citizens provides a comprehensive set of recommendations to protect personal data online [https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/empfehlungen_node.html].

In terms of phishing attacks in Germany, the BSI has identified a particular focus on bank customers, as well as customers of online shops like Amazon or payment systems such as PayPal. As seen previously, the current spate of phishing campaigns closely tracks social trends and topical issues. In the most recent reporting period, attackers have again utilised the popularity of blockchain, tax rebates, and the uncertainty surrounding the topic of the new EU General Data Protection Regulation (GDPR) to provoke as many users as possible into disclosing their personal data. As a follow-up to successful cases of identity theft, an increased incidence of attempted blackmail via e-mail has been observed. In these cases, attackers have reproduced the victim's passwords in the e-mails, for example, or have claimed to have recordings of the victim engaging in sexual practices while using online pornography ('sextortion').

The sheer volume of publicly available identity data (which is readily accessible from social media or data leaks, for example) enables attackers to conduct personalised phishing attacks that are increasingly characterised by the quality of their overall presentation. Joint analyses conducted by the Consumer Association of North Rhine-Westphalia (Verbraucherzentrale Nordrhein-Westfalen) and the BSI have examined the available data (reports to the 'Phishing Radar') and concluded that in Germany, phishing e-mails are not typically sent using text-only formats (28%), but instead contain links (72%) that redirect those clicking them to the phishing website. In terms of appearance, these websites seem almost identical to the original websites and, although spurious, this seeming authenticity encourages users to disclose their identity data. To further enhance their credibility, the phishing websites created by attackers increasingly use the Secure Hypertext Transfer Protocol (HTTPS), which is used to secure data transmissions against eavesdropping and manipulation. The use of encryption is not an indication of a website‘s actual content, however. Phishing websites can also obtain an HTTPS certificate that facilitates encryption between the victim and web page. According to the aforementioned analyses, one can assume a ratio of approximately 55% HTTP to 45% HTTPS for phishing attacks in Germany. A corresponding uptick in the use of HTTPS for phishing has been observed since mid-2017. Free certificates, which are currently the weapon of choice for attackers, are typically sourced from Let’s Encrypt or Sectigo. Alongside the use of HTTPS, the URL itself can also include certain words that enhance the trustworthiness of a website, such as technical terms (e.g. ‘Security-218309sad.de’), familiar abbreviations (‘AWS-anmeldungs-seite.de’) or provider trademarks (e.g. ‘facebook-142.de’ or ‘gotrock.org/facebook’). Stating the name of the provider in the domain name and adding in unusual suffixes like a string of digits is also known as ‚combosquatting‘. Alongside the above methods, the following techniques are also used to disguise a phony URL:

1. Adding subdomains (e.g. ‘wikipedia.org’ becomes ‘wikipedia.some.nested.subdomain.domain.org’)

2. Including subtle typos (e.g. ‘wikiepedia.org’ instead of ‘wikipedia.org’)

3. Including digits that closely resemble letters in the original URL (e.g. ‘w1kipedia.org’)

4. Using Unicode characters that closely resemble letters in the ASCII character set (Cyrillic https://www.apple..com/ (Punycode https://www.xn--80ak6aa92e.com) seems to point to https://www.apple.com/). (IDN homograph attack)

### Analysis of the Data Collections bigDB, Collection#1 to Collection#5, Zabagur and Anti Public (in the box in the ‘Identity Theft’ section)

**Situation**

In January 2019, the BSI Situation Centre received knowledge of a publicly accessible collection of personal data. This soon became known in the media as ‘Collection#1’. Shortly afterwards, word spread that other collections of data – known as bigDB, Collection#2 to Collection#5, Zabagur and Anti Public – existed alongside Collection#1 and were also connected to this initial publication.

**Cause and impact**

The data was sourced from several data leaks affecting various websites and online services that had occurred in recent years (such as the data leaks affecting Yahoo, LinkedIn, Adobe and MySpace). It can be assumed that the data packages had been put together over a longer period of time. Accordingly, the overall collection consists almost entirely of outdated datasets and duplicate records.

In combination with the problem of password reuse, these kinds of lists are excellent candidates for ‘credential stuffing’. Credential stuffing involves automated attacks against the login mechanisms of service providers using linked or generated combinations of user names and passwords. Another problem is that this kind of information can be used to design phishing attacks that are increasingly targeted and more personalised.

**Response**

The BSI acquired and analysed the data with the aim of identifying the degree to which the Federal Administration was affected and taking any other necessary measures. All federal agencies and federal states that were clearly identifiable from the data were informed. Feedback from those contacted confirmed that most of the data was very old and no longer in current use.

**Recommendation**

To find out if you are affected by these publications of personal data – regarding private e-mail addresses in particular – you can use the Leak Checker maintained by the University of Bonn (https://leakchecker.uni-bonn.de/) and the HPI Identity Leak Checker (https://sec.hpi.de/ilc/). Services offered by your ISP or international security researchers can also be used. Further information about the projects can be found on the websites of the respective providers. Recommendations for preventing identity theft and the next steps to take if you discover that you have been affected can be found on the BSI’s website (https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/ID-Diebstahl/Schutzmassnahmen/id-dieb_schutz_node.html and https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/ID-Diebstahl/Hilfe/Hilfe_Betroffene_node.html).

5. Loading a phishing page via Google Translate (e.g. https://translate.google.com/translate?hl=en&sl=de&u=https://Phishingseite.de/&prev=-search).

Another way to mask phishing websites is to embed seemingly authentic login windows in the form of pop-ups. The aim here is to obtain user login details for other kinds of services.

As an alternative to conventional phishing methods, attackers have regularly turned to hijacking legitimate websites with correctly issued certificates and converted these into phishing websites by embedding appropriate code. This can be done either by compromising a web server directly or by planting JavaScript malware. One known group of attackers that deploys this method is Magecart. These attacks involve embedding a malicious piece of JavaScript capable of skimming credit card details and shipping/payment addresses from the site's shopping cart system.

Reports of data leaks involving entire databases of customer information are now a daily occurrence, placing ever more onerous responsibilities on the shoulders of service providers. The digital leaks confirmed to date show that the responsibility each of us must take for our digital activities is a crucial part of ensuring long-term information and cyber security. These leaks also highlight the limited security offered by a user name and password system. The BSI therefore recommends using two-factor authentication if this is offered by an online service. While many services deactivate two-factor authentication as the default method, this can be activated in account settings. Users of online services should therefore ensure they have checked which login methods are available. If two-factor or multi-factor authentication is used, the theft of a password does not necessarily result in the disclosure of other sensitive data.

From 25 May 2018 onwards, the new EU General Data Protection Regulation (GDPR) has stipulated certain circumstances that require the providers responsible to report the loss and unauthorised disclosure of personal data to the appropriate data protection authority, and potentially to the affected data subjects, as well. This will ensure users are better informed about potential data leaks.

### 1.2.2 Malware

The term 'malware' is a catch-all term for any kind of computer program that is capable of executing unsolicited or malicious code on a host computer system. In the press and media, several terms – such as 'Trojan', 'virus' or 'worm' – are used interchangeably to refer to any kind of malware. Malware forms an integral part of most attack scenarios; it is involved in infecting clients with ransomware, in botnet communications and even in APT attacks, for example.

In the reporting period at hand, the IT security company AV-TEST (a long-standing supplier of one of the largest malware databases to the BSI, https://www.av-test.org/en/) registered around 114 million new malware variants. Of these, around 65 million affected the Windows operating system, 3.4 million affected Android, approx. 0.09 million affected MacOS and over 39 million were placed in the 'Other' category (these include OS-independent scripts, malicious documents, Java malware, etc).

On average, this amounts to almost 320,000 new pieces of malware every day – a slightly lower figure than in the previous reporting period. It should be noted, however, that these numbers cannot be compared directly with figures previously published. This is because more detailed options for data collection are now available that have made it possible to separate out PUAs (potentially unwanted applications, i.e. application software that cannot be definitively classified as malware) from total figures.

As in previous years, malware infections continued to be one of the biggest IT-related threats to private users, businesses and public authorities during the reporting period at hand. Originally identified in the cyber security survey conducted by the Alliance for Cyber Security in 2017, this fact was again confirmed by the most recent cyber security survey completed in 2018. In 53% of the cases reported in 2018, the attacks involved malware infections where the program or code penetrated corporate IT systems in order to perform malicious activities. Some 87% of those affected also stated that the cyber attacks had had serious consequences in the form of disruptions to company operations or even downtime (see Section 2.2.1.3, Insights and Findings from the Cyber Security Survey Conducted by the Alliance for Cyber Security).

"Introduction of malware via removable storage devices and external hardware" and "malware infections via the Internet and intranet" were also identified as major, upwards-trending risks in the 2019 list of the top-10 threats and countermeasures published for industrial control systems (ICS; version 1.3, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_005.pdf).

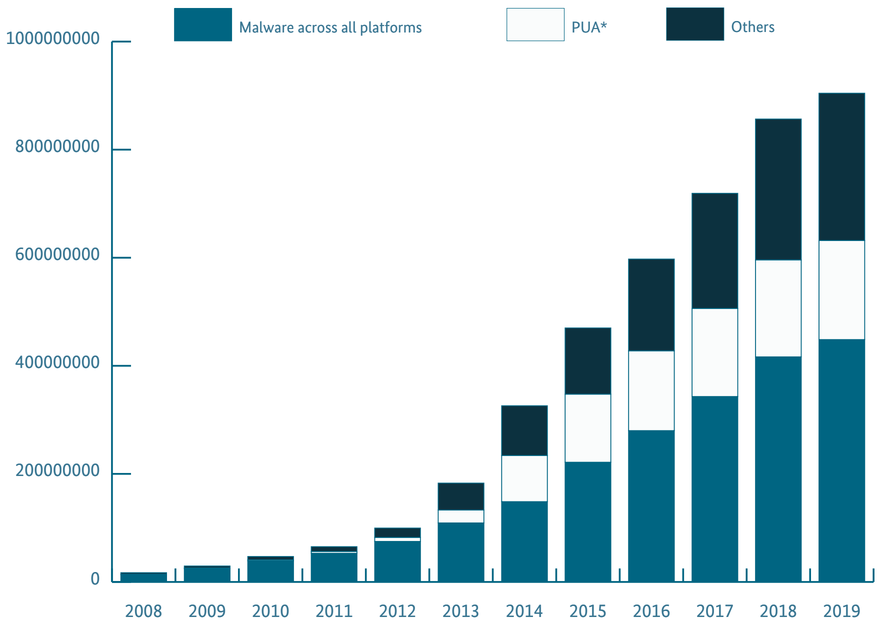


**Figure 01:** Overall known malware variants, source: AV-Test

## APT28 Modifies the Identify Theft Prevention Software LoJack

### Situation

In 2018, several security firms published analyses of a rarely used piece of malware from the cyber espionage group APT28. These analyses showed that the group had introduced slight changes into the legitimate anti-theft software LoJack to repurpose it into a root kit. Instead of reporting to a server operated by the software manufacturer, the modified variant instead contacted the group's servers. This enabled APT28 to send commands to infected computers. By altering an originally legitimate piece of software (LoJack), the group made good use of the fact that the malware was very unlikely to be detected by security products.

### Cause and impact

The effects of the manipulated LoJack software were limited. The attackers did not manipulate existing LoJack installations. Instead, they installed manipulated versions on computers that had not previously been equipped with anti-theft software. To do so, however, they required administrative access to the target systems. Accordingly, LoJack is not a new attack vector, but a method to further propagate an attack from an already comprised system.

APT28 also only deployed this malware in a few cases. First, the malware was installed only in certain sectors – primarily in military facilities, and even there only on individual systems. The manipulated LoJack versions were not used for day-to-day work by the attackers in the target network, but acted as backup options in the event that other malware programs (some of which were publicly known) were discovered and purged from the system.

### Response

The LoJack incident is a good example of a topic that does not require any fundamentally new or additional responses or recommendations for action despite attracting a lot of media attention. One the one hand, the group of users potentially affected is very limited due to cautious deployment by the attackers. On the other, LoJack is only deployed in the later phases of an attack and is only one tool among many. The BSI's recommendations, which are intended to help ensure attackers do not gain access to systems in the first place, therefore remain unchanged.

### Recommendation

Detecting the LoJack root kit is much more difficult than detecting other tools used by APT28. Accordingly, the BSI recommends deploying standard methods for detecting malware and attacker activity in day-to-day operations. In the event of a system being compromised by APT28 with other malware, however, the BSI recommends checking for the existence of the root kit as part of incident management.

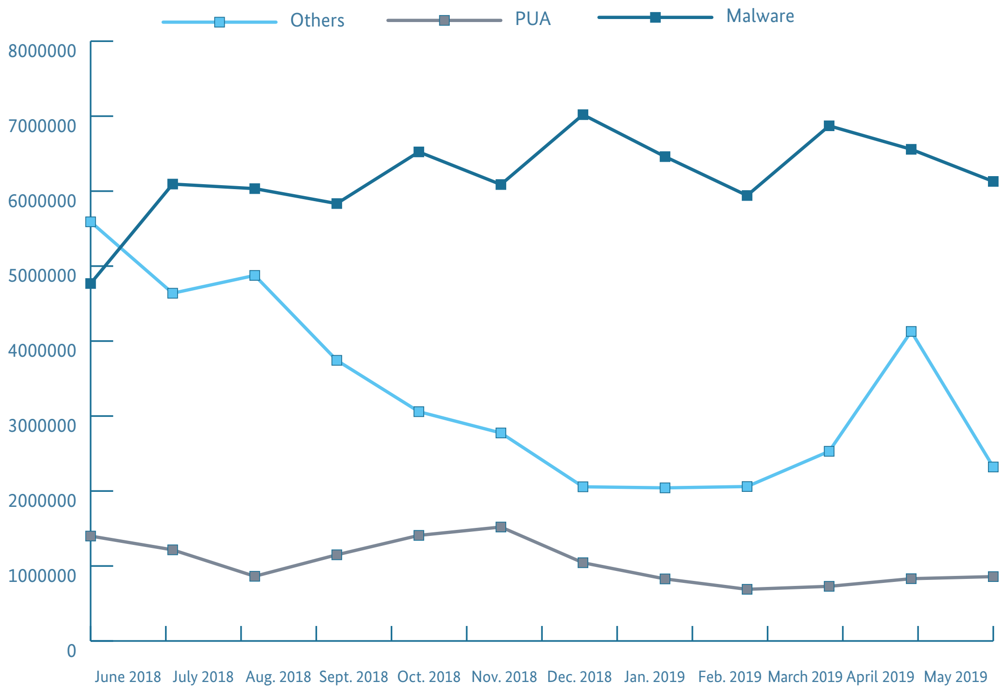


**Figure 02:** New malware variants per month over time

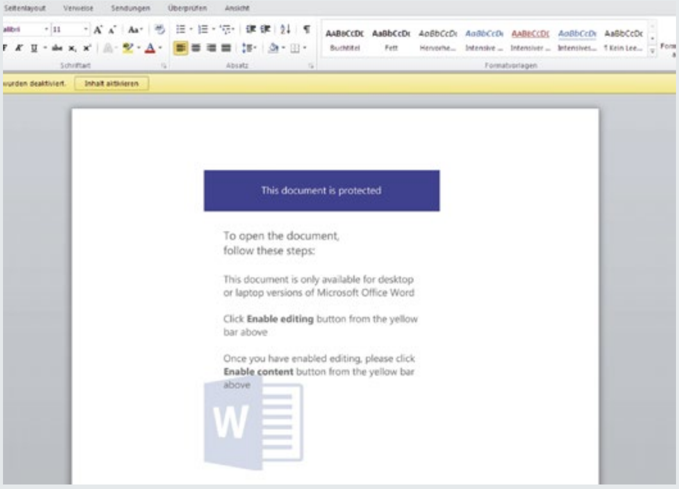
* PUA = potentially unwanted application. Describes application software (often distributed as bundled software) that cannot be classified definitively as malware and is therefore collectively referred to as 'greyware'. While PUAs will typically have been installed by the user, they then exhibit unexpected behaviour or execute certain functions covertly that could be construed as 'undesirable' (collecting information and disclosing a user's behaviour, displaying advertising banners, etc).
** 'Other': operating-system-independent scripts, malicious documents, Java malware, etc
*** Malware: operating-system-dependent malware

## Be Aware of the *Emotet* Malware

### Situation

Emotet (also known as Feodo, Bugat) was first encountered as a banking Trojan in 2010. Later variants of this malware were also referred to as Geodo and Heodo. Emotet contains a number of modules used to sniff out information on infected systems, as well as spam mailers and tools to propagate the malware. Spam waves featuring forged invoices with the aim of propagating Emotet had already caused many infections between 2013 and 2015. From November 2018, an increase in the spread of the Emotet malware was registered by means of manipulated Office documents. A new feature seen at the end of October 2018 was that the Outlook harvesting module was not just accessing contacts, but e-mail content, as well. However, this data was first used in April 2019 in order to send spam that looked even more convincing. Once a computer has been infected by Emotet, the malware utilises contact details and e-mail content from the Outlook inboxes on the infected system. This information is used by perpetrators for the further propagation of the malware in subsequent spam campaigns in which recipients receive seemingly authentic e-mails from senders with whom they have recently been in contact.

From November 2018, an increase in the spread of Emotet was registered by means of malicious Office documents. Social engineering methods are used to convince potential victims to execute Microsoft Office macros (VBA scripts) that then act as downloaders for a variety of malware programs (see Case Study: Be Aware of the Emotet Malware).



This document is protected

To open the document,
follow these steps:

This document is only available for desktop or laptop versions of Microsoft Office Word

Click **Enable editing** button from the yellow bar above

Once you have enabled editing, please click **Enable content** button from the yellow bar above

Attackers make use of how Windows handles file type recognition to smuggle malicious Office documents past security systems. In a first step, an Office document is saved as an Office 2003 XML file and given the file extension '.xml'. Following this, the file is renamed and the '.xml' extension is changed to '.doc'. Common file type recognition libraries such as 'libfile' therefore identify this file as '.xml' and do not consider it to be all that dangerous. Windows, on the other hand, identifies this file as a '.doc' by its file extension and opens it by default with the installed Office program.

**Figure 03:** Screenshot from a malicious Office document prompting the user to activate an Office macro (Source: BSI)

As regards the communication between the malware and the corresponding command and control server, a significant rise in HTTPS communication can be observed. The ratio of encrypted to unencrypted communication between malware programs and their command and control servers was around 15% (HTTPS) to 85% (HTTP) in the reporting period.

**Cause and impact**

Malicious Office documents and scripts act as downloaders and attempt to use social engineering methods to convince potential victims to execute Office macros (VBA scripts). These Office documents are backwards-compatible as far as Microsoft Office 2003. This means the malware can be run by a wide variety of Office versions, which significantly increases the number of potential victim systems. Looking to the future, the BSI predicts a further increase in well-implemented and automated social engineering attacks of this kind, which are virtually unidentifiable as such by recipients.

A key feature of Emotet is that any kind of malicious code can be downloaded later. In a manner similar to a modular system, Emotet has mostly downloaded Trickbot, QBot, IcedID or Ursnif/Gozi, and sometimes Dridex, Gootkit or Azoruit, as well. This offers perpetrators a further range of attack options. Emotet's extended functionality and impact include:

- Adaption of techniques previously observed primarily during APT attacks
- Outlook harvesting on infected systems
- Theft of browsing history and stored credentials from web browsers
- Subsequent downloading of any type of malware
- Exploitation of old, unpatched vulnerabilities
- Losses resulting from production downtime

The developers of broadly distributed malware such as Emotet and Trickbot are increasingly adapting methods of propagation in local networks (lateral movement) that have previously been observed primarily during APT attacks. The attackers first use a 'scattergun' campaign, but then proceed opportunistically through highly specific selection of targets to which they then spread further and download additional malware. Lateral movement in the network is also used to find backups, which are then manipulated or destroyed. The figure below illustrates this new approach:

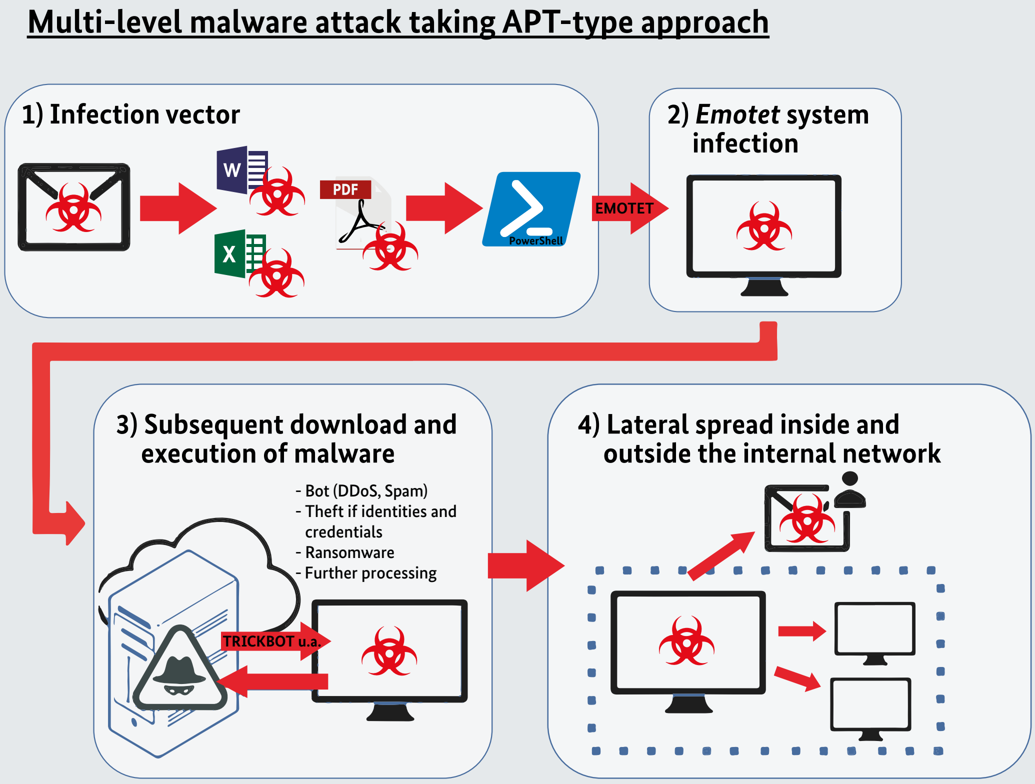

Multi-level malware attack taking APT-type approach
1) Infection vector
W
X
PDF
PowerShell
EMOTET
2) Emotet system infection
3) Subsequent download and execution of malware
- Bot (DDoS, Spam)
- Theft if identities and credentials
- Ransomware
- Further processing
TRICKBOT u.a.
4) Lateral spread inside and outside the internal network

**Figure 04:** Graphics: https://www.fortinet.com/resources/icon-libary.html, Microsoft, Adobe

The BSI is aware of several cases in which ransomware was downloaded and corporate data was then encrypted. This resulted in production outages, as entire company networks had to be set up again from scratch. For private users, an infection can result in the loss of data, and login credentials in particular.

**Response**
Even 'minor' infections resulting from a broad-based attack wave of malware like Emotet must be treated immediately and access data must be changed. If these efforts are not taken, this entry point can result in losses or damage of a far greater magnitude.

**Recommendation**
The following measures generally increase the level of protection against Emotet: timely installation of security updates for the operating system and applications, regular offline backups, log file monitoring, ensuring users are regularly educated about social engineering attacks, and implementing network segmentation for production and office networks. Further information about Emotet is available from the BSI for Citizens website:

https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/emotet.html.

### 1.2.3 Ransomware

Ransomware entered the public consciousness with the WannaCry attack in 2017. The term refers to malware that prevents or severely restricts a user from accessing their personal computer or personal data. Ransomware usually announces itself by displaying an on-screen message. The message content may in fact be spoofed and restrictions may be easily circumvented.

Ransomware attacks aim to force the user to pay a ransom or act in some other way to regain access to the restricted or locked resources. In most cases, payments are demanded using a cryptocurrency such as Bitcoin or Ethereum so as to preserve the perpetrator's anonymity. Since techniques for monitoring payment flows using these currencies have improved, some data about ransom payments made for individual ransomware variants is now available. In many cases, the victim's situation does not actually improve even after the ransom payment. Observations have shown that some perpetrators were unable to decrypt the data even after receiving the payment due. Others did not offer any decryption options, made subsequent demands or simply failed to respond.

## Cyber Attack at an Aluminium Company

**Situation**

In the night of 19 March 2019, a Norwegian aluminium group became the victim of a cyber attack conducted with the ransomware LockerGoga. According to its own figures, the company employs 35,000 people in 40 countries and posted revenue of approximately EUR 11 billion in 2017. The company's core business is aluminium production, although it is also one of Norway's three biggest electricity producers.

It was established that IT systems in most of the company's business segments were affected. As an initial reaction, facilities were taken off the network and production was switched over to manual operations wherever possible. A ransom payment of an unknown amount was demanded, but the company refused to pay. Instead, the company used its available backups to restore its operations. The company website was occasionally unreachable as a result of the attacks. Many units were still operating manually even four weeks after the incident.

**Cause and impact**

The attack utilised the ransomware LockerGoga. According to press releases, the company's Active Directory server was tampered with beforehand, admin passwords were replaced, logged-in users were logged out and network devices were deactivated. One may therefore assume that this was a targeted attack with preparations tailored to the victim in question. LockerGoga had also been used at the beginning of the year in an attack on a French company. The attack on the aluminium company was also followed shortly afterwards by two LockerGoga incidents involving US chemical companies.

According to company statements, the company suffered an economic loss of approximately USD 35-43 million in the first week after the cyber attack alone. During these seven days, production in the units most heavily affected virtually came to a standstill.

The price of aluminium rose significantly in the first two days after the incident. In contrast, the company‘s share price suffered no losses – in fact, it actually rose in value.

**Response**

The company immediately informed the public and the stock market about the cyber attack (via Facebook, for example). A press conference was held on the day after the attack and the public was kept informed about the state of play in the weeks that followed. The company was praised for its handling of the incident (no ransom payment, use of backups, public relations work). This approach is also in line with BSI recommendations.

**Recommendation**

This case study demonstrates that the best defence against ransomware is a verified backup strategy that will guarantee the successful recovery of data. The increased focus on larger targets such as companies (which may be expected to have a greater motivation to pay ransom demands) means that further recommendations may be advisable, however. These include the company-wide management of macros, preventing executable files from accessing document directories, and deactivating parts of the system that are automated by default – the scripting host, for example. To prevent the propagation of malware within the corporate network regardless of its physical spread across one or more (national or international) company sites, more granular segmentation of the network can also be advantageous. External remote access should also be avoided wherever possible. If necessary, each and every access channel should be protected with passwords that comply with strict policies (a prescribed character set and length).

To avoid such situations while also removing the incentive for perpetrators, the BSI continues to advise against making ransom payments.

Ransomware is distributed using a number of attack vectors. All target groups can be affected by the following attack vectors:

- Spam e-mails with malware included as an attachment or linked to via URLs
- Drive-by exploits (vulnerabilities in browsers, browser plug-ins or operating systems) that are triggered by accessing an infecting website or an advert placed on it (possibly without requiring further interaction by the user)
- Exploit kits, which affect a range of vulnerabilities in separate products and make both the attack type and the malware transport method available to the perpetrator at the touch of a button

Companies and institutions with more complex IT infrastructure can also be affected by the following attack vectors:

- Exploiting vulnerabilities or brute-forcing weak passwords on publicly accessible web servers. Highly prevalent malware is also available for intercepting other passwords on the internal network.
- Vulnerabilities in remote administration tools (RATs) are used to access systems scheduled for maintenance. This often means that the attacker is granted an extensive set of rights from the outset.
- After the target system has been infected, the malware may also use vulnerabilities in the operating system to appear as a legitimate process and avoid early detection.

There has been a sharp increase in the threat level associated with ransomware since 2016. WannaCry and NotPetya / ExPetr were the most notable cases to make the headlines in 2017. Some legal disputes concerning claims made against insurance policies are still ongoing today. This is largely because NotPetya was probably an act of sabotage, not ransomware that was designed for extortion. The losses suffered can easily exceed the amount demanded as ransom. This is particularly the case if larger companies fall victim to such attacks.

While more recent incidents from 2019 did not attract the same media interest as those mentioned above, a number of trends can still be identified. First encountered in 2018, the ransomware known as GandCrab has followed an agile development path and even includes a version number – indicating that the attackers are well-organised. GandCrab presents an example of personalised ransomware-as-a-service and is typically used to launch broad-based attacks. Other ransomware variants, on the other hand, seem to take a more targeted approach:

- SamSam is one of the more active ransomware variants and achieved notoriety because of its attack on the city of Atlanta. This attack marked a stronger orientation towards targeted attacks on organisations.
- SamSam, BitPaymer and CrySIS showed that active remote maintenance tools are regularly co-opted as backdoors. These tools are attacked individually – with published credentials or brute-forced passwords, for example – or by using exploits.
- During the last year, various ransomware attacks were reported on ports and airports, companies in the (container) logistics sector, newspapers and restaurant chains. While most of these attacks affected companies outside Germany, hospitals were one category of institutions that suffered attacks within the country.
- The persistence of this threat is also illustrated by the ransomware variant Ryuk. Detailed monitoring of the Bitcoin addresses used suggest that ransom payments totalling at least USD 600,000 have been made. Since the turn of the year (2018/2019), Ryuk has also been often encountered as part of Emotet/Trickbot waves, which indicates the increasingly modular nature of malware in general and of ransomware in particular (see Case Study: Be Aware of the Emotet Malware).

A large Norwegian aluminium company offers an example of the sheer scale of damage that ransomware has the potential to cause – even if a solid backup and incident response strategy is in place (see Case study: Cyber Attack at an Aluminium Company). In March 2019, the company fell victim to a ransomware attack and, according to its own figures, reported a loss of approximately EUR 40 million after just one week, although it did not pay the ransom fee and attempted to reconstruct the compromised data from backups. The ransomware deployed was the relatively new variant LockerGoga, which seems to have been first tested on one organisation and then launched against multiple companies simultaneously soon afterwards. This suggests a carefully planned attack.

The repercussions from ransomware attacks were also very severe in many other cases, with reports ranging from the failure of systems and networks to stoppages affecting entire production lines. Apart from the manufacturing sector, community facilities have also been repeated targets of such attacks – such as hospitals in Germany or municipal administrations in the USA. One key feature is observable here: the attacks are directed against centralised service providers. Once an attack has succeeded, systems operated by customers or in connected networks can then be infected. It is clear that, for many institutions, digitalisation has been accompanied by a failure to properly assess the risks posed by always-on connectivity, with the initial focus instead being on functionality and serving as many users as possible.

In summary, the following trends can be identified in relation to ransomware:

- As with commercial software, ransomware uses a modular development strategy to penetrate target systems and propagate itself. Ransomware differs from other types of malware only in terms of the module that performs the actual encryption/lockdown. With the ransomware-as-a-service business model, the share of profits may even be negotiated beforehand.

- Ransomware is increasingly targeting larger companies, which may be more prepared to pay a high ransom fee. The methods used to penetrate systems are also adjusted to match the company in question.

- If a broad-based attack type is selected, it requires a high level of agility in order to overcome existing protection mechanisms (including free decryption tools, early detection, etc). This leads to a constant stream of adjustments to attack vectors (vulnerabilities, social engineering) and encryption algorithms.

The following aspects should therefore be taken into consideration:

- At the end of the day, surviving a successful ransomware attack is best achieved by an advance effort to create a usable backup of valuable or critical data. As the example discussed above makes clear, however, major losses can still occur despite having a solid backup and an incident response strategy.

- The working hours lost in restoring systems and copying backups will always be one cost factor for a company, of course. If a company's critical workflows cannot be handled by an IT department crippled by ransomware, however, much more significant costs result from temporary downtime, including damage to operating facilities, the procurement of costly interim solutions and a loss of confidence and trust among staff, customers and business partners.

- Exposure must therefore be kept to a minimum. This includes minimising the number and variability of computers that are accessible externally, ensuring that updates to operating systems and server or application software are performed as promptly as possible and having a sensible and restrictive policy for identifying users that need to access a given system from the Internet. Where access is needed, stringent requirements must be applied in the form of policies on passwords and protocols.

- If an infection is successful despite all of these precautions, appropriate segmentation of internal networks will help to limit the extent of the damage.

### 1.2.4 Distributed Denial of Service (DDoS)

If a website is no longer reachable, network services go down or critical business processes cannot be accessed because they are overloaded, a DDoS attack is often the cause. DDoS attacks are generally used by cyber criminals to damage specific targets, extort money from victims or attract attention to a particular cause. They may also be used to disguise other kinds of attacks – or enable them in the first place. These attacks are typically coordinated across a large number of computers or possibly servers.

The effects of DDoS attacks can be very serious indeed, ranging from major economic losses for the institutions affected to considerable damage to their reputation. According to a study published by Netscout, German companies reported total losses of around four billion euros in 2018 due to DDoS attacks. [internet world business, Netscout's 14th Annual Worldwide Infrastructure Security Report]

DDoS attacks typically target services that are reachable over the Internet, with systems that will be sorely missed by service customers being a particular focus for attackers.

The situation with regard to DDoS attacks is characterised by multiple developments, some of which reinforce each other:

- An increasing level of specialisation in executing attacks by utilising new attack vectors (such as 'Memcached' from the previous reporting period – see 'The State of IT Security in Germany in 2018'), the aggregation of DDoS attacks to focus on a single target (multi-vector attacks) and the deployment of new attack tools (DDoS from the cloud)

- The existence of DDoS booter services (such as 'webstresser.org', which has since been taken offline), which are making it increasingly easy for large-scale attacks to be launched by users without technical expertise

- Event-related DDoS activities that are timed to coincide with dates on the e-commerce or online gaming calendar

In the fourth quarter of 2018, multi-vector attacks accounted for the majority of DDoS attacks, totalling some 59% of such attacks. The same figure was only 45% during the same period in the previous year. In addition, up to nine separate attack vectors could be observed in these attacks. Of these, the most important were NTP Monlist, CLDAP, DNS reflection and SSDP reflection. [https://www.link11.com/de/blog/link11-ddos-statistiken-fuer-q4-2018-veroeffentlicht]

By combining different attack vectors, a much greater effect can be applied at the

- network level (attacks on OSI layers 3 (network layer) and 4 (transport layer) utilising SYN flooding, TCP connection flooding, DNS amplification attacks, Tribe Flood Network [TFN] and/or ping of death), as well as at the
- application level (attacks on OSI layer 7 (application layer) utilising HTTP floods, slow attacks, SMTP floods, etc)

on the specific attack target. Instead of simply overloading a system, an attack can focus simultaneously on vulnerabilities at the application and network levels.

The misuse of modern cloud solutions by cyber criminals has also been rising steadily over time, particularly in the context of conducting DDoS attacks.

To be able to exploit the technical potential of the cloud for their attacks, perpetrators need to take control of individual server systems or segments of cloud infrastructure. To do so, attackers deploy malware to compromise cloud services or rent appropriate public cloud services in order to then utilise superior levels of cloud service connectivity and bandwidth for their malicious purposes.

Analyses of data supplied by Link 11 (www.link11.com) show that a new record was set in winter 2018: over half of all attacks (59%) were executed with compromised cloud servers or servers that were legitimately rented, but then misused. In summer 2018, the figure for cloud-based DDoS attacks in Central Europe was 52% – after being recorded at a mere 2% back in January 2016.

Almost every cloud service provider has now been misused by criminals to execute DDoS attacks, although this unlawful use of their platforms has affected some cloud providers more often than others. Cloud servers that have memcached or SSDP services installed are particularly attractive for criminals. Public cloud servers hosted by Microsoft Azure, Amazon Web Services and Alibaba are the ones most frequently used for executing DDoS attacks. In contrast, Google's cloud solution is much more rarely used for criminal purposes. [https://www.link11.com/en/downloads/ddos-report-for-central-europe-q3-2018/]

For attackers who lack technical expertise, more and more ways of conducting effective DDoS attacks are becoming available.

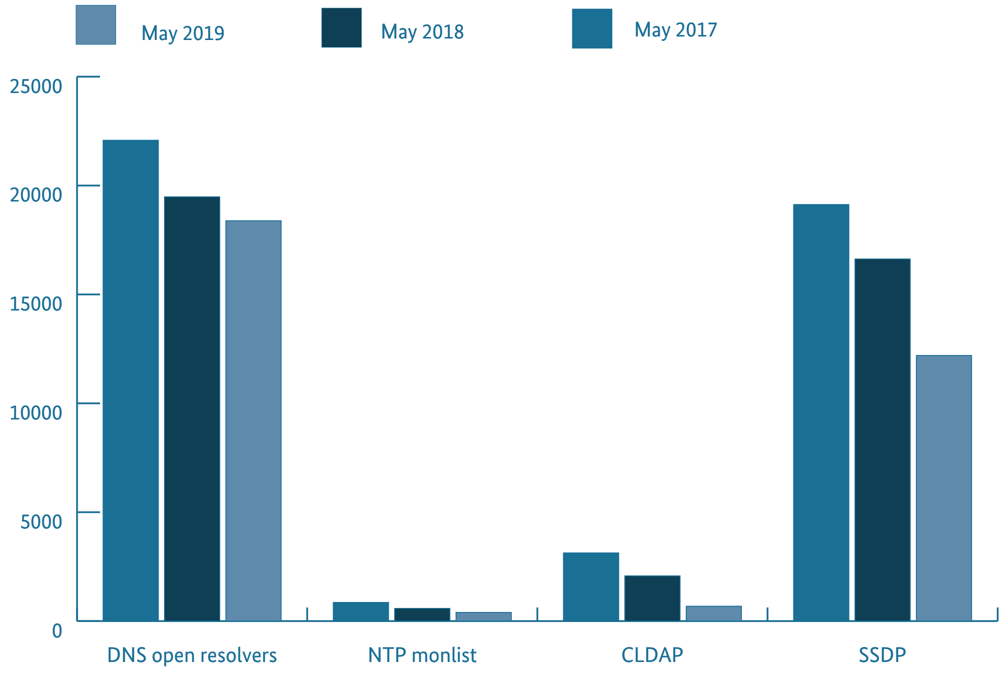


**Figure 05:** BSI, europol, security-insider

This is essentially the result of a growing 'cyber-crime-as-a-service' industry. In the context of DDoS in particular, attacks are offered as booter services. Setting up a booter service is comparatively straightforward and inexpensive: it is based on the misuse of server services available over the Internet and the setup of an infrastructure that provides access to these same services. One of the best-known providers, 'webstresser.org', offered multi-gigabit DDoS attacks for a 'subscription' of just USD 15/month until the site was finally taken down at the end of April 2018 in the 'Power OFF' operation, which was conducted by international law enforcement agencies. Shortly after the takedown, however, other service providers soon stepped in to fill the gap.
With these kinds of DDoS services, would-be attackers are given a set of tools that puts them in a position to trigger highly effective DDoS attacks that cost virtually nothing and require little to no technical expertise. In 2018, the services offered by Webstresser were responsible for a number of highly successful attacks against several Dutch banks and many other financial and government service providers in the Netherlands, with a great many customers being denied access to their bank accounts for days on end.

CERT-Bund has kept German network operators and providers informed on a daily basis about open UDP-based server services on their networks that could be misused for DDoS reflection attacks. Within the reporting period, for example, 11.5 million cases were investigated based on sinkhole data from various sources. This included IP addresses affecting German network operators or providers receiving daily reports (https:/reports-cert-bund.de/schadprogramme). The number of these open services was able to be further reduced in the reporting period as a result.

Note: while the figures for NTP monlist are comparatively small, misuse of this service enables much higher amplification factors.

Analyses performed by the BSI on incidents occurring on Black Friday and Cyber Monday show that there is a much higher risk of DDoS attacks on particularly busy days in the e-commerce calendar. These attacks can also last several hours. The associated loss of revenue on these key days for online shops is very serious (see 'Case Study: DDoS Attacks on Black Friday and Cyber Monday').

The overall threat landscape in relation to DDoS can be described as consistently high. Meanwhile, the benchmark for the success of a DDoS attack depends on whether the attack bandwidth is adequate for taking the target system offline for a shorter or longer period of time. The spectrum of DDoS attack technologies is constantly expanding to include new attack vectors, methods (e.g. multi-vector attacks) and tools (e.g. DDoS from the cloud). In this context, the DDoS 'service industry' acts as a distribution system for DDoS attack technologies by deploying current developments in the DDoS segment to its many 'customers'.

With multi-vector attacks, service denial is combined with attacks on vulnerabilities at the application and network layer, which are particularly difficult to counter.

Server-based botnets (attacks from the cloud) make it possible to leverage tremendous amounts of resources. While individual systems such as IoT devices, bots or PC systems generally use Internet connections with low Mbps ratings, cloud providers offer connectivity of 1 to 10 Gbps. Measurements performed by Link11 show that peak volumes during attacks from the cloud regularly exceeded values of 150 Gbps in recent months, with values as high as 300 Gbps in isolated cases.

Attackers without technical expertise can make use of booter services as described above. An investigation conducted by BSI in mid-2017 and current analyses of attacks show that the booter services analysed offer a broad choice of modern attack vectors that can be used as 'building blocks' for an actual attack.

Instead of implementing individual countermeasures against the wide variety of DDoS attack vectors, a more effective means of defence is to identify dynamic attacks before the operator actually connects and then introduce specific measures to clean up (purge) the data stream. In September 2018, the BSI published an overview of qualified DDoS mitigation service providers as a service for both companies and operators of larger-scale websites.

### 1.2.5 Botnets

The use of bot software gives cyber criminals access to a large number of third-party systems (computers, smartphones, routers, IoT devices, etc), which they can then misuse for their own purposes. Apart from spying out the user's own personal data and committing online banking fraud, the resources of the hijacked system can also be misused by an attacker – for the purposes of generating cryptocurrencies, for example, or executing DDoS attacks. Thanks to the modular design of modern malware, these programs can have their feature set adjusted dynamically or expanded by downloading additional extensions. This allows botnet operators to make purpose-built adjustments and modify the bot software individually to suit current circumstances.

In the period under consideration, botnets were primarily used for stealing information, perpetrating online banking fraud and distributing other kinds of malware. While the number of DDoS botnets based on Mirai has in fact risen, no parallel increase in botnet-based DDoS attacks has been observed. Observations made by the BSI have revealed that botnets are being used less often for DDoS attacks in comparison to other attack methods. One reason might be that attackers have a range of cheap and easily accessible alternatives at their disposal, such as DDoS booter services (see 1.2.4 DDoS). Many new Mirai variants have extended the original version to include new infection mechanisms, which has also expanded the portfolio of potentially infected systems to include further types of computer architectures or device classes like web servers or enterprise systems. The general rise in IoT botnets based on Internet-capable consumer electronics that was observed in the previous year continued into the current reporting period. According to media coverage and the BSI's own research work, however, most of these infections took place outside Europe.

A rise in the numbers of Android systems infected with bot software was also observed, and this also went hand-in-hand with a comparatively high rate of infection in Germany. In one aspect of note, some of the Android devices affected had actually been shipped out with the infection already in place (see 'Case Study: Pre-Installed Malware on Android Devices'). The functionality of this malware went far beyond simple information theft; it actually enabled full access to the infected devices. While most of the Android botnets observed clearly focused on enabling leaks of personal data, they were also capable of downloading other modules in order to add extra types of malware functionality.

In the Windows-based botnet segment, Emotet deserves special mention: this piece of malware has been active for several years now and was responsible for large-scale infections in Germany in particular in this reporting period. Alongside many private users, larger companies also fell victim to attacks, which caused large-scale downtime as a result of malware programs such as Trickbot (see Case Study: Be Aware of the Emotet Malware).

During the reporting period, up to 110,000 bot infections of German systems were registered on a daily basis and reported to German Internet providers via the BSI. The providers then notify affected customers about the infection and may also provide additional information about how to clean compromised systems. To detect botnet infections, sinkhole systems are deployed that accept contact requests from bots instead of their regular command and control servers (for a description of the sinkholing technique, please see https://www.bsi.bund.de/EN/Topics/IT-Crisis-Management/CERT-Bund/CERT-Reports/Reports/malware-infections/malware-infections_node.html).

As in previous years, the threat posed by botnets remains consistently high. Figures for visible infections can vary widely depending on the botnets selected for observation and the domains utilised for the control servers. Since it is impossible to obtain a complete set of data for the botnet infections in existence, numbers derived from sinkholing should always be seen as a lower limit. Experience gained in botnet takedowns has shown that the real figures are considerably higher. Among private users in particular, a kind of 'digital recklessness' can be observed; it is expressed, for example, by the numbers of new botnet infections reported every day which would have been easy to prevent with simple, basic precautions.

An examination of current trends shows that attackers are now concentrating on mobile end-user devices and IoT systems. Since these kinds of systems are now increasingly widespread and also becoming more common in new areas of our daily lives, they also offer perpetrators more and more points of attack. To complicate matters further, IoT devices are primarily manufactured for the mass market, and security is often passed over in favour of functionality in order to minimise the costs of production. Many systems are shipped out in an insecure state, for example, and receive little to no support from manufacturers in the form of security updates or patches. As a result of these factors, IoT devices offer attackers an open goal. This is an area where manufacturers need to be obliged to place more secure products on the market.

The comparatively low rate of infection of IoT devices in Germany can be attributed primarily to the typical kinds of Internet connection utilised by German end customers. Typically, these customers go online via a router that does not normally permit direct external access to systems in the customer's internal network, unless this has been explicitly configured and allowed. This contrasts with common practice outside Europe, where devices on an internal network are often exposed directly over the Internet. The key role played by the router in the security of home networks is reflected in the technical guidelines for routers that were published by the BSI in November 2018, which formulate a set of security requirements for these devices. Similar requirements documents are planned for IoT devices (see 2.3.1.2 Smart Homes and the Internet of Things).

Another problem affecting Android devices is a lack of availability of security updates and patches, especially in the low-price segment – as has been demonstrated impressively in the case of the Andr/Xgen2-CY Trojan. If devices are al-

## DDoS Attacks on Black Friday and Cyber Monday

**Black Friday**
On Black Friday (23 November 2018), Link11, a German provider of DDoS mitigation services, recorded a number of attacks on certain e-commerce providers that was over 70% higher than the monthly average. [Link11 blog]

When all attacks reported by Link11 in November 2018 are considered, 28 of the top 40 attacks in terms of duration occurred on Black Friday. The BSI's own analysis of the 55 longest DDoS attacks on Black Friday is shown below:

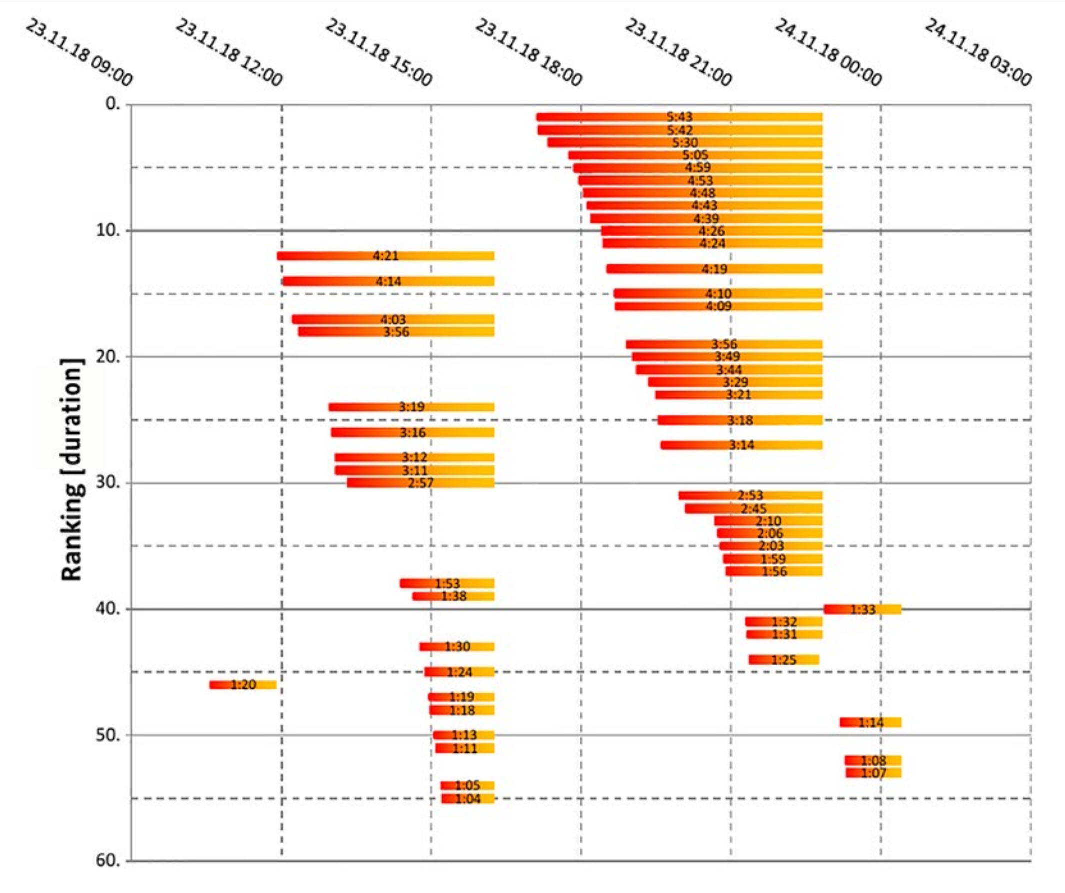


**Figure 06:** Top 55 of the longest DDOS attacks on November 23, 2018 (Black Friday)

Essentially, two attack waves with defined ends can be seen here. The simultaneous cessation of the attacks at approximately 16:15 CEST and 23:00 CEST resulted from the fact that the mitigation measures implemented at these points in time successfully terminated the attacks. An analysis of metadata from the attacks reveals marked similarities that suggest the attacks were launched from the same source (such as DDoS booter services).

An attribution to a specific individual or organisation was not possible. The execution of the attacks in two attack waves and the coordinated timing of the follow-ups to the attacks are indications that the number of attackers involved was limited and the attackers were also in communication during the attacks.

In all likelihood, the attackers were pursuing economic objectives, such as:

- Extorting money from individual companies (the attack will be terminated on payment of a fee)
- Securing a competitive advantage (forcing co-competitors offline)

To maximise the damage caused, the attackers scheduled their attacks to hit at times when e-commerce platforms, online services, web applications and apps were in particularly heavy use.

An analysis of attack metadata shows that the attacks were preceded by preparatory activities. In terms of attack bandwidth and packet counts, the figures for these attacks are actually in the lower third of the DDoS attacks observed in November 2018. Rather than attack individual targets with a 'hit and hope' strategy using a lot of bandwidth, the attackers instead used the bandwidth available to them to attack as many targets as possible simultaneously. To achieve this, targets seem to have been selected based on the attackers' assumption that the attacks would still achieve the required effect even though they actually had less technical potential to cause damage.

The attacks were timed to coincide with a specific event (Black Friday). It can be assumed that similar attacks will be repeated on similar key dates for online activities (major e-sports tournaments, special events hosted by major online companies, etc).

**Cyber Monday**
Link11 also recorded a huge rise in attacks on specific e-commerce providers on Cyber Monday (26 November 2018). Attacks rose by 109% compared to the monthly average – an even higher figure than the percentage for Black Friday.

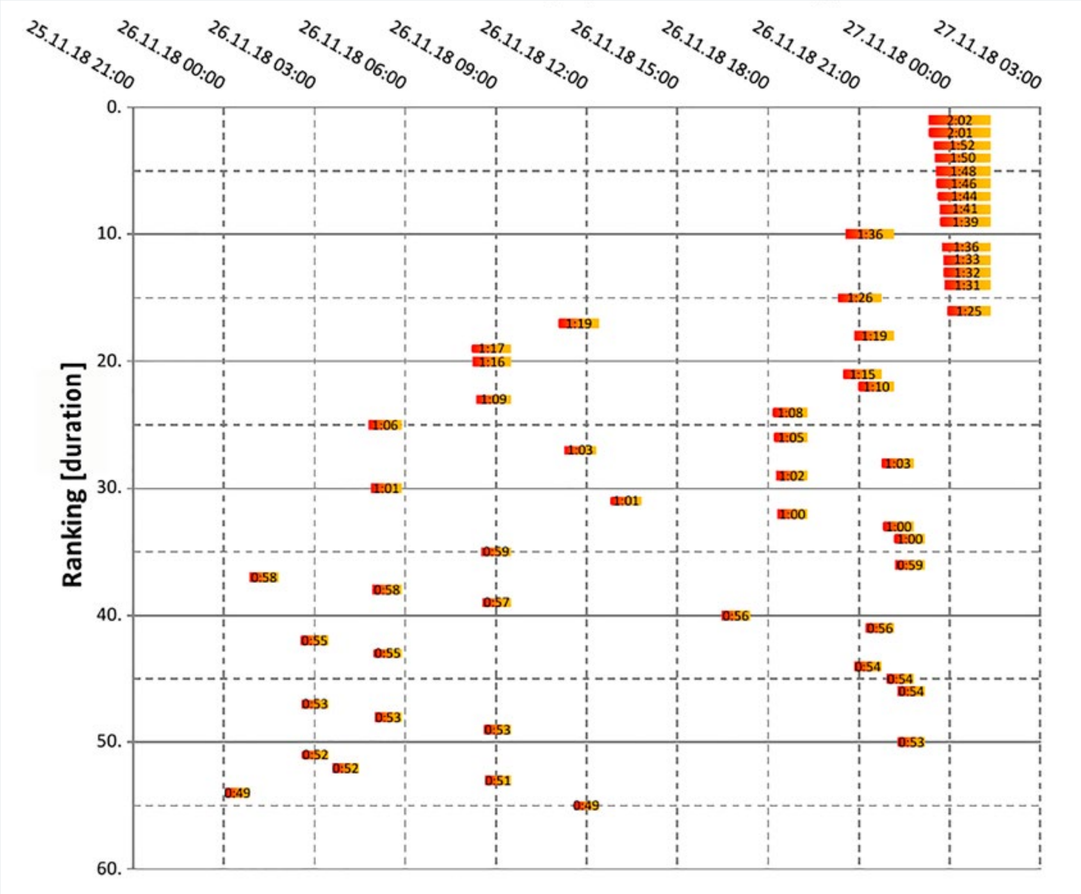


**Figure 07:** Top 55 longest DDoS attacks on November 26, 2018 (Cyber Monday)

Unlike the attacks on Black Friday, however, the time distribution of the 55 longest attacks on Cyber Monday is largely homogeneous. The only grouping that can be seen with these attacks occurs in the hour before midnight (CEST). All of these attacks end at 00:00 on the following day. The attack durations are also shorter than for Black Friday, ranging from 49 minutes to 122 minutes, although this does put them significantly above the average for November 2018 at 25 minutes per attack.

An analysis of metadata from the attacks reveals the same sorts of similarities that were observed in the case of the attacks on Black Friday, which also indicate that the attacks were made from the same source (e.g. DDoS booter services).

As already observed on Black Friday, no attribution can be made to a specific individual or organisation. Since the attacks are distributed virtually homogeneously, no conclusions can be drawn about the number of attackers or any kind of communication between them.

ready shipped out in an infected state and do not receive any updates to resolve these infections, the devices should not be utilised in any circumstances. In the reporting period, however, most Android infections could be traced back to malicious apps, most of which were from third-party sources and had been installed intentionally by users.

From these observations, one can assume that the trends will persist, and that the size and diversity of botnets will continue to increase. Measures for prevention and detection are urgently needed here. While the vast majority of IoT infections are not located within Germany's borders, infected devices nonetheless pose a threat to German systems because these devices can be used to conduct international DDoS attacks or misused in order to propagate malware or spam.

### Pre-Installed Malware on IT Devices

In June, the Federal Office for Information Security (BSI) detected pre-installed malware on a number of smartphones. These devices had been purchased on several different online marketplaces and tested for a malware variant first identified in February. Acting on the basis of Section 7 of the BSI Act, the BSI issued a warning about using the devices Doogee BL 7000 and M Horse Pure 1; it also advised users to exercise particular care in this context (https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2019/bsi-warnung-smartphones-060619.html). Malware was also detected on Keecoo P11 devices with the firmware version V3.02. For this device, however, firmware V3.04 (which did not contain the malware) was made available via the manufacturer's 'wireless update' service. In addition, the BSI detected the same malware on the device VKworld Mix Plus in firmware versions V3.05 and V3.07, although this malware had not been activated. Some retail platforms removed the devices affected by the BSI warning from their product ranges.

In late February 2019, the BSI had already issued a warning about Android devices with pre-installed malware that had been sold via online platforms in Germany [https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2019/Warnung_vorinst_Schadsoftware_260219.html]. Although the BSI first detected an infection on a single tablet brand, further investigations revealed a number of other devices from different manufacturers that were similarly affected. While corrected software versions have since been supplied for individual models, the old firmware versions provided on the respective manufacturer websites still contain the malware identified by the BSI. It was therefore assumed that devices had been shipped out earlier containing the outdated and infected firmware.

The investigations were conducted in response to a high rate of infections in Germany involving a new class of malware being tracked by sinkholing systems, which was first discovered by the Sophos security company on a Ulefone S8 Pro smartphone. The BSI recorded up to 20,000 infections of different German IP addresses every day, and therefore assumed a major wave of propagation was taking place with this malware variant in Germany. The malware, dubbed 'Andr/Xgen2-CY' by Sophos [https://news.sophos.com/en-us/2018/10/02/the-price-of-a-cheap-mobile-phone-may-include-your-privacy/], was embedded in the device firmware and transmitted characteristic device data to a control server at regular intervals. The malware was also equipped with a download function, which enabled it to receive functional enhancements dynamically from a command and control server. This mechanism can be used to store and execute a banking Trojan on the device, for example. Since the malware program is embedded in the device firmware, manual cleaning of the device is not possible.

The BSI detected an infection with 'Andr/Xgen2-CY' on several devices (five smartphones and one tablet in all) that could be purchased in Germany and informed the affected manufacturers accordingly. Some manufacturers then provided corrected versions of the firmware as downloads. Since the first occurrence of infections in the sinkhole data, German network operators have been kept informed about infected devices in their respective networks by means of reports from CERT-Bund [https://reports.cert-bund.de/schadprogramme]. These providers were asked to inform their affected customers accordingly. Recommendations for action for purchasers of affected devices – along with general advice for IT users when purchasing new IT equipment – is presented by the BSI on its website for citizens at www.bsi-fuer-buerger.de.

## AVALANCHE: PROTECTIVE MEASURES EXTENDED

On 30 November 2016, the Verden public prosecutor's office, together with the Lüneburg Central Criminal Inspectorate (ZKI) and other international partners, took down 'Avalanche', the world's largest botnet infrastructure. The BSI had a supporting role in this operation. Part of the work involved in breaking up this organisation used the 'sinkhole server' technique to identify the IP addresses of infected systems. This meant that Internet service providers were able to inform and warn affected users. Originally designed to last for one year, the protective and informative measures deployed were extended for another 12 months in November 2017; analyses had shown that while infection rates were falling, many of the affected users had not yet cleaned up their systems. The sinkholing system set up in the course of the Avalanche shutdown was also extended to include domains used by the 'Andromeda' botnet, which achieved an increased level of visibility for infections with the Goznym Trojan for the month of October.

In November 2018, another extension of these measures was agreed and implemented. This involved checking and blocking around 850,000 domains to prevent botnet takeovers by criminals, and in turn also ensured that botnet activities would remain visible for another 12 months. As a result, over 1.9 million computers (unique IPs) are being identified as part of Avalanche every day around the world – 3,900 of them in Germany. The forwarding of this data by the BSI to providers and other international partners will enable the prompt cleaning up of affected systems. To ensure lasting success, however, cooperative efforts between providers and domain owners are required.
The current achievements in uncovering botnet activity can be seen in the following figures: on 28 November 2018, around 1.3 million infections were detected and reported worldwide, of which 3,300 were in Germany.

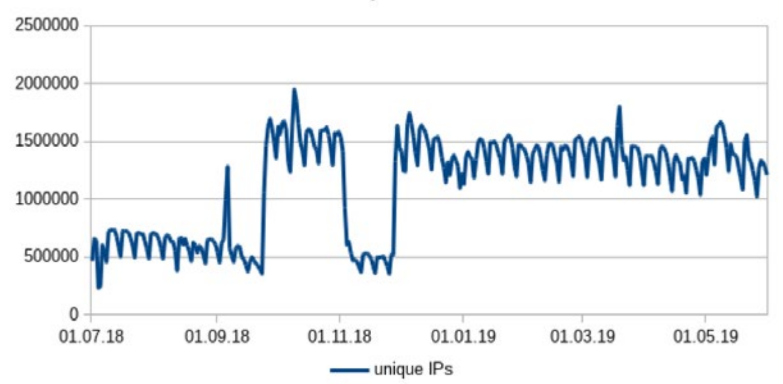


**Figure 08:** Infected systems worldwide

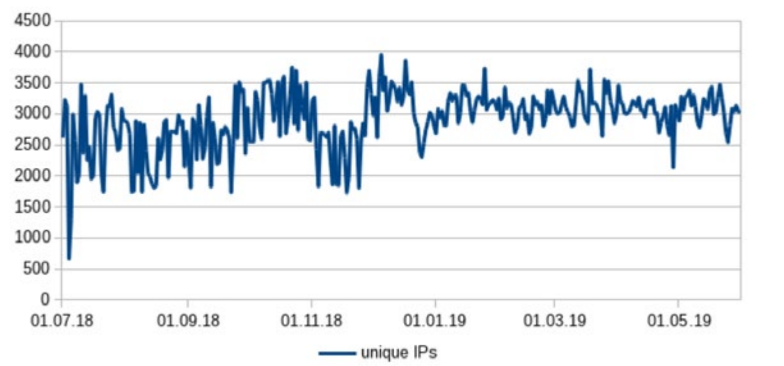


**Figure 09:** Infected systems Germany

### 1.2.6 Spam

Spam, a general term for unsolicited e-mails, can be roughly categorised into three types:

- Conventional spam is often used to advertise products, securities or services, and may also be deployed when attempting fraud (with regard to ‚advance fees', for example). An advance-fee scam aims to convince the victim to wire money in advance for services or goods that will never be supplied or shipped.

- Malware spam is used by attackers to infect recipients' systems with malware. This malware can be attached directly to an e-mail or introduced indirectly by means of a link in the e-mail body or its attachments. This link either leads to the malware directly or to a website containing drive-by exploits (see Section 1.2.2 Malware).

- Phishing communications try to trick users into entering their login details (for online banking, payment services, social networks, shopping portals, etc) on websites that are under the control of the attackers (see 1.2.1 Identity Theft).

In most cases, spam is sent either from compromised servers or infected client systems or via legitimate e-mail accounts using intercepted user credentials. Systems that distribute spam are often aggregated into a botnet (see Section 1.2.5 Botnets), which makes it easier for cyber criminals to market their spamming activities as a service.

Another feature that can be observed in recent spam e-mails is the misuse of personal data from data leaks or identity data acquired by some other unlawful means (such as from infected internal clients or published data research (doxing), for example). These tactics significantly increase the likelihood of an infection.

Compared to the last reporting period, the volume of spam sent declined by approximately 40%. The decline in malware spam was much sharper (approx. 97%).

While the actual volume of malware spam has fallen drastically, observations made by the BSI show that the potential impact remains the same (or has even increased in certain cases) due to much more targeted distribution methods. The Emotet botnet should be noted in this context (see Case Study: Be Aware of the Emotet Malware). The reuse of contact relationships from recent e-mails on infected clients resulted in messages that seemed to have been sent from known communication partners. This modus operandi, paired with the use of hijacked e-mail accounts for distribution, was instrumental in causing damage on a much larger scale.

The attachments sent (largely MS Office documents and JS files) were also constantly modified with the aim of

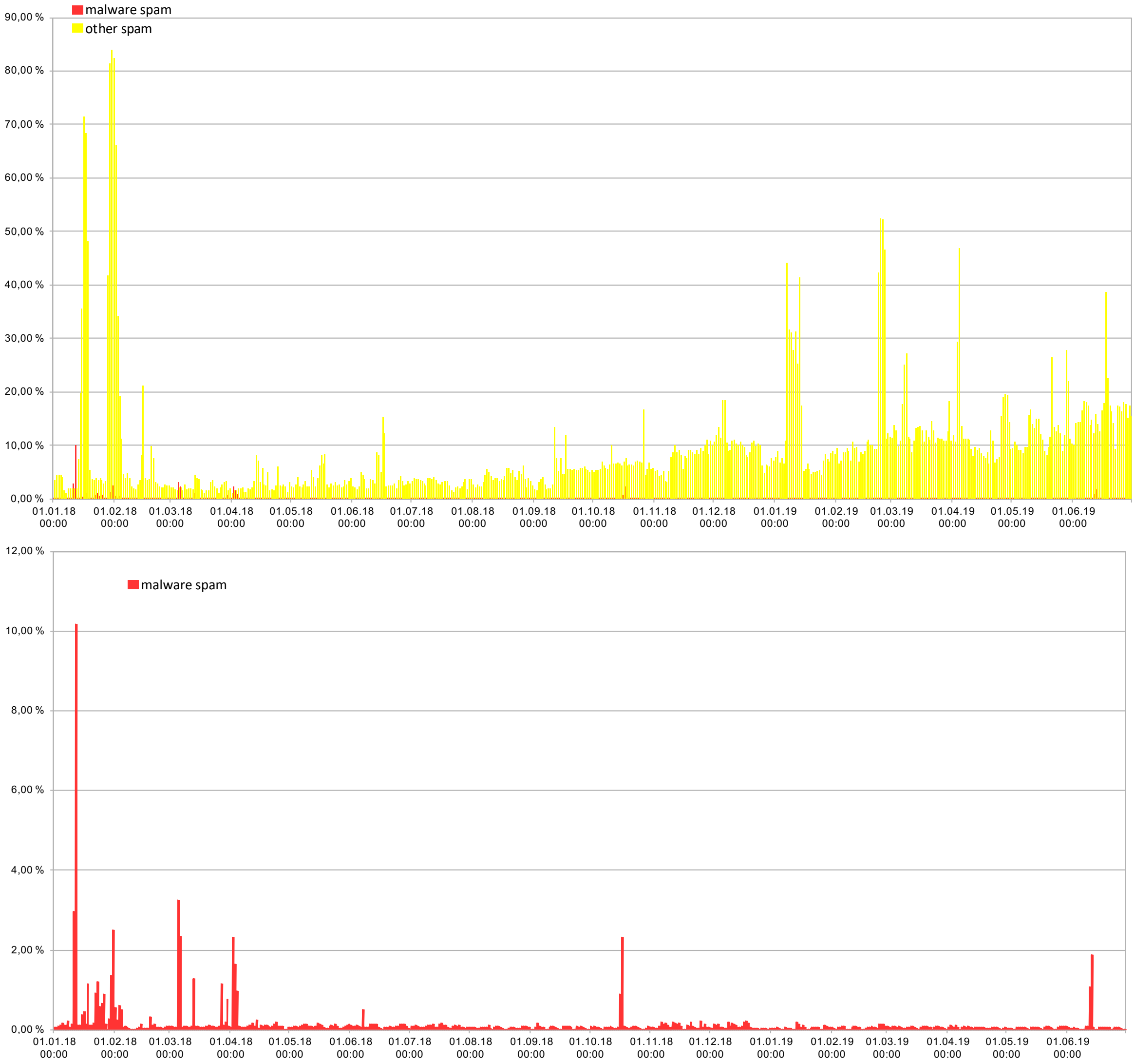


**Figure 10:** Malware spam and spam over time since 1 Jan 2018 as a percentage of the daily total volume from mid-December 2016 (the highest volume of daily spam measured to date), presented as a stacked area graph. The bottom chart offers a higher-resolution view of malware spam over time.

bypassing detection by antivirus software. In early April 2019, for example, documents were sent as encrypted ZIP files and the password was provided in the e-mail body. The fictitious e-mail content, which was often composed in good German, urged the recipient to respond quickly to a pressing matter (an unpaid bill, an order confirmation, etc).

Alongside Emotet, other smaller-scale waves were also observed. The sending of unusual file formats such as ACE, ISO and UDF was also observed on multiple occasions; these typically included the corresponding malware code in the form of an executable file (.exe). The e-mail body in these cases was usually formulated in English, however. Also worthy of mention is the sending of RTF files and some MS Word documents that exploited the MS Equation vulnerability (CVE-2017-11882). One further trend relates to the sending of MS Office documents that do not themselves include malware code, but use MS Office mechanisms to download this code when the attachment is opened. In isolated cases, very old software components such as Excel 4.0 macros were also exploited for attacks; these continue to be embedded in modern software for compatibility reasons.
In contrast to the last reporting period, no one category can be singled out in the context of conventional spam, which was broadly distributed across multiple attack vectors.

As observations have shown, the quality – and thus the effectiveness – of malware spam continues to rise. This means that the threat potential has remained constant or has even risen in some areas despite the sharp drop in absolute volumes. Attackers display a high degree of innovative ingenuity and technical expertise. A considerable level of personal effort also seems to have been applied in developing a host of new techniques to overcome antivirus protection and devising new social engineering tactics to convince users to execute malware code. The exploitation of features or vulnerabilities from outdated software components or file formats can initially succeed undetected, as these are unknown to a wider public.

In some cases, Emotet incidents were believed – even by IT experts – to be ‘targeted attacks’ and were reported to the BSI as such. This demonstrates the effectiveness of the tactics deployed.

The case of password-protected ZIP files also shows that some of the attackers’ techniques, while technically sophisticated, did not have the desired result. While these files easily bypassed perimeter antivirus solutions, the users themselves proved to be the stumbling block, as they were either unwilling or simply unable to enter the passwords when opening the attachment.

Restrictive attachment handling (using a white list for file types) in conjunction with a restrictive content policy for documents (such as filtering out Office download requests and documents that contain macros or download functionality at the central HTTP gateway) should be able to frustrate most of these new techniques attempted by attackers.

### 1.2.7 Trends in APT Attacks

APT (Advanced Persistent Threat) attacks differ in terms of the technical methods that are used to execute them, and in terms of their respective targets and originating organisations. The resulting threat landscape is therefore very heterogeneous. The trends below therefore describe phenomena that are not limited to individual groups or suspected countries of origin.

**Publicly available tools:** A clear trend being adopted by APT groups with very different technical resources and backgrounds involves the use of publicly available penetration test tools that offer the same functionality as espionage programs. Examples here include the ‘Cobalt Strike’, ‘Meterpreter’, ‘Koadic’ and ‘Powershell Empire’ frameworks. Having been developed to conduct professional penetration testing, these tools offer a wide range of features and are generally easy to use. Doing so gives perpetrators several advantages. First, it saves the time needed to develop proprietary tools. Second, the use of these tools makes it more difficult for security teams to associate a specific attack with campaigns or APT groups.

There are also opportunities for security teams to leverage, however: log data and network traffic can be checked for the typical characteristics of these familiar and well-analysed attack tools, which could enable the detection of more groups of perpetrators. While the frameworks do offer many configuration options to make detection more difficult, inexperienced groups of attackers in particular will typically use the defaults. Consider the following example: unlike other webservers, the Cobalt Beacon control servers replied to certain requests with an additional space character until January 2019. This mechanism made it possible to conduct a global scan for all available Cobalt Strike servers and ultimately use them as a network signature.

In general, the availability of these public tools has resulted in a slight levelling-off of the technical complexity of APT attacks – although only at the low- and medium-severity level. For inexperienced groups, the barriers to entry are lowered and they can start at a higher level (at least in terms of malware). Experienced and technically advanced groups, on the other hand, combine use of these public frameworks with the parallel development of their own arsenal of malware. Examples here include APT28, Snake and APT10. While the reasons for this remain unclear, it is likely that custom-developed malware has not been as well analysed by IT security companies as the publicly available and familiar frameworks, and perpetrators are therefore hoping to achieve lower rates of detection. Sometimes, new functions are also needed that are not included in the public frameworks.

**International service providers:** Reports from IT security companies strongly suggest that there is a growing number of service providers that offer spyware and exploits or actually carry out cyber attacks themselves. Some of these services are offered not merely in the provider's home country, but internationally, as well. As a result, nations that previously lacked the expertise to develop espionage programs can now possess highly professional tools and/or use them for attacks. This development has not only resulted in a worsening threat landscape; it has also made it more difficult to attribute individual attacks to the same perpetrators because several clients use the same service provider (and therefore identical observable techniques). Opportunities do exist for network defence teams, however. Errors made by inexperienced perpetrators can lead to the detection of espionage programs and thereby reveal operations being conducted by other actors.

**Use of legitimate services:** Another development that can be observed among groups as diverse as APT28, MuddyWater or DarkHydrus is the deployment of legitimate services to conceal malware control systems. Known as the 'dead drop resolver' method, this involves malware programs contacting an address at a legitimate online service such as Dropbox, Github, Google Groups or some other forum as the first step after a successful infection. Since these services are encrypted with TLS, network monitoring systems cannot distinguish between malware communication and legitimate use of these services. The dead drop destination hosts the real addresses of the control servers to which the malware program then connects. This method offers perpetrators a flexible way of changing control server addresses while reducing the probability of being detected.

In technical terms, security teams can counteract this phenomenon by interrupting encrypted TLS traffic in the company or public authority network and running it through existing security products. Data protection aspects have to be considered here, however, and the rollout also involves a major organisational effort. That said, the use of such TLS proxies does offer opportunities to detect other phenomena (e.g. exploits or malware) on websites that have been encrypted with readily available TLS certificates from free certificate providers such as Let's Encrypt.

**Obstructing malware analysis efforts:** Technically advanced groups are now increasingly taking steps to make the systematic analysis of their malware by security companies more difficult. One typical approach taken by such companies is to collect malware from customer systems or from web-based services with which users can have their files checked for malicious code. These malware samples are then analysed with the aim of developing detection signatures. Several APT groups are now undermining this kind of sample collection by ensuring that their primary malware programs remain inaccessible until a chain of 'droppers and downloaders' has been completed. In some cases, compromised systems have first been combed through for information capable of identifying the system as a worthy target or, alternatively, an analysis system set up by a security firm with the deliberate aim of becoming infected. If a security firm captures only a first-stage downloader, it may prove impossible to obtain the main malware program from this file because it may no longer be downloadable from the attack server or a specific configuration may be needed that is known only to the perpetrators. While this approach has been observed in practice for a number of years, it is now becoming more common.

**Adoption of APT techniques in criminal campaigns:** As originally reported last year, a number of criminal groups are now adopting techniques that were still seen as characteristic of APT attacks until only recently. This includes lateral movement, a technique whereby perpetrators spread manually within a compromised internal network. Within the reporting period, several cases were observed in which other types of attacks followed successful compromising by a general-purpose piece of malware like Emotet. In several cases, perpetrators deployed ransomware – probably by means of access initially achieved via Emotet – in an apparent attempt to introduce it manually on servers in internal company networks (see Case Study: Be Aware of the Emotet Malware).

**Technical attribution to APT groups:** One key aspect of the technical prevention and detection of APT attacks is the ability to assemble similar incidents into abstract APT groups, which are termed 'intrusion sets'. Such categorisation enables the prioritisation of resources by security departments while leveraging experience to enable more efficient searches for potential approaches used by perpetrators during actual incidents. While the phenomena mentioned above – such as publicly available tools and service providers – introduce a degree of opacity at earlier stages in terms of attributing attacks to intrusion sets, the BSI nonetheless continues to recommend accounting for activity by APT groups as part of any organisation's internal risk assessment process.

**Attack analysis and prioritising countermeasures:** One methodology for the structured analysis of incident data via APT attacks is the MITRE ATT&CK framework [https://attack.mitre.org/]. An internal analysis of incident reports conducted by the BSI according to this methodology shows that the following techniques are very commonly used for APT attacks:

- Spear phishing: e-mails with malware attachments (phase: initial access)
- General deployment of scripts, specifically PowerShell scripts and execution by the user (phase: execution)
- Anchoring via autostart mechanisms in the registry or as a new service (phase: persistence)
- Gathering information about the system or running processes (phase: discovery)
- Standard protocols such as HTTP(S) (phase: command and control)

While these insights are not new or surprising, they do help to prioritise countermeasures to APT attacks. Focusing on prevention and detection measures for the above-mentioned attack techniques leads to a significantly higher level of effective protection against APT attacks.

Despite the trends discussed above, many APT attacks can still be prevented by conventional IT security precautions (cf. https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/BasisschutzGeraet/BasisschutzGeraet_node.html) if these are implemented in a systematic way. Conversely, a lack of attention to security precautions simply makes life easier for perpetrators and means they need to deploy fewer resources. For those who are unsure where to begin, the first step is to concentrate on basic, tried-and-tested IT security precautions. Any APT-specific measures that then need to be applied are particularly effective if a risk assessment has first been performed for the organisation concerned. Security managers should be familiar with the threat model relevant for their organisation and should use it (possibly supplemented by an analysis of relevant APT groups) to derive potential attack techniques for which internal countermeasures are not yet in place.

### 1.2.8 Attack Vectors in a Cryptography Context

The security functions of many IT products are based on cryptographic mechanisms. State-of-the-art cryptographic algorithms such as the Advanced Encryption Standard (AES) symmetric encryption method or the asymmetric Diffie-Hellman key exchange using elliptic curves can generally guarantee an excellent level of security. In Technical Guideline TR-02102, the BSI recommends a series of cryptographic algorithms and protocols that are generally regarded as secure based on rigorous mathematical cryptanalysis work. Typically, however, the security of these procedures is linked to certain preconditions. If these preconditions cannot be met, additional protective measures must be taken.

The following factors can cause a cryptosystem to fail in practice:

- Weaknesses in cryptographic mechanisms or protocols
- Implementation errors
- Failure to properly protect side channels
- Hardware vulnerabilities (e.g. Spectre; see Section 1.2.9)
- Weak random numbers

As one widespread example illustrates, some devices may be operated within a secure environment, but communicate with other IT products over an insecure network. For mutual authentication as well as the protection of confidentiality and integrity of communications,  cryptographic protocols such as TLS, IKEv2/IPsec and SSH are available. For these protocols, it is assumed that an attacker with network access can neither gain access to the secret key nor decrypt messages or change them without the changes being detected. In order for these cryptographic protocols to be effective, their correct implementation must also be assured. In particular, important cryptographic tests must not be skipped – even if these are not considered necessary from a functional perspective (see the 'Invalid Curve Attacks' sidebar, for example). Furthermore, any device behaviour that can be monitored at the network interface (error messages, response time, etc) must not result in leaks of information about processed secrets (see the 'CBC Padding Oracle Attacks' sidebar, for example).

When securing cryptosystems that are intended to resist attacks even from perpetrators in physical proximity to the system, other kinds of information useful for side channel attacks apart from runtime – such as the device's current consumption or electromagnetic radiation – must also be considered. In-depth research in this field has led to countermeasures, but also to new attack vectors.

The most recent development in side channel analysis is the use of artificial intelligence (AI) methods that aim to identify patterns in measurement data. Some initial approaches to deploying AI tools for cryptanalysis are also under development. The BSI is building up practical expertise in these fields (see Section 2.4.5).

A key prerequisite for the secure use of cryptography is the generation of random numbers that meet certain quality criteria. In AIS 20 and AIS 31 (application notes and interpretations of the scheme), the BSI defines functionality classes of random number generators for various use cases. One positive aspect to be highlighted here is that many products now utilise a physical random number generator certified according to the German Common Criteria (CC) scheme. As semiconductor products become physically smaller and achieve ever-increasing performance at lower levels of power consumption, newer products have also integrated cryptographic post-processing of random numbers. This entirely prevents the theoretical exploitation of the (already very small) residual statistical weaknesses present in physical noise sources.

For block ciphers (e.g. AES) using the CBC mode of encryption, messages must be padded to a multiple of the block length. As a result of insecure use of CBC mode within the TLS (Transport Layer Security) protocol, instances of 'CBC padding oracles' can be created if an implementation reveals information about the result of a padding check based on its response time or some other behaviour. A CBC padding oracle can enable an attacker to decrypt TLS messages. The basic principles of this kind of attack were set out in a publication by Serge Vaudenay in 2002. Since then, and despite a number of improvements to TLS standards, security researchers continue to identify vulnerabilities in this context. Most recently, the new attack variants 'Zombie POODLE' and 'GOLDENDOODLE' were presented by security researcher Craig Young at the Black Hat Asia conference in March 2019.

In the latest TLS 1.3 standard, published by the Internet Engineering Task Force (IETF) in August 2018, CBC padding oracle attacks are no longer possible, since this standard has removed CBC mode. The BSI has included a recommendation to use TLS 1.3 in Technical Guideline TR-02102-2..

Invalid curve attacks are attacks that target elliptic curve cryptography by manipulating curve points in order to force the use of weak (invalid) curve parameters. These kinds of attacks were first described in 2000 in a paper published by Biehl, Meyer and Müller (Ingrid Biehl, Bernd Meyer, Volker Müller: 'Differential Fault Attacks on Elliptic Curve Cryptosystems'). They are generally easy to thwart using point validation. In the reporting period, there were two incidents where this important check was omitted or not adequately performed.

In July 2018, Biham and Neumann (Eli Biham, Lior Neumann: 'Breaking the Bluetooth Pairing: Fixed Coordinate Invalid Curve Attack') presented a novel invalid curve attack against current Bluetooth pairing protocols that enables both the decryption and spoofing of Bluetooth messages. This resulted in corrections to the Bluetooth specification.

In April 2019, security researchers Ronen and Vanhoef (Mathy Vanhoef, Eyal Ronen: 'Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd') identified cases of omitted point validation in multiple implementations of the password-based authentication protocol EAP-pwd; these omissions could enable an attacker to achieve authentication without a password. EAP-pwd is deployed to authenticate the WPA2 Wi-Fi encryption method, for example.

## CBC PADDING ORACLE ATTACKS

For block ciphers (e.g. AES) using the CBC mode of encryption, messages must be padded to a multiple of the block length. As a result of insecure use of CBC mode within the TLS (Transport Layer Security) protocol, instances of 'CBC padding oracles' can be created if an implementation reveals information about the result of a padding check based on its response time or some other behaviour. A CBC padding oracle can enable an attacker to decrypt TLS messages. The basic principles of this kind of attack were set out in a publication by Serge Vaudenay in 2002. Since then, and despite a number of improvements to TLS standards, security researchers continue to identify vulnerabilities in this context. Most recently, the new attack variants 'Zombie POODLE' and 'GOLDENDOODLE' were presented by security researcher Craig Young at the Black Hat Asia conference in March 2019.

In the latest TLS 1.3 standard, published by the Internet Engineering Task Force (IETF) in August 2018, CBC padding oracle attacks are no longer possible, since this standard has removed CBC mode. The BSI has included a recommendation to use TLS 1.3 in Technical Guideline TR-02102-2.

## INVALID CURVE ATTACKS

Invalid curve attacks are attacks that target elliptic curve cryptography by manipulating curve points in order to force the use of weak (invalid) curve parameters. These kinds of attacks were first described in 2000 in a paper published by Biehl, Meyer and Müller (Ingrid Biehl, Bernd Meyer, Volker Müller: 'Differential Fault Attacks on Elliptic Curve Cryptosystems'). They are generally easy to thwart using point validation. In the reporting period, there were two incidents where this important check was omitted or not adequately performed.

In July 2018, Biham and Neumann (Eli Biham, Lior Neumann: 'Breaking the Bluetooth Pairing: Fixed Coordinate Invalid Curve Attack') presented a novel invalid curve attack against current Bluetooth pairing protocols that enables both the decryption and spoofing of Bluetooth messages. This resulted in corrections to the Bluetooth specification.
In April 2019, security researchers Ronen and Vanhoef (Mathy Vanhoef, Eyal Ronen: 'Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd') identified cases of omitted point validation in multiple implementations of the password-based authentication protocol EAP-pwd; these omissions could enable an attacker to achieve authentication without a password. EAP-pwd is deployed to authenticate the WPA2 Wi-Fi encryption method, for example.

## POST-QUANTUM CRYPTOGRAPHY

However, the guarantees of security offered by the cryptographic mechanisms in use today will remain valid only until a sufficiently powerful quantum computer becomes available. Quantum algorithms have been available since the 1990s that are capable of significantly reducing the level of security offered by conventional methods (the Grover algorithm for symmetric cryptosystems) or breaking these methods entirely (the Shor algorithm for asymmetric cryptosystems).

An alternative is offered by 'post-quantum' cryptography. The term refers to cryptographic procedures based on a class of mathematical problems that are presumed to be extremely difficult to solve, even with a quantum computer. As it becomes increasingly probable that a quantum computer of a sufficient size can in fact be built, there has been a huge increase in research and standardisation activities in the field of post-quantum cryptography in recent years (see Section 2.4.3). One important task for the BSI in the coming years will be to actively support these activities and implement its own projects.

To obtain a sound assessment of the current state of development and the potential future availability of a quantum computer, the BSI commissioned a study, 'Status of Quantum Computer Development', from researchers at Saarland University (Germany) and Florida Atlantic University (USA). The final report examines current technological approaches and quantum algorithmic innovations in detail, and discusses their implications in the context of public-key methods currently in use. A first revision to the study has suggested that recent progress (in error correction, for example) has the potential to reduce the number of quantum bits (qubits) required for a specific task. A second revision is planned for the end of 2019. The study, together with an executive summary, can be downloaded from the BSI website at https://www.bsi.bund.de/qcstudie.

### 1.2.9 Exploits Using Modern Processor Architectures

The vulnerabilities published in 2018 that are inherent in the design of high-performance CPU microarchitectures have been characterised and further developed in detail – especially in the academic field. This class of attacks, which are known as transient execution attacks, comprises the Spectre variants Spectre V1, Spectre V2, Spectre V3a and Spectre V4, as well as Meltdown, Foreshadow, LazyFP and SPOILER. While almost all recent models of high-performance processors are essentially susceptible to these kinds of attacks, such attacks tend to focus on the major manufacturers Intel, AMD and ARM.

Transient execution attacks exploit details of the CPU microarchitecture to read information from areas of storage that are technically read-protected. Many of the performance improvements achieved by processors over the last 20 years are based on the principle that commands – even within the CPU core – are not processed at the microarchitecture level in a strictly serial fashion ('out-of-order execution'). As one example, modern hardware attempts to predict the result (jump target) of a conditional branch and therefore executes code speculatively even before the correct target is in fact known. While results from incorrect predictions or unauthorised access attempts are discarded and therefore not committed (execution is transient), they do cause a change in the CPU state at a microarchitectural level – such as the contents of the cache. Under certain conditions, this change can be detected by an attacker – by measuring cache access times, for example – which leads indirectly to disclosure of the protected content.

During the past year, over 20 specific methods utilising these microarchitectural side channel attacks were announced, mostly by academic researchers. Since some of these methods are specific to a particular (micro-)architecture and the attacks are generally probabilistic in nature, widespread exploitation of this class of attacks is particularly difficult. Targeted attacks are certainly plausible, however, especially in a cloud virtualisation context.

One method, dubbed SPOILER, attempts to reconstruct the assignment of virtual to physical storage addresses that is implemented within Intel CPUs, for example. Information gleaned in this fashion can be used in particular to make more effective use of the row hammer effect, a known weakness present in DRAM cells that are used as main memory. Exploits based on this effect involve attempts to make changes to individual bits by repeatedly reading neighbouring memory rows at high frequencies.

So far, monitoring has not indicated that transient execution attacks have been deployed actively in the field, however.

For their part, CPU makers have developed and released countermeasures for the original attack variants that are intended to render such exploits more difficult or impossible. According to information from the company, Intel CPU architectures released from autumn 2018 ('Whiskey Lake' (mobile), 'Cascade Lake' (server)) have hardware protection against the especially critical attack types Meltdown and Foreshadow. For older processors, security updates are available at the operating system level.

Countermeasures at the OS level have also been developed for the attack types Spectre V1 and V2, as well as a microcode update (Spectre V2). Often, however, these are effective only against specific attack variants.
Some of the available countermeasures also involve significant drops in performance that will only be properly resolved in future generations of processors. For the Spectre V1 attack type in particular, no solutions have been identified that are based exclusively on countermeasures in hardware.

The experience gained to date in this relatively young field of transient attacks on CPU microarchitectures tells us that these problems will require long-term monitoring and analysis. Threat assessments now form part of current security analyses and are increasingly being taken into account when evaluating the security characteristics of standardised platforms.

The impact of the class of transient execution attacks on existing systems can be mitigated by installing available updates for applications (and for web browsers in particular), operating systems and microcode. For users, however, no information is typically available about the degree to which applications have specific protective mechanisms suitable for the processor deployed.

As a result of the diversity of the processor architectures affected, obtaining an up-to-date overview of potentially susceptible systems is a hugely complex undertaking. To complicate the matter further, critical security updates may not be deployed automatically despite their availability, or may not be available for every device as a result of high market fragmentation (e.g. for smartphones and for Android-based systems in particular). Potentially significant performance drops after installing all available countermeasures can also be expected, which makes installation unappealing in the first place.

Compared to threats stemming from other malware and exploits, transient attacks appear to be less of a pressing problem, at least outside virtualised cloud applications. Using conventional methods – such as malware or spear phishing attacks – to infiltrate a system also seems to be the most promising kind of attack vector from a long-term perspective.

There is no indication that full mitigation of transient attack vectors will be provided in hardware over the medium term. When designing secure systems, more focus is therefore needed on ensuring that the physical separation between applications and sensitive secrets is both effective and as complete as possible; here, one option is to make greater use of dedicated security components..

# Cyber Security Situation 2019

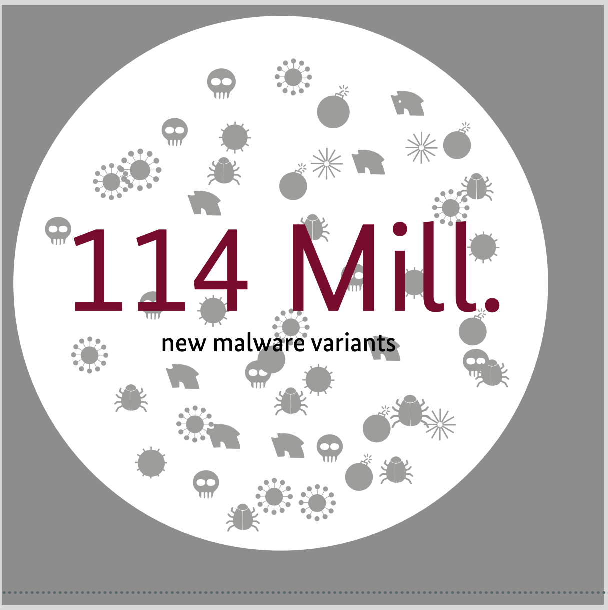
## Action and Reaction

**EMOTET**

Highly efficient social engineering

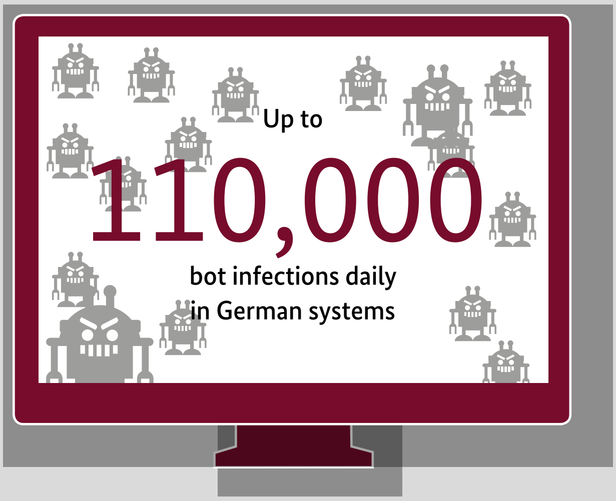
**RANSOMWARE**

Advanced attack techniques lead to massive consequences



114 Mill.

new malware variants



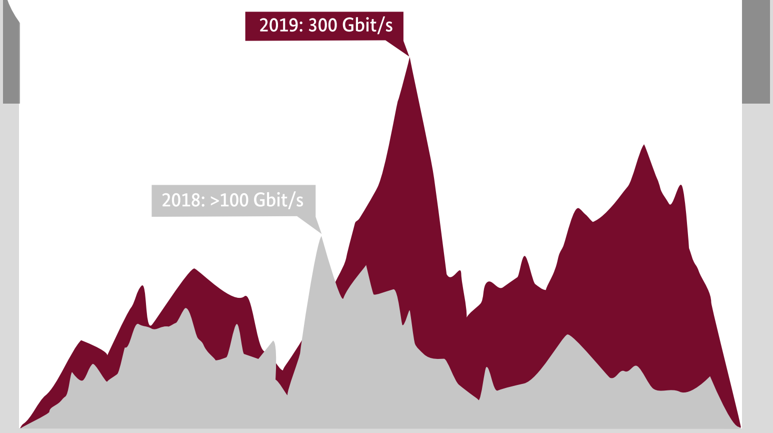
Up to

110,000

bot infections daily in German systems

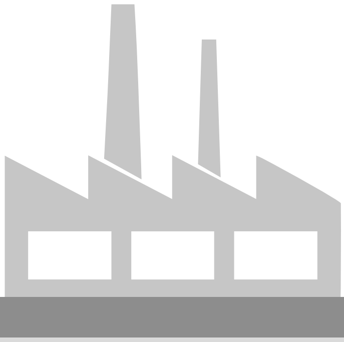
300 Gbit/s

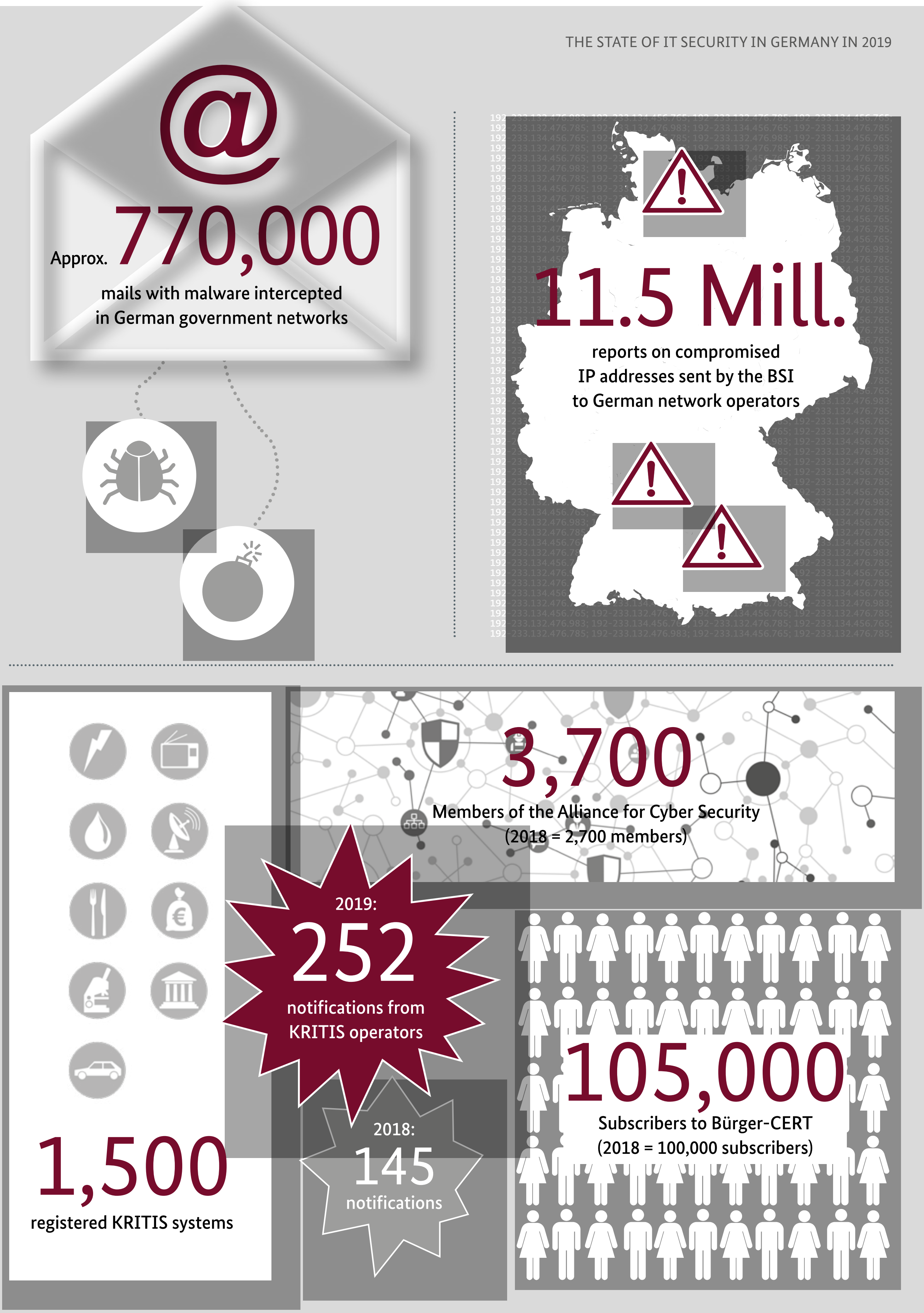
peaks in attack bandwidth reached via the cloud



40 Mill. euros

the damage suffered by a single company due to a Ransomware attack





Approx. 770,000

mails with malware intercepted in German government networks

11.5 Mill.

reports on compromised IP addresses sent by the BSI to German network operators

3,700

Members of the Alliance for Cyber Security (2018 = 2,700 members)

2019: 252

notifications from KRITIS operators

2018: 145

notifications

1,500

registered KRITIS systems

105,000

Subscribers to Bürger-CERT (2018 = 100,000 subscribers)

*Source: Federal Office for Information Security*

# 2 Solutions and Services for Specific Target Groups

# 2 Solutions and Services for Specific Target Groups

This section uses select topics to present BSI solution strategies and services in the context of the current threat landscape for IT security. It focuses on four key areas: the Federal Government/Administration, critical infrastructure/the business world, civil society/private citizens and international affairs/research. Links are included to many BSI publications and the BSI's online presence to enable the practical use of these solutions/services.

## 2.1 Federal Government/ Administration

German public authorities, especially those at the federal level, are an important core target group for the BSI. The BSI offers these agencies many services, which are described in brief below. Public authorities face a growing need for highly secure encryption for the creation, transmission and storage of confidential information. In our digital age, users also expect to be able to communicate quickly and easily using highly secure channels. Information technology and traditional methods of handling classified government information are having to offer each other increasing mutual support. From the technological approaches being developed, opportunities for use are being created that make it possible to deploy IT products designed to protect classified government data in entirely new areas. The BSI provides support for the planning and implementation of highly secure information technology.

### 2.1.1 Threat Landscape for Germany's Federal Administration

Countering threats to the security of the information technology used by the Federal Government is one of the BSI's core tasks. Since its formation, the BSI has fulfilled its specific duty to protect the core networks of the Federal Administration. Alongside the BMI and the Federal Agency for Public Safety Digital Radio (BDBOS), the BSI therefore shares responsibility for the IT security policy applied to the government network.

The federal information security guidelines [UP Bund] define the general and binding conditions for protecting the information processed by the Federal Administration, as well as the IT systems, services and communication network infrastructure it uses. These are to be understood as a set of binding and uniform minimum requirements, and are based on the BSI's standards for IT-Grundschutz (IT baseline security) in their most recent version. These requirements are to be implemented independently by the various departments and for the relevant spheres of responsibility, and expanded to include any other necessary requirements for specific units. The BSI provides support here as required by the BSI Act (BSIG). The BSI also maintains a general overview as the Central Reporting Office and an IT security consulting provider.

The most important measures taken to protect the central government network are end-to-end encrypted communications and a robust, redundant architecture. Efforts are also undertaken to ensure regulated and reliable operations. Network security configurations are also subject to continual improvement, and close links are maintained with the networks of Germany's federal states and municipalities.

The BSI has established a multi-level security system to protect the networks and IT systems as effectively as possible. It encompasses individually adapted and developed measures in tandem with commercial protection solutions. These measures are continuously reviewed, advanced and adapted to changing threat scenarios. By combining these various defensive measures, the BSI maintains a solid overview of the current IT security status across the German government's networks and is therefore in daily contact with the government network operator BDBOS.

#### 2.1.1.1 Insights from the Protection of Government Networks

Cyber attacks on the German government's networks occur on a daily basis. These networks include the Federal Government networks (NdB) and the shared federal/state network. In addition to mass random attacks, government networks are also exposed to targeted attack campaigns.

E-mails containing malware are among the most frequently detected attacks on the Federal Administration. By deploying automated antivirus protection, an average of 64,000 such e-mails were intercepted every month in real time before they reached the recipients' mailboxes. Of these, an average of around 39,000 malicious e-mails were detected each month only by using the BSI's internal antivirus signatures. The sharp rise in these figures compared to the previous year's report can be attributed in particular to the large number of Emotet waves, which were also observed outside the government's networks. As in the previous two years, the practice of sending malware not as a file attachment, but by means of a link in the e-mail is a trend that looks set to continue.

With HTTP traffic, an average of around 750 malware programs were detected and blocked each month in the reporting period, with peaks as high as 2,000 per month.

Downstream from these automated antivirus measures, the BSI operates another system for detecting malware in government network data traffic. This system combines automated testing processes with manual analysis and is particularly suitable for detecting targeted attacks and new malware variants. BSI analysts were able to identify another 6,100 attacks per month on average that could not be detected or blocked by the commercial protection products in use.

Alongside this volume of detected attacks, two million further attempts to connect to servers within the government's network – involving malicious code, fraud or data theft – were also prevented.

### 2.1.1.2 Insights from Federal Administration Notifications

According to Section 4(3) of the BSIG, federal agencies are obliged to inform the BSI immediately if they have information that is important for countering threats to the security of information technology systems. These messages are known as 'SOFORT' ('immediate') notifications. The aim of these notifications is to establish an accurate picture of the current IT security situation in the Federal Administration. As a result, any need for action and the action choices available – both at a federal level and in terms of business practices – can be assessed both quickly and competently.

SOFORT notifications are incident-related and therefore irregular in frequency. In principle, however, the volume of notifications received is another indicator available for assessing the threat landscape.

In 2018, a total of 140 SOFORT notifications were reported to the Central Reporting Office and National IT Situation Centre.

### 2.1.1.3 Insights from Information Security Consulting

The publication of dossiers of personal information about politicians, public officials and people in the public eye at the turn of the year 2018/2019 (see 'Case Study: Doxing'), which received a lot of media attention, once again demonstrates what is possible in terms of the unauthorised disclosure of data and that anyone can be affected – as many indeed have been. The key distinction here is not in the mere publication of information obtained unlawfully, but in the aggregation of this data with publicly available information. This type of information aggregation can help to produce an extensive digital personality and activity profile for an individual, thus enabling or simplifying digital or analogue forms of attack against this person. Identity theft and targeted malware e-mails including highly personal details are just two types of attack that are enabled by the collection and analysis of comprehensive sets of data about an individual. The aforementioned incident shows that private digital identities and personal data must be given even better protection against unauthorised access, and that individuals should act to minimise the volume of potentially sensitive information that they themselves publish. The incident also highlights the fact that persons acting independently are not necessarily protected by an institution's comprehensive and secure information security management system (ISMS), and must thus act in the interests of their own safety.

According to surveys on user requirements and insights from information security consulting work, there is a growing need to extend information security consulting at the state and municipal level. The consulting services provided by the BSI also include activities aimed at implementing the Online Access Act (OZG): these include articles on information security for the portal network's online gateway and other principles for digitalisation projects involving overarching administrative processes at the federal, state and municipal levels. A key focus here is on the procedures to be digitalised, including those required to enable citizens to handle official business online. Accordingly, attacks targeting these procedures could in principle not only impact local government stakeholders as procedure owners, but also damage private citizens and companies as users of the services. Due to the large reach of these services, stringent information security requirements apply for which there is a growing need to provide support and advice. The same also applies for plans to digitalise judiciary services. The BSI

| 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | up to 30/05/2019 |
|---|---|---|---|---|---|---|---|---|---|
| 136 | 138 | 216 | 79 | 149 | 150 | 182 | 157 | 140 | 48 |

**Table 01:** SOFORT Notifications Submitted According to Section 4(3) of the BSIG

provides supportive consulting services to the judiciary, as well, thereby helping to establish and maintain an appropriate level of security.

### 2.1.2 BSI Solutions and Services at the Federal, State and Municipal Levels

How is the BSI meeting current threats, and which countermeasures can be deployed against these risks? This section uses a selection of topics to present an overview of the BSI's IT security solution approaches and services.

#### 2.1.2.1 Cyber Response Centre

The National Cyber Response Centre (Cyber-AZ) facilitates exchange and sharing of information about cyber security incidents among multiple authorities in Germany. Besides the BSI, Cyber-AZ comprises the following agencies as permanent participants: the Federal Office for Military Counter-Intelligence (BAMAD), the Federal Office of Civil Protection and Disaster Assistance (BBK), the Federal Office for the Protection of the Constitution (BfV), the Federal Criminal Police Office (BKA), the Federal Intelligence Service (BND), the Federal Police (BPOL), the Cyber and Information Domain Service (CIR) of the Federal Armed Forces (Bundeswehr) and the Customs Investigation Service (ZKA). Other federal and state agencies as well as public and private enterprises are involved on a case-by-case basis.

As the platform's lead agency, the BSI provided the director, in the premises and the executive office for Cyber-AZ during the reporting period. Spatial and organisational proximity between Cyber-AZ and the National IT Situation Centre/Crisis Response Centre, CERT-Bund and the BSI's Mobile Incident Response Teams (MIRTs), as well as close cooperation with the other participating agencies, ensure efficient collaboration, including in crisis situations.

In addition to sharing information on cyber security situation, collaborative work in Cyber-AZ also has a focus on coordinating responses to individual cyber incidents in Germany, harmonising activities and orchestrating operational measures among the various agencies. This also includes joint developments of recommendations for countermeasures and protective action. Concrete measures are then carried out by the respective specialist units at the participating agencies, each operating within the scope of their individual responsibilities and competence. Results are continuously communicated, consolidated and evaluated in the Cyber-AZ framework, and are reported to other bodies and institutions as appropriate.

Cases of note and notice on which the Cyber-AZ participants collaborated during the reporting period included the unauthorised publication of hundreds of datasets concerning politicians, public officials and people in the public eye (see 'Case Study: Doxing'). Cyber-AZ served as the central platform to consolidate approach, correlate findings and coordinate measures

The reporting period also saw further development of collaborative structures and processes within Cyber-AZ, which will be implemented during the course of 2019.

#### 2.1.2.2 Federal Security Operations Centre (BSOC)

The BSI is observing a continuous increase in the professionalism of attackers, alongside a decrease in the effort required to actually execute attacks. For many years, the BSI has acted to counter this threatening situation by continuously improving measures designed to protect government networks. However, recent attack formats (such as APT attacks) have shown that the typical supplementary and independent detection and countering of cyberattacks are no longer adequate when each public authority acts on its own to protect its own IT systems. In light of its remit as BSOC, the BSI has thus worked to achieve the greatest possible degree of automation by deploying current standard products, in-house developments and AI-driven processes. This has freed up enough resources for indispensable manual analyses, which have served as the necessary basis for the highly successful detection of attacks to date. The BSOC also aims to centrally coordinate the Federal Administration's decentralised detection and countermeasures, which are supplemented by centralised services as part of the Federal Government's IT consolidation work.

The tasks handled to date by the BSI as Bundes-CERT and a centralised Cyber Security Incident Situation Centre for the Federal Government ensure that any attacks detected can be responded to quickly, and even locally (through the Mobile Incident Response Team) if necessary.

#### 2.1.2.3 National Liaison Office and Expansion of Federal-State Cooperation

In the digital era, cyber security policies must be designed by the Federal Government and federal states together in order to be successful. Accordingly, the BSI offers the federal states wide-ranging support and takes any measures necessary to develop cooperation at various levels and realise synergetic effects.

The primary goal of this cooperation is to create an appropriate level of information security within the Federal Republic of Germany. This goal is becoming increasingly important as digitalisation continues to advance within government administration and IT structures become ever more interlinked.

The expansion of the BSI's National Liaison Office is strengthening cooperation with the federal states. Single points of contact for the federal states make detailed discussions possible with states and municipalities on a routine basis. The BSI has posted liaison officers to Wiesbaden and Berlin for this purpose since 2017. Since 2018, region west has also received support from the National Liaison Office from the BSI in Bonn. In early 2019, contacts for the South and North regions were added in Stuttgart and Hamburg, respectively. As a result of the successful pilot run of the National Liaison Office, an additionaldesignated BSI liaison officer was posted to Dresden in May 2019.

As a national centre of excellence for cyber security, the BSI provides the federal states with support in increasing their cyber security. The aim here is to ensure that the federal states are also provided with the BSI's expertise via a number of interfaces. The exact nature of the cooperation is specified in each case in a memorandum of understanding. The first such memoranda were signed at the end of 2017. By the end of the reporting period, the BSI had signed memoranda of understanding with nine federal states. Memoranda with other states are now being prepared for the second half of 2019.

### 2.1.2.4 Evaluation of Implementation of the Federal Implementation Plan

When the new version of the Federal Implementation Plan (UP Bund) entered into force as a guideline for information security in the Federal Administration in September 2017, it offered an opportunity to adjust and modernise the planned annual evaluation of this implementation to reflect new conditions. The primary goal of UP Bund and the associated annual survey on the progress made in its implementation is the continued improvement of information security in the Federal Administration by means of a monitoring process and a targeted, interdepartmental control system. For the redesign of the evaluation, a process-driven approach was therefore selected to enable more suitable analysis and control methodologies for the departments and units within the Federal Administration. One key new feature is that the evaluation is now made on the basis of a maturity model calibrated for these purposes, which gives the current state of development of information security in a given department or unit a step-by-step rating based on the UP Bund specifications. For this purpose, a maturity methodology was used to convert the requirements from the individual sections of UP Bund 2017 into criteria and indicators. The results of multiple evaluations of UP Bund across the various and coordinated reporting periods can be compared using the questionnaire based on the maturity model, which has remained the same throughout. As a result of the development of the maturity levels, short-, medium- and long-term conclusions can be drawn. Individual areas of potential improvement and the measures needed to achieve this improvement can be more easily identified and appropriately prioritised by the maturity model. Supplementary data on a number of specific issues is also collected on an ad hoc basis outside the adjusted maturity methodology. This enables current topics such as the modernised IT-Grundschutz or threat landscapes for the Federal Administration to be included in the annual report without affecting the ability to compare such reports across the various reporting periods. As part of the update process, the conceptual and analytical tool for surveys developed by the BSI (KATE) has been revised in parts, and also adjusted to the technical requirements for data collection so as to enable standardised and automated analysis and control.

### 2.1.2.5 Information Security Consulting

In early 2019, the unauthorised publication of personal data and documents online presented the information security consulting unit with the task of offering affected politicians, public officials and other people in the public eye consulting and support services that needed to go beyond the previous well-established security consulting services provided for the Federal Administration.

Alongside detailed personal and individual consultations provided in person, the security consulting unit worked with other units within the BSI to develop specific, individual packages of measures, as well as recommendations and tips to improve information security for those affected. This included information about appropriate ways to secure e-mail inboxes and user profiles, including those used on social networks. Recommendations for the secure use of messaging and cloud services, the basic hardening of IT devices like smartphones and contact options in the event of an incident supplemented the help offered.

The information security unit also provided support in the reporting period for major digitalisation projects run by public administrators and the judiciary, including work on implementing the Online Access Act (OZG) and the hardening of electronic legal correspondence. In addition to the consulting offered on topics such as the 2021 census, a key role was played in helping the Federal Returning Officer safeguard the European elections. In partnership with the Federal Academy of Public Administration (BAköV), courses offering continuing education for IT security officers in the administration were also continued successfully.

On 15 April 2019, the BSI was reorganised to form a new information security consulting department for federal states and municipalities, primarily to meet an increased need for information security consulting services at the state and municipal levels for specific target groups.

The BSI's information security consulting unit for federal states and municipalities advises and supports state administrations and the three municipal umbrella organisations on questions of information security while focusing on the key topics of information security management, security design and IT-Grundschutz. In this work, the provisions of the information security guideline for public administration (ISLL) and the respective state-specific specifications and requirements must be taken into account. The memoranda of understanding signed with each state are an important part of the basis of the consulting services provided.

The information security consulting unit also works closely with the municipal umbrella organisations. Due to the sheer number of municipalities, support at the municipal level can largely only be provided by adopting a 'train-the-trainer'/bundled approach; here, the roles involved still need to be established in many cases.

Since 2018, the management board of the operative arm of the Information Security Working Group (AG InfoSic) of the IT Planning Council (IT-PLR) has provided the information security consulting unit for federal states and municipalities with a continuous overview of the information security situation in state administrations, as has the unit's own regular cooperation with relevant bodies. As a result, the unit is able to help shape cyber security not only at the federal level, but also at the level of the federal states (and the municipalities).

## 2.1.2.6 Information Security for European and State Parliament Elections

The BSI's information security consulting unit also provided support for the 2019 European elections as part of its strategy to safeguard elections. Working closely and proactively with a working group of federal and state returning officers (Bund-Länder-AG), information security goals were developed that were then put into place to protect the reporting of election day results. The overall aim was to bolster the integrity and availability of the core election process. In this respect, the Federal Returning Officer was advised on information security for the core election process when reporting preliminary results. This was considered at the municipal, federal state and federal levels. A procedure modelled on the BSI's IT-Grundschutz was adopted. Insights gained during the 2017 Bundestag elections were also applied. A further goal was increasing resilience against technical manipulation attempts in a wider electoral context. In this respect, the BSI offered consulting services to political parties and candidates, provided support for the national election cooperation network, monitored and analysed the situation before and during the European elections in its Situation Centre, conducted talks with operators of social media platforms and took part in a 'dry run' for the elections on 5 April 2019. The BSI is also working on establishing a European compendium on cyber security in relation to election technology.

Alongside the EU elections, a further point of focus for consulting was offered by the State Parliament elections in Hesse and Bavaria. Here, the BSI contributed its experience in safeguarding the processes needed to determine preliminary election results. The BSI's work helped to ensure an appropriate level of information security. The insights gained into securing parliamentary elections will also be included in future consulting service portfolios offered by the BSI. The long-term goal of the BSI's activities here is to create a uniform and consistent level of security at all stages of the election process for all parliamentary elections in Germany. This also includes a requirements specification for election software.

## 2.1.2.7 Federal IT Consolidation

The IT consolidation at the federal government level, which was started in 2015 following a Cabinet decision, seeks to achieve the following:

1. Consolidation of the IT operations of Federal Administration offices at a small number of service providers (operational consolidation)

2. Consolidation of the Federal Government's common IT services (service consolidation)

3. Bundling of IT procurement into a centralised IT procurement unit (procurement bundling)

In 2018, clearer signs were seen that the Federal Government's IT consolidation project was having a significant impact on IT governance within the Federal Administration. This resulted from the increasing dependency of government offices on a few centralised IT service providers and the fact that decisions regarding consolidated IT necessarily affect multiple departments.

As part of this IT consolidation project, new committees such as the Provider Advisory Council are therefore being formed to prepare relevant IT steering decisions. In such committees, the BSI offers guidance on matters of information security.

In another development, the BSI is also leveraging its consulting remit to ensure that the future consolidated IT systems in the Federal Administration maintain the information security level achieved to date.

### 2.1.2.8 Public Safety Digital Radio

Since 2010, the public safety and emergency services (BOS) in the Federal Republic of Germany have used a digital radio network for their tactical communication. By deploying the end-to-end encryption system developed by the BSI for voice and short message traffic, a very high level of confidentiality has been achieved for communication within the public safety digital radio network. One of the core elements of the encryption system is the security card developed by the BSI that simultaneously enables access to the digital radio network. There are now over 800,000 of these security cards in use.

The BSI also develops corresponding management systems for security card and key administration. Some of these are operated by the BSI, whereas others are operated by individual customers. This dynamic security architecture offers each user the opportunity to implement their own requirements in terms of operations and the level of security required.

The continued advance of technology will also require continuous further development of these systems. An additional switchover from ISDN to TCP/IP also became necessary as a result of the discontinuation of ISDN connections by telecoms companies.

The BSI's primary tasks in the field of public safety digital radio over the last year were as follows:

- The further development of management systems and their extension to include TCP/IP functionality in particular
- The development of a migration tool that can be used to migrate legacy user data from existing systems while also consolidating and purging this data
- Consulting services and training provided to customers at the federal and state levels, which were carried out in close consultation with the Federal Agency for Public Safety Digital Radio (BDBOS)
- Preparations for further development work on the security cards, which will migrate to a new hardware technology and also offer a new set of functions
- The cryptosystem infrastructure was successfully extended to include IP functionality.

### 2.1.2.9 Technology Verification in Security Labs

The BSI is in contact with numerous manufacturers of information and communication technology and deepens the technical level of this dialogue with 'security labs'. These labs serve as a platform for holding meetings and video conferences with development departments around the globe, and can also be used to pursue more in-depth technical discussions and achieve insights that extend to the perusal of products at the source code level. In this work, BSI employees are supported by experts from accredited testing labs that specialise in code audits, among other areas. Thanks to this close collaboration with development units at manufacturers, trends and risks can be identified at an early stage. From early prototypes to products that are already in widespread production use, the focus of such investigations is always on information security. In this work, the BSI discharges its responsibility for helping to shape information security in Germany. Throughout such collaborations, the BSI is careful to treat all manufacturers equally and to conduct audits using equivalent standards.

### 2.1.2.10 App Testing for Mobile Solutions

Mobile solutions are now increasingly important – not just for businesses and consumers, but also for state actors. Applications on mobile devices extend the functionality provided by the base system and also play a key role in the success of mobile solutions. However, the deployment of apps does present security risks for both the security of the data that an app processes and the security of the overall solution. These security risks must be evaluated in order to be able to make a general statement about the security of a mobile solution.

The app testing service provided by the BSI offers an important basis for decision-making for those in management positions who need to decide whether to deploy an app and under which conditions. This affords the greatest possible flexibility when deploying additional apps that are popular or required in specific cases. The app tests that are performed take into account issues relating to both security and data protection. The test reports also include tips and recommendations for end users about the settings or general conditions that should be considered to ensure the app in question can be used as securely as possible.

Users from public authorities can both access a more wide-ranging repository of past test results for apps already tested and initiate new tests as required. Another option is to have apps tested on a continuous basis so as to ensure that apps previously approved for use can be kept up-to-date.

In June 2019, the app testing service was used by registered users from 40 public authorities and organisations; test results were available for a total of 71 previously tested apps.

### 2.1.2.11 Emission Security

To comply with Section 57 of the VSA (General Administrative Ordinance from the Federal Ministry of the Interior, Building and Community on Material Protection of Classified Information), public authorities must take measures to ensure emission security if information classified as 'VS-VERTRAULICH' ('CLASSIFIED-CONFIDENTIAL') or higher is processed electronically. The BSI has established a tightly integrated test system in order to provide customers with emissions-tested IT hardware on the basis of standard, off-the-shelf platforms. Alongside a series of standardised solutions for typical office requirements, customers can also source and assemble custom solutions for specific requirements from providers accredited by the BSI; they are then accompanied through the approval process. In this way, the BSI awarded a TEMPEST certificate for 524 sets of equipment according to the National Zone Model and 11 sets of equipment for the maximum security level ('Level A') during the reporting period.

Thanks to its extensive participation in international TEMPEST expert committees, the BSI also ensures that international confidentiality requirements remain compatible with national procedures. In this context, the BSI provides active input in the form of technical articles and analyses of state-of-the-art technologies. The BSI therefore helps to shape international standards in a way that safeguards German interests.

### 2.1.2.12 Countersurveillance

The BSI's countersurveillance unit has conducted numerous audits of units within federal and state public authorities that are at risk of eavesdropping, as well as businesses that work with classified information.

Conferences at which classified information was to be discussed were also provided with consulting and auditing services.

### 2.1.2.13 VS Approval

According to the BSI Act (Section 3 (1) Sentences 2, No.7), the BSI is legally authorised to test IT security products as part of its evaluation and to make binding statements with regard to their security standard. This applies to IT security products that are used for the processing, transmission and storage of officially classified information within the scope of the General Administrative Regulation of the Federal Ministry of the Interior, Building and Community for the substantive and organisational protection of classified information (Classified Information Directive – VSA) or at companies within the scope of public administration contracts with reference to classified information

According to Section 51 of the Classified Information Directive (VSA), approval must be provided by the BSI for products that execute IT security functions in order to handle classified information (VS-IT). Section 52 of the VSA listed these security functions inside VS-IT, which are required an approval by the BSI. The application for approval for an IT security product can only be submitted by a governmental user in principle.As in previous years, the BSI again issued or extended over 50 approvals in the reporting period. This increases the number of VSA-compliant products and product versions to 240. An up-to-date list of generally approved IT security products can be found in BSI publication 7164, which is available from the BSI website (https://www.bsi.bund.de/DE/Themen/Sicherheitsberatung/Zugelassene-Produkte/zugelasseneProdukte_node.html).

In order to continue to meet the Federal Administration's need for approved products, the BSI is currently handling more than 60 ongoing procedures seeking approval.

### Qualified Approval Procedure

Using the "Qualified Approval Procedure", IT security products handling classified information up to the level "Restricted" which are designed by a so-called "Qualified Developer" allows to run through the well-defined evaluation activities of the BSI approval process in an efficient and effective manner.Instead of a pure product evaluation based solely on technical aspects, the procedure is supported by the following three pillars:

- Security of the Development-Environment & Process
- Conceptual Product Evaluation
- Substantial complete Developer FA

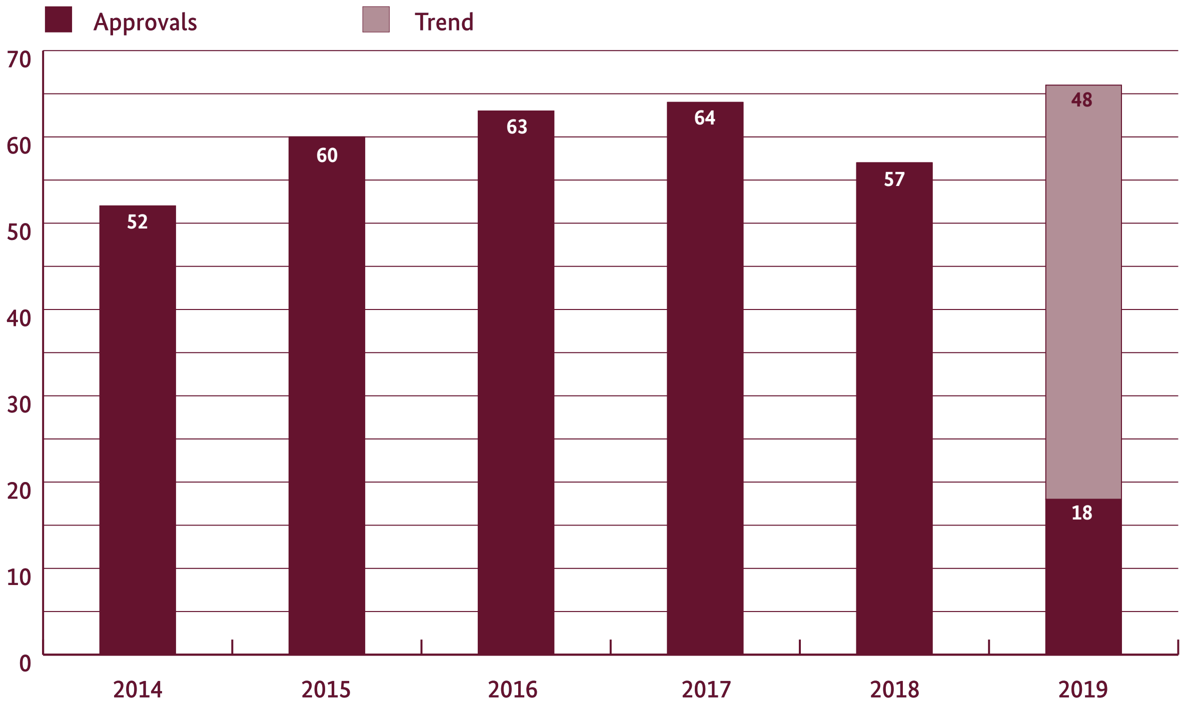


**Figure 11:** Approvals of the past five years

With this approach, products with the classification VS-NfD from qualified manufacturers pass through an efficient, yet effective and well-defined process. In this sense, 'efficient' and 'effective' are understood to mean the capacity to achieve timely evaluation results by means of an optimised and resource-conserving process while also safeguarding the fundamental requirements for the trustworthiness of IT security products.

Since the BSI approved this procedure in mid-2018, it has been possible to use the qualified approval procedure to its full extent within the BSI's approval scheme. The next step is to complete its anchoring within the approval processes and increase the number of 'qualified manufacturers'. The qualified approval procedure has been integrated into the approval processes as follows:

- The standard approval process retains its validity as before and is applied to approvals at the level above VS-NfD, as well as for manufacturers that have not yet achieved qualification.

- As part of the qualified approval procedure, the BSI reserves the right to subject products to the standard procedure even if the corresponding manufacturer requirements are satisfied. The reasons for doing so may include the complexity or the specific nature or features of a product to be approved.

- The structure of the procedure ensures that a seamless transition is possible between the standard and the qualified approval procedure. This is justified in particular by application of the Common Criteria, whereby manufacturer records are available in a manner identical to the standard procedure.

The amount of extra work required for the initial completion of the develper declaration by passing an additional process evaluation is minimal compared to the significant reduction in the effort necessary in the qualified approval procedure. Once completed successfully, all of the subsequent approval procedures for information with VS-NfD classification can be performed using the qualified approval procedure.

Apart from the effort involved, the duration of the qualified approvalprocedure is also significantly reduced. This is because only a conceptual product assessment needs to be completed if the develper is already qualified. The more detailed, more in-depth and iterative assessment applied in the standard procedure (which thus takes considerably longer) is no longer required in the qualified approval procedure.

Overall, the qualified approval procedure therefore enables the demand for approved products to be met much more efficiently. For participating companies, the time-to-market aspect not only offers financial gains from the procedure itself; it also results in better and more secure IT security products, as the procedure is easier to handle and market launches can be scheduled sooner.

Working with developers that are already qualified, it should already be possible to issue a series of further placeholder certificates in 2019. This will enable the BSI to better meet the increased need for approved IT security products, which has resulted in part from the VSA amendment.

## VS requirements profiles

In order to accommodate the rising demand from the Federal Administration for secure IT solutions, the BSI is optimising the approval process. In terms of the processing, transmission and storage of classified information (VS), the creation of VS requirement profiles (VS-APs) for information security systems significantly accelerates evaluation and approval. This is reflected not least in the increasing number of approved VS-IT systems.

VS requirement profiles (VS-APs) describe IT security requirements for specific product classes and types. On the one hand, they are directed at users and operators, such as agencies who want to use products when dealing with classified documents and therefore need the basic requirements to be met by suitable products. On the other hand, VS-APs address manufacturers of such products in order to give them a general technical guideline for the implementation of relevant IT security requirements.

Standardising new basic technical security functions is an important precondition for approving systems dealing with classified information. Numerous governmental users, manufacturers and operators have already been involved in round-table talks to help shape the future-proof design of information security systems in the VS sector.

The objectives for defining VS requirement profiles should meet the following key criteria:

1. Design of information security systems and components for the VS area by the BSI

2. Harmonisation of IT security requirements for certain product classes and types

3. Appropriate determination of contemporary requirements by directly involving users, operators and product manufacturers in the development of corresponding VS-APs

4. Efficiency enhancement of the approval process in the BSI by early provision of relevant VS-APs

In the reporting period, four VS requirement profiles were published, two were revised and a further two were restarted. As a result, the BSI already covers a wide range of product classes for the protection and processing of classified information. In parallel, a large number of VS-APs and national protection profiles (nPPs) for use with VS applications are being prepared for the standardisation of additional IT security products. Details of the progress made in developing requirements for IT security systems to protect classified information can be found on the BSI website (https://www.bsi.bund.de/VS-Anforderungsprofile).

The BSI's decision to involve customers, product manufacturers and operators in the active design of such IT security requirements at an early stage has generated consistently positive feedback and achieved strong participation in the described procedure. In 2019, the BSI's further expansion of the topic of VS requirements profiles has built on the acceptance earned and relevance gained while responding to the increasingly shorter development cycles within the VS market.

## 2.2 Economy/Critical Infrastructure

Networking and dialogue are important factors of productivity and economic growth in Germany, and therefore key elements of driving digitalisation within manufacturing. Intelligent machines are networked to exchange information in real time; production systems coordinate workflows and schedules with each other. This makes production more flexible, dynamic and efficient. However, the many advantages of digitalisation also increase a specific set of risks that stakeholders must be aware of and prepare for appropriately. Most production machinery is connected directly to all the IT systems in a given company and therefore communicates indirectly with employees. This increases the susceptibility of products and businesses to hacker infiltration and cyber attacks. The following section summarises the insights gained by the BSI about the IT security landscape for businesses, as well as services and measures offered by the BSI in this context.

### 2.2.1 Threat Landscape for the Industry/ Critical Infrastructure

Critical infrastructure (CI) comprises organisations and institutions of vital importance to the wellbeing of our society. Their systems and services, such as the supply of water or heat, their infrastructure and their logistics, are increasingly dependent on information technology that must function properly at all times. Any disruption, impairment or even failure due to a cyber attack or an IT security incident can lead to lasting bottlenecks in supply, considerable disruptions to public security and all sorts of other dramatic consequences.

Other commercial enterprises may also become targets of cyber attacks because of their technological expertise, their international activities or simply due to the broad sweep of a particular attack. In particular, the financial consequences of production stoppages, damage to machine pools, patent theft or cyber extortion are what make increased IT security precautions necessary.

### 2.2.1.1 Insights from CI Notifications and Audits

While the threat landscape in relation to critical infrastructure remains serious, no threats were detected in the reporting period that had been designed to target critical infrastructure exclusively.

In this context, cyber security is an asymmetric matter: while an attacker needs to exploit just one vulnerability to cause severe damage to critical infrastructure, operators of critical infrastructure must achieve end-to-end protection for it to be truly effective.

This end-to-end protection for critical infrastructure cannot be ensured merely by adopting technical measures for IT security. Instead, the interplay of technology, organisation and personnel must be considered as a whole.

The importance of **technology** is underlined by reports from CI operators that outages in relation to hardware/ software, especially after applying updates and patches to relevant IT infrastructure, caused problems and even crashes in critical services. The industries most heavily affected here were those whose critical infrastructure is generally to be found within IT rather than operational technology (OT). Typical examples here include the healthcare sector, as well as finance and insurance.

CI operators submit audit records as evidence that they have taken appropriate precautions to avoid disruptions. The BSI's perusal of the audit records received has shown that the implementation of the German IT Security Act and its associated obligations – not merely to implement IT security using state-of-the-art technology, but to provide evidence of this implementation to third parties – has led to an improvement in IT security at CI operators. For example, it is apparent that the auditing process has also improved IT security from an **organisational** perspective as a result of the implementation or modification of an information security management system (ISMS), together with the processes and responsibilities stored in this system. In many of the ISMS setups at CI operators, both an internal and external reporting system for security incidents has been introduced as an additional module. This means that operators are not merely in a position to satisfy their legal obligations to report significant IT disruptions; these reporting structures also make a significant contribution to the overall scenario regarding cyber threats.

The human factor of **personnel** continues to make a major contribution to improving cyber security. Operators of critical infrastructure reported a series of persistent social engineering and spear phishing campaigns during the reporting period. These spear phishing e-mails were often crafted with great care, which is why regular training to raise awareness among employees in CI organisations remains an ongoing requirement. As part of implementing the IT Security Act, CI operators reported that they have established drills to ensure they will be able to act even in a crisis situation. These drills enable the testing of incident handling workflows in a crisis situation. The BSI's Reporting Office is also regularly involved to keep the corresponding communication channels open

### Fraudulent Support Calls

**Situation**

For several years now – including in the latest reporting period – there have been waves of social engineering attacks where criminals have made unsolicited calls and pretended to be support engineers from Microsoft. By repeating a seemingly authentic litany of untrue facts (relating to licence problems, malware infections, etc), callers attempt to convince their targets to reveal personal data or even to give the person calling access to their computer. In the typical attack scenario, these supposed support engineers offer their help, receive access credentials in order to solve non-existent problems and then proceed to install a remote maintenance or remote access tool. Microsoft reported a large increase in fake support calls for the first quarter of 2019. For criminal callers who gain control of a computer in this way, access to the victim's online banking account is a common motive. The successful misuse of online banking accounts by criminals has been confirmed by banks and law enforcement agencies as a widespread phenomenon in cyber crime that results in a large number of victims.

**Cause and impact**

Fake support calls and other social engineering attacks do not require any particular technical skills on the part of the attacker. The weakness exploited is the person called – due to their willingness to cooperate, for example, combined with ignorance of technical matters and new issues related to digitalisation. The large number of incidents suggests that these criminals proceed in a planned and organised manner, and even operate criminal 'call centres'. The misuse of online banking accounts or credit card data can result in significant financial losses for the victims. Financial institutions also have to expend additional effort to investigate cases of misuse and cancel erroneous bank transfers. The overall level of trust in digitalisation itself is also affected.

**Response**

If individuals suspect such an attack, they should change their PC login details and check their online banking accounts and other services. The bank must be notified immediately of any unusual payment transactions and the offence may also need to be reported to the police.

**Recommendation**

Individuals who receive such calls should simply terminate the call. Further recommendations to prevent social engineering attacks are available from BSI for Citizens: https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/IT_Sicherheit_am_Arbeitsplatz/SoEng/Social_Engineering.html

## 2.2.1.2 Insights from Notifications from Commercial Enterprises

Ransomware is a recurrent topic in notifications received from the world of commerce. Vulnerabilities, errors and simple negligence on the part of IT operations and users alike have resulted in far-reaching consequences for businesses thanks to the sophisticated methods used by attackers. Even in cases where backups had been created, businesses suffered losses due to outages affecting networks and systems and to the time required to restore the backups. Data losses also resulted from gaps between the last backup and the time that the malware took effect.

In cases where, despite widespread information and awareness-raising campaigns, no backups were available or they were not adequately protected (and were thus also locked by encryption), the losses suffered ranged from high to devastating. Just the time required to complete a (partial) recovery involves major losses due to the resulting production downtime. In individual cases, this can pose an existential threat to smaller companies.

Based above all on reports and cases from the world of business, the BSI has issued warnings in recent months about various new developments in attack methods.

| Energy | Food | Finance | Health | ITC | Nuclear power facilities | Transportation and traffic | Water | TOTAL |
|---|---|---|---|---|---|---|---|---|
| 29 | 5 | 60 | 47 | 59 | 2 | 41 | 9 | 252 |

**Table 02:** Figures reported in the reporting period 1 June 2018 to 31 May 2019

## EFFECTS OF THE IT-SIG ON IT SECURITY IN CRITICAL INFRASTRUCTURE

The passing of the Act to Increase the Security of Information Technology Systems (German IT Security Act, IT-SiG) in 2015 modified the BSI Act (BSIG) to require operators of critical infrastructure to take ‚appropriate precautionary measures to avoid disruption to their information technology systems, components and processes'; these must also be ‚state-of-the-art' measures (Section 8a(1) of the BSIG). Operators must furnish proof of compliance with this provision to the BSI, unless they are already subject to a similar requirement to submit proof to some other authority – as is the case, for example, with energy suppliers or operators of telecommunications networks (Sections 8a(3) and 8d(2) of the BSIG).

The BSI has now received such records of proof for over 280 critical infrastructures. Their sectoral distribution is as follows:

- Around 150 records from the water sector
- Around 60 records from the energy sector
- Around 35 records from the food sector
- Around 30 records from ITC sector

The sectors of healthcare, transportation/traffic and finance/insurance form a 'secondary tier' within the BSI CI Ordinance. Operators in these sectors therefore do not need to submit their records until later in 2019.

From the records of proof now available and discussions since held with operators, it can be seen that operators of critical infrastructure have begun treating IT security as a high-priority topic. That said, differences in the maturity of IT security models can certainly be seen when comparing industries with one another. In industries where IT security has not played an important part to date, the implementation of the IT Security Act has achieved a comprehensive improvement in the level of security:

- A significant number of operators first introduced an ISMS in order to comply with the provisions of Section 8a(1) of the BSIG.
- In some cases, IT security teams were extended and new IT security officers appointed in the company, or existing employees were assigned dedicated roles for this purpose.
- One common approach was to commission services from external consultants to set up or optimise processes, expand the company's existing knowledge or raise employees' awareness accordingly.
- Technology upgrades were also applied to some CI facilities. In one instance, new control facilities were installed to follow the letter of the law in securing plants with ‚state-of-the-art' systems.
- In general, more money is now being invested in IT security than was the case only a few years ago.

Both operators and their IT service providers, as well as IT security consultants active in these industries, have been building up their expertise and capabilities in securing critical infrastructure, with a particular focus on the availability of critical services.

In regulated industries, the objective of increasing the level of IT security as formulated in the IT Security Act has therefore been achieved. At the same time, IT security is now being maintained at a more uniform high level within the industries themselves.

The targeted collection of postal and e-mail address details – known as 'Outlook harvesting' – can enable the creation of attack (spam) e-mails that look authentic. Malware is also able to read data about contact relationships and even (since the end of 2018) e-mail content from inboxes on already infected systems (see 'Case Study: Be Aware of the Emotet Malware). This information is used by perpetrators for the further propagation of malware in subsequent spam campaigns; recipients thus receive fictitious e-mails from senders with whom they have recently been in contact. Each infected party therefore becomes a threat to their contacts. In the future, technical measures will be required here to prevent infections as broadly and as promptly as possible and, even in cases where attacks are successful, to ensure that the compromising of an individual system does not endanger the entire network.

By deploying techniques previously only seen in the context of state-of-the-art APT attacks, recent forms of malware have been capable of spreading within corporate networks (lateral movement) and thereby achieving large-scale infiltration. By accessing login details and exploiting vulnerabilities in popular network protocols, for example, these malware programs enable attackers to move around independently within an IT network and gain remote access to its systems. When coupled with poorly configured networks, this has resulted in the failure of entire corporate networks. Thanks to their constant adaptation, the malware programs are not initially detected by common antivirus programs and can therefore make far-reaching modifications to infected systems. Attempts to remove malware are typically unsuccessful and also run the risk of leaving parts of the programs embedded in the system. Any previously infected system should therefore always be seen as fully compromised and must be reinstalled from scratch. In several of the cases reported to the BSI, this fact resulted in huge production losses because entire corporate networks had to be rebuilt from the ground up.

In addition, attackers also utilised remote maintenance tools (such as RDP, RescueAssist or LogMeIn) to gain manual access to networks previously infected by automated means and thereby install backdoors on various systems in the victim's IT network. These networks are then examined and evaluated for valuable data or used to 'stalk' other victims. Attackers may also attempt to manipulate or delete any backups they find. As a final step, ransomware is then deployed to computer systems owned by promising targets in a selective and coordinated attack. This sophisticated approach now enables attackers to demand much higher ransom payments from companies than had previously been the case in essentially 'random' ransomware campaigns. Very large Bitcoin payments have been demanded in some cases. Time and again, these have not been 'one-size-fits-all' demands; they have requested very specific sums of money.

Alongside individual companies, IT service providers are also being increasingly affected as attackers try to use their networks to gain access to customers. In one case, it was revealed that the attacker, following an unsuccessful initial ransomware-based demand, then attempted to blackmail the victim by threatening to publish confidential data stolen at an earlier point in the attack. When the victim also refused to make this ransom payment, this data was then in fact published (see 'Case Study: IT Service Provider Blackmail and Publication of Leaked Data').

### 2.2.1.3 Results and Insights from the Alliance for Cyber Security (ACS) Survey

In 2018, malware was the most common type of cyber attack on German companies and institutions, accounting for 53% of the cases. In 90% of the cases, malicious attachments or e-mail links were deployed as lures to unwary users. Technical measures prevented infection in half of the cases of e-mail-based attacks that were successfully thwarted; in the remaining cases, awareness campaigns and employee training proved to be effective and successful.

These are the findings of the most recent cyber security survey conducted by the the Alliance for Cyber Security – an initiative by the BSI. A total of 1,039 companies and other institutions took part in the survey. The cyber security survey for the 2018 reporting period was implemented as an online survey running from 21 February 2019 to 7 March 2019. Invitations to participate were sent out via the BSI's communication channels. A random sample shows that the IT industry is the part of the economy most strongly represented: no fewer than three quarters of respondents were IT security managers in their institutions.

Overall, one in three (33%) of the organisations responding to the survey had been affected by cyber security incidents in 2018, with large companies being more frequently affected (43%) than small and mid-sized firms (26%). Some 87% of those affected by cyber security incidents also

#### IT Service Provider Blackmail and Publication of Leaked Data

**Situation**

In the second quarter of 2019, a German provider of IT services became the victim of a cyber attack. The perpetrators first managed to acquire a set of company-internal and customer data before proceeding to encrypt data held in core IT systems. The IT service provider, not wishing to provide an incentive to other criminals, refused to pay the six-figure ransom demanded. The perpetrators then made good on their threat and published the stolen data on a web server.

**Cause and impact**

IT security incidents can severely damage a company's reputation, which can in turn result in immense financial damage as a result of losing orders or receiving claims for compensation from customers. Also notable here is the novel approach taken by the perpetrators. Previously, perpetrators of ransomware attacks had sought to extort money from their victims, promising to then decrypt the data again. If the payment is not made, the victim suffers a data loss that can be remedied by backups. By publishing previously stolen data, however, the perpetrators have another means of exerting pressure on their victim – even if the latter has usable backups.

**Response**

In this serious case, the IT service provider involved law enforcement immediately in the form of the State Criminal Police Office. Since personal data such as names, telephone numbers and e-mail addresses were also affected by the attack, an incident report was also submitted to the competent State Data Protection Officer in accordance with the EU GDPR, and customers were also notified. The police investigations were conducted by the competent State Criminal Police Office. The incident was also lodged with the National Cyber Response Centre. The BSI used the information provided by the IT service provider to inform affected operators of critical infrastructure; it also asked them to conduct a risk assessment in light of the leaked data. No related disruptions of any kind were reported to the BSI.

**Recommendation**
The specific point of entry into the system was not identifiable in this case. To prevent such IT security incidents in the future, the main thrust of protective measures should be to ensure that the compromising of an individual system – which cannot always be prevented – does not result in losing control of the entire network. This can be ensured by deploying a combination of detection and prevention measures. On the detection side, this includes the use of an antivirus program with signature- and behaviour-based detection mechanisms, the checking of incoming e-mail for malicious code and centralised network-/host-based intrusion detection systems with current signatures and adequate numbers of personnel to perform analysis. In the case of prevention, measures include securing remote maintenance access points and services available over the Internet (web applications can be secured using two-factor authentication, for example); network segmentation, at minimum for office systems, servers and centralised directory services such as Active Directory (including at an administrative level); the use of minimal user rights; the implementation of a whitelist approach for applications (using Microsoft AppLocker on Windows systems, for example); and ensuring that browser use is sandboxed. Advice and assistance is available on the BSI website from the Alliance for Cyber Security (https://www.allianz-fuer-cybersicherheit.de/) and the IT-Grundschutz Compendium (https://www.bsi.bund.de/EN/Topics/ITGrundschutz/ itgrundschutz_node.html).

stated that these resulted in disruptions to operations or outages in 2018. Costs were also often incurred in investigating incidents and restoring IT systems (65% of those affected), and companies suffered reputational damage, as well (22%).

Many companies have already implemented appropriate protective measures. For example, a total of 71% of the institutions surveyed stated that they had a structured patch management system in place in 2018 in order to respond quickly to published vulnerabilities. Around 53% of the companies surveyed also deployed a central management system for mobile device security in 2018. While 72% of large companies had such a system in place, this was the case for only 39% of small and mid-sized businesses.

An information security management system (ISMS) was often lacking, however: only 47% of respondents stated that they had adopted a fully integrated approach to cyber security. While 61% of large companies operated a system of this kind, this was the case for only 37% of small and mid-sized businesses. A full third of the respondents stated that they investigated log files and other records for indications of cyber security incidents in a thorough and systematic fashion. Business continuity management and routine drills are not standard practice, however: in 2018, the proportion of respondents operating a business continuity management system to enable rapid responses to cyber incidents was only 43%. In large companies, BCM systems were operated by 49% of respondents – a significantly higher number than the 38% of small and mid-sized companies operating such systems.

The results of the cyber security survey demonstrate that cyber attacks are now considered to be a serious threat to the success of an enterprise and can cause business losses on a substantial scale. According to the companies and institutions participating in the survey, many protective measures were already put in place in 2018. In this context, raising awareness among employees is just as important as rolling out technical safeguards. By providing suitable information and making practical recommendations, the Alliance for Cyber Security continues to provide support to companies aiming to expand their protective measures for countering cyber threats.

### 2.2.2 BSI Solutions and Services for the Industry and Critical Infrastructure (CI)

The following section summarises the BSI's solutions and services for enterprise customers. This includes information about the BSI's renowned services for certification, IT-Grundschutz, the Alliance for Cyber Security (ACS) and the CIP Implementation Plan, as well as a summary of digitalisation projects in Germany and developments in the field of modern telecommunications infrastructure (5G). It is clear that the BSI is an innovation leader in many areas when it comes to fulfilling its duties in the world of business.

#### 2.2.2.1 Certification

The BSI service portfolio includes a number of certification procedures. Alongside established procedures in the field of product certification, the BSI also offers Common Criteria certification (ISO/IEC 15408). Products can be certified according to the BSI's technical guidelines, as well. In the field of management systems, the long-established IT-Grundschutz (baseline security) standard has also facilitated the certification of information security management systems (ISMS). This procedure is considered in more detail in the following sections.

### Common Criteria certification (ISO/IEC 15408)

When the BSI certifies the IT security of a product, this means that it has been tested by an independent party on the basis of public test criteria in a fully documented process (https://www.bsi.bund.de/EN/Topics/Certification/certification_node.html).

For procurement agents, a BSI certificate provides the following:

- Full documentation of the effectiveness of the product's security features
- A decision-making aid for product usability
- Comparability of the product's security performance
- Conformity with national or international standards

The Common Criteria (CC) test criteria, which were drawn up and maintained by the nations represented in the Common Criteria Recognition Agreement (CCRA, https://www.commoncriteriaportal.org) at the time, have now been adopted by the International Organization for Standardization (ISO). The standard is currently being updated and expanded. The BSI actively participates in this programme together with experts from testing bodies and industry via the German Institute for Standardisation (DIN). The aim is to extend both the concepts for specifying security requirements and the evaluation methodology in order to improve the applicability of the standard to new technologies.

The demand for certified products has also been enshrined in numerous laws and regulations in recent years. This has been true of many of the German Government's digitalisation projects, such as those relating to e-health, sovereign documents and Smart-Metering-Systems, as well as digital signatures for many years. Since mid-2016, the EU member states have been subject to an extended regulation that replaced an earlier EU Directive on electronic identification and trust services for electronic transactions (eIDAS Regulation, (EU) No 910/2014). This regulation also covers the necessary certification for IT products that generate digital signatures. In line with the national Trust Services Act (VDG), the BSI is the public body that verifies the conformity of signature-creating units with the requirements of the regulation. The EU Commission is notified of certificates issued in this context.

The Mutual Recognition Agreement (MRA) on the recognition of IT security certificates in Europe is now actively supported by 17 nations, with Slovakia and Belgium being the most recent signatory parties (https://www.sogis.org). The member nations of the Senior Official Group Information Systems Security (SOGIS) form a strong alliance to promote proof of trustworthiness for IT security products supported by public authorities.

The EU Commission has taken up the issue of certification as part of its efforts to promote cyber security in Europe. The legislative package on cyber security (the Cybersecurity Act), which will also enshrine an EU-wide certification model, has been agreed at the EU level. With SOGIS-MRA, the EU member states already have a strong, well-established certification model in operation which will now form part of the new EU umbrella legislation.

Product certification is being supported by new protection profiles (PP), which describe a standard of security requirements for a particular product type. Examples of new protection profiles applied to product certifications:

- PP for a 'Security Module Application for Electronic Record-Keeping Systems (SMAERS)' – e.g. for electronic till systems

- PP Cryptographic Service Provider (CSP), which describes cryptographic requirements on technical platforms

Product certifications using these new protection profiles have already been submitted and are now being processed.

Manufacturers are now increasingly moving security inspections of development and production sites out of the product certification process and into separate site certification. This streamlines the product certification process and makes it more efficient.

### Certification according to technical guidelines

Functionality and interoperability as product features are described as a standard within the BSI's technical guidelines (TRs) in terms of functional requirements, and can be implemented accordingly. The BSI can then confirm the conformity of an IT product or system to a TR by issuing a certificate.

In the course of this procedure, a conformity test is carried out by a neutral testing body on the basis of the test specifications defined in the TR. The test is monitored by the responsible certification body within the BSI and confirmed on completion with a notice of conformity and a certificate. For some TRs, certification is handled by the German National Accreditation Body (DAkkS).

### ISMS certification according to BSI IT-Grundschutz

In addition to product certification, certification of management systems is also offered based on the commonly used certification according to ISO/IEC 27001. It is carried out on the basis of IT-Grundschutz, the baseline standard developed within the BSI. The IT-Grundschutz procedure and the recommendations for standard security measures contained in IT-Grundschutz now represent a de facto standard for IT security.

### Other certifications

The BSI is the accreditation and supervisory body for De-Mail providers, whose services offer an infrastructure for legally compliant electronic communications in Germany. The following accredited providers have been active in the market since 2012: Mentana-Claimsoft GmbH, Telekom Deutschland GmbH, T-Systems International GmbH and 1&1-Mail GmbH.

European Citizens' Initiatives (ECIs) need to collect one million statements of support and reach the minimum levels in at least seven member states in order for the European Commission to decide on whether it will take action. In order to collect statements of support via the Internet, organisers must make an online collection system available on their website that complies with the technical specifications set out in Implementing Regulation (EU) No. 1179/2011. They must then have their system certified by the relevant authority. The BSI is the national authority responsible for issuing certificates of compliance with the ECI Regulation (Regulation (EU) No. 211/2011) for online collection systems.

## 2.2.2.1.1 Further Development of Testing Standards

The testing standards developed by the BSI in the form of technical guidelines typically describe products – specifically, IT products – that are nowadays subject to short innovation cycles. In following the laws of the market economy, manufacturers and sellers of such products seek to develop new products or improve existing products as a continuous process in order to encourage consumers to make a purchase.

As a corollary, however, existing standards that describe such IT products must also be continuously developed in order to take into account the modified or new functionality included in IT products. Alongside the actual standard that defines the functionality of a given IT product in the form of specifications, the product test standard must also be revised. As a final step, test cases must be adjusted in or added to the test standard in order to match the modified functionality; otherwise, new test cases must be defined.

A new test standard can only be applied as the basis for new certifications once it has been published. Consideration must also be given to the fact that testing bodies that test IT products as part of certification according to technical guidelines may also need further qualifications in order to test the modified or new functionality contained in such products.

## 2.2.2.1.2 Certification in Figures

As part of CC certification work conducted by the BSI, a total of 119 certificates were issued in the reporting period in the nine product categories (Operating Systems, Digital Signature, Digital Tachograph, Healthcare, Sovereign Documents, Smart-Metering-Systems, Network and Communications Products, Server Applications, and Smartcards). Alongside initial certification, follow-up certification was also provided following product modifications.

In addition, 55 certificates were issued according to technical guidelines from 15 testing categories, with 33 of these being initial or re-certifications and 22 being maintenance procedures.

In the context of IT-Grundschutz, a total of 37 'ISO 27001 Certificates for IT-Grundschutz' were issued, with 74 surveillance audits also being conducted in the reporting period.

Three certificates for online collection systems were also issued.

## 2.2.2.1.3 Certification in a European and International Context

The BSI enjoys a solid reputation internationally with regard to the Common Criteria. This stems from the BSI offering its expertise to technical working groups of the two agreements on the recognition of IT security certificates, namely SOGIS-MRA and the Common Criteria Recognition Arrangement (CCRA). In these working groups, the BSI contributes its knowledge of topics such as cryptography, embedded device security and chip security. In addition, the BSI supports the Common Criteria Users Forum (CCUF), an expert group of Common Criteria users, with its expertise in the fields of cryptography, operating systems, databases and encrypted

USB pen drives. The BSI integrates the findings from these international working groups into its standardisation work.

Alongside its work in the multilateral agreements, the BSI is currently preparing a bilateral certificate recognition process with France; these certificates will be issued on the basis of a penetration test. The aim here is to bring additional European certification bodies on board alongside the mutual recognition of CSPN ('Certification de Sécurité de Premier Niveau') certificates from the French ANSSI and the BSI's own 'Accelerated Security Certification' (BSZ) certificates, and to integrate these into the new European certification framework as a certification scheme.

### 2.2.2.1.4 International Committee Work

The new European cyber security legislation (the EU Cybersecurity Act) introduces a certification framework for the cyber security of products, procedures and services that applies throughout the EU. In close collaboration with the Federal Ministry of the Interior, Building and Community (BMI), the BSI has contributed its expertise in the field of IT security certification to the legislative plans of the European Commission. This background work is a precondition of the BSI's future ability to shape IT security from a German perspective by means of standardisation and certification. Currently, the BSI is making all the preparations necessary to ensure the SOGIS (Senior Officials Group on Information Security) agreement is the first certification scheme to be migrated to the new European certification framework.

Alongside activities focused on the Cybersecurity Act, the updating of Common Criteria within the International Organisation for Standardisation (ISO/IEC 15408) is strongly influenced by the BSI's involvement.

### 2.2.2.2 Digitalisation Projects in Germany

The BSI is a neutral and independent centre of excellence for the IT security of all government departments, and therefore plays an interdepartmental role in digitalisation projects run by these departments. Some examples of the support offered to departments include IT security consulting (all departments), the electronic health insurance card (BMG), Smart-Metering-Systems (BMWi) and autonomous driving (BMVI). The BSI's cooperation with other departments on questions of IT security is an elemental part of designing information security in connection with digitalisation.

### 2.2.2.2.1 Smart-Meter-Gateway Certification

On 20 December 2018, the BSI issued the first certificate based on the protection profile for the Smart-Meter-Gateway at the Federal Ministry for Economic Affairs and Energy. The product was developed by Power Plus Communications together with OpenLimit SignCubes. Apart from providing a record of compliance with security specifications, the certification procedure also considered the manufacturer's production and development processes, as well as the supply chain for the devices.

The Smart-Meter-Gateway, which is the key technology for the digitalisation of Germany's energy transition and the smart grid, guarantees data protection and data security at the highest level. It provides stakeholders – from the network operator to the electricity supplier and on to the consumer – with information about generation and use.

With the help of the smart grid, the wind- and solar-dependent power grids of the future can be managed as intelligently as light and heating within our buildings. The Smart-Meter-Gateway is therefore a cornerstone of the intelligent and secure smart grid of tomorrow. The 'mandatory rollout' will start once at least three entirely independent manufacturers have successfully completed the certification procedure and three Smart-Metering-Systems, which are fully compliant with legal requirements, are offered on the market.

### 2.2.2.2.2 Energy Transition

On 31 January 2019, the BSI published the first market analysis according to the Metering Point Operation Act (MsbG). This market analysis in line with Section 30 of the MsbG documents progress made in implementing the BSI standards, as well as in applying the requirements of weights and measures relations, for the whole value chain of metering equipment: Smart-Meter-Gateways, gateway administrators and backend systems on the market. The infrastructure necessary for the secure operation of Smart-Metering-Systems (smart meter gateway administrators and smart metering public key infrastructure) is now available in full. As only one smart meter gateway has been certified to date, the BSI is not yet able to determine the technical prospects for a mandatory installation rollout.

At the same time, the technical minimum standards for Smart-Meter-Gateways also need to be continuously developed. To meet the growing requirements resulting from the energy transition and cyber security, the Federal Ministry for Economic Affairs and Energy and the BSI published a joint paper entitled 'Standardisation Strategy for Sector-Neutral Digitalisation According to the Act on Energy Transition Digitalisation' on 29 January 2019. This roadmap provides a definitive task list for the further development of the Smart-Meter-Gateway into the communication platform for the energy transition. The roadmap also provides stakeholders with help in implementing the legal requirements, and includes worklists and schedules that are being continuously developed in dialogue with affected industries and public authorities.

### 2.2.2.2.3 IT Security in Cooperative Intelligent Transportation Systems (C-ITS)

In early 2019, the European Commission submitted a draft for a delegated act concerning cooperative intelligent transport systems (C-ITS). This is intended to establish the foundations for the introduction of services based on vehicle-to-vehicle and vehicle-to-infrastructure communication. The security of this communication is an important point of focus for the envisaged legislation. The delegated act includes detailed provisions for establishing a European public key infrastructure (PKI) for intelligent traffic services. The certification of the components used in the vehicles and in the traffic infrastructure for the services according to Common Criteria is also envisaged.

The BSI advised the BMVI in relevant preparatory work and was also involved in consultations concerning the delegated act itself.

### 2.2.2.2.4 Electronic Identity (eID): EU-Wide Recognition of Germany's National eID Card

The reliable identification of people and things is crucial in the context of digital transformation. Therefor, with regard to the digital transformation of the European Single Market, the eIDAS Regulation (EU) 910/2014 established in 2014 a framework for the mutual recognition of electronic identification means and trust services at the EU level.

With the intensive assistance of the BSI, Germany successfully completed the notification process in 2017 being precondition for the EU-wide mutual recognition of the eID function of the German national ID cards and electronic residence permits as the first member state at all. Since the end of the transition period one year after the publication of the notification in the Official Journal of the EU – at the highest level of assurance according to the eIDAS Regulation – the mutual recognition obligation entered into force in September 2019. Since that, all EU/EEA member states must recognise the German eID function in public-sector applications, i.e. in the context of e-government.

Until April 2019, in total 14 EU member states (Austria, Belgium, Denmark, the Czech Republic, Estonia, Finland, Greece, Luxembourg, Malta, the Netherlands, Slovakia, Slovenia, Spain, and the United Kingdom) and the European Commission had successfully integrated the German eID function into their eID infrastructure supported by the BSI. As a result, it is possible to use the German eID function in the familiar way for online services in already almost the half of all EEA member states. With another 11 countries (as of April 2019) now conducting tests, this coverage is expected to expand further.

Also other countries are working on notifications of their eID schemes. After Germany, in 2018, eight other member states also completed their notification processes (Belgium, Croatia, Estonia, Italy, Luxembourg, Portugal, Spain, and the United Kingdom). Furthermore, more eID schemes are currently in the notification process or nearly completed. The BSI actively contributes its technical expertise to these notification processes.

The eID schemes in use in various countries differ considerably. While most of the ID systems already assessed do in fact base on the national chip card-based ID documents, one eID scheme is based on certified SIM cards. Another approach is even using multiple so called identity providers that are partially organised as private enterprises and offer multiple types of identification means (app OTP, SMS OTP, etc.) at the same time.

These varying approaches naturally lead to a variety of outcomes of the peer reviews that are part of the notification process. While the chip card-based eID schemes had generally been assessed with the highest level of assurance, systems based on the usage of VideoIdent or SMS OTPs have previously only been assigned to a substantial level of assurance.

With the support of the BSI, also the preparations for the recognition of the other notified electronic ID schemes in German e-government are ongoing. As a result, Germany is well prepared for of the start of the recognition obligation according to eIDAS in September 2019.

### 2.2.2.2.5 eHealth and the Electronic Health Insurance Card

The example of the electronic health insurance card (eGK) in conjunction with the expansion of telematics infrastructure (TI) demonstrates how advancing digitalisation and the increasing networking of service providers in healthcare can be targeted to improve the efficiency of the care provided to patients while also increasing their safety. One current focus here is on the development and forthcoming deployment of new applications, such as emergency data management (NFDM), the e-medication plan in conjunction with the safe use of medicines (AMTS), and the electronic patient record (ePA). The groundwork here is now complete.

On the basis of specifications from the Gesellschaft für Telematikanwendungen der Gesundheitskarte GmbH (gematik), the BSI has drawn up a set of technical guidelines (TR 03154, TR 03155, TR 03157). These are intended to help ensure that the BSI-certified connectors for interfacing with TI – which are equipped with the basic functionality available to date and are currently in use in doctors' practices and hospitals, among other locations – can now be reliably extended to include new functions. As a result, information required in the event of a medical emergency and in e-medication plans can be stored securely together with the eGK and is ready for use as needed. In the case of an e-medication plan, patients prescribed new medicines can have these compared against their existing medication by the attending doctor so as to identify any harmful interactions and reduce any potential risks.

As a further step, patients who have public health insurance can access an electronic patient record in addition to the previous functionality available together with their eGK. The German Appointment Service and Care Act (TSVG), which was adopted by the Bundestag on 14 March 2019, requires public health insurers to offer their policyholders these kinds of electronic patient records by 2021 at the latest. Once consent has been sought from and given by the insured party, attending doctors or hospitals can be given secure access to the respective record so as to store or browse through the patient's corresponding medical data. The precondition here is a connector certified by the BSI and enhanced with a corresponding technical module.

This enables medical treatment plans issued by different practices to be coordinated with one another while potentially also avoiding stressful multiple medical exams for the patient. Insured patients are to have the ability to access their medical records on their own devices (PCs or smartphones/tablets for mobile use) in conjunction with application software approved by gematik and certified by the BSI.

### 2.2.2.2.6 Two-Factor Authentication

Secure authentication is required in many areas of electronic business processes, from online shopping to home banking. Up to now, single-factor authentication has usually been the method of choice, which typically relies only on the user having to know one password. This has several disadvantages:

- First, possession of this one factor is sufficient to crack the authentication mechanism.
- Second, it is extremely demanding for users to have to think up and memorise a secure and unique password for each service.

Passwords continue to be the method of choice for online authentication by a wide margin, even though they do not offer a sufficient level of security in many scenarios. The same, easy-to-remember password is often used with many different service providers. However, this shortcut does not only make it easier for the authorised user to access the service. If an attacker has gained access to passwords from one service provider, they can then utilise this stolen data to gain unauthorised access to other service providers.

This is where secure two-factor authentication can help with  two factors being used for authentication instead of one. The factors must be sourced from different categories (physical possession, knowledge, biometrics). Combining the strengths of these individual factors makes attacks much more difficult. In the process, biometric features should not be stored at the service provider, but used locally to unlock e.g. a smartphone, which then proves physical possession by applying cryptographic methods to authenticate itself to the service provider.

Secure two-factor authentication solutions are still not widespread. The Fast IDentity Online (FIDO) Alliance was formed in 2013 by a large and diverse group of stakeholders with the aim of developing open and licence-free industry standards for worldwide authentication online. FIDO has resulted in three standards being developed to date:

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

However, proof of the security of the FIDO authenticator used is necessary to ensure secure implementation of the protocols within products. As a member of the FIDO Alliance, the BSI is involved in the definition of verifiably secure authentication tokens. Evidence of a high level of security can be provided by Common Criteria certification. The BSI published a protection profile with high assurance level for secure FIDO U2F tokens, which has been used to successfully evaluate a FIDO U2F token developed by the BSI. The BSI is currently creating a modular protection profile containing all of the variants and implementation options from FIDO authenticators so that these can be certified according to a uniform protection profile.

### 2.2.2.2.7 Technical Security Device for Electronic Record-keeping Systems

As part of the digital transformation, the electronic recording of business transactions – such as cash register operations – is now more frequent. As a result, the technical challenges for tax audits have changed radically because subsequent manipulations of electronic records can be practically undetectable if appropriate safeguards are not used.

To counter this kind of tampering, electronic record-keeping systems in Germany will need to be protected by a certified technical security device as of 1 January 2020, according to the Fiscal Code of Germany. This device is contacted by the electronic recordkeeping system, proceeds to handle the storage of the data to be recorded and files the secure records using a standardised format. The technical security device is also equipped with a security module that ensures that records cannot be made illegible, erased or created anew at a later point in time without those actions staying unnoticed.

The new piece of legislation explicitly does not restrict the technical security device to be designed in a certain way and therefor encourages manufacturers to provide a variety of customised solutions to the market. A standardised digital interface simplifies integration with existing and future electronic cash register systems. In particular, no special requirements for the corresponding physical interface are planned for the digital interface; common standard interfaces such as USB, Ethernet, and microSD cards can thus be used. To complement local security devices, scalable solutions have also been planned right from the start by the security module's optional client/server architecture. These solutions could be deployed in branch locations or be part of online services.

The technical requirements and testing standards for the components used in the technical security device have been specified by the BSI in technical guidelines and protection profiles. These were finalised and published in agreement with the relevant associations and manufacturers in 2018, exactly as planned.

The BSI has also being actively supporting the certification of a technical security device for use in electronic cash registers since autumn 2018 as part of the ZERSIKA project.

This allows for a sufficient period of time to develop technical security devices and bring them to market.

### 2.2.2.2.8 Secure Electronic Identities on Smartphones

Today's consumers use their smartphones to connect to a large number of services requiring a high level of security: they can unlock the doors of car-sharing vehicles, grant access to bank accounts or report a change of address to a city's administrators. All of these require a sufficiently high level of security. Alongside logins and registration with service providers, the secure electronic identity (eID) can also be used locally with near-field communication technology (NFC). In this case, the user holds the mobile device next to another object with an NFC chip, such as a hotel room door handle. This makes it very easy to use the eID.

The OPTIMOS 2.0 project, which the BSI has been part of since August 2018 as an associate partner, is working to define the requirements for supplying new technologies for secure eID services. These technologies will enable providers to offer mobile eID services at the 'Substantial' and 'High' security levels in accordance with the eIDAS Regulation. The ecosystem developed in the project is to be notified by the EU at the 'Substantial' security level and therefore made usable anywhere in Europe.

Providers of mobile services can benefit from the open ecosystem if they are looking to store other kinds of sensitive data on the smartphone alongside the eID: airlines could store boarding cards, transport companies could store a personal annual pass, and car-sharing companies and hotels could store digital vehicle or room keys. Securely storing this application-specific data on the customer's smartphone has previously presented each service provider with a complex challenge, not least because the wide variety of smartphone models and mobile network providers means hardware is extremely diverse.

The publicly funded OPTIMOS 2.0 project is creating a platform that spares service providers the complex part of the process while simultaneously enabling a high level of hardware-based security.

### 2.2.2.3 Modern Telecommunications Infrastructure (5G)

In summer 2018, 5G developed from an insider topic for mobile network aficionados into a subject of public debate. The aspect of security – both the security of important information threatened by unauthorised access and the security of supply in terms of centralised telecommunications infrastructure – remains part of this discussion today.

The security of German mobile networks has a clearly defined legal basis which is set out by the Telecommunications Act (TKG). Section 109(6) of the TKG specifies that the German Federal Network Agency, working with the BSI and the Federal Commissioner for Data Protection and Freedom of Information, should create a catalogue of security requirements that is also definitive for the operators and suppliers of the 5G networks, and which can be continuously updated to reflect the latest technical developments. The latest revision of the security catalogue, which was announced in March 2019 through the publication of its key topic areas, took place around the same time as the start of the auction for the first German 5G frequencies. On this basis, the BSI should, as a national cyber security agency, be given responsibility for testing network components to verify their objective security properties. As a result, recognised proof of security for security-relevant components in mobile networks is now mandatory for the first time since the start of modern mobile telephony in Germany in 1992. The German 5G networks will therefore be set up from 2020 according to much more stringent security criteria than was the case for the older mobile networks (3G and 4G).

The fact that 5G is perceived by the public as a challenge in terms of its security is not surprising given the complexity of not only the technology itself, but its interplay with current second-, third- and fourth-generation networks, as well. The introduction of 5G will also see the resolution of a number of vulnerabilities known to have existed for a long time in previous technologies. These innovations include improved cryptography, improved roaming and comprehensive measures to secure signalling procedures among different mobile networks.

While the new technology is popularly referred to as the '5G network', the mobile network of the future should rather be seen as a modular system in which services and structures with very different properties can be implemented simultaneously. One of the more obvious changes is the opportunity to acquire a geographically limited licence for the use of 5G frequencies. Many German commercial enterprises have already announced an interest in doing so. The implementation of separate virtual networks within the public infrastructure will also be possible. As part of 'network slicing', virtual networks or services can also be designed to offer low latencies or a high level of security. As a result, security is not an exclusively global property of the entire network that is identical regardless of how the network is used. Instead, the security level can be adjusted individually to even higher requirements when necessary.

The introduction of the 5G mobile network standard has the potential to develop into the biggest infrastructure project for the coming decade and establish the digital transformation of government, business and society on an entirely new basis. The BSI has accompanied this process from the outset. It is one of few state organisations worldwide that is a member of GSMA, the mobile network industry's leading umbrella organisation, and will use its close ties here in a constructive manner.

### 2.2.2.4 IT-Grundschutz Profiles and Attestations

For the last 25 years, IT-Grundschutz has been a long-standing service from the BSI that aims to improve information security within institutions. This comprehensive portfolio includes recommendations and requirements for all issues related to information security. These services are aimed not only at users first tackling IT-Grundschutz, but also at advanced users at companies and public authorities. The BSI standards provide basic knowledge of methods and procedures. The modules from the IT-Grundschutz Compendium can then be worked through in a targeted manner in order to improve the status of information security within an institution.

IT-Grundschutz profiles offer sample security models to make it easier to understand the concepts of IT-Grundschutz. These profiles also help users to take their first steps towards setting up an information security management system (ISMS) and drafting a security policy. An IT-Grundschutz profile is a template that represents a reference architecture for a specific use case.

Since the introduction of the IT-Grundschutz Profile system last year, several institutions and associations have been working with the BSI on the creation of initial IT-Grundschutz profiles. The first IT-Grundschutz profiles have also been published on the BSI website and can be utilised for internal security assessments. These include:

- Chambers of trades
- Tradespersons
- Shipping lines (onshore operations)
- Local authorities

IT-Grundschutz profiles are now being created for other industries. Users who are thinking of creating an IT-Grundschutz profile for their industry are invited to contact the BSI. In the long run, the aim is to publish IT-Grundschutz profiles on as many topics and for as many industries as possible so that other users can make use of these proven and practicable guidance documents.

The Basic Protection procedure from IT-Grundschutz can be used by an institution as an entry-level methodology for setting up its ISMS. Here, the security assessments focus on the Basic Requirements from the IT-Grundschutz Compendium, which offer a basic and initial level of protection across all business processes. These can be implemented with comparatively small amounts of time, money and human resources. As a result, Basic Protection is suitable for SMEs or smaller municipal authorities that want to pursue an integrated approach to setting up an ISMS.

Companies and public authorities can use a Basic Protection attestation to prove that they have implemented IT-Grundschutz in accordance with this level of protection. With a Basic Protection attestation, an institution can prove that it has safeguarded all of its business processes, activities, data and components within the information domain assessed to a minimum level of information security while considering aspects relating to systems, infrastructure, organisation and human resources.

The Standard/Core Protection from IT-Grundschutz refers to the procedures that should be pursued to protect an institution appropriately and comprehensively according to the technical state of the art. These also make it possible to acquire an ISO 27001 certificate on the basis of IT-Grundschutz.

### 2.2.2.5 Implementation of the German IT Security Act (IT-SiG) and the CIP Implementation Plan

The German IT Security Act (IT-SiG) has introduced new duties for CI operators in the BSI Act and other legislation. For CI operators, the BSI Act now sets out measures for the prevention (Section 8a) and management (Section 8b) of IT security incidents.

#### IT-SiG implementation status

In order to implement Section 8a(1) of the BSIG, CI operators must “take appropriate organisational and technical precautions to avoid disruptions.” They must keep up with technical developments and can also develop industry-specific security standards (B3S) to do so, which the BSI audits for suitability on request. Over 20 CI operators have now created B3S or are in the process of doing so. Ten of these have already been successfully audited for suitability by the BSI.

In the reporting period, the BSI confirmed suitability for B3S from the following industries:

- Food
- District heating
- Insurance
- Laboratories (medical)
- Electricity

Operators must also have the implementation of the state-of-the-art technology in their systems audited in accordance with Section 8a(3) of the BSIG; the BSI receives these audit records.

Since 2015, critical infrastructure operators have set up the reporting system according to Section 8b of the BSIG together with the BSI. They have registered over 1,500 CI systems with the BSI so that these can be provided with warning notifications from the BSI. At the same time, operators report major security incidents to the BSI so that it can use this information to create a detailed picture of the situation and warn other operators.

The BSI receives many enquiries about implementing the provisions of the IT Security Act. The BSI has published guidance on creating B3S and also on the subject of security audits. The guidance for security audits and the forms for submitting audit records have now been revised. Version 1.0 of the guidance on the content and requirements for industry-specific security standards (B3S) according to Section 8a(2) of the BSIG is still available. The BSI also regularly updates its FAQs on issues related to the BSI Act, which are made available on the BSI website.

### Cooperation in the CIP Implementation Plan ('UP KRITIS')

For the cooperative implementation of the new requirements from the BSIG, operators and public authorities make use of the CIP Implementation Plan (http://www.upkritis.de), the public-private partnership between CI operators, their associations and the government. Here, the B3S are developed in joint working groups, for example, while insights and ideas about reporting and submitting proof of cyber security drills are also discussed.

As a platform for issues affecting the operators of critical infrastructure, the CIP Implementation Plan has received a mandate from the BMI. The CIP Implementation Plan is intended to be a participatory institution that is also consulted for regulatory projects and other matters affecting the critical infrastructure sector as a whole. At the same time, this mandate also offers operators a way to formulate their requests to public authorities.

### Services from the IT-SiG: warnings and situation reports

As a result of the 2015 German IT Security Act, the BSI has also acquired new duties alongside its new powers. According to Section 8b(2) of the BSIG, the BSI is tasked with analysing all of the available information on the IT security situation, updating this situation map on a continuous basis and providing operators of critical infrastructure with information that affects them.

These notifications are issued using a variety of BSI products, such as cyber security warnings, BSI management information, topical situation maps and monthly reports.

In the reporting period, over 60 ad hoc warnings and notifications of circumstances with special relevance were sent or made available, alongside 21 situational products and reports for various target groups, in order to provide a general picture of the IT security situation.

One important source of information for the generation of warnings is the reports from CI operators about IT disruptions. If the BSI is informed in good time about existing IT disruptions, it can warn other operators and provide them with recommendations. These operators can then promptly introduce suitable defensive or protective measures to appropriately secure their facilities.

In addition, the BSI has also discussed specific exchange formats and platforms such as the Malware Information Sharing Platform (MISP) for technical signatures and parameters with a number of operators of critical infrastructure. A number of models are now in preparation for exchanging operational information with larger groups in the future. The first of these are likely to be offered from mid-year 2019.

### Incident support and MIRT

The BSI provides support for serious IT security incidents to affected parties, especially its various target groups in the Federal Administration and critical infrastructure sectors. This support ranges from initial, phone-based advice with guidance about help and services available from the BSI to detailed phone or videoconferences, which are repeated as necessary and attended by various experts of the affected party. It also includes dedicated on-site assistance provided by the BSI's Mobile Incident Response Teams (MIRTs). The level of support provided is always adjusted to the requirements and needs of the affected party. The aim in all cases is to determine the depth and extent of an attack, prevent its spread, and work with the affected party to decontaminate the IT infrastructure and harden it against reinfection. The BSI was able to contribute its experience and specific recommendations for action for a range of cyber crime attacks and malware incidents of varying degrees of severity. While the field of cyber crime had been characterised by broad-based and opportunistic attacks until only very recently, perpetrators are now also deploying techniques previously observed primarily in the context of targeted attacks (APTs). Such techniques include connecting manually to infected systems, for example, as well as the active use of malware or administrative tools to spy on victims in order to estimate the 'value' of a potential extortion attempt, to achieve lateral movement and trigger propagation in the internal network, or to take over centralised IT systems such as Active Directory servers.

In analysing attacks and providing on-site support to affected parties, the BSI, as part of the National Cyber Response Centre, works closely with other security agencies at the federal and state levels. This enables affected parties to be addressed and advised as a group, while the continual exchange of information between stakeholders makes sure that intelligence is both shared and up-to-date. To protect the interests of affected parties, this advice and assistance is always provided in the strictest confidence. Only rarely do affected parties publicise the fact that they were affected, along with details of how the attack was handled. Once they are sanitised of actual details about individual affected parties, the BSI can nonetheless derive abstract information and recommendations from these incidents. This material is then provided via the existing platforms for information exchange to other potential targets or victims of potentially similar attacks on the Federal Administration, critical infrastructure or the business sector.

### 2.2.2.6 Alliance for Cyber Security

In 2012, the BSI launched its Alliance for Cyber Security, which consists of a free portfolio of services for companies and institutions based in Germany. Since then, a large number of organisations – particularly (but not exclusively) small and mid-sized enterprises – have benefited from its cyber security recommendations, training courses and events for the mutual exchange of information.

The Alliance for Cyber Security now has over 3,700 participants (as of June 2019) who make active use of its services. The Alliance also has 120 partners who create content independently and over 90 expert users who distribute information about cyber threats and available solutions within their own networks. Feedback from these members has enabled the portfolio of services to be optimised on a continuous basis. While the setup of information portals with regularly updated data was a priority at the outset, a further point of focus for current work is the exchange of expert knowledge, experience and practical recommendations, as well as networking.

In 2019, the Alliance for Cyber Security developed a series of special services entitled 'Networks Protect Networks': these provide IT security personnel with practical, real-world solutions and can therefore lead directly to a greater level of cyber security within businesses in Germany.

### 2.2.2.7 Dialogue on Cyber Security Initiatives in Germany

Initiated in mid-2017, the BSI's focus on dialogue with German cyber security initiatives has been continued and further strengthened. The aim is to exploit synergy effects, raise awareness of cyber security in Germany and maximise the impact of individual awareness-raising campaigns. The organisation of regular dialogue between members is handled by the Alliance for Cyber Security.

In October 2018, the BSI provided campaign material for dissemination across social media to interested initiatives participating in European Cybersecurity Month (ECSM). During the four weeks of ECSM, awareness graphics with tips about handling unfamiliar USB drives, security updates and phishing or social engineering attacks was shared over Twitter, Facebook and other platforms. This first joint campaign was a concerted effort to advertise the importance of implementing cyber security measures in business.

During this year, the cyber security initiatives have developed a campaign for ECSM in October 2019 to raise awareness of the secure handling of IT systems among businesses and make further progress towards the common goal of strengthening cyber security in Germany. The results of this work will be presented to the public on 26 September 2019 at Cybersecurity Day in Berlin and distributed jointly as part of this year's ECSM.

### 2.2.2.8 Other Solutions/Services for Business

#### Investment review

The Federal Ministry of the Interior, Building and Community (BMI) involves the BSI as part of its duties in procedures for controlling investments made by foreign investors in domestic companies and production facilities in accordance with Sections 4 ff. of the Foreign Trade and Payments Act (AWG) and Sections 55 ff. and Sections 60 ff. of the Foreign Trade and Payments Regulation (AWV).

The benchmark for these reviews is whether essential security interests, public order or the security of the Federal Republic of Germany are endangered by an intended acquisition. This applies in cases where the target company manufactures or has manufactured products or essential components for VS-certified systems, for example, or if the target company operates critical infrastructure or manufactures sector specific software for operating critical infrastructure.

Taking into account the respective economic, legal and technological situations of the buyer and the target company, the BSI analyses and assesses possible risk situations with regard to IT security. This risk assessment influences the BMI's verdict from a security policy perspective. To avoid causing unnecessary stress to the company with the procedure, the BSI conducts its occasionally highly complex individual reviews very quickly – typically within only one or two working weeks.

A number of factors have led to a significant increase in the review procedures in which the BSI has been actively involved:

- The effective rewriting of the AWG and AWV in 2017 and 2018 tightened both the act and the ordinance to close gaps in procedural rules and provide greater detail about protective measures for critical infrastructure. The critical infrastructure sector was most recently extended at the turn of the year 2018/2019 to include the new area of Broadcasting, Telemedia and Printed Matter, while the threshold for reporting the acquisition for manufacturers  of sector specific software was lowered from 25% to 10%.

- The number and volume of non-EU investments in German companies and corporations have been rising steadily for years.

The number of individual reviews handled by the BSI in connection with investment control procedures doubled once again last year. The figure rose from four procedures in 2015 to 49 procedures in 2018. The number of procedures received since January has confirmed the trend towards an annual twofold increase in this figure, meaning that the BSI expects to see up to 100 procedures in 2019.

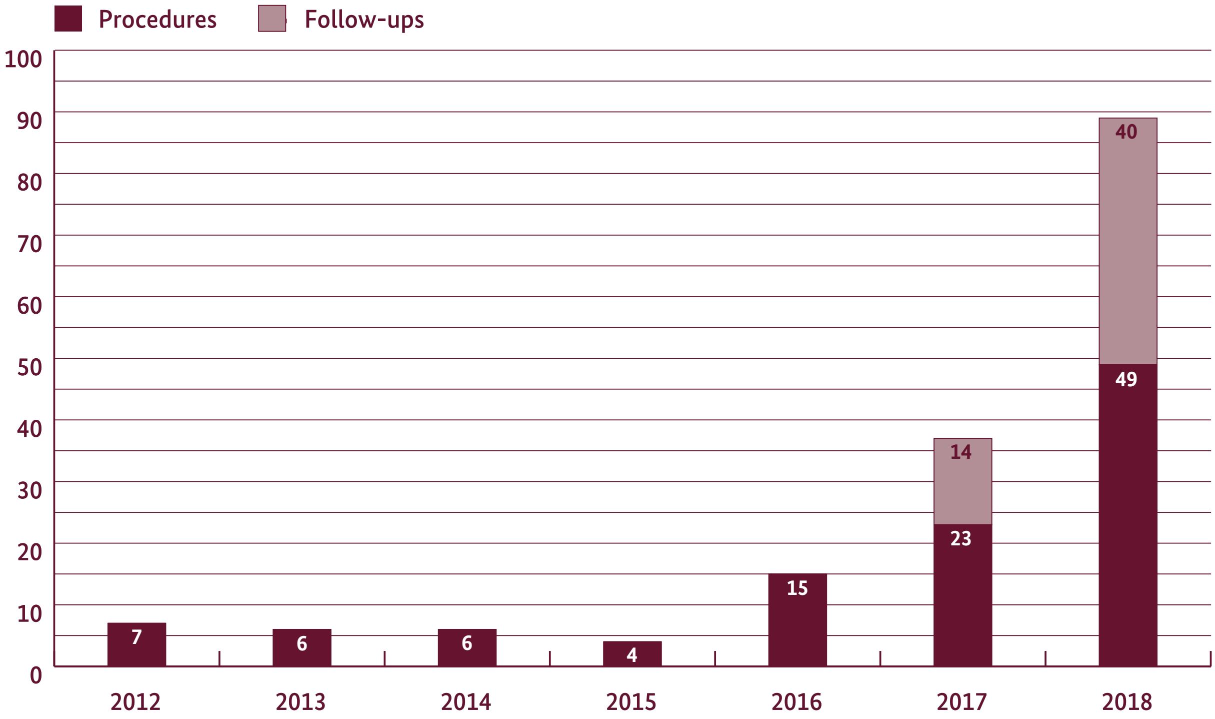


**Figure 12:** Number of AWG procedures and associated follow-ups processed by the BSI, 2012-2018.

## BAFA export controls

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

1. Support and (self-)protection of the German cryptography industry

2. Protection of certified IT security products, components such as smart cards and other technology (against re-engineering, manipulation, etc)

The BSI processed 112 applications in 2018, generating overall revenue of around EUR 134 million.

The following topics were also addressed in the reporting period

- Since May 2016, the processing of applications has concentrated on
export/shipment authorisations for certified IT security products to
reduce the overall number of BAFA applications processed by the BSI in response to the rising number of such applications (see Fig. 1). This was completed in mutual agreement with the BAFA.

- This has resulted in comprehensive, rapid and quality-oriented processing of applications in accordance with the expectations of the BAFA, BSI and applicants in comparison with previous years.

- Cooperation in revising EU General Export Authorisations (GEAs)
- Participation in the sale/acquisition of companies in relation to information security as part of exemption/ participation processing
- Assisting the BAFA with advice on the list of goods (AzG) to determine the export obligations of a product in the above context
- Assisting the BAFA with enquiries regarding various technologies such as 5G and quantum cryptography.

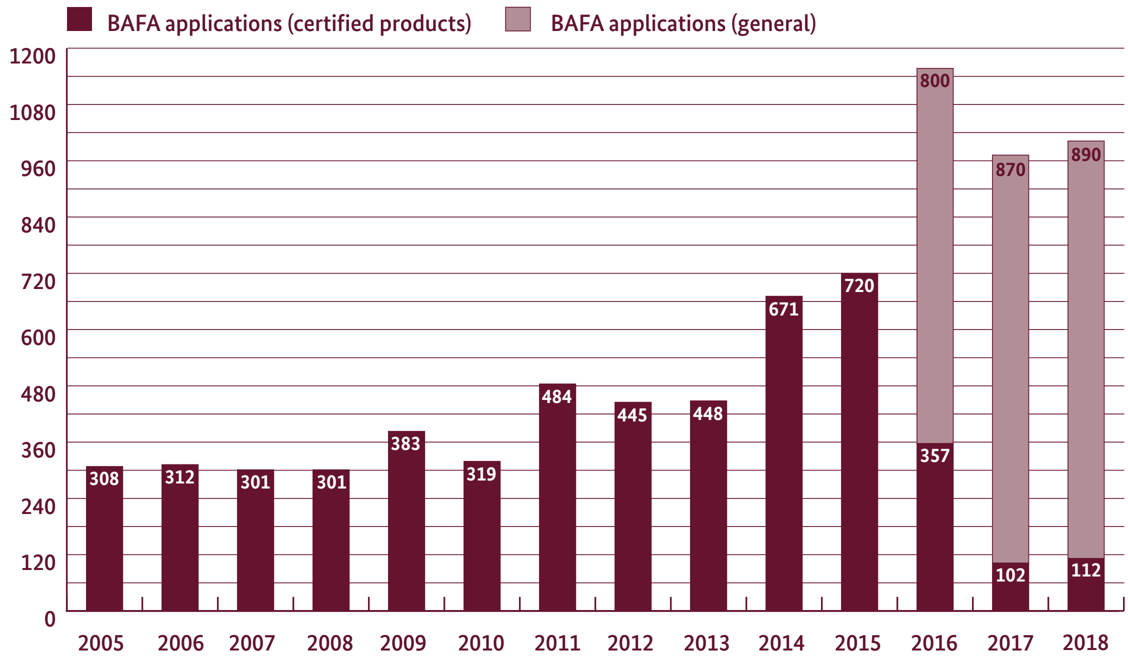


**Figure 13:** Number of BAFA applications processed by the BSI from 2005 to 2018.

## 2.3 Civil Society/Private Citizens

An important task of the BSI is to provide information and raise the awareness of private citizens to ensure the secure handling of information technology, mobile communication tools and the Internet. A comprehensive portfolio of information services entitled 'BSI for Citizens' is available to interested parties. Digital Consumer Protection is also a task that was established in the German Government's 2018 Coalition Agreement.

### 2.3.1 Threat Landscape for Civil Society/ Private Citizens

Insights from the survey that the BSI has conducted in cooperation with the State and Federal Police Crime Prevention Commission (ProPK) are summarised in the following section. The focus is on protecting Internet users from the dangers of the digital world. In this context, the concepts of 'Smart home' and 'Internet of Things' are becoming increasingly significant. Other topics include the safety of medical products and the security of payment systems.

#### 2.3.1.1 Results and Findings from the Joint BSI and Police Crime Prevention Commission (ProPk) Survey

The BSI and ProPK work together to ensure that citizens are comprehensively informed about Internet risks and how to stay safe online. In a representative survey, the two partners collected data on the importance of online security for private users, the extent to which they protect themselves from the dangers of the digital world and how they inform themselves about vulnerabilities and risks.

The results show that the topic of 'online security' is generally important to a majority of users: over 80% of respondents were concerned about their own safety on the Internet. The degree of anxiety varied, however: half of respondents (51%) were rarely worried, while a third (31%) had frequent or constant concerns.

Almost one in four users (24%) had already been a victim of online crime. Here, the respondents had most frequently encountered fraudsters in the areas of online shopping (36%), phishing (28%) and malware (26%). Following the encounter of a crime, 39% of the respondents resorted to self-help. Precautions most commonly mentioned by those concerned about their safety online included antivirus programs (61%), secure passwords (58%) and a modern firewall solution (52%). Only 36% install new updates as soon as they are available.

When questioned about keeping themselves informed, only a third (31%) stated that they stay up-to-date on Internet security issues; most people questioned only do so once they have already become a victim of a cyber attack. Half of the survey respondents are familiar with recent security recommendations to guard against Internet crime. Roughly a quarter of these get this information from the BSI and are familiar with the 'BSI for Citizens' website (24%).

The respondents viewed online activities involving financial data as especially critical, including security for online banking (62%) and online shopping (44%). General surfing activities (33%) and e-mail communication (30%) were also mentioned relatively often. Security is less important for citizens when using social networks (14%) and communicating using messenger programs (11%). The topics of 'installing apps' and 'using public Wi-Fi' are of almost no importance for the respondents (each at 6%), and the same applies to the secure use of networked home equipment and online games (each at 3%). The results of the survey will be incorporated into future educational work carried out by the BSI and the ProPK.

#### 2.3.1.2 Smart Homes and the Internet of Things

Broadband routers (also referred to simply as 'routers' in this document) are used to access the Internet in many households. As well as providing access to the Internet, they can be used to manage a home network. Some routers may also offer smart home functionality. Positioned as the doorway to the digital world, however, they can also be attacked from two sides – locally (e.g. via the Wi-Fi network) and from the Internet. As explained in Section 1.2.5, 'Botnets', this means they are both a potential threat and capable of playing a special protective role.

Broadband routers are relatively powerful integrated systems. While this means that they can successfully defend themselves against attacks, they are also a popular target for attackers wishing to misuse a router's resources to carry out malicious activities. Once control over a router has been achieved, the router itself becomes a risk. Users can be spied on unawares, for example, and attacks can be initiated from the compromised device itself. In 2016 attackers attempted to infect almost a million routers with malware via a remote maintenance port and integrate the devices into the Mirai botnet. This failed because the routers crashed while attempting to install the malware. A basic level of protection must therefore be provided for routers. In the best case, this means attacks on the router can be prevented in advance, thereby maintaining adequate protection for the home network.

From the BSI's perspective, prevention and detection are also urgently needed in relation to smart homes. The publication of the technical guideline (TR) for routers ('Router-TR') by the BSI in November 2018 established a basis for protecting routers against attacks while also making them more resilient. Following its publication, the Router-TR was both widely praised and criticised, which marked the beginning of a longer period of discussion and improvement for this guideline.

The BSI simultaneously began development on a test specification for the Router-TR in early 2019. Together with the test specification, the guideline can be used as the basis for a test or a certification procedure. This enables consumers to compare different routers in terms of the level of security performance they offer.

Alongside the router as the central 'hub' of a smart home, the smart home consists of various devices and services in the context of home automation or consumer electronics. User interaction with these devices is typically handled less by conventional desktop PCs or laptops than by voice-controlled systems, smartphone and tablet apps or wearables. The development in this sector is characterised by the growing importance placed on the ability of individual components to communicate with one another and with online services reachable over the Internet via the router.

To introduce a suitable level of IT security in the market for Internet-ready products for the end consumer, the BSI engages in dialogue with many stakeholders concerning appropriate requirements and test criteria. It was in this context that the recently published DIN SPEC 27072 was developed in a working group headed by the German Institute for Standardisation (DIN). The document presents generic requirements of IT security for the private end-customer segment and is intended to provide a basis for various evaluation and certification procedures.

### 2.3.1.3 Security of Medical Devices

The current situation in Germany is characterised to a large extent by advances in the digitalisation of healthcare, networked medical devices and the feeling that smart products for the health sector are brought to market on virtually a daily basis. Especially in healthcare, where legal provisions apply (such as to the launch of electronic patient records for citizens with public health insurance), there is a palpable trend and market pressure towards mobile solutions. The daily routine in the use of mobile devices (tablets, smartphones), major improvements in functionality and user-friendly access independent of time and place are also helping to ensure the widespread popularity of mobile applications in civil society.

The range of medical applications covered by mobile solutions is rising rapidly. Most of these are used to store and transmit health data (fitness trackers, for example) that is then served up to the private user (e.g. via health apps). Apps are now also being developed for patients with chronic conditions (such as diabetes) and to accompany clinical trials. Many of these applications are already classified as medical devices, and many others in this specific category are likely to be brought to market in the near future. Mobile technologies allow doctors and qualified medical staff to access personal data quickly and easily, and to transfer this and other data to patients. No specialised equipment is necessary other than a smartphone or tablet. The familiar kinds of personal data – such as first and last name, age, gender and height – can be expanded to include medical parameters such as blood sugar levels, blood pressure and oxygen saturation, or diary data for diabetes, blood pressure monitoring and pregnancy.

The use of mobile applications saves patients and doctors alike both time and paper over the long term. Here, the term 'mobile applications' refers to health/fitness apps in a broader context, and therefore to all mobile applications that store personal health data. A given app may also be used in combination with a medical device. Such solutions are available for insulin pumps or sleep apnoea treatment devices, for example. In the field of telemedical and follow-up care, mobile application scenarios are becoming increasingly important in an effort to improve the ability of patients, doctors and qualified medical staff to take advantage of the independence these scenarios offer in terms of time and location.

For makers of mobile applications, cyber security is often not given any particular priority. This is demonstrated by two BSI projects in the networked medical devices/geriatric nursing products sector. In the eCare project (which involves networked geriatric nursing products), vulnerabilities were found in mobile applications that had not even been made public. The results of the eCare project are expected to be published in autumn 2019. The results of the ManiMed (manipulation of medical devices) project are expected in autumn 2020. Since product testing is scheduled to start shortly, no vulnerability findings are currently available. The increasing degree of networking and distribution, coupled with society's rising acceptance of mobile applications, is now associated with an elevated level of risk of cyber attacks. Section 7a(1) of the BSIG authorises the BSI to audit products and systems with IT relevance that are offered on the German market, and to issue warnings that account for the potential consequences of a failure to take appropriate and adequate security precautions. Alongside networked medical devices, a number of mobile applications from the healthcare sector were also investigated. With many of the mobile applications examined, it was found that sensitive, personal data was often stored temporarily in an unencrypted format in working memory and that onboarding mechanisms were either lacking or not implemented in a secure fashion. Here, the term 'onboarding' refers to the first time a user logs into a given mobile application. In many cases, the person's identity is not checked. The initial login either utilises an mTAN, a one-time password, authentication via the ID card app or some other method – or no particular procedure at all. The procedures vary in their level of security (no-factor, one-factor, two-factor authentication). Insecure apps can offer an opportunity to read, store and even manipulate data without the patient's knowledge.

Medical Device Regulation (MDR), which will apply throughout the EU from 2020, will usher in sweeping changes for manufacturers, operators, notified bodies and users. Medical devices will be required to have certain cyber security properties, and many products will be assigned to higher risk classes. The design of such products has previously focused on ensuring that they do not cause the patient harm.

The threat landscape can be considered critical, meaning that more effective security mechanisms for networked medical devices and mobile healthcare applications must continue to be developed in the future. The BSI is responding to these developments in its cooperation with the competent supervisory authorities and through the projects 'eCare: Digitalisation in Nursing' and 'ManiMed: Manipulation of Medical Devices'. Publications in these areas and initial project findings are both planned for release before the end of this year.

### 2.3.1.4 Security of Payment Methods

PSD2 (Payment Service Directive 2) is the common name for the extended Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market. The Directive entered into force on 13 January 2018 and (at least in terms of oversight legislation) has been transposed into national law in Germany by the new Payment Services Oversight Act (ZAG).

Working in close cooperation with the European Central Bank (ECB), the European Banking Authority (EBA) is tasked by PSD2 with drawing up regulatory technical standards (RTS) and guidelines for various aspects of PSD2. In January 2018, the RTS for secure communication and strong customer authentication was published; it must be implemented by 14 September 2019.

The RTS does not provide any specific implementation details, although it should provide a technical interpretation of PSD2. Instead, it leaves room for interpretation. What is specified is that, from its entry into force, two of three factors from the categories of physical possession, knowledge and inherence should be used for authentication for online access to a bank account. Left unexplained are the specific strength of the authentication procedure and the level at which these security requirements are to be fulfilled.

In the BSI's opinion, there is a risk that financial institutions will decide not to implement strong customer authentication in order to ensure fast processing for users and avoid subjecting them to extra effort. This is possible if the instrument of internal risk assessment is applied. In this case, a payment service's risk management system must select an authentication procedure depending on its internal level of risk tolerance.

PSD2 and its associated documents primarily aim to strengthen competition in payment services, increase the security of payment service providers and offer better protection to consumers when they make online payments while also promoting the development and use of innovative online and mobile-phone-based payments. For example, online shopping should become more secure through the use of strong customer authentication and cases of fraud should become less common. From the BSI's perspective, however, this can only be achieved if secure authentication procedures are offered and also employed by end users. Mobile banking is now increasingly being used, whereby the familiar chip card (credit or debit card) is being replaced by moving the data onto a banking app installed on the customer's mobile device. This not only allows users to make payments online; it also means they can pay at points of sale in shops using increasingly widespread NFC (near field communication) terminals. Just like a contactless chip card, a digital card stored on a mobile device uses the NFC interface to communicate with a point-of-sale terminal.

In online banking, the use of an account name and a four- to six-digit PIN to log in – plus TANs to confirm transactions – is now virtually standard practice. Payments at the point of sale have previously been confirmed with a PIN or signature. In the case of contactless credit cards, one needs only to place a card on the terminal (under certain conditions). Other authentication procedures are conceivable with the use of mobile devices. Instead of interacting with a point-of-sale terminal, users could identify themselves on their own mobile devices in order to authorise a payment. This approach is also known as Consumer Device Cardholder Verification Method (CDCVM). For authorisation, the user simply activates the unlocking mechanism on their mobile device. This can include entering the device PIN or password on the user's mobile device, or the use of biometric procedures (fingerprint or iris scanning or voice/face recognition). The availability of these functions ultimately depends on the hardware provided by the mobile device, such as its screen, cameras, sensors or microphones. Since these mechanisms are integrated into the mobile device's underlying platform (the operating system) and also managed by this platform, the payment service provider does not have control over the procedure deployed in the end-user device. Whether a fingerprint pattern or a secure PIN is used is decided entirely by the user.

In addition, the biometric features and the PIN are not directly processed by the payment service provider. From both a data protection and a security perspective, the biometric values that are compared with one another remain on the mobile device, meaning that any comparison takes place only with reference values held in the mobile device's storage.

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

Essentially, it is important that users not be forced to use additional security methods; instead, they should be encouraged to adopt user-friendly and secure procedures.

## 2.3.2 BSI Solutions and Services for Civil Society/Private Citizens

Alongside its comprehensive 'BSI for Citizens' portfolio, Digital Consumer Protection is a key priority in the BSI's solutions for society and citizens. The 'IT Security Mark' is also part of the efforts made in this area. In this context, the BSI is currently working in close cooperation with the competent ministries to create a basis for the introduction of a general-purpose security mark for IT products that gives consumers an easily recognisable way of assessing security when making purchase decisions.

### 2.3.2.1 Digital Consumer Protection

In this reporting period, the threat landscape for consumers continued to be characterised by large-scale incidents resulting from security deficiencies in IT systems and online services. One key challenge for consumer protection as part of the digital transformation is therefore to ensure systems and services are secure, to raise awareness among consumers about their risks and to enable consumers to act in a way that fosters security.

The German Government's Coalition Agreement, adopted in February 2018, added the new task of 'Digital Consumer Protection' to the BSI's remit. In the future, this task will also be explicitly governed by the BSI Act. To implement this topic, a Digital Consumer Protection project group was set up in April 2019. Drawn from several departments, the members of this group will build on previous work to promote activities in the field of consumer protection.

With its technical expertise, the BSI views itself as a cooperative and proactive centre of excellence for IT security in the field of consumer products. One particular asset here is seen in the BSI's combination of competencies and powers from legislation, which can be used to achieve the best possible results for consumer security when utilising networked devices. One example of this is the BSI's partnership with the Consumer Advice Centre in North Rhine-Westphalia. This has involved the partners investigating and taking action against insecure smartphones, cooperating on the subject of networked toys and smart home devices and maintaining a 'Phishing Radar'. The BSI intends to expand its cooperation with established actors in consumer protection even further. Thereby the BSI makes a contribution to ensuring effective protection for consumers in the digital world.

### 2.3.2.2 IT Security Mark

The introduction of a seal of approval for IT security was announced by the BMI in its cyber security strategy for Germany, which was published in 2016. This seal is intended to enable consumers to make IT security an integral part of their purchasing decisions. The project was confirmed in the 2018 Coalition Agreement.

The certification of IT security products is already one of the BSI's established procedures. Manufacturers can have their products certified by the BSI and thus prove that their products comply with the state-of-the-art standards in terms of IT security. Products certified by the BSI are typically used in digitalisation projects run by the Federal Government. So far, these certificates have addressed professional users. A solution for consumers must take a different approach, such as by presenting the security properties and their applicable scope in a way that is appropriate for consumers.

The BMI has now designed a new procedure for products and services distributed on the consumer market, which it refers to as the 'IT Security Mark'. The BSI is currently planning the details of this procedure.

The awarding of an IT Security Mark is dependent on a set of clear-cut criteria that determine whether a certificate can be issued or use of an IT Security Mark approved. These criteria are published by the BSI in the form of protection profiles or technical guidelines, for example, and will be extended in the future by requirements for IT products sold on the consumer market. Standards agreed with the industry may also be applied if the BSI views these as appropriate.

At the same time, a legal framework must be established that makes it possible to monitor the IT Security Mark in a way that engenders trust among consumers. This framework will be implemented as part of the amended IT Security Act.

Overall, an IT Security Mark passes through a three-stage life cycle:

1. Determining and updating the state of the art

2. Confirming compliance with the state of the art

3. Monitoring legal use of the mark

Broadband routers will be the first products to be awarded an IT Security Mark for consumers.

### 2.3.2.3 Dialogue on Cyber Security in Civil Society

The social challenges associated with the digital transformation and the topic of cyber security in particular can be managed only by an approach that involves all levels of society. The BSI is therefore aiming to design and shape cyber security for, with and in society at large.

Since 2016, the BSI has been intensifying community dialogue on the topic of cyber security as part of a multi-stakeholder approach designed with a strongly participative focus. This dialogue process, which is conducted as part of 'Institutionalisation of the Community Dialogue' project, comprises an annual think tank workshop as well as topic-specific workshops, events and incident-oriented working groups.

The think tank workshop, which was held for the fifth time in February 2019, brings together the various stakeholders from the areas of civil society, arts and media, research, government and business at a single shared event, while also offering a platform for the discussion of current topics in cyber security.

With the second phase of the project in summer 2018, an important step was taken in the direction of deepening and strengthening dialogue at all levels of society. Based on the group of participants attending the think tank workshops, a 'core group' was formed in June 2018 by drawing an equal number of members from each of the various social groups; this group is now working on three self-selected topics until September 2019:

Topic 1: Establishing a community dialogue. Based on a strongly participative approach, the core group has developed a model that would be appropriate for establishing this dialogue on a permanent basis and has presented this model to the BSI.

Topic 2: Mapping actors in civil society. Building on research findings and in-depth interviews, this mapping is being devised to provide a clear and collective illustration of the civil society actors in the field of cyber security, along with their key activities, objectives and networking structures.

Topic 3: Networking day on knowledge transfer. An event is being designed and organised that will help to network actors in the fields of knowledge transfer and cyber security, generate synergy effects and bring into focus the requirements that should be met when creating information materials.

Dialogue at all levels of society remains a central instrument for the BSI in its efforts to promote the exchange of different perspectives on the topic of information security and ensure the topic is made accessible to a wide range of target groups.

Building on existing project findings and those still to be expected – and with the clear knowledge that cyber security can only be designed through dialogue at all levels of society – the BSI is making every effort to further intensify and consolidate this dialogue with the various target groups beyond this one project.

### 2.3.2.4 BSI Services for Private Citizens

The BSI offers a broad-based portfolio of information and consulting services for private users, which is entitled 'BSI for Citizens'. This portfolio of services is based upon the www.bsi-fuer-buerger.de website, which provides information about cyber risks and protective mechanisms. The focus is on recommendations for secure and self-determined conduct in the digital space. Current cyber security incidents are responded to directly, and recommendations for action are offered about vulnerabilities or waves of malware. While the topics are often complex, they are presented in a simple, straightforward manner as checklists, informative graphics and interactive quizzes. Expert interviews and animated films are also offered.

The BSI's free Bürger-CERT warning and information service issues technical warnings and includes a fortnightly newsletter – 'Stay Secure · Stay Informed' – that discusses vulnerabilities while offering appropriate help and advice. Around 105,000 people are currently subscribed to this service.

A five-part brochure series covers the topics of basic digital protection while offering practical tips on surfing, staying secure with mobile devices, social media, the Internet of Things and the cloud. These brochures can be downloaded from the website and print versions can also be ordered.

In addition to website, the BSI also maintains a profile on the popular social media platforms Facebook (around 39,000 followers) and YouTube (since March 2019, around 450 subscribers as of June 2019). A service centre handles user enquiries on the topics of IT and Internet security. The centre can be contacted by calling 0800 2741000 or by sending an e-mail to mail@bsi-fuer-buerger.de.

To leverage synergy effects, BSI for Citizens works together with a large number of organisations and initiatives that also focus on the topic of cyber security for private citizens. Strong partnerships are maintained with consumer advice centres, for example, sharing communication on topics when warnings are about to be issued. Information about identity theft was provided jointly with the ProPK in relation to the doxing incident in late 2018/early 2019. Alongside a joint press release, various case studies were published to highlight the ways in which cyber criminals can access sensitive data. Together with the 'Deutschland sicher im Netz' (DsiN; translated: 'Germany safe online') association, a 'cyber guide' was produced to provide orientation for key users and educators. Other cooperative ventures, including with the 'Bundesarbeitsgemeinschaft der Seniorenorganisationen' (BAGSO; translated: 'Federal Working Group of Senior Organisations'), were initiated that will provide support in the future when developing educational and awareness campaigns aimed at specific target groups.

#### European Action Month

In 2018, the BSI once again participated in European Cyber Security Month (ECSM) as a national coordinator. With over 200 initiatives and events organised by over 100 partners, this campaign made it possible to present the importance of cyber security in Germany to a wider public. Participating partners included companies, industries and public authorities, chambers of industry and commerce, business associations, colleges and universities, as well as cyber security initiatives cooperating under the leadership of the ACS.

BSI for Citizens also participated with its own initiatives: on its website, Facebook and Twitter, the BSI service focused on how users can ensure the basic IT protection for equipment in their homes.

## 2.4 International and Research Roundup, Plus Select New Technologies

As Germany's national cyber and IT security authority, the BSI is represented in the cyber security bodies of the EU and NATO, and thereby works to shape cyber security at an international level. The BSI also communicates actively with German cyber and IT security researchers.

### 2.4.1 International Matters

The BSI's engagement at an international level is strongly influenced by its role as a responsible national cyber and IT security agency. To fulfil this task and meet its responsibilities at an international level as well, the BSI's sphere of influence was expanded in the previous year to include dialogue with partners and institutions abroad. In the course of conference participation, bilateral talks and contributions made to bodies and relevant legislative projects, the BSI intensified its networking and partnerships with agencies, enterprise actors, researchers and civil society outside Germany. These international activities concentrated on ensuring the BSI's capabilities to make technical judgements and maintaining its international focus.

The BSI's activities and priorities as part of its international engagement were focused on the action areas of the EU and NATO, as well as bilateral and multilateral relationships. Its bilateral cooperation focused on intensifying partnerships in the context of Europe and NATO. One advantage of its long-standing collaboration with close partners is the BSI's ability to ensure the rapid and targeted exchange of information in relation to the detection of and responses to cyber attacks. With this end in mind, a number of new relationships were established last year and existing cooperations were intensified, including with Asian partners.

As both a central piece of legislation and a milestone at the EU level, the Cybersecurity Act resulted in the creation of a new and permanent mandate for the newly named European Union Agency for Cybersecurity (ENISA), as well as in the introduction of a uniform European cyber security certification framework for ICT products, services and processes – the latter being co-designed with the help of the BSI.

Apart from these direct relationships with close partners, the BSI is increasingly viewed abroad as a competent partner in the field of cyber security and as a recognised centre of excellence for IT security.

### 2.4.1.1 Smart Borders (Biometrics)

A concrete example of the BSI's international collaboration is the Smart Borders initiative from the EU Commission. One aspect of this is the introduction of a European entry/exit system (EES) for travellers from third countries. The EES marks the digitalisation in a centralised EU database of the entry and exit stamps formerly applied physically to travel documents on crossing a border in order to both counter irregular migration and obtain information about visa overstays. In the future, portrait photos and fingerprints of travellers from third countries will also be stored in the EES as biometric features to facilitate unequivocal recognition of travellers when they cross borders.

#### 2.4.1.1.1 Smart Borders Project: State of Play

Along with the EES, the Smart Borders project includes the introduction of the European Travel Information and Authorisation System (ETIAS). Following the passing of ordinances concerning the introduction of EES and ETIAS, the BSI has worked with various national public authorities (the Federal Police, the Federal Office of Administration, the Federal Criminal Police Office and the Federal Centre for Information Technology) on the national and international design and implementation of the EU Smart Borders project. Here, the BSI forms part of the Smart Borders project group, which involves all the relevant national agencies and is overseen by the BMI.

Over the last year, the BSI has contributed extensively to work on European regulations and helped to draft numerous items of transposition legislation. As part of the national drafting work, several technical guidelines were also created and published concerning both the statutory inspection of electronic travel documents and biometric procedures applied as part of border controls. These serve as the technical basis for the implementation and certification of new border control systems that form part of future border control processes introduced by EES and ETIAS. Here, support is offered in particular for the implementation and specification of systems for the self-recording of biometric features by third-country travellers in the run-up to the actual border control process. The aim is the efficient implementation in operational practice of the security specifications for the effective identification of travellers.

To ensure dedicated operational support will continue to be provided for the further development of the new border control systems, the BSI has set up its own specialist Smart Borders unit.

### 2.4.1.1.2 Training for Frontex Schengen Evaluators

The use of biometric systems is now part of the standard repertoire for information security. The field of applications in this area continues to expand and now extends from smartphone authentication to the systems mandated for use in the control of national border crossings. As a result of their complexity, however, the actual performance of these systems – as well as their resilience to being circumvented – can only be determined by extensive testing and a wealth of expertise. The BSI has spent over 15 years developing an internationally recognised set of competencies here, particularly in the field of analysing vulnerabilities in biometrics and developing forgery detection technologies. As a service provider to both sovereign and non-sovereign customers, the BSI makes every effort to offer these competencies across a broad spectrum that extends from technological principles and the development of new technologies to consulting services for manufacturers and advice and training for core end users. In this work, the BSI aims to make a lasting contribution to the availability of more secure and reliable systems, as well as their professional use in the field. As part of the national implementation of the EU's Smart Borders/EES initiative (see Section 2.4.1.1.1, 'Smart Borders Project: State of Play'), the provision of consulting and training programs for the Federal Police therefore forms part of the BSI's remit.

The European Border and Coast Guard Agency (Frontex) once again commissioned the BSI to provide a specialised training course for Frontex Schengen evaluators. This course covered the topics of biometric and non-biometric attack vectors on border control systems, document authenticity checking, an overview of the EU entry/exit system and self-recording systems. The first training event, entitled 'Vulnerability Assessment and Testing for Automated Border Control Systems', was held in March 2019 on the premises of the Biometric Evaluation Centre (BEZ) on the campus of the Bonn-Rhein-Sieg University of Applied Sciences (see also the LinkedIn article on Frontex at https://www.linkedin.com/company/frontex/). The participants were Schengen evaluators and official delegates of their native countries, most of whom also held responsibilities for parts of the respective national implementation programs for the Smart Borders/EES initiative.

One two-day BSI training event focused on the particular dangers arising from forgery attacks in the field of face and finger biometrics and electronic identity documents; it also covered detection techniques and countermeasures currently available at an organisational or technical level.

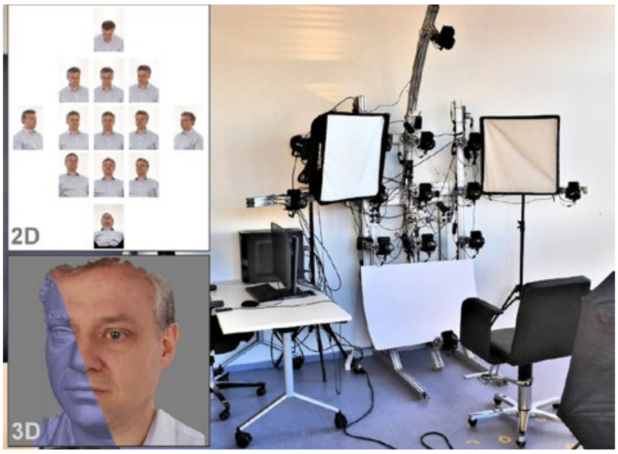


**Figure 15:** Portrait studio for reference photos of test persons. A special DSLR camera array is used for the simultaneous recording of 13 multi-pose photos (shots taken at various angles) and the creation of a highly detailed 3D model. As part of Frontex training courses, participants are photographed in order to create morphed images for vulnerability analysis.

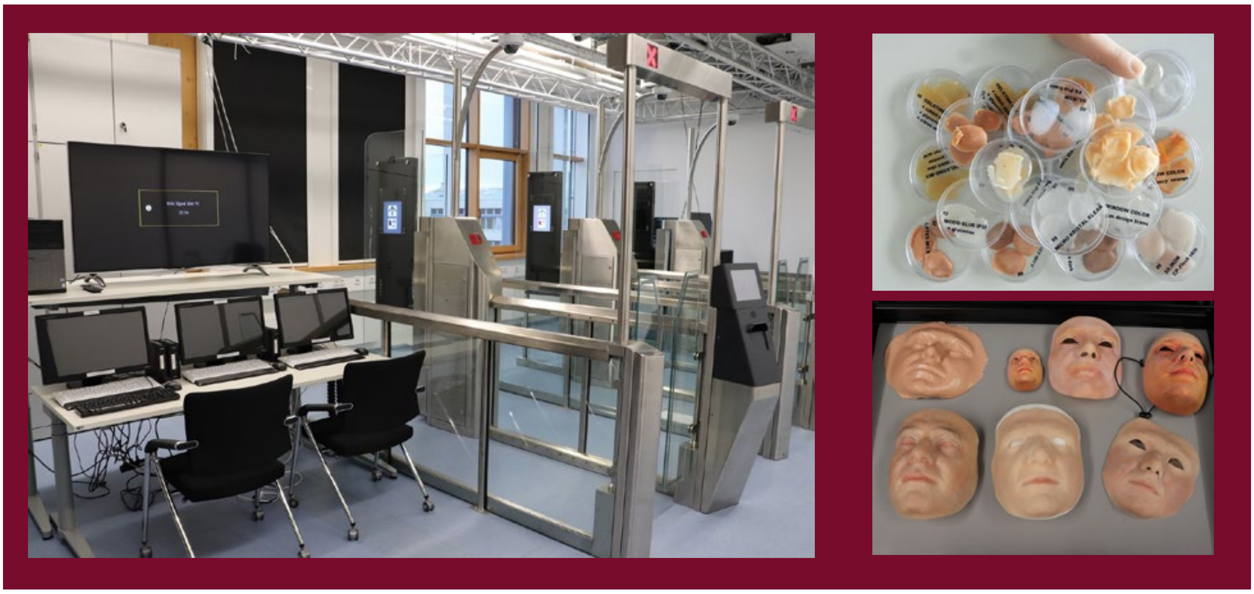


**Figure 14:** (l) Test facility for the evaluation of national border control systems, as used for parts of the Frontex training courses. By using the EasyPass systems, participants could first observe normal operation of the gates (as used in German border controls) and then attempt attacks aimed at bypassing the systems using forged biometrics. (r) Examples of test equipment used for the vulnerability analysis of face and finger biometrics systems, as utilised in the Frontex training courses.

Following positive feedback from attendees, Frontex has announced that it will expand its cooperation with the BSI. Another training event is planned for November 2019.

### 2.4.2 Cooperation with Academic Research

Many aspects of our present-day social and economic lives are now dependent on the reliability of information and communications technology, as well as an implicit level of trust in the security of these ICT systems. As the potential for innovation in the field of ICT expands rapidly, this is associated with a rising threat level due to IT security risks, which means that dedicated IT security research is now increasingly important alongside technology research itself.

IT security research is therefore an important part of being able to develop innovative IT security techniques based on new developments. With the early involvement of IT security as an integral part of developing new technologies, IT security research now plays an important role in increasing the level of security in Germany, as well as in offering preventive and long-term protection for private citizens, businesses and government and strengthening the competitiveness of Germany as a research location.

The BSI is involved in efforts to develop IT security research at the national and European levels. Alongside the co-development of national and EU-wide research programs, this includes consulting activities in the political sphere which aim to establish and further expand IT security research over the long term. Relevant points of focus and current topics in research are actively pursued by in-house projects orchestrated with the major IT security research centres in Germany, other HEIs and a number of Fraunhofer Institutes. The BSI also advises the Federal Ministry of Education and Research (BMBF) on the selection of research projects as part of its work in providing expert opinions, supports select research projects related to IT security as an associate partner and provides subject-specific support to German centres of excellence in IT security research and several other leading IT security research institutions. Representatives of the BSI and research centres for cyber and IT security in Germany hold technical meetings at regular intervals to stay abreast of recent research findings. This has resulted in the organisation of expert workshops and dialogue events with representatives from the IT security research community on topics of strategic importance for IT security, such as machine learning and quantum technologies.

The BSI has also provided resources to support the setup and design of the new Agency for Innovation in Cybersecurity, which is intended to promote and fund research and development projects and key technologies with major potential for innovation in the field of cyber security. This will enable the BSI to commission projects from the agency that are not without a certain degree of inherent risk, but also involve fundamental (and therefore potentially game-changing) long-term research that can then be supported by the BSI's own expertise as a project partner.

### 2.4.3 Cryptography

In cryptography, the all-encompassing topic in recent years has been the development and standardisation of post-quantum cryptography, i.e. cryptographic techniques that are resistant against attacks using quantum computers. In November 2016, the US National Institute for Standards and Technology (NIST) started a selection process for the standardisation of quantum-computer-resistant cryptographic techniques.

Algorithms could be proposed until the end of 2017, and these were then presented in the course of a workshop in April 2018. Of the 82 algorithms submitted, just 17 encryption or key transport techniques and nine signature schemes proceeded to the second round following the first candidate analysis phase. Among the encryption and key transport techniques submitted, lattice-based and code-based techniques were generally the most prevalent, while most of the signature techniques were based on multi-variate and lattice-based approaches.

The announcement of candidates for the second round launched a second analysis phase. Algorithm authors had until mid-March 2019 to make any modifications to their submissions. The updated documents have been available on the NIST website since early April. A second standardisation workshop was held in Santa Barbara (USA) at the end of August. The first drafts of the standard will presumably not be published for another two years.

Alongside the development of cryptographic algorithms resistant to quantum computing, adjusting cryptographic protocols to the new techniques also presents a major challenge. One major problem that is encountered when utilising quantum-computer-resistant secure key exchange schemes in the Internet Key Exchange (IKE) protocol is that the public keys in many of these algorithms are significantly larger than those used by current techniques, which means they do not fit into the initial IKE message.

Standardisation bodies such as the European Telecommunications Standards Institute (ETSI) are also focusing their attention on quantum topics. An ETSI working group on quantum-safe cryptography (ETSI TC Cyber QSC) is not only investigating algorithms immune to quantum computing, but also examining practical aspects of migrating to post-quantum cryptography, such as requirements for quantum-safe virtual private networks.

### 2.4.4 Blockchain Technology

Blockchain is now one of the most hotly debated topics in the field of information security. As with all new technologies, the security of blockchain should be considered from the outset and a secure-by-design approach should also be pursued. In early 2018, the BSI therefore published a position paper on blockchain security, thereby initiating a public discussion.

In early 2019, the BSI published a comprehensive document entitled 'Designing Secure Blockchains: Concepts, Requirements and Assessments'. Building on the BSI's previous blockchain technology position paper and picking up on previous discussions, this provided developers and potential users of blockchain solutions with tools to fully assess the technology's opportunities and risks and integrate IT security from the outset. Examples were also included to illustrate various aspects, such as long-term security.

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

In parallel, the BSI has also commissioned a market surveillance report on blockchain applications and subsequently commissioned an evaluation of select products from various product classes as examples of this technology.

### 2.4.5 Artificial Intelligence

The field of artificial intelligence (AI) has been under continuous development for many years. Particularly as a result of increases in computing power, the development of new algorithms and the availability of large quantities of data, AI systems have successfully entered into a number of areas in recent years. Familiar applications here include text analysis and translation, image and voice recognition and autonomous driving. AI algorithms are also starting to play a more important role in cyber security.

These new methods are evaluated continuously by the BSI, which has also developed and deployed them for its own applications. In one recent paper [https://eprint.iacr.org/2019/037], the BSI has shown that AI methods can accelerate the cryptanalysis of encryption algorithms. The BSI is also evaluating the use of AI systems in the detection of cyber attacks that target IT systems and IT infrastructure. Other fields of application include authentication procedures in the context of sovereign documents and automated text processing for the efficient creation of situation maps.

In the reporting period, a new unit was set up as a technical centre of excellence to handle questions in the field of artificial intelligence and IT security in particular; it now serves as a central point of contact for the BSI and the Federal Administration. The new unit also reflects the growing importance of this topic, not least because AI methods are not only able to improve IT security, but may also present novel attack vectors once AI systems enter into widespread use. These factors need to be identified and analysed in good time, and countermeasures need to be developed to ensure that systems with AI components can be designed to be robust and secure.

Two points of focus for the work of the BSI in the reporting period were machine learning and artificial intelligence. As a result, the BSI is expanding its internal expertise in AI-based approaches to side channel analysis and examining the conditions under which these are superior to conventional techniques. Side channel analyses are a core component of Common Criteria evaluations of chip cards, for example.

#### BSI attends international side channel competition

The prestigious international Conference on Cryptographic Hardware and Embedded Systems (CHES) organised a side channel competition in the summer of 2018. A team from the BSI entered two challenges in this competition – and won both of them. The entrants were tasked with reconstructing the AES key used from power traces that had been recorded by a masked AES implementation on a microcontroller. The team won by deploying a combination of machine learning and conventional techniques [https://eprint.iacr.org/2019/094]..

## THE BSI AS AN EMPLOYER – WE WANT YOUR DIGITAL PERSPECTIVE

Following the BSI's successful response to the challenge of handling growth in its workforce of over 40% in recent years, this trend continued recently with the allocation of 100 additional positions for 2018 and another 350 positions for 2019. With well-qualified STEM personnel having no shortage of employment offers, promoting the BSI as an attractive employer continues to be a key factor in hiring. Successfully completing onboarding and integration work for new colleagues also requires a great deal of dedication and effort on the part of the whole organisation.

### Spread the Word: The BSI Is the Most Popular Place to Work in Public-Sector IT

The BSI accomplished a major success in the reporting period when students and graduates from IT degree courses placed the agency 14th nationwide, making it the most popular IT employer in the public sector ('Trendence Absolventen Barometer', IT Edition, 2018). This excellent result should now be promoted in order to reach even more graduates and (young) professionals. Complementing its long-running campaign 'What We Want: Your Digital Perspective', the BSI also utilised a number of other recruitment channels. Alongside in-person interactions at university events or BSI Open Days, a 'recruitainment format' has also been developed which takes a gaming-style approach to promoting the BSI to interested candidates as an employer. An additional storytelling format is also intended to present the BSI's activities in a set of interesting and compelling snapshots and thereby provide interested specialists with a look behind the scenes at the agency. The campaign imagery has also been expanded: alongside the objects used to date from the day-to-day lives of IT specialists, real-life BSI employees will now also be shown with their personal and digital profiles.

### Lots of New Faces: Onboarding and Integration

In order to integrate new employees into the BSI, a number of mandatory introductory events put together from several different modules were initiated to make the employees more familiar with the specialist tasks in their different areas. This not only provided an overview, but also introduced STEM specialists – who have often had no contact with these kinds of requirements – to the basic fundamentals of work in the Federal Administration. In-house training courses were also offered on basic topics relating to methodology or social skills, such as project management, presentations, resilience, conflict management, time management, communication and cooperation, conducting negotiations and stress management. These reflect the different interdisciplinary requirements for new and more experienced employees. Above all, the courses promote cross-divisional cooperation and collaboration while introducing BSI-specific procedures, including in project management. In addition, training courses in conflict management, remote leadership, common goals, human resource law, feedback meetings and general management were offered specifically for managers along with the established management trainee programme. The concept of health leadership was also emphasised to ensure that health management was properly anchored as a management topic.

Apart from basic in-house training for employees and management staff, the BSI also regularly sends its employees on specialised external training courses in accordance with subject-specific requirements..

# 3 Overall Assessment and Summary

# 3 Overall Assessment and Summary

Modern technological developments have created a highly dynamic ecosystem in which all of us operate – in government, in business and in our private lives. The challenge is to keep pace with the changes in this ecosystem so that they proceed in an orderly fashion and can bring the greatest possible benefits to as many people as possible. The insights and trends described in this report further confirm the expectations that the BSI had already expressed in last year's report: even in 2018, the BSI was already warning of a new quality to cyber attacks, and these kinds of attacks have now indeed taken place. Back in 2018, the BSI described the Emotet malware as one of the world's biggest cyber threats while also warning of the potential for it to be improved with professional techniques. The BSI also considers this to have been sound advice, given the targeted ransomware attacks on companies in the latest reporting period.

Independently of Emotet, ransomware also continues to pose the biggest threat to companies, public authorities and other institutions, and private users. Time and again, ransomware has taken down entire servers and networks, and even production plants. Public facilities have also recently become the target of ransomware attacks on several occasions. These have included hospitals in Germany and local administrations in the United States. One trend that can be observed here is the way attacks target a central service provider, which can then be used to infect customers or connected networks with ransomware. The potential losses are enormous: the costs involved in production downtime, data loss and cleaning and restoring systems can run into the millions, while the provision of services by public facilities may become difficult or even impossible.

The new approach taken by cyber attacks, which was forecast by the BSI, was also reflected in a series of serious cases of identity theft that made the headlines in 2018/2019. Those affected included users of social networks and customers of a major hotel chain, as well as hundreds of celebrities and politicians from Germany as part of a doxing incident that became well publicised in January 2019. Other incidents, referred to as 'Collection #1' to 'Collection #6', also impacted hundreds of millions of other Internet users whose data was published online. What is significant here is not only the frequency of these incidents, but also the huge volume of the personal data leaked and subsequently posted on the Internet.

As before, attackers continue to display a great deal of ingenuity in developing (and improving) their malware and attack mechanisms. Around 114 million new malware variants were identified in the reporting period and the potential threat posed by malware spam continues to rise, even though its absolute volume has actually decreased. E-mails containing malware are among the most frequently detected attacks on the Federal Administration. Apart from its effect on traditional office communication, malware is also having a growing impact on company production facilities. In mechanical engineering in particular, ongoing digitalisation and an increased level of networking due to IoT and Industry 4.0 is opening up new avenues of attack: if not properly implemented, these developments can magnify the damage caused by malware.

The botnet threat landscape continues to remain serious: here too, attackers are exploiting the digital transformation and focusing strongly on mobile end-user devices and IoT systems. As more and more of these devices come online, often with only rudimentary kinds of protection, they offer criminals a welcome opportunity to take over and misuse these systems without the owner's consent. Every day, up to 110,000 bot infections are registered on German systems and reported to the respective network operators by the BSI for subsequent decontamination. Much greater potential for attacks is offered by server-based botnets, particularly in light of the increasing use of cloud infrastructure. Over half of all attacks are now executed with compromised cloud servers or servers that are legitimately rented, but then misused. Accordingly, almost every cloud service provider has now been misused by criminals to execute DDoS attacks on at least one occasion.

This already problematic cyber security situation is being worsened unnecessarily by the frequent helplessness of users in relation to all things digital. Perpetrators are keen to exploit these casual attitudes towards security in combination with products and systems that are not properly protected. The situation can be remedied by the systematic use of best-practice IT security measures, as well as by strengthening the sense of 'digital responsibility' felt by individual users.

## An Integrated Value Chain to Protect Government, Business and Society

Even in light of the difficult threat landscape described in this report, it is nonetheless possible to design digitalisation in a secure manner in Germany. As digitalisation finds its way into all areas of our lives and the economy, cyber security needs to match this pace of development. To ensure that Germany remains a strong and secure location in the future, the opportunities offered by digitalisation must be seized while also countering potential risks appropriately from the outset. As a centre for business and innovation, Germany must be in the vanguard of digitalisation while ensuring that safeguards for IT products and corporate networks are built in from the start, and that the principles of security-by-default and security-by-design become second nature.

As a federal centre of excellence for IT and cyber security, the BSI has laid the groundwork in this context and is responsible for managing this task, which must be embraced by society as a whole. Each and every day, the BSI considers the types of applications where risks due to digitalisation may occur and examines how they can be rendered both knowable and manageable. The many years spent in establishing and bundling knowledge and expertise in the field of cyber security have made the BSI a highly competent agency and a nerve centre for cyber security. The BSI uses the insights gained in this work to derive appropriate recommendations, products or services capable of meeting the various requirements of government, business and civil society. This integrated cyber security value chain, which combines prevention, detection and response under one roof, is a feature of the BSI that makes it unique worldwide.

The BSI actively participates in new developments in our increasingly digitalised society and uses its close partnerships with national and international players to apply its insights and requests to strengthen cyber security directly to the respective development processes at an early stage. As a thought leader in the fields of artificial intelligence, quantum computing, blockchain and the latest 5G mobile network standards, the BSI makes a decisive contribution to maintaining Germany's digital sovereignty and safeguarding the relevant security aspects.

Whether in Bonn, the Dresden metropolitan area or at any number of other local branches, the BSI tackles issues that are of immense importance for the economic and social development of Germany as a whole and demonstrate digitalisation 'Made in Germany' at its best. Cyber security is the answer to the new challenges that public authorities, businesses, critical infrastructure and private users are now facing on a daily basis because it enables them to use the advantages of their digitalised business processes or enjoy the benefits of their digital lives. Users in all target groups are supported not only by the specific services offered by the BSI – such as Digital Consumer Protection, the planned IT Security Mark, the expansion of consulting services for federal states and municipalities and the services provided by the Alliance for Cyber Security and the CIP Implementation Plan – but also by the options available in certification and standardisation. As a result, the BSI makes a decisive contribution to ensuring continuous improvement in information security at all levels of society while countering potential risks preventively and, where necessary, ensuring an appropriate response. The threat landscape is becoming more complex as digitalisation continues apace. These go hand-in-hand, and the BSI has answers for both of them. With its new remit, an ever-expanding workforce of highly qualified and motivated employees and trusted collaboration with its national and international partners, the BSI is taking charge of the situation and continuing to develop strategies and solutions to ensure that digitalisation can be a success story for us all..

# 4 Glossary

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

**Attack vector**
An attack vector is the combination of attack routes and techniques through which the attackers gain access to IT systems.

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

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

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

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

**Cloud/cloud computing**
Cloud computing denotes the provision, use and billing of IT services via a network. Such arrangements can adapt dynamically to the customer's current needs. These services are offered and used solely by means of defined technical interfaces and protocols. The range of services offered within cloud computing covers the entire spectrum of information technology, including infrastructure (such as computing power and memory), platforms and software.

**Digital personality protection**
Digital personality protection refers to the protection of the activities of important personalities in the digital sphere. In addition to protecting private inboxes, this also includes measures such as the verification of Twitter and Facebook accounts.

**DNS**
The Domain Name System (DNS) assigns the relevant IP addresses to the addresses and names used on the Internet, such as www.bsi.bund.de.

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

**Doxing**
Doxing refers to the dissemination and publication of documents containing dossiers of personal data with the aim of compromising or causing harm to the individuals or organisations concerned.

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

**Exploit kit**
Exploit kits or exploit packs are tools for cyber attacks that are placed on legitimate websites. A variety of automated exploits are used in an attempt to discover vulnerabilities in the web browser or its plug-ins and exploit these to install malware.

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

**Padding**
In cryptography, padding is used in encryption procedures to fill up empty data areas. With a block cipher, for example, the data to be encrypted is stored in blocks of a fixed size. To ensure the last block becomes 'full', padding can be used to fill out the last few bytes.

**Patch/patch management**
A patch is a software package that software manufacturers use to resolve security vulnerabilities in their programs or implement other improvements. Many programs offer an automated update function to make the installation of these patches easier.

Patch management‘ is the term used to describe the processes and procedures that enable an IT system to obtain, manage and install available patches as quickly as possible.

### Phishing

The term ‘phishing’ is a combination of the words ‘password’ and ‘fishing,’ i.e. ‘fishing for passwords’. The attacker attempts to access the personal data of an Internet user via bogus websites, e-mails or messages and to misuse this data for their private purposes, usually at the victim’s expense.

### Plug-in

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

### Ransomware

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

### Sinkhole

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

### Social engineering

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

### Spam

Spam refers to unsolicited messages sent by e-mail or using other communication services to a large number of people in a non-targeted way. Harmless spam messages generally contain unsolicited advertising. However, spam is also often sent with attachments that contain malware or with links to infected websites, or can also be used for phishing attacks.

### SSL/TLS

TLS stands for Transport Layer Security, which is an encryption protocol for the secure transmission of data on the Internet. SSL (Secure Sockets Layer) is a similar protocol which preceded TLS.

### UP KRITIS

The CIP Implementation Plan (www.upkritis.de) is a public-private partnership between critical infrastructure (CI) operators, their associations and public authorities such as the BSI.

## Imprint

**Published by:**
Federal Office for Information Security (BSI)

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

**email:**
bsi@bsi.bund.de

**phone:**
+49 (0) 22899 9582-0

**fax:**
+49 (0) 22899 9582-5400

**Last updated:**
October 2019

**Printed by:**
Appel & Klinger Druck und Medien GmbH, Schneckenlohe

**Concept, editing and design:**
Fink & Fuchs AG

**Content and editing:**
Federal Office for Information Security (BSI)

**Image credits:**
all pictures: GettyImages KTSDESIGN_SCIENCE PHOTO LIBRARY

**Graphics:**
Federal Office for Information Security (BSI)

**Item number:**
BSI-LB19/508e

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

www.bsi.bund.de