




# Cybersecurity Report 2020





# **Cybersecurity Report 2020**

Vienna, 2020

 Federal Chancellery  
Republic of Austria

 Federal Ministry  
Republic of Austria  
Interior

 Federal Ministry  
Republic of Austria  
Defence

 Federal Ministry  
Republic of Austria  
European and International  
Affairs

## **Imprint**

Media owner, publisher and editor:  
Federal Chancellery – Republic of Austria  
Ballhausplatz 2, 1010 Vienna, Austria  
[bundeskanzleramt.gv.at/en](https://www.bundeskanzleramt.gv.at/en)  
Photo credit: iStock  
Layout: BKA Design & Grafik  
Printing: Druckerei Walla GmbH  
Vienna, 2020

# Content

<b>Introduction</b> .....	<b>9</b>
<b>1 Cyber situation/threat</b> .....	<b>11</b>
1.1 Cybersecurity situation—operative level.....	13
1.1.1 EMOTET.....	18
1.1.2 Ransomware.....	18
1.1.3 DDoS (ÖBB, Municipality of Vienna).....	19
1.1.4 EU election.....	19
1.1.5 Vulnerabilities (BLUEKEEP [RDP], Foreshadow, PDF signature).....	20
1.1.6 Penetration into computer networks.....	22
1.1.7 Advanced Persistent Threats (APTs).....	22
1.1.8 Publication of access data online.....	23
1.2 Cybersecurity situation—and security service providers.....	24
1.2.1 Companies working in critical infrastructure and constitutional facilities.....	24
1.2.2 Leading private companies from the cybersecurity industry.....	33
1.3 Cybercrime situation.....	46
1.3.1 Internet fraud.....	46
1.3.2 Cybercrime in the narrow sense.....	48
1.3.3 Other online criminality.....	49
1.4 Cybersituation in national defence.....	52

<b>2 International developments</b> .....	<b>57</b>
2.1 European Union (EU).....	59
2.1.1 Horizontal Working Party on Cyber Issues.....	59
2.1.2 NIS Cooperation Group.....	60
2.1.3 Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats.....	61
2.1.4 EU certification framework (Cybersecurity Act).....	62
2.1.5 Cybersecurity of 5G networks.....	63
2.1.6 Cyber diplomacy.....	65
2.1.7 Network of National Coordination Centres and European Competence Centre.....	66
2.1.8 Action plan against disinformation.....	68
2.2 United Nations (UN).....	72
2.3 NATO.....	78
2.4 Organization for Security and Co-operation in Europe (OSCE).....	78
2.5 Organisation for Economic Co-operation and Development (OECD).....	80
2.6 Council of Europe.....	81
2.7 Computer Security Incident Response Teams Network (CSIRTs Network).....	82
2.8 Other committees and forums.....	83
<b>3 National actors</b> .....	<b>89</b>
3.1 Cyber Security Center (CSC).....	90

3.2 Cyber Crime Competence Center (C4).....	91
3.2.1 Competent investigating authorities.....	91
3.2.2 Activities.....	91
3.3 CIS and Cyber Security Centre (CISCSC).....	92
3.3.1 Military Cyber-Centre (MilCyZ).....	92
3.3.2 Self-protection.....	94
3.3.3 milCERT (Military Computer Emergency Readiness Team).....	94
3.3.4 Cyber military training area.....	95
3.3.5 Information security.....	95
3.3.6 Electronic warfare.....	95
3.4 Austrian Armed Forces Security Agency (AbwA).....	96
3.5 Austrian Strategic Intelligence Agency (HNaA).....	96
3.6 GovCERT, CERT.at and Austrian Energy CERT.....	97
3.7 Office for Strategic Network and Information System Security.....	101
<b>4 National structures.....</b>	<b>107</b>
4.1 Inner Circle of the Operative Coordination Structure (IKDOK).....	108
4.2 CERT Verbund Austria.....	109
4.3 Cyber Security Platform (CSP).....	110
4.4 Austrian Trust Circle (ATC).....	111
4.5 ICT security portal.....	113

<b>5 Cyber exercises</b> .....	<b>117</b>
5.1 Cyber Coin 2019.....	119
5.2 HELIOS 2019.....	119
5.3 Blue OLEX 2019.....	121
5.4 EU ELEX19.....	121
5.5 CyberSOPex 2019.....	121
5.6 Locked Shields 2019.....	122
5.7 Common Roof 2019.....	123
5.8 Thor's Hammer 2019.....	123
5.9 Coalition Warrior Interoperability eXploration, eXperimentation, eXamination eXercise (CWIX) 2019.....	124
5.10 Crossed Swords 2019.....	124
<b>6 Summary/outlook</b> .....	<b>129</b>







# Introduction

In accordance with Austria's Cybersecurity Strategy (ÖSCS), the Cyber Security Steering Group (CSS) has to prepare an annual report on cybersecurity in Austria. The last report was presented in May 2019.

The current Cybersecurity Report for 2020 is based on the content of last year's report with the addition of current developments focusing in particular on the areas of international and operational developments. The observation period is 2019 with the inclusion of a few current developments from 2020.

The aim of the report is to provide a summary review of the cyber threats and important national and international developments. The basis for this is department-specific reports on the topic.



1

Cyber situation/  
threat

The increasing penetration of almost all areas of society and daily life with digital technology offers considerable opportunities and possibilities. At the same time, society is becoming more vulnerable and more dependent on the confidentiality, availability and integrity of digitally processed and saved information, in other words on cybersecurity. States, factions and even criminal actors are continuously opening up new ways for digital networking to be used for spying, sabotage or other criminal activities. The abilities of individual are sufficient to carry out cyber attacks with consequences for Austria's security which cannot be predicted in advance.

## 1.1 Cybersecurity situation—operative level

The 2019 reporting period showed a further increase in attacks motivated by money or state strategy. These primarily include those carried out using ransomware, with an increased tendency towards targeted ransomware. There has also been an increase in the number of cases of data theft using Advanced Persistent Threat (APTs). Organisations are generally extremely reticent about communicating the occurrence and management of these. Attribution<sup>1</sup> is difficult and potentially prone to error, and is therefore often not communicated. There was also a slight increase in DDoS (Distributed Denial of Service) attacks during the reporting period.

Cases of CEO fraud also occurred. The effectiveness of these remains largely limited—despite a consistently high volume of attacks only a very small number of these were actually successful. This is due to a higher level of sensitivity among end users in authorities and companies.

The risks for companies dependent on cloud infrastructures and digital supply chains are increasing. The assumption can be made that the number of attacks on company data in the cloud will rise in the near future.

Possible compromises to the supply chain, in other words the malicious falsification of software updates which allegedly boost security mean medium-sized companies in particular are exposed to increasing dangers.

Increase in  
monetary  
or state-  
strategically  
motivated  
attacks

---

1 Allocation or liability

**” In close collaboration in the “Inner Circle of the Operative Coordination Structure” (IKDOK), increasing numbers of early detection mechanisms were able to be used alongside reactive measures to protect and strengthen resilience.**





Threats caused by the possible manipulation of elections were particularly important during the reporting period. This included the 2019 European elections and the 2019 National Council elections. Various measures were taken by the security authorities to protect the resilience of the democratic system through free, fair and secure elections:

- a risk analysis of the election process with the affected stakeholders,
- the targeted minimisation of organisational and technological risks,
- the implementation of awareness training sessions on cybersecurity with electoral authorities at the federal and provincial level and
- the on-site presence of the Cyber Security Center (CSC) in electoral authorities on election days.

In close collaboration in the “Inner Circle of the Operative Coordination Structure” (IKDOK), increasing numbers of early detection mechanisms were able to be used alongside reactive measures to protect and strengthen resilience.

At the European Union (EU) level, the Cybersecurity Act entered into force on 27 June 2019 (among other things with a European certification framework for the cybersecurity of products, processes and services applicable across the EU). A uniform approach to the attribution of cyber attacks was developed in the form of the Cyber Diplomacy Toolbox. The plan is also to establish a European network of national competence centres (NCCC).



### **1.1.1 EMOTET**

A massive increase in the dissemination of the malware EMOTET was identified in 2019. This malware can access existing email conversations and send authentic-looking “tailored” emails as responses to correspondence received. There was a further intensification in the fourth quarter as cyber criminals attempted to circumvent the measures (anti-virus software and general policies) which are now better tailored to EMOTET on the target systems. The classical approach in which the victim is enticed to activate the malicious code by opening infected email attachments was used less, with victims instead being encouraged to click on a link placed directly in the email text received. Links of this type looked similar to legitimate addresses but were malicious in nature and took the victim to a server from which EMOTET automatically starts the attack. Systems compromised in this way caused a further wave of spam and therefore additional high infection numbers. Numerous companies of different sizes including operators of critical infrastructures and constitutional facilities were affected in Austria.

### **1.1.2 Ransomware**

Along with the EMOTET wave, there were numerous “successful” ransomware attacks, some of which caused significant damage. These not only included those aiming to achieve breadth and depth without specific preselection and reconnaissance measures being carried out by the attackers. Instead, ransomware attacks were also observed in which there was a targeted selection of the victim and which aimed to infiltrate target systems with malware by means of “targeted” spear phishing. These attacks occurred using Ryuk, one of the most prominent of the targeted ransoms. Ryuk also infects operators of critical infrastructures and public institutions and is distributed via EMOTET. The amount of money subsequently demanded depends on the economic power of the respective victim, whose background was researched accordingly in advance by the attacker. Overall, the danger of the improper use of sensitive company data for attacks using social engineering techniques (e.g. spear phishing) has increased. The

reasons for this include the existing disclosure obligations for companies, occasionally excessive information policies on the part of companies themselves or even (unintended) indiscretions on the part of employees on social media.

### **1.1.3 DDoS (ÖBB, Municipality of Vienna)**

In 2019, ÖBB (the Austrian Federal Railways) and the Municipality of Vienna were the victims of increased numbers of DDoS attacks. Since nobody claimed responsibility and no demands for money were made to the victims, there is no information about specific motives. Parts of the ÖBB online sale infrastructure and the Ballot Card Office of the Municipality of Vienna before the European Parliament elections in May 2019 were affected. Countermeasures taken by the targets made significant contributions to containing the DDoS attacks, so total failures of important services were able to be avoided.

### **1.1.4 EU election**

The NIS Cooperation Group already addressed the issue the year before last and published a “Compendium on Cybersecurity of Election Technology” in July 2018.<sup>2</sup> The federal authorities paid particular attention to ensuring correct and uninterrupted operations and maintaining cybersecurity both in advance of the European elections in late May 2019 and during these elections. This was achieved by raising awareness among the bodies implementing the elections on the one hand and by monitoring the cyber infrastructure used on the other. The aim of a task force which was specifically set up to defend against hybrid threats was to identify possible influences by foreign state actors and to take suitable countermeasures if necessary. An exercise was also carried out by the European Parliament (EP) in Brussels to increase awareness and check processes (see Chapters 5.4 and 5.5).

---

2 [https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber\\_security\\_of\\_election\\_technology.pdf](https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf)

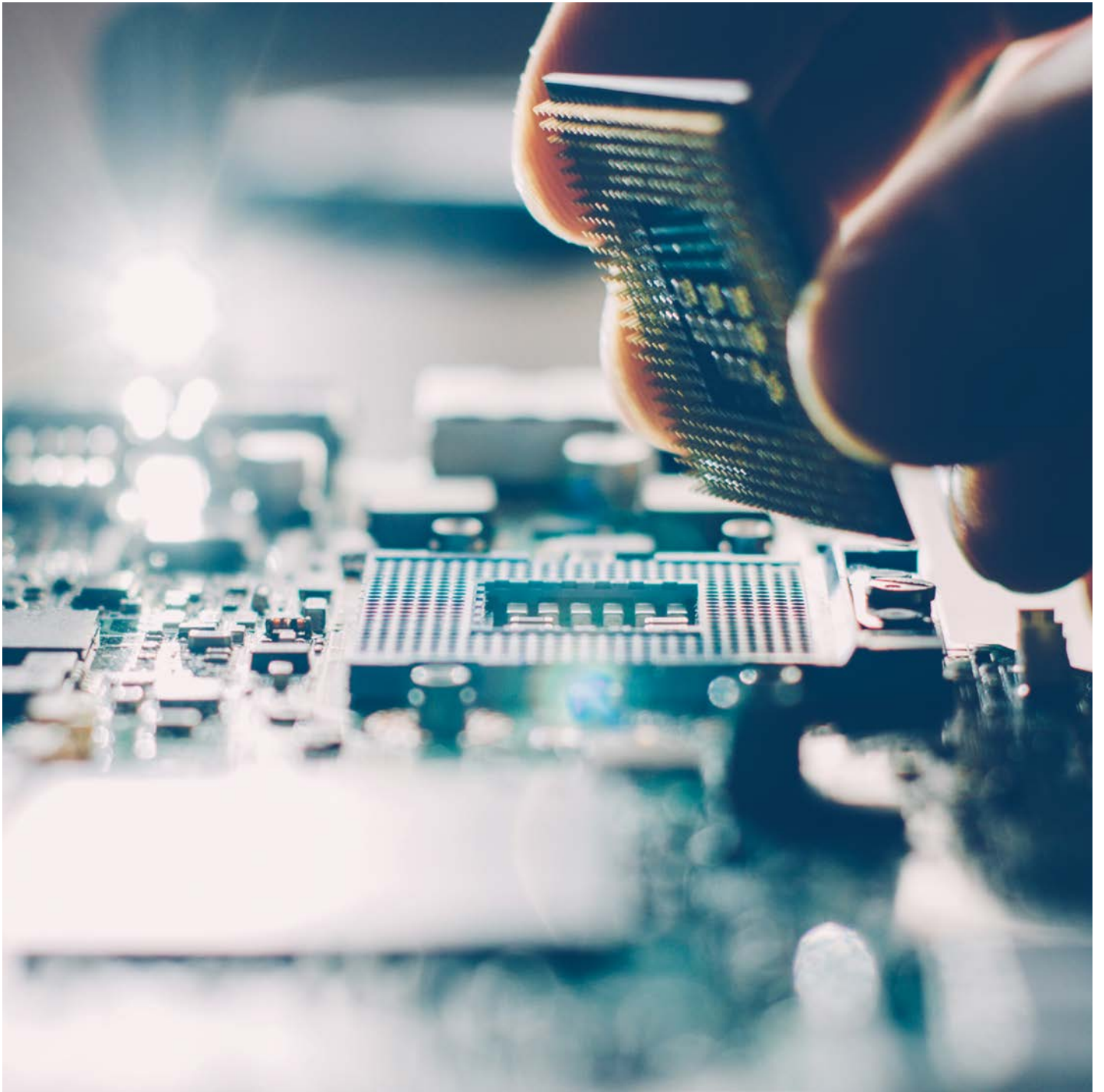
### 1.1.5 Vulnerabilities (BLUEKEEP [RDP], Foreshadow, PDF signature)

Numerous software vulnerabilities were once again identified during the reporting period. Of these, BLUEKEEP, Foreshadow and a validation weakness in electronic signatures must be mentioned, as these need to be classified as critical vulnerabilities.

**BLUEKEEP** is a loophole in the Remote Desktop Protocol (RDP) service of Microsoft Windows which allows external access to computers with Windows operating systems. Shortly after authorities became aware of the vulnerability, the number of vulnerable computers in Austria reached four figures. Prompt information measures helped to effectively contain the existing risk.

**Foreshadow** is a loophole which affects virtual environments (mostly cloud services) and enables the unauthorised export of codes. As a result of a design error in Intel processors, programs can access storage areas to which they should not actually have access. Foreshadow is therefore a further vulnerability within the Intel processor architecture, in addition to the Meltdown/Specter loophole identified in 2018.

**PDF signatures** enable forms in PDF format to be signed electronically in a legally compliant manner. The vulnerabilities in the signature identified in the 2019 reporting period enabled the attacker to change the content of PDF files without authorisation while not harming the PDF signature itself. This means authenticity and integrity were no longer ensured and the entire system of electronic and document-based reliability was undermined. The parties in Austria which may have been affected were informed immediately.



### **1.1.6 Penetration into computer networks**

Over the course of the reporting year, there were attacks on the network infrastructure of Austrian parties and a ministry, with partial loss of data. Unauthorised access was identified in two Austrian parties in the period from July to August 2019. The information which was obviously obtained as a result of these accesses ultimately became public knowledge.

The attack on the BMEIA (Federal Ministry for European and International Affairs) network around new year was the largest and most extensive cyber attack on a ministry in Austria. It led to the activation of the general government crisis mechanisms set out in the Network and Information System Security Act for the first time. The initial response started as soon as the irregularities were identified.

Once the dimension of the incident was realised, the crisis mechanisms set out for incidents of this type were started together with the Inner Circle of the Operative Coordination Structure (IKDOK) and the Cyber Crisis Management Coordination Committee (CKM KA). An operations team made up of representatives from the Federal Ministry of the Interior, the Federal Ministry of Defence, the Federal Ministry for European and International Affairs and the Federal Chancellery (including GovCERT) was set up and managed by the Cyber Security Center. The first risk minimisation measures were carried out promptly and the incident continued to be handled in the new year.

### **1.1.7 Advanced Persistent Threats (APTs)**

APTs are a permanent threat for both the public administration and for companies in Austria, although the number of cases detected is significantly lower than is the case for attacks using ransomware or EMOTET. While the latter are used by cyber criminals to make money, APTs primarily aim to obtain information in the context of economic and industrial espionage or politically motivated spying. APTs also allow the attackers



to sabotage computer networks in production and supply chains. This can lead to consequences up to and including the systems being completely unusable, either as a result of data wiping or by causing physical damage.

In spring 2019, the media reported that the EU delegation in Moscow was the target of an attack that was likely to have been an APT.

At the start of 2019, an attack on the EU's COREU/CORTESY network was able to be prevented. This network, which is used by EU member states, is for exchanging documents linked to the Common Foreign and Security Policy (CFSP). In Austria, an APT attack on a constitutional facility (see 1.1.6) was able to be identified promptly and damage prevented as a result. As far as we are currently aware, however, this attack was not linked to the two EU cases mentioned above.

### **1.1.8 Publication of access data online**

At the start of 2019, an extensive collection of login details (credentials) was published online. Numerous Austrian internet users were affected, among others. The leak, which was subsequently called "Collection #1–5", consisted of five tranches published one after the other totalling more than 1.3 billion sets of access details from various sources. Although this data leak was just one of numerous similar attacks in the reporting period mentioned, it was a temporary peak because of its size. As far as we are currently aware, information provided in good time was able to prevent more serious damage at least in the case of the state bodies affected.

**50 %**  
of companies surveyed increased their budget for cybersecurity

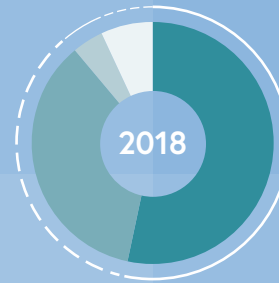
## 1.2 Cybersecurity situation—and security service providers

State bodies are only able to gain an overview of a fraction of the situation in Austria as part of their activities, and they rely on collaboration with users. Companies working in critical infrastructure, constitutional facilities and leading private companies from the cybersecurity industry were therefore once again invited to contribute to the volume of information collected from their own perspective and to provide their expertise to support the preparation of this report in this reporting year. This is the most likely means of achieving a valid and largely complete picture of the cyber situation in Austria. Focus is not primarily on specific cases but instead on trends and developments in the sense of an abstract overview.

### 1.2.1 Companies working in critical infrastructure and constitutional facilities

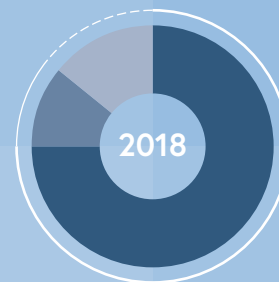
All of the Austrian companies surveyed which work in critical infrastructure made further investments in cybersecurity in the 2019 reporting year. Half of the companies increased their budget for the reporting period while the other half kept the 2019 budget at the previous year's level. In contrast to the previous reporting period, no company reported a decreased budget for cybersecurity this time. Overall, expenditure on IT security has stabilised at a high level.

## Change in the available cybersecurity budget

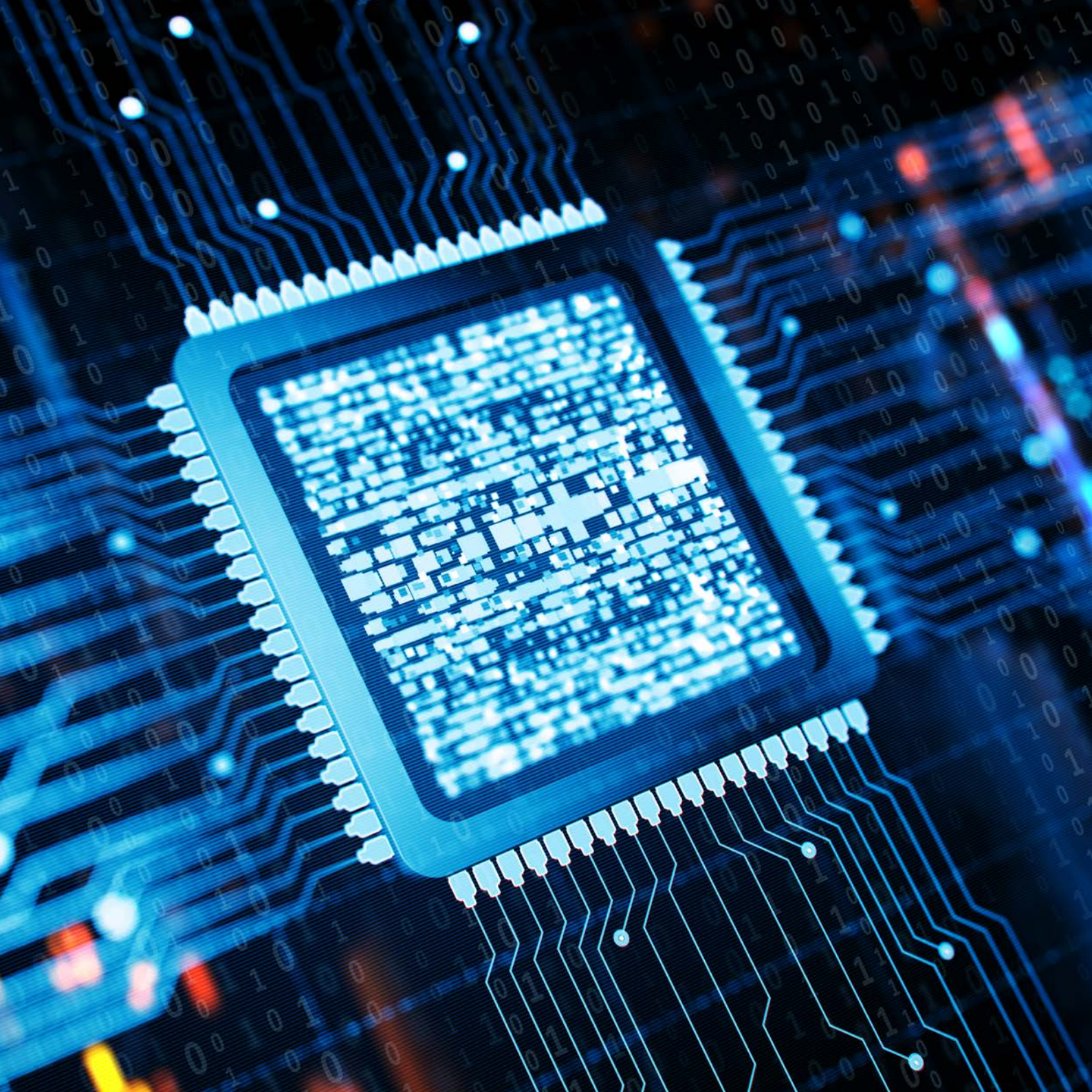


- more ●
- same ○
- less ●
- n/s ○

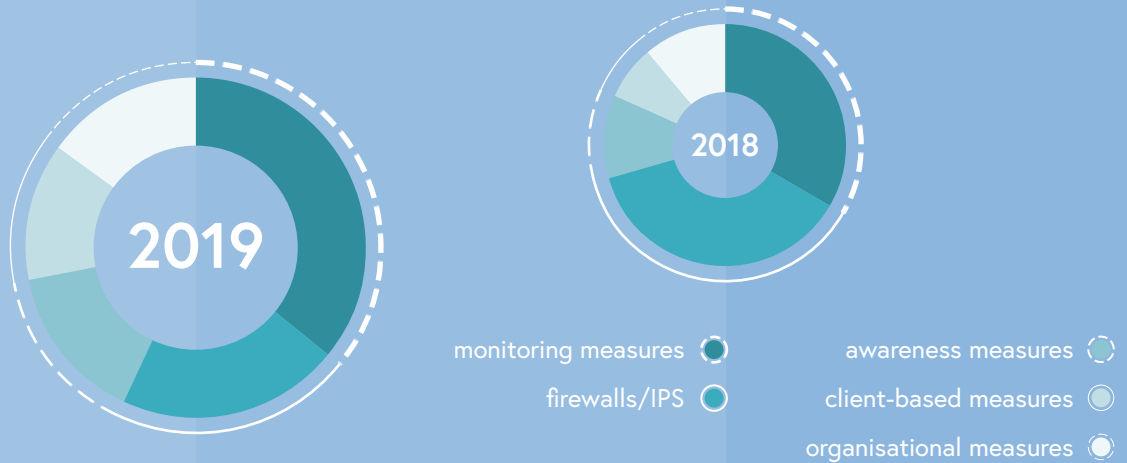
## Additional IT security measures



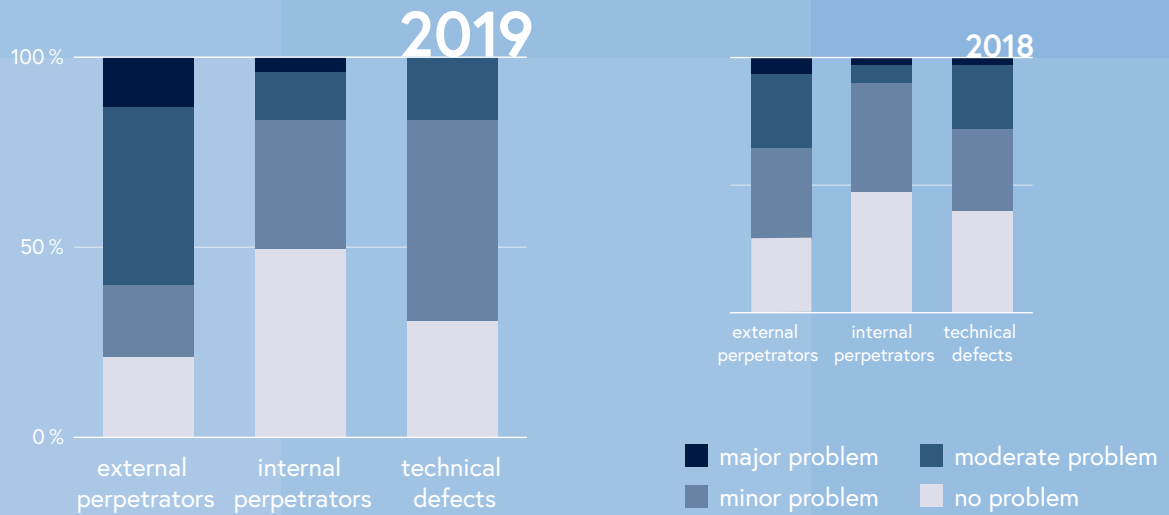
- yes ●
- no ●
- n/s ●



## Additional IT security measures



## Causes of incidents



## Trend towards active monitoring of corporate networks

Along with increasing budgets, the companies and organisations which responded almost all (over 96%) took additional IT security measures. Increased awareness of security is most likely due to the simultaneous design of state framework conditions. The Network and Information Systems Security Act (NIS Act) was passed in early 2019 to create a high common level of security among operators of essential services and providers of digital services. In 2018, Austria also adapted the Data Protection Act to the new General Data Protection Regulation (GDPR), which provides for increased statutory IT security requirements.

The security measures taken in the field of IT included monitoring, the operation of firewalls/IPSs, the implementation of awareness training sessions, client-based measures and measures which were organisational in nature. The most noticeable difference compared to the previous year was a clear increase in the use of firewalls/IPSs. Technical advancement has on the one hand made scalable products which are simple to configure available but has also increased the effective defences of the systems.

Independently of this, a trend has been identified among companies and organisations to no longer rely on “isolation” (through firewalls) alone but rather to use active monitoring measures to identify attackers who have already penetrated the company or organisation’s network. This involves searching for current threats to the respective organisation and in a second step the targeted checking of systems after infections. Alongside this, in many places preparatory measures were also taken to analyse security incidents using forensic methods.

In many cases, awareness measures were either introduced for the first time or existing measures were strengthened and their output rated as effective and in some cases essential in terms of preventing a large number of cyber attacks in “lessons learned”. These measures included specialist lectures and simulated phishing or ransomware

attacks. In parallel to this, companies also stated that the measures taken in the past were successful in 2019 and that as a result attempted attacks and attacks were able to be identified in advance. Many of those surveyed also established Security Information and Event Management (SIEM) systems and Security Operations Centres (SOC).

A large number of the companies took organisational measures in the 2019 reporting year, including establishing stricter policies for passwords or adapting corporate processes.

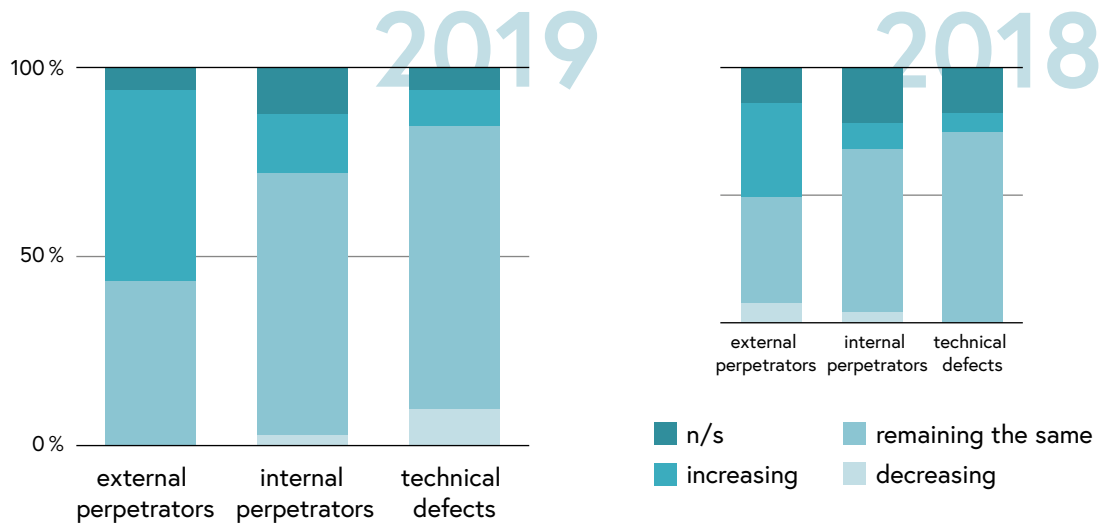
Here, too, there was a link to the feedback given as “lessons learned”: according to this, in 2019 the organisations surveyed were increasingly engaging in new regulatory measures such as the GDPR or the implementation of the NIS Act, which entered into force in 2019.

On the whole, the assessment of the causes of incidents also shows a comparable picture for 2019 as for the previous reporting year. According to this assessment, it was primarily external attackers or technical defects which caused the incidents with internal attackers involved in just a small number of incidents. There were, however, slight shifts compared to 2018 indicating that the risk from external attackers is dropping while the risk from internal attackers is rising. The risk of a technical defect is rated as increasingly problematic.

Endangerment by  
interior offenders  
increases

Looking at the information on the trend, all of the causes of incidents were indicated as increasing, albeit with low rates of increase compared to the previous year. In terms of external attacks, this interaction could be due to the fact that the increased defence measures, particularly in the field of ransomware and phishing, have resulted in a rise in the volume of attacks but these attacks are more frequently being identified and therefore defended against in advance.

## Trends in the causes of incidents



In terms of general developments in the IT security industry, there was once again an expansion in cloud computing in 2019. This trend, however, is viewed with increased scepticism by the companies surveyed. There is a loss of control and sovereignty over a company's own data (albeit only a perceived one) linked to the increasing dependence on external providers. Local (on-site) solutions are being replaced more and more aggressively by cloud solutions, and in the long term these will become established. The increasing lack of an alternative to cloud solutions has resulted in a degree of resignation among those surveyed which should not be underestimated.

Other trends (regulatory measures, Internet of Things, Artificial Intelligence, Distributed Denial of Service, Social Engineering) are very much falling behind the issue of cloud provisions.





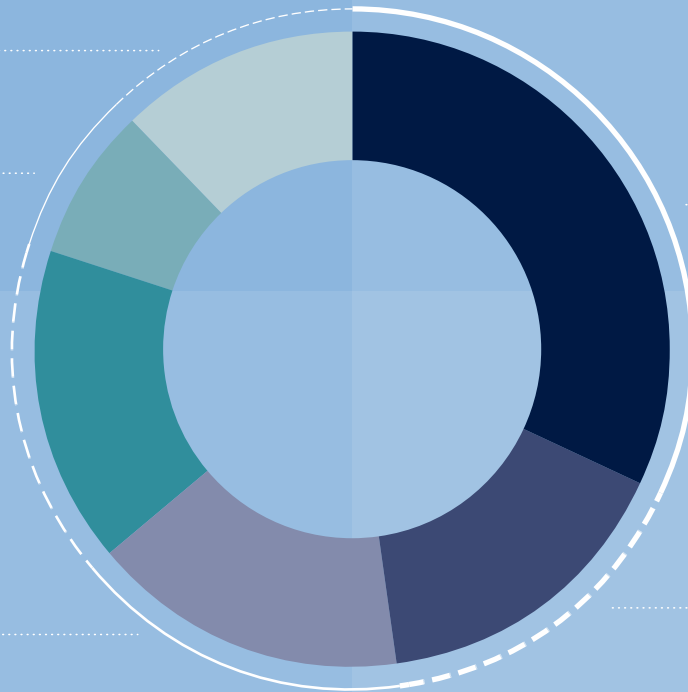
## General trends 2019

Social Engineering

DDoS

AI

IoT



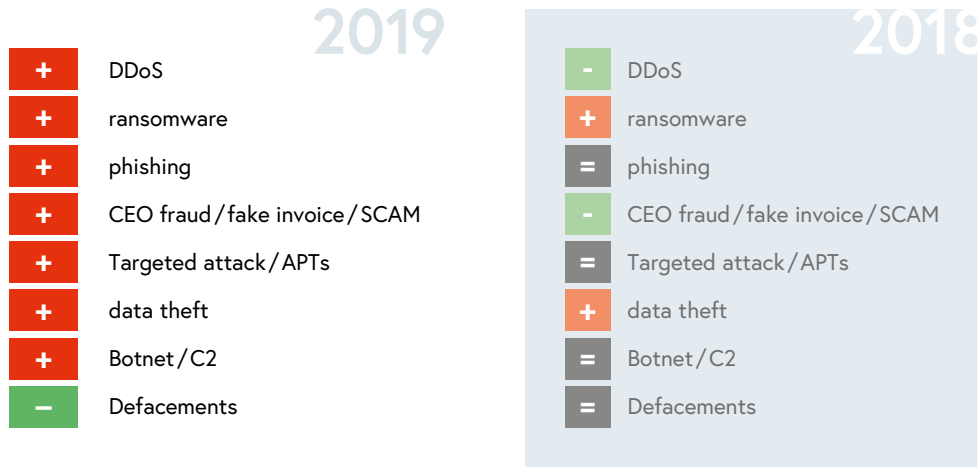
cloud

regulatory  
measures

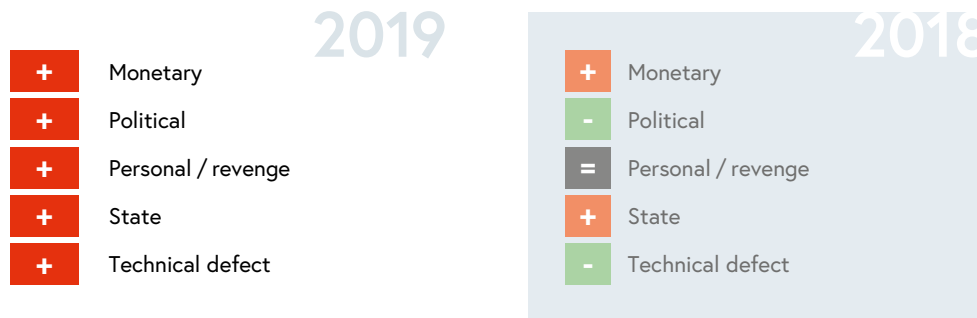
## 1.2.2 Leading private companies from the cybersecurity industry

The survey of leading private cybersecurity service providers received a comparatively low response rate again in the 2019 reporting year.<sup>3</sup> The survey responses that were received, however, enabled us to identify a number of trends:

### Trends in type of incident



### Trends in motivation



<sup>3</sup> Our thanks go to the companies Alpha Strike Labs GmbH, Kapsch BusinessCom AG and SEC Consult Unternehmensberatung GmbH in particular for their answers.





## Increase in espionage using APTs

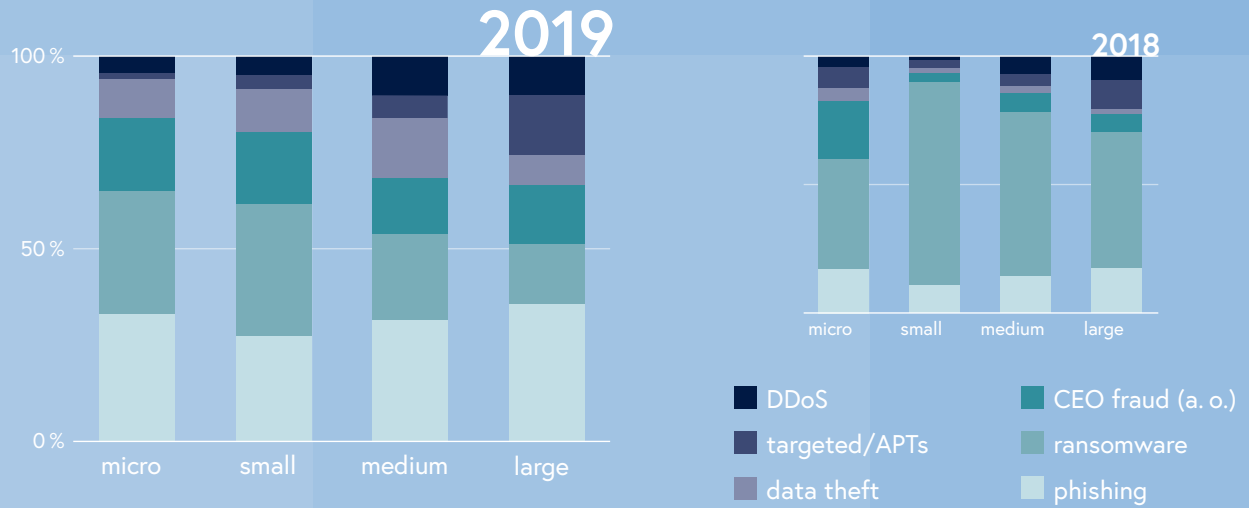
Overall, an increase in all areas was reported for the incident types. The only area where a slight decrease was reported in 2019 was defacement. There was also an increase in motivation across all areas in 2019. The increase in politically-motivated incidents (espionage) should in particular be noted with a degree of concern, since these could have been incidents involving the use of APTs. These not only have the potential to cause significant damage, but due to the large number of unreported cases in the 2019 reporting year could make up a higher overall share.

Small and medium-sized companies report a high percentage of broad attacks, in other words ransomware and phishing, in 2019. As the size of the company increases, targeted attacks for the purposes of industrial espionage or to disrupt operations through a DDoS attack become increasingly relevant.

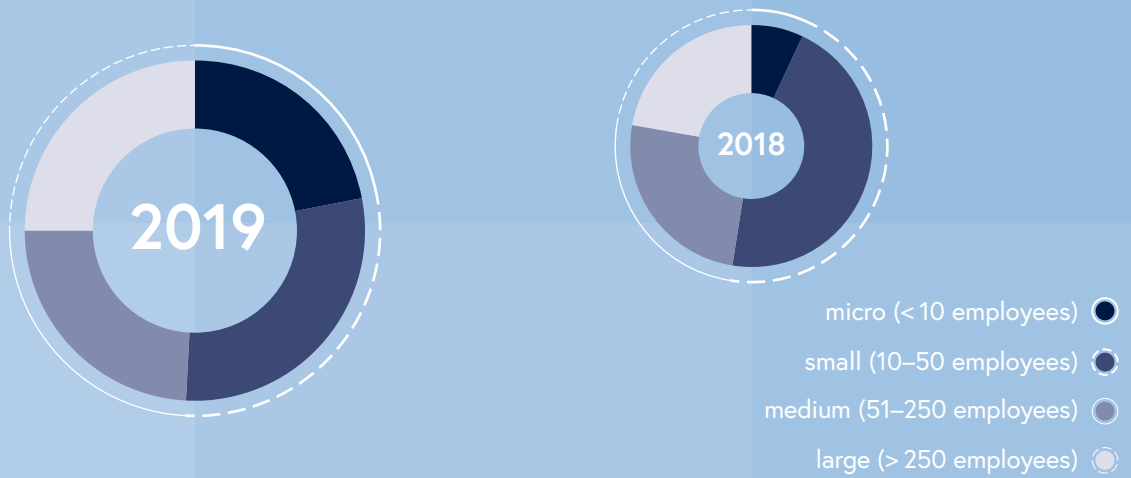
In terms of the types of incident that are obviously increasing the most, the corresponding “lessons learned” and knowledge from the leading private companies in the cybersecurity industry are particularly relevant.

There was a further increase in known attempted ransomware attacks in 2019. Overall, awareness of the problem has increased in companies and organisations, and more money has been invested in prevention measures (of a technical and non-technical nature). This can be seen in particular in the fact that very small companies (< 10 employees) who reported no ransomware attacks in the previous year are now more strongly represented in the statistics. User training sessions on awareness and simulated phishing attacks along with new methods of detecting malware were able to stop many attacks in advance, with large companies remaining in the lead thanks to the capacities they have available.

## Incident types by company size



## Ransomware attacks by company size







In the case of phishing attacks, security service providers strike a positive balance: although there was an overall increase in attacks, only a very small number of attacks were successful. There was a significant decline among large companies in 2019. This could also be due to the employees being sensitised to the matter and other security measures coming into effect. Very small companies (<10 employees) have some catching up to do: more incidents of phishing were reported in 2019 than in the previous year. The situation for small and medium-sized companies, however, appears to have stabilised.

Security service providers draw a positive balance

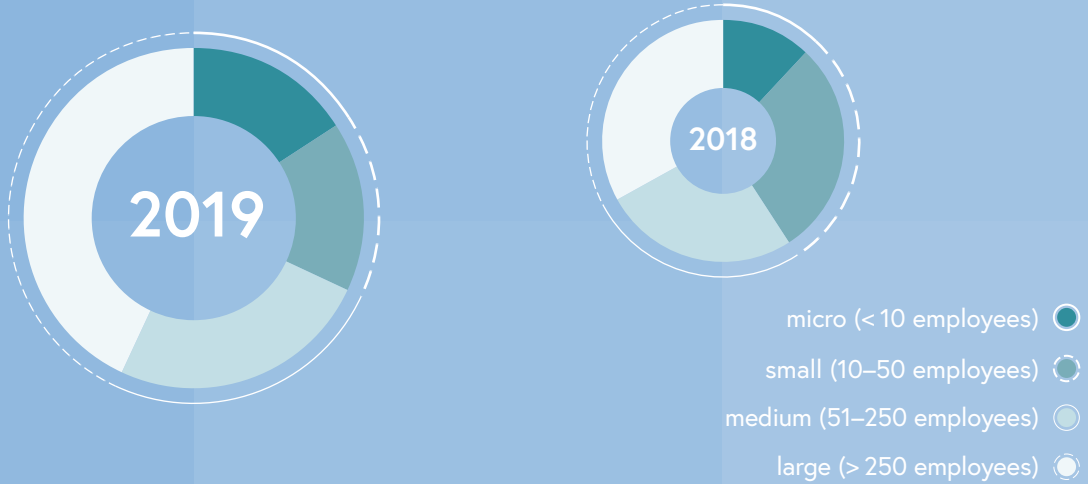
Attacks using CEO fraud/fake invoices/scamming were also identified in the 2019 reporting year. In some cases, they were linked to actual hacking attacks in advance. The information acquired by hacking was then used for the “actual” attempted fraud. A decline in volume compared to 2018 was identified in large companies, probably because companies and their staff are now more sensitised to the issues and suitable processes have been set up. In contrast to this, the number of attacks on very small companies (<10 employees) increased significantly. The need to catch up on protective measures is much higher for these companies. Small and medium-sized companies, however, were largely able to stabilise the situation.

A significant increase in targeted attacks/APTs (focusing on obtaining information) was reported among large companies in the 2019 reporting year. This was associated with an unmistakable drop in the other company sizes (very small, small and medium-sized). The reasons for this could be increased focusing of the attack strategy on large companies, or better opportunities for large companies to identify attacks.

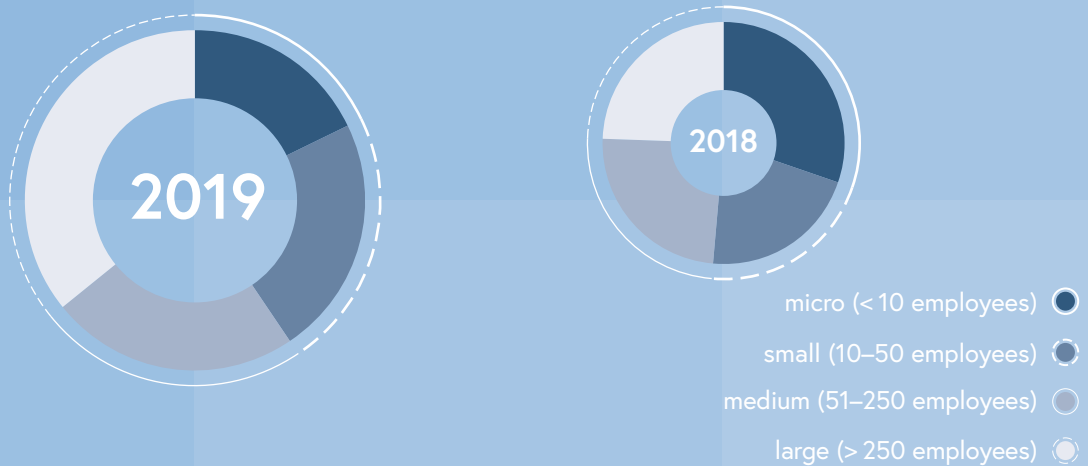
DDoS attacks also increased again in the reporting year. In addition to actual defence, the inability to clearly attribute actions to attackers and their motivation was found to be a significant problem. These campaigns, which are often political or otherwise actionist in nature, primarily of course affect medium-sized and above all large companies known from public discourse. It is striking, however, that there was an increase in DDoS attacks on small and even very small companies (>10 employees) in the 2019 reporting year.

DDoS-attacks even on companies with less than ten employees

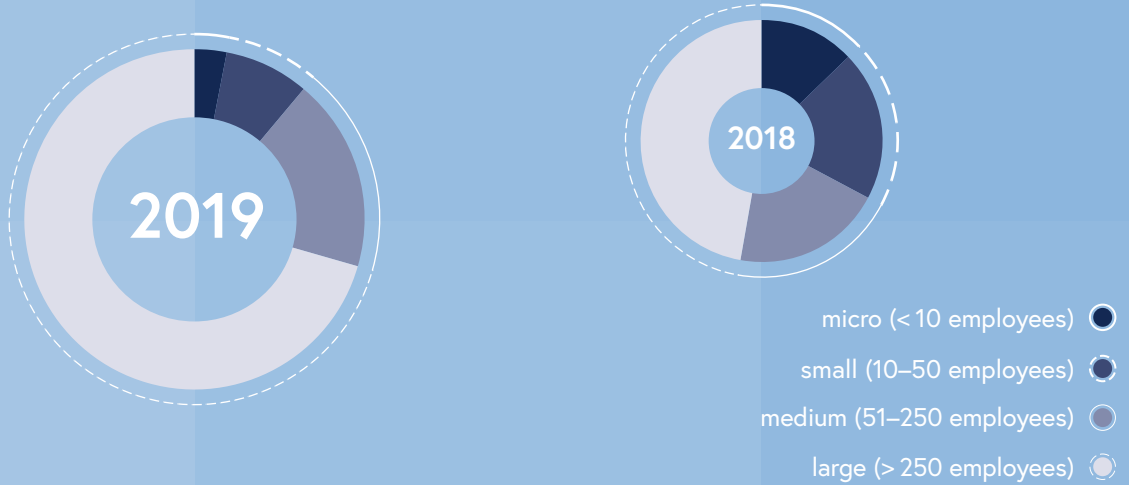
## Phishing attacks by company size



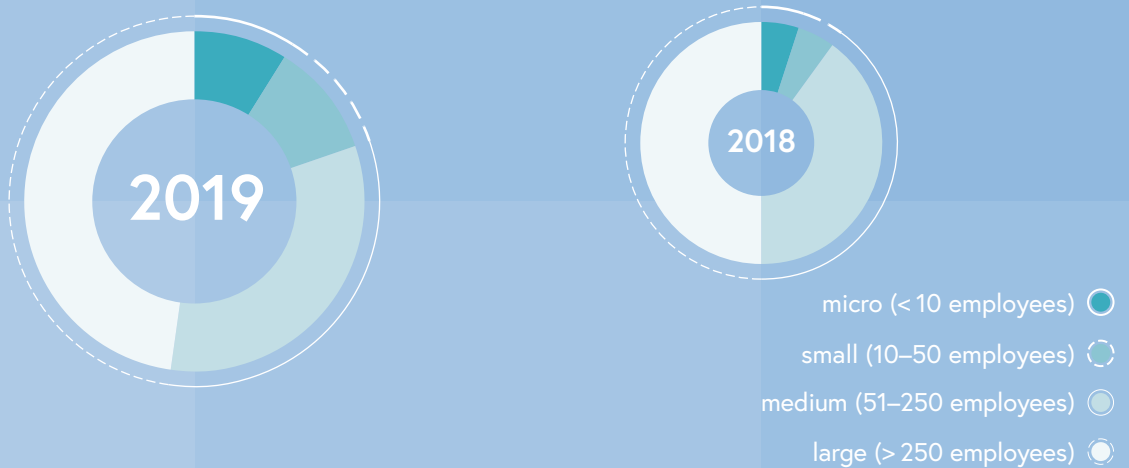
## Attacks using CEO fraud / fake invoices / scamming by company size



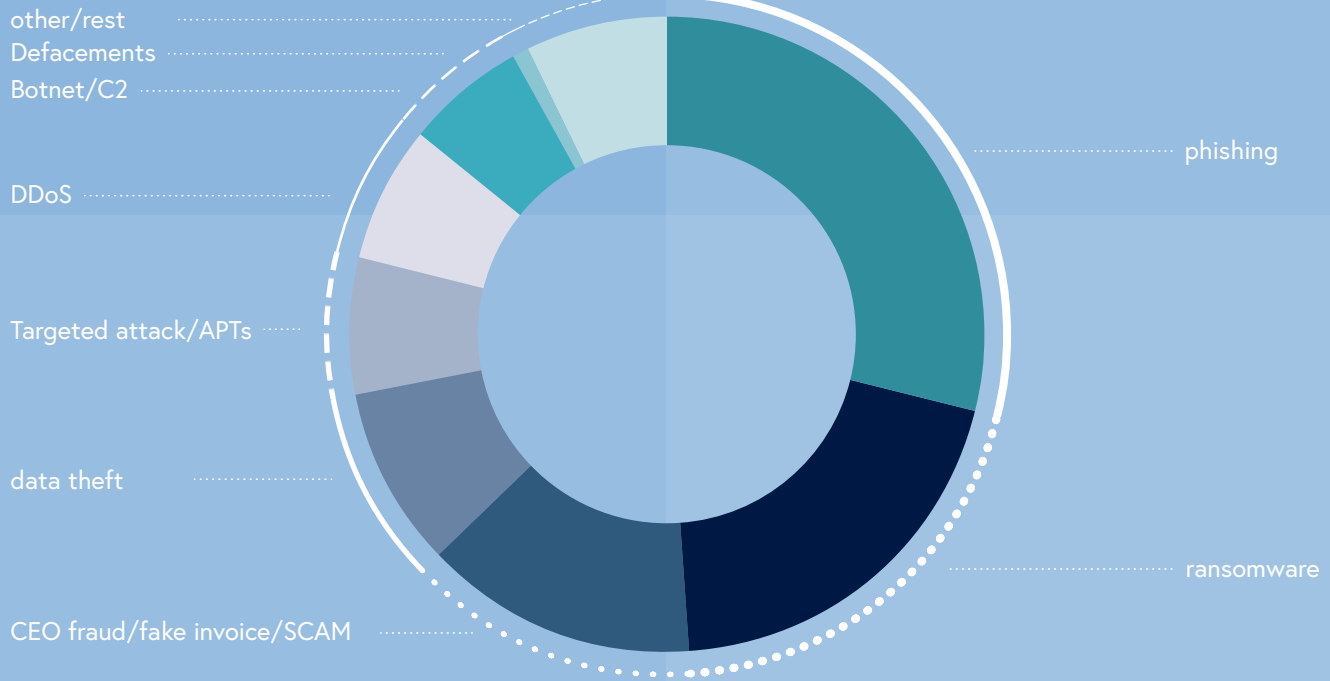
## Targeted attacks/APTs by company size



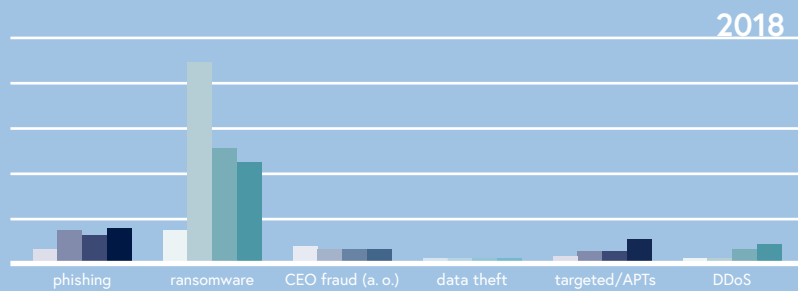
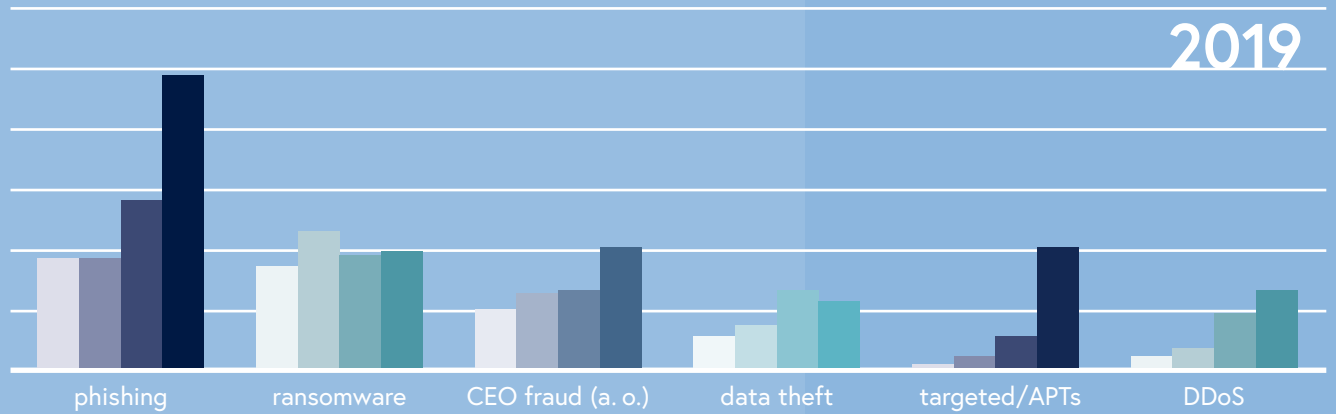
## Attacks using DDoS by company size



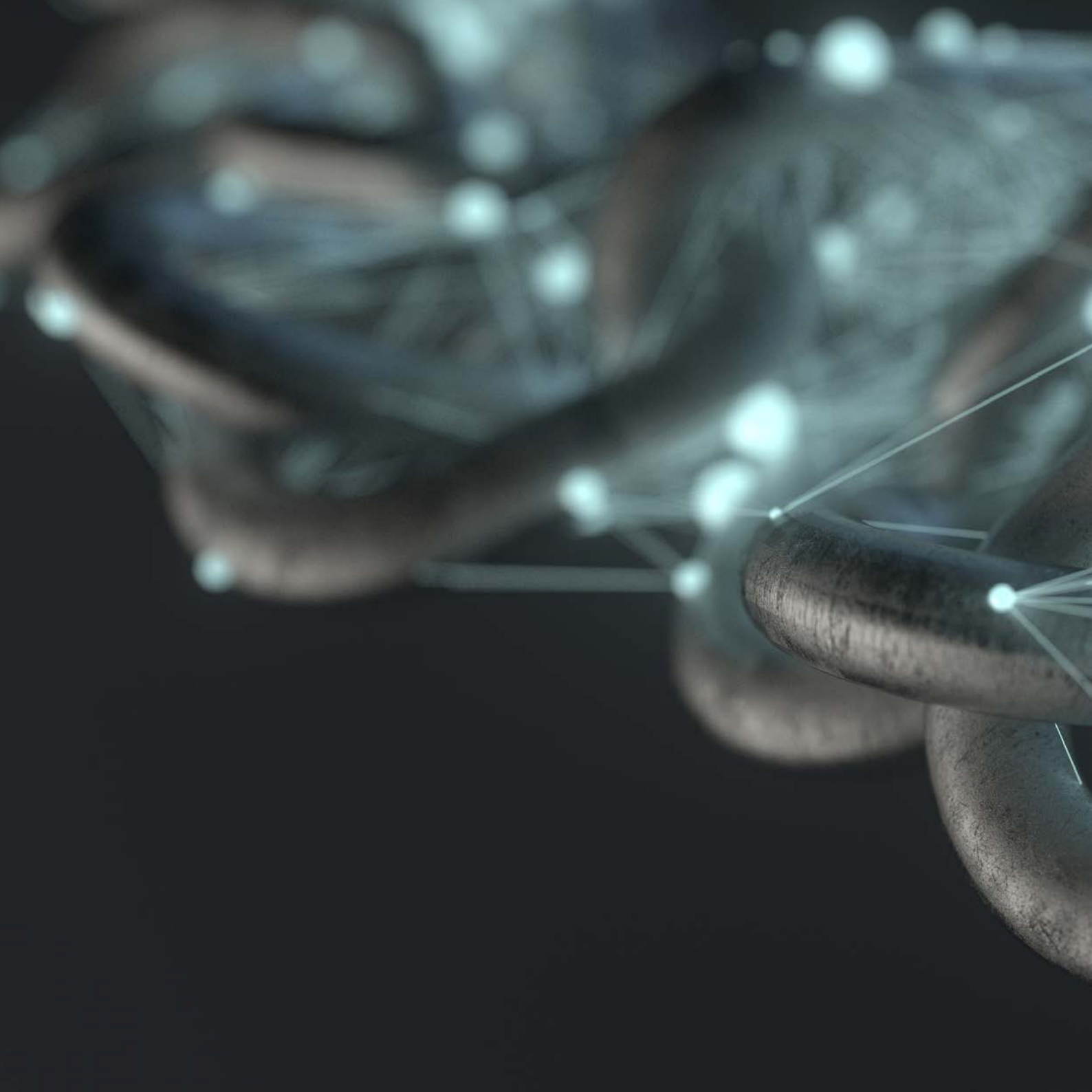
## Types of attacks 2019

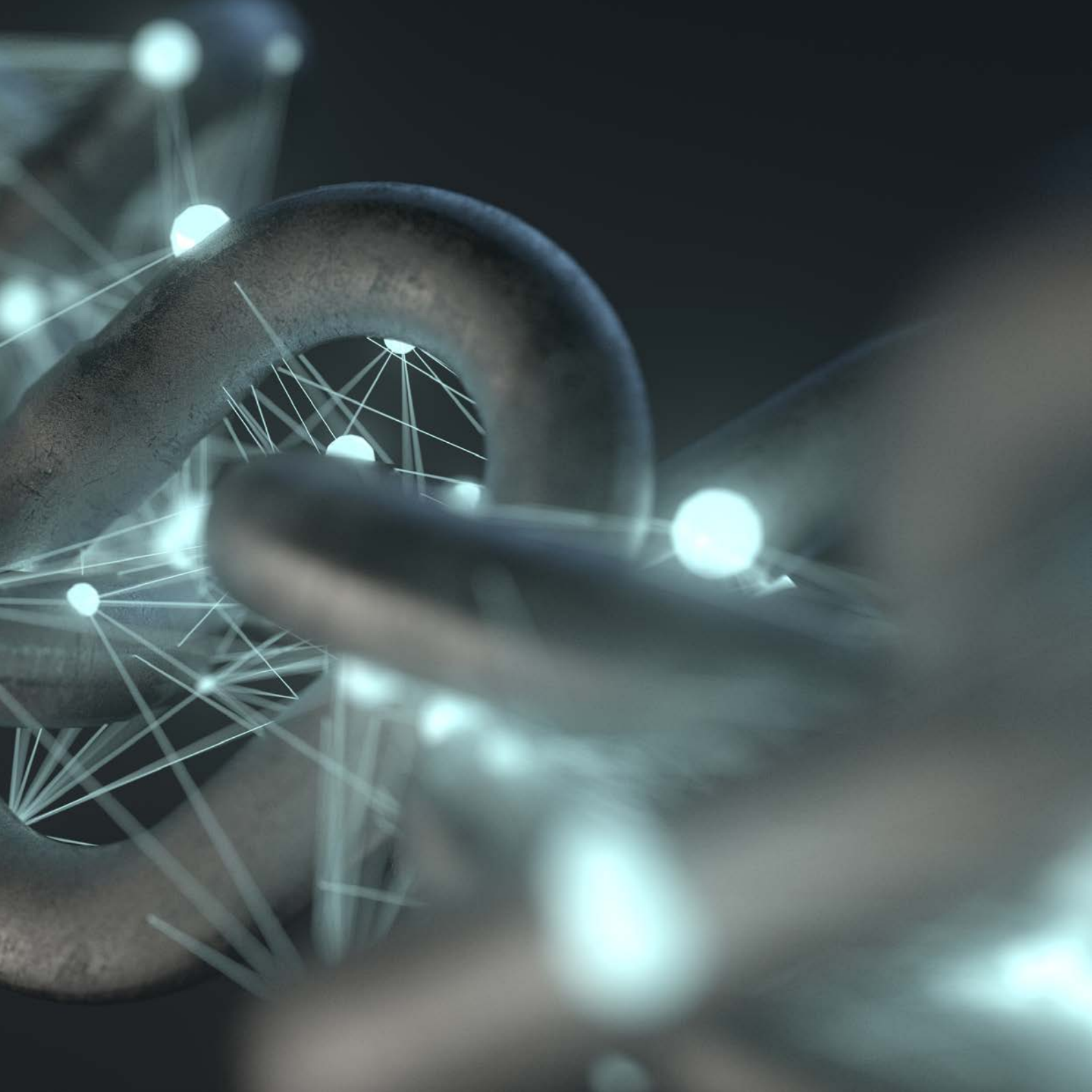


## Threats by company size



- micro (< 10 employees)
- small (10–50 employees)
- medium (51–250 employees)
- large (> 250 employees)





## 1.3 Cybercrime situation

With over 13,000 crimes reported in the first six months of 2019, the assessment of the provisional police crime statistics shows an increase of around 50 percent compared to the corresponding period in 2018. The exact crime statistics were published in the criminal police department's criminal statistics in spring 2020. A more in-depth analysis and description of the criminal phenomena is provided in the form of the annual cybercrime report published by the Criminal Intelligence Service Austria.

The term cybercrime comprises:

- attacks on data and computer systems (“cybercrime in the narrow sense”)
- internet fraud
- other types of criminality in which it is not the computer systems themselves which are the target and they are merely used as a means to commit classic crimes (“cybercrime in the broader sense”)

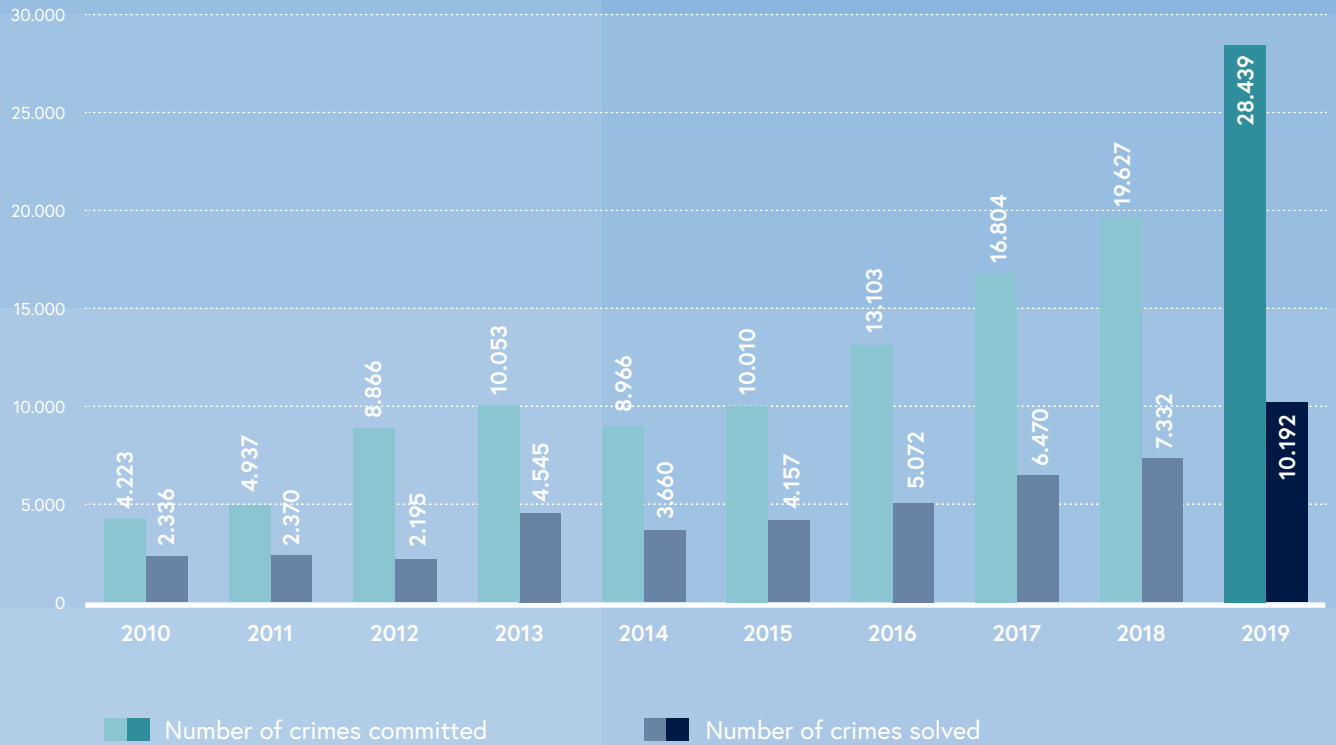
### 1.3.1 Internet fraud

The largest factor in terms of numbers is internet fraud. It is also largely responsible for the increase in cybercrimes last year. An increase in crimes of around a third was estimated for the first six months. As digitisation progresses, fraud is increasingly moving online. For perpetrators, it is easy to carry out fraud undetected and therefore “safely” due to technical anonymisation and concealment of the financial flows. In addition to this, global access to the internet means increasing numbers of people are potential victims. Commonly used methods of fraud include sending emails promising that a person has won something and order fraud using what are known as fake online shops. Around 200 new fake online shops were able to be identified, primarily in the field of technology and clothing, which can be attributed to a few small groups of perpetrators. The figures doubled in the pre-Christmas period in 2019, with an average of up to 10 new fake and phishing shops observed per day. Numerous cases of fraud using fake identities and

Ten new fake and phishing stores every day



## Cybercrime trends



## Social Engineering is the major attack vector

contact details when filling online orders and by fraudsters getting in touch by telephone, email or social media were recorded. In addition to feigning romantic relationships, common approaches were to offer particularly lucrative business models and alleged technical support services (known as the Tech Support Scam). The first cases of attempted CEO fraud via WhatsApp were reported in May 2019. In autumn, there was an exponential increase in attacks on Facebook and Instagram through old accounts which are no longer used by their previous owners but have been reactivated by criminals.

Social engineering remained a major vector for attacks in the previous year.

### **1.3.2 Cybercrime in the narrow sense**

In terms of cybercrime in the narrow sense, the complaints filed in the reporting period of the first six months increased by around 60 percent. This included crimes in which attacks were made on data or computer systems by exploiting the information and communication technologies. Examples of this are unlawful access to computer systems or damage to data. There were a very large number of reports of unlawful financial transactions, mostly from private bank accounts, in the period from May to June. From June, technical security gaps (such as RDP vulnerabilities in Microsoft products) became a major threat for companies and institutions which did not carry out system updates promptly. Towards the end of the year there were massive attacks on telephone systems (VoIP systems) which were not sufficiently well secured. The criminals predominantly used non-working hours to penetrate companies' telephone systems. Expensive premium rate numbers or fraudulent carriers were then called using a programmed call centre mode.

As a result of the large number of data leaks in 2018 and 2019, large quantities of personal data were published online or offered for sale on the dark web. Unlawful access using access data obtained in this way increased considerably. Phishing attacks on organisations working in critical infrastructure were also recorded, in which changes to Outlook email rules meant incoming messages were forwarded to external email addresses.

There were also increasing numbers of spam phishing campaigns on the DNS infrastructure which used an improved version of the malicious EMOTET code to carry out more targeted attacks on public facilities. The threat remained for small and medium-sized companies in particular over the entire year. The criminals generally use this Trojan to access the victim's IT system, with the data only being encrypted by other devices in the network after a few days or weeks.

Like for 2019, it is likely that next year criminals will continue to use increasing numbers of DDoS attacks in the form of crime as a service. These attacks do not aim to achieve a broader effect and instead are much more targeted activism to restrict the availability of certain websites.

### **1.3.3 Other online criminality**

The third sub-section of "other online criminality" increased around 140 percent in the first six months of 2019. The reason for this was the increasing shift in classic criminal offences online. At the same time, "crime as a service" is also offered on the dark web. These are mainly hacking tools or Trojans used for extortion. An increased market in counterfeit money, child pornography, credit card details and counterfeit documents has also been identified. It is primarily extortion with ransomware and mass extortion emails, mostly accompanied by a demand for money in Bitcoin, which are increasing to a vast extent as a result of the services offered on the dark web. Over the course of the year, the criminals pursued their victims in an increasingly targeted manner and their methods became more sophisticated and tailored with a technical compromise of an average of fourteen days. Extortion amounts have even been tailored to victims' alleged income. In this context, an "extortion email working group" started work at the beginning of the year in the C4 of the Criminal Intelligence Service Austria in order to be able to process operations of this type centrally in the future.

**” ‘other online criminality’ recorded an increase of about 140% in the first half of 2019.**



## 1.4 Cybersituation in national defence

In addition to the physical domains of land, air, sea and space, technological developments and global digital networking mean that cyberspace as an intangible domain has become massively more significant in the military sector.

Implementation of strategic objectives also takes place in cyberspace

In present and future military conflicts and the “grey area” between war and peace, “hybrid conflicts”, efforts will be made to achieve effects in cyberspace. It should be noted in particular that the attribution of defensive and offensive actions can be concealed in cyberspace. This can also favour the (hidden) implementation of strategic and strategic military objectives.

For the Federal Ministry of Defence, this means aligning itself with national military defence in cyberspace as well as possible in the sense of the core mission of the Austrian Armed Forces as set out in Section 2 letter a of the National Defence Act and to prepare for this. This includes both all measures in Information and Communication Technology (ICT) security and all measures to defend against cyber attacks on the military ICT system.

As a result of the current overall situation in the Austrian Armed Forces, when it comes to protection in cyberspace, the focus is primarily on military ICT systems.<sup>4</sup>

In general, the following trends can be inferred from the experiences of the past few years:

- an increasing number of automated attacks at a network level,
- more professional, larger scale social engineering attacks via email.

---

4 “Unser Heer 2030” [Our Army 2030] report

## **Border protection**

Data from the Federal Ministry of Defence security systems indicate that trends that were identified previously will continue unchanged. An accelerating increase in incidents of access to network levels in security facilities that were able to be blocked by in-house security measures was observed. These were mainly caused by automated attacks and scans. In addition to this, increasing numbers of manual attacks in combination with automated attacks were observed. A further increase in this form of attacks can be assumed for the coming year as was the case in 2019.

## **Attacks via email**

More large-scale attacks in the form of email attachments, for example containing the widespread malicious EMOTET code, were identified compared to the previous time period. An increase in personalised attacks was also observed.

A further increase in attacks must be expected

## **Outlook**

A further rise in automated attacks and these increasingly being combined with manual attacks is expected in the future. The assumption of a trend towards automated personalisation, particularly when email is used as a vector, has been confirmed and should also be assumed for the next year. This means that the attackers not only pose as known services (bank, post office, invoices etc.) but are also and will also increasingly make references to the company or person themselves.

As a result of the current overall situation in the Austrian Armed Forces, future prompt early detection and support for defence from the Austrian Armed Forces cannot be ensured<sup>5</sup>.

---

5 "Unser Heer 2030" [Our Army 2030] report









2

# International developments

Cybersecurity issues have been addressed and discussed (in some cases very controversially) by numerous international organisations and multilateral forums in the last few years. The relevant external and security policy measures are being coordinated by the Federal Ministry for European and International Affairs. When it comes to the European Union (EU), the topic of cybersecurity is coordinated by the Federal Chancellery.

The rapid developments in the field of cybersecurity raise a number of fundamental questions about international law, particularly international humanitarian law and fundamental and human rights. At an international level, Austria generally advocates a free, open and secure internet and the exercise of all human rights in the virtual space too. An appropriate balance must be struck between the interests of law enforcement and respecting fundamental human rights such as the right to freedom of expression and freedom of information and the right to a private life and privacy.

## 2.1 European Union (EU)



### 2.1.1 Horizontal Working Party on Cyber Issues

The Horizontal Working Party on Cyber Issues (“HWP Cyber”) was set up in 2016 and is responsible for coordinating the work of the European Council on cyberspace issues, in particular cyber policy and legislative activities. It sets the cyber priorities and strategic objectives of the EU as part of a comprehensive political framework and ensures a horizontal working platform which enables harmonisation and a uniform approach to issues of cyber policy.

The Council Working Group works closely with other related working groups and the European Commission (EC), the European External Action Service (EEAS), Europol, Eurojust, the European Union Agency for Fundamental Rights (FRA), the European Defence Agency (EDA) and ENISA.

In 2019, there were a total of 35 sessions of the HWP Cyber. One focus of the work was the negotiations on the proposed EU Regulation on setting up the European Competence Centre for Cybersecurity in Industry, Technology and Research and the Network of National Coordination Centres, which were accepted under Austrian Presidency after being submitted on 12 September 2018. Under Romanian Presidency, a mandate was able to be achieved and two trilogues were held with the European Parliament. The negotiations were not, however, able to be completed before the end of the EP’s legislative term. Since then, the HWP Cyber has been working on a new version of the negotiation mandate. For more information on the content of the proposed Regulation, see Chapter 2.1.6.

The HWP Cyber focused on the European Competence Center for Cyber Security and the further development of the EU’s diplomatic response to malicious cyber activities.

In the field of cyber diplomacy, the focus was on the further development of the EU's joint diplomatic response to malicious cyber activities ("Cyber Diplomacy Toolbox"). A table-top exercise on this called "CYBER-DIPLO TTX 19" was carried out in late November. The focus was on achieving a joint EU position on international developments in cybersecurity, for example in a UN context or in relation to the cyber sanction regime, specific steps as part of the Cyber Diplomacy Toolbox or discussions on attribution.

The "Council conclusions on cybersecurity capacities and cyber capacity building in the EU" prepared by the HWP Cyber was accepted by the Council (General Affairs) on 19 March 2019.

### **2.1.2 NIS Cooperation Group**

The objective of the NIS Cooperation Group set up by the NIS Directive is to support and facilitate strategic collaboration and the exchange of information between the member states. The NIS Cooperation Group is made up of representatives of the member states, the European Commission and ENISA, with the chair held by the country holding the Council Presidency.

The NIS Cooperation Group performs its activities on the basis of two-year work programmes. The focus continues to be on activities linked to the implementation of the NIS Directive. The trend continued in 2019, with the NIS Cooperation Group addressing more comprehensive issues of cybersecurity policy. The "Work Stream on Cyber Security of Election Technology" was set up in 2018 and the result of this was accepted by the NIS Cooperation Group in July 2018 (CG Publication 03/2018—Compendium on cybersecurity of election technology). The flexible structure of the NIS Cooperation Group meant that, in addition to "NIS and cyber authorities", other domestic authorities were also able to take part to address this issue together with the NIS and cyber authorities. On 26 March 2019, the European Commission published the recommendation on cybersecurity of 5G networks, which assigned the NIS Cooperation Group the essential operationalisation role.



The main results from the NIS Cooperation Group include non-binding guidelines for the member states. Reference documents were also developed and published by the NIS Cooperation Group in 2019. One focus was the work on the topic of the cybersecurity of 5G networks. In addition to this, an extensive reference document about the implementation of the NIS Directive in the energy sector was also accepted. Specifically, the reference documents published are:

- CG Publication 01/2019—Guidelines for the Member States on voluntary information exchange on cross-border dependencies,
- CG Publication 02/2019—Risk assessment of 5G networks,
- CG Publication 03/2019—Sectorial implementation of the NIS Directive in the Energy sector.

There were four plenary meetings of the NIS Cooperation Group in 2019, along with more than 16 sessions as part of the Work Streams. In 2019, one Work Stream was started on the digital infrastructure sector and another on the security of 5G networks. In a continuation of the idea implemented for the first time under Austrian Presidency, the strategically oriented NIS Cooperation Group and the operative CSIRTs network took place as back-to-back meetings as part of the plenary sessions in order to enable an exchange about the most important topics for both groups.

### **2.1.3 Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats**

The Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats (HWP ERCHT) was created in 2019 from a “Friends of Presidency Group”.

The aim of the working party is to offer a horizontal overview of issues linked to hybrid threats to support coherence and collaboration between the EU and its member states. The work focuses on countering hybrid threats, enhancing the resilience of both states

The NIS cooperation group is increasingly dealing with broader cyber security policy issues, e.g. cybersecurity of 5G networks.

and society to threats of this type, improving strategic communication and fighting disinformation.

On 10 December 2019, the European Council accepted conclusions on “additional efforts to enhance resilience and counter hybrid threats”. These conclusions set out priorities in the context of the implementation of the new Strategic Agenda for the period 2019–2024. These include, among other things, protecting societies, citizens and freedoms and the security of the Union from hybrid threats. The aim is to achieve this by promoting a comprehensive security approach with improved coordination, more funds and better technical capacities. The approach aims to build on the extensive work which has already been carried out in various political areas, including as part of security and defence policy collaboration. Furthermore, the Council noted that malicious cyber activities can be part of a hybrid threat and underlined the importance of the NIS Directive.

#### **2.1.4 EU certification framework (Cybersecurity Act)**

The Cybersecurity Act came into force on 27 June 2019.

With the entry into force of the Cybersecurity Act on 27 June 2019, a European certification framework for cybersecurity was created, among other things. The European certification framework for cybersecurity sets out a mechanism by means of which European schemes for cybersecurity certification are created. The intention is for these to certify that ICT products, services and processes assessed according to a scheme of this type meet the security requirements set out. This should enable the availability, authenticity, integrity or confidentiality of data which are stored, sent or processed and functions or services which are offered by these ICT products, services and processes or made available by these to be protected over their entire life cycle.



In collaboration with the member states and stakeholders, the European Commission is working on what is known as the Union's continuing work programme on European cybersecurity certification, within the scope of which the strategic priorities for future European schemes for cybersecurity certification are to be set out.

The European Cybersecurity Certification Group (ECCG) was created by the Cybersecurity Act and started work with its first formal meeting on 18 September 2019. The ECCG is made up of representatives of national cybersecurity certification authorities and representatives of other relevant national authorities. Austria is represented in the ECCG by the Federal CIO (Federal Ministry for Digital and Economic Affairs) and the strategic NIS Office (Federal Chancellery).

### **2.1.5 Cybersecurity of 5G networks**

The security of the technology known as the “fifth generation of the mobile network” (5G) was the focus of the attention of cybersecurity authorities in 2019.

In the Resolution of 12 March 2019 on security threats connected with the rising Chinese technological presence in the EU, the European Parliament asked the European Commission and the member states to take measures at a Union level. Furthermore, the Joint Communication by the European Commission and the High Representative of the EU “EU-China – A strategic outlook” of 12 March 2019 highlights the fact that a joint approach by the EU on the security of 5G networks is required to protect against the potentially serious effects on the security of critical digital infrastructures. Finally, in its conclusions of 22 March 2019 the European Council declared itself in favour of the European Commission making recommendations for a coordinated approach to the security of 5G networks.

To this effect, the European Commission published a recommendation about the cybersecurity of 5G networks on 26 March 2019, which recommends the following measures in particular:

- the implementation of a national risk analysis focusing on 5G networks;
- checking the national measures which have been put in place;
- increased collaboration at an EU level and the implementation of an EU-wide coordinated risk analysis and
- the creation of a joint tool for risk minimisation measures.

In the field of cybersecurity, a coordinated European risk assessment, based on risk analyses of all member states, was carried out for the first time on the topic of 5G.

As a first step and implementing the recommendation, a national risk analysis of the possible dangers which could arise as a result of the new standard was carried out. To this end, the existing national risk analysis was updated to include risks which could arise from the new standard. A separate work stream which is part of the NIS Cooperation Group was created to support member states. The national risk analysis was sent to the EC and ENISA promptly in July 2019.

The CG Publication 02/2019 – Risk assessment of 5G networks was published on 9 October 2019 with the premise of forming the basis for a future toolbox. A European overview based on the joint elements of the individual risk analyses carried out by the member states was created in this coordinated risk assessment. The greatest dangers for 5G networks, the most active threat agents, the most important assets and their degree of sensitivity, the main weaknesses and the main risks and associated scenarios were identified.

The “ENISA Threat Landscape for 5G Networks” was published in November 2019 and offers an in-depth insight into the risks and challenges which need to be overcome in connection with 5G networks. A technical overview of the 5G architecture, the identification of important assets (asset diagram), the assessment of 5G threats (threat

taxonomy), the identification of the risk to assets (asset threat mapping) and an initial assessment of the possible motives of the threat agents.

On 3 December 2019, the European Council accepted conclusions “on the importance of 5G for the European economy and the need to limit the security risks linked to 5G”, according to which the EU and the member states need to focus on promoting the cybersecurity of 5G networks in particular.

### **2.1.6 Cyber diplomacy**

Significant expansions for practical implementation were made to the Cyber Diplomacy Toolbox (framework for a joint diplomatic response from the EU to malicious cyber activities) in 2019. In May 2019, the Council accepted a cyber sanctions regime which can be used to target individuals and entities (not states) with account freezing and travel restrictions. There is a lack of international contracts and organisations on which it would be possible to build in the field of cybersecurity, so the foundation work needed to be done on this. A further difficulty of the work lay in developing options for attributing cyber attacks and a coordinated European approach to serious incidents based on the Cyber Diplomacy Toolbox. Attribution is fundamentally a sovereign, political decision made by each member state. Attribution is not a requirement for all of the measures included in the Cyber Diplomacy Toolbox. Some of the measures the EU can use to react to cyber attacks are public, for example Council conclusions or explanations.

An important part of cyber diplomacy at an EU level is the development of joint positions on and strategies for cyber issues at an international level, particularly in the United Nation, where two parallel standard-setting processes were started in 2019 (see Chapter 2.2).

The EU adopted a cyber sanctions regime in 2019.

There is a lack of international treaties in the area of cybersecurity.

### **2.1.7 Network of National Coordination Centres and European Competence Centre**

On 12 September 2018, the European Commission submitted the proposal for a Regulation to set up the European Competence Centre for Cybersecurity in Industry, Technology and Research and the Network of National Coordination Centres to Establish the Competence Community for Cybersecurity<sup>6</sup>. The proposal was a specific measure to implement the joint memo issued by the European Commission and the High Representative of September 2017 for measures to increase defensive capacity, to deter and to defend against cyber attacks and to ensure an effective increase in cybersecurity in the EU.

The Network of National Coordination Centres and the European Cybersecurity Industrial, Technology and Research Competence Centre is already supporting existing EU initiatives and developing new European capacities in the cyber field.

The European Competence Centre aims to coordinate the use of funds set aside for cybersecurity for the years 2021–2027 for the programmes “Digital Europe” and “Horizon Europe”. The Centre will support the Network of National Coordination Centres and the competence community and drive forwards research and innovation in the field of cybersecurity. It will also organise joint investments by the EU, member states and industry.

Within the Network of National Coordination Centres, each member state must appoint a national coordination centre which will work to develop new cybersecurity capabilities and further develop competence. The network will contribute to the determination and support of the most relevant cybersecurity projects in the member states.

---

<sup>6</sup> See COM (2018) 613



The competence community in turn will create a large, open and diverse group of interested parties in the field of cybersecurity from science and the private and public sectors, including civil and military authorities.

For more information on the progress of the negotiations, see Chapter 2.1.1.

### **2.1.8 Action plan against disinformation**

Increase in  
targeted  
disinformation  
campaigns  
against the EU

The right to freedom of expression is a key value of the EU. For open, democratic societies it is essential for citizens to have access to high quality, verifiable information and therefore to be able to form an opinion on various political topics. EU citizens can currently participate in 25 public debates on political processes, obtain information about these and express their wishes. The conscious, comprehensive and systematic dissemination of disinformation can lead to threats to democratic processes and to public goods such as human health, environment and security.

An increase in persistent, targeted disinformation campaigns against the EU, its bodies and its policies was expected before the elections to the European Parliament. The rapid change in the instruments and techniques used means a response to them needs to be developed just as quickly. State actors are increasingly using disinformation strategies to influence social debates, cause divisions and intervene in democratic decision-making.

The EC College therefore adopted an Action Plan against Disinformation on 5 December 2018. The Action Plan provides for various measures in the following four areas:

- improving the capabilities of Union institutions to detect, analyse and expose disinformation;
- strengthening coordinated and joint responses to disinformation;
- mobilising the private sector to tackle disinformation and
- raising awareness and improving societal resilience.

The measures in the various areas are having an effect: the joint communication of the European Commission and the High Representative of the EU for Foreign Affairs and Security Policy, Federica Mogherini, of 14 June 2018 on the implementation of the Action Plan stated that attempts to influence the EP elections were able to be prevented as a result of the coordinated approach.







## 2.2 United Nations (UN)

The First Committee (Disarmament and International Security) of the United Nations General Assembly (UN-GA) addressed cybersecurity for the first time in 1998. The UN-GA has looked at the topic with increasing intensity since then. Within this framework, states are aiming to minimise the risks arising from the use of cyberspace for international stability. Four priority areas which are particularly relevant in terms of establishing and implementing an international framework of standards for cyberspace were able to be identified over the course of the negotiations:

- international law,
- non-binding standard of responsible state actions,
- confidence-building measures (CBM) and
- improving capacities.

Two independent negotiation formats established by the UN General Assembly on cybersecurity.

In 2019, the cybersecurity processes in the UN-GA context reached a new phase. The long period of precarious political consensus between “Western” states on the one hand and Russian and a number of like-minded states on the other disintegrated in 2018, resulting in the creation of two independent negotiating formats by the UN-GA. There is a Group of Governmental Experts (GGE) and an Open-ended Working Group (OEWG). The GGE is being deployed for the sixth time and consists of 25 appointed experts, while the OEWG has been set up for the first time and is open to all MS. Both the GGE and the OEWG held their first sessions in 2019. For the first time, states were being requested to take a position on the two groups in a substantial manner. Austria supported the creation of the GGE and has also taken an active part in the discussions as part of the OEWG. Whether and to what extent effective division of labour between the GGE and OEWG is established will be relevant for further work.

The differences in content between the states, particular the issue of the precise applicability of international law, remained in 2019 too.

In addition to the UN-GA, other UN bodies are also looking at maintaining the stability of cybersecurity. The main reference document for this was the Agenda for Disarmament by the General Secretary of the United Nations. Two areas of action are dedicated to cybersecurity in the associated implementation plan: one relates to peaceful conflict resolution and the other to strengthening the developing standard in cyberspace. The implementation measures to this effect were continued by the states in 2019.

During the 41st session of the UN Human Rights Council (UN-HRC) in June 2019, Austria was one of the main sponsors (alongside South Korea, Brazil, Denmark, Morocco and Singapore) to table a resolution on the topic of “new and emerging digital technologies and human rights” (A/HRC/Res/41/11), which was able to be adopted by consensus. In this, the advisory committee was tasked with carrying out a study on the topic with the aim of initiating a broad discussion in the UN-HRC on human rights challenges and potentials linked to the rapid development of digital technologies (particularly in the field of Artificial Intelligence (AI)).

The resolution on the right to privacy in the digital age (A/HRC/Res/42/15) tabled again by Austria in September 2019 during the 42nd session of the UN-HRC was again able to be adopted by consensus. This resolution focuses on the topic of AI and privacy and the opinion that risks to the protection of human rights would arise if adequate protective mechanisms are not used when developing and using AI. The right to privacy is also jeopardised if the quantity of data required for AI is used for the facial recognition, scoring or profiling of individuals without regulation.

Artificial  
intelligence as  
a topic of the  
41st session  
of the Human  
Rights Council

The report of the High-level Panel on Digital Cooperation (HLPDC) is a committee on digital collaboration which was created in 2018 to make recommendations on improving collaboration between governments, the private sector, civil society, international organisations, science, the technical community and other relevant stakeholders in the digital space.

Recommendation number 4, “trust, security and stability” includes the development of a “Global Commitment on Digital Trust and Security”. The intention is for a core group of interested stakeholders to propose options for following up on this recommendation. In response to this, Microsoft, Hewlett-Packard and Mastercard founded the “Cyber Peace Institute” in Geneva in October 2019 with the aim of improving the stability of cyberspace by supporting non-state victims of cyber attacks, closing the responsibility gap and promoting international law and standards which encourage responsible behaviour in cyberspace. “Safety, Security, Stability & Resilience” was one of the three areas of focus of this year’s Internet Governance Forums (IGF), which took place from 25 to 29 November 2019 in Berlin. The discussion focussed on standards for the field of cybersecurity, concentrating more on the role of the private sector than on the behaviour of states in cyberspace.

In the context of the UN in Geneva, the International Telecommunication Union (ITU) is continuing to work on its “Global Cybersecurity Agenda”, which aims to improve trust in and the security of the information society but is viewed very negatively by some Western states.

Cybercrime has rapidly become a global and extremely profitable area of crime. The United Nations Office on Drugs and Crime (UNODC) in Vienna continues to be an essential component of the effective global battle against cybercrime. The comprehensive study,<sup>7</sup> which was published in 2013, focuses its support for affected member states on the following three main areas:

- improving the identification, prosecution and assessment of cybercrime, particularly in the field of sexual exploitation and child abuse on the internet;
- promoting an integrated and government-wide approach including national coordination, data collection and effective legal framework conditions to sustainably combat and provide an effective deterrent against cybercrime;
- strengthening national and international cooperation between governments, law enforcement authorities and the private sector and improving public awareness.

The UNODC Cybercrime Division implements new initiatives in school and university education at an operative level. In this context, UNODC is showing an interest in the comic book created by the Internet Service Providers Austria (ISPA) called “The Online Zoo”, which is also used in school classes.

The Intergovernmental Expert Group (IEG) set up in 2010 in the field of cybercrime met in March 2019 for the fifth time. The issue under dispute of whether a new cyber convention needed to be negotiated or whether the Budapest Convention should be expanded was not able to be resolved. Finally, a resolution was passed to continue the IEG’s discussions on fundamental topics and developments relating to cybercrimes and

UNODC in Vienna is an indispensable component in the effective world-wide fight against cybercrime.

---

7 [http://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME\\_STUDY\\_210213.pdf](http://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf)

to exchange on national legislation, examples of best practice, technical support and international collaboration.<sup>8</sup>

In 2019, Russia launched a resolution on cybercrime in the UN General Assembly, which provides for the creation of a separate working group to develop a new treaty under international law on cybercrime. Cybercrime was also the main topic of the 28th session of the Commission on Crime Prevention and Criminal Justice (CCPCJ)<sup>9</sup> in May 2019. Together with Canada and Columbia, Austria submitted a resolution focusing on cybercrime, which was able to be adopted by consensus.

The International Atomic Energy Agency (IAEA) is continuing to look at the topic of the cybersecurity of nuclear plants and nuclear material as a priority in 2019. The Austrian Institute of Technology (AIT) created a special virtual IT training and simulation platform designed for highly sensitive industrial control systems for an IAEA research project.

The implementation of the Agenda for Disarmament and the work of the United Nations Group of Governmental Experts (GGE) and the Open Ended Working Group (OEWG) are being supported by the United Nations Office for Disarmament Affairs (UNODA). The United Nations Institute for Disarmament Research (UNIDIR) is contributing to the international cybersecurity discussion by publishing scientific papers. UNIDIR also organises an annual conference on cyber stability.

---

8 CCPCJ Res 26/4 ([https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ\\_Sessions/CCPCJ\\_26/CCCPJ\\_Res\\_Dec/CCPCJ-RES-26-4.pdf](https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_26/CCCPJ_Res_Dec/CCPCJ-RES-26-4.pdf))

9 UNODC Bericht über die 28. CCPCJ: <https://undocs.org/E/2019/30%20>





## 2.3 NATO

As a military and political alliance with a significant focus on security and common defence, NATO has been dealing with the defence aspects of cybersecurity since the adoption of its applicable strategic concept in 2010 and the recognition of cyberspace as a domain in 2016 and space as another domain in 2019. As a partner country, Austria is cooperating closely with NATO and is involved at a technical level in sessions of the NATO-C3 (Consultation, Command and Control) Board and those linked to relevant smart defence projects.

The Austrian Federal Ministry of Defence has been cooperating with NATO since 2013 by sending an Officer to the Center of Excellence in Tallinn. The aim of the collaboration is to increase cyber defence capabilities. The Austrian department is making use of the extensive range of courses available as a result and is using the exercises offered to check its national skills against those of other countries. In addition to this, Austria also provides a Federal Ministry of Defence employee for the “European Centre of Excellence for Countering Hybrid Threats” in Helsinki, in which NATO is also involved.



## 2.4 Organization for Security and Co-operation in Europe (OSCE)

As the largest regional security organisation in the world, the Organization for Security and Co-operation in Europe (OSCE) has a dual role in the field of international cybersecurity policy. On the one hand, it supports the implementation of decisions passed at a UN level, in particular the increases in capacity, through its executive structures and network of field missions. On the other hand, the OSCE took the lead on developing



confidence-building measures (CBM) in cyberspace. The acceptance of the 16 CBM with the aim of minimising the inter-state tensions which arise from the use of cyberspace between the participating countries in the OSCE by exchanging information, establishing communication channels and improving capacities is, from a global perspective, the most ambitious attempt to increase international cooperation in the field of cybersecurity outside of the UN.

The informal working group on cyber (Cyber IWG) is primarily responsible for developing and implementing the CBM. The understanding of security used by the OSCE also guides the work of the Cyber IWG: The topic is addressed taking into account the political and military, economic and human rights aspects. In 2019, the Cyber IWG continued its activities as part of the “adopt a CBM (Confidence Building Measure)” initiative, as part of which states or groups of states promote the implementation of CBM. Important steps in this context are the setting up of a network of contacts, regular checking of the communication channels and ensuring effective collaboration in the event of a cyber crisis.

In addition to the institutionalised handling of the topic by the Cyber IWG, the state currently chairing the OSCE has put cybersecurity on their agenda for a number of years. It has been established that regular cybersecurity conferences will be held by the respective OSCE Chair. In 2019, this took place under Slovak Chairmanship. The conference looked at current developments in the field of international cybersecurity policy and offered an opportunity for the OSCE and the GGE set up by the UN to exchange for the first time.

## 2.5 Organisation for Economic Co-operation and Development (OECD)

The Working Party on Security in the Digital Economy (WPSDE) is one of four working groups under the “Committee on Digital Economy” of the Organisation for Economic Co-operation and Development (OECD). The aim is to develop evidence-based guidelines for digital security and practical guidelines to build confidence in digital transformation and to support the resilience, continuity and security of critical activities. The focus is on the management of digital security risks for economic and social activities and the improvement of the security of digital products and services. The working party relies on expertise from OECD and partner countries, economics, civil society and the technical internet community to develop approaches for the future. The WPSDE meets twice a year in Paris and organises workshops and conferences, which take place in various host countries. In Austria, the Federal Chancellery coordinates the content of this working party.

In late 2019, the “OECD Recommendation on Digital Security of Critical Activities” was passed, replacing a recommendation from 2008. Instead of a purely technical risk management approach, an economic and social risk management approach will be taken for digital security. In 2019, the working group also looked at promoting responsible management and identifying security gaps, as well as improving the digital security of products. In this regard, for example, a list of the IoT certifications which exist around the globe was developed.

## 2.6 Council of Europe



The core of the Council of Europe's activities in the field of cybersecurity is the Convention on Cybercrime (Budapest Convention) from 2001, which has achieved significance well beyond the borders of Europe with 64 ratifications to date (including San Marino, Ghana and Peru in 2019). The main purpose of the Convention is to pursue a common criminal policy to protect society from cybercrime, particularly through corresponding legal regulations and the promotion of international collaboration.

The implementation of the Convention is supported by capacity-building projects coordinated by a Cybercrime Programme Office of the Council of Europe (C-PROC) in Bucharest, such as advising on relevant legislative measures, providing support for the training of judges and public prosecutors, the "iProceeds" project in South-Eastern Europe, which focuses on the profits of cybercrime, the "Cyber South" project in North Africa and the global project carried out in collaboration with Interpol, "GLACY+". In 2019, these projects were supplemented by the "Cyber East" project, which provides support in the Eastern Partnership and is funded by the European Neighbourhood Instrument.

Negotiations are currently underway for a second additional protocol to the Budapest Convention looking at international legal assistance and the associated cross-border access to data. Close collaboration with the EU on the relevant documents that are currently under development is planned. In July 2019, "Guidance Notes" on the Budapest Convention on the topic of "election interference" were also compiled. Guidance notes of this kind aim to facilitate the effective use and implementation of the Convention,

The additional instruments of the Council of Europe include the Council of Europe's Convention on Data Protection, which was modernised in 2018 (ETS 108) and the Lanzarote Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, which makes a significant contribution to the protection of children online. What was known as the "Octopus Conference" in 2019 dealt with evidence in cyberspace and work on the second additional protocol to the Budapest Convention.



## **2.7 Computer Security Incident Response Teams Network (CSIRTs Network)**

In summer 2016, the EP and the European Council passed EU Directive 2016/1148 (NIS Directive), and through this also created the CSIRTs Network (CNW) and set out its area of activities. The CSIRTs Network is made up of representatives of the CSIRTs of the member states (according to Article 9 of the NIS Directive) and CERT-EU. The European Commission (EC) takes part in the CSIRTs Network as an observer. ENISA manages the secretariat and actively supports the collaboration between the CSIRTs. Austria's participants in the CSIRTs network are GovCERT Austria, CERT.at and the CERT for the Austrian energy sector (AEC). The network mainly works online: communication is via a web portal, mailing lists and an instant messaging service. At CNW meetings, there is an information exchange on the services, activities and cooperation capabilities of the CSIRTs. Representatives of the CSIRTs of the member states exchange and provide information on individual security incidents on a voluntary basis and knowledge gained from exercises looking at the security of network and information systems is shared. The main job of the CNW is to develop and strengthen trust between member states and promote rapid and effective operational collaboration to ensure a high joint security level of network and information systems in the EU. In 2019, the CNW meetings were in Brussels, Bucharest and Helsinki. The CNW's Standard Operating Procedures (SOPs)

were also tested in advance of the 2019 European elections in the form of an exercise. Since Austria took over the Presidency in the second half of 2018, it was also invited to be involved in the governance of the network in 2019 as a “standing representative”. There was active collaboration in the “Tooling” working group of the CNW, where the project MeliCERTes is discussed, among other things. In this project, the European Commission commissioned a toolbox for CNW members. It will be continued in 2020 with the direct involvement of CERT.at.

## 2.8 Other committees and forums

In addition to the forums mentioned above, Austria is also involved in a range of other international collaboration committees in the field of cybersecurity.

These include:

- The “Freedom Online Coalition”—this coalition, which Austria has been part of since it was set up in December 2011 at the initiative of the Netherlands, is an informal association of states which works around the globe for the effective implementation of human rights online. Switzerland became the 31st member in 2019. In May, the coalition published a joint declaration on maintaining the civic space online.
- The “Central European Cyber Security Platform” (CECSP) is a cooperation platform of countries (and the CERTs/in some cases milCERTs) of the Visegrad Group (Hungary, Czechia, Slovakia and Poland) and Austria created in 2013 on the initiative of Czechia and Austria. Austria held the Chair of the CECSP in 2019.
- The Global Forum on Cyber Expertise (GFCE) is a global platform that was founded in 2015. Austria has been a member since 2017.



- The Internet Governance Forum (IGF), which came out of the World Summit on the Information Society (WSIS) took place in Berlin. There have to date been no specific final documents issued by this meeting, which focuses in particular on civil society and the private sector. The “Paris Call for Trust and Security in Cyberspace”, which was launched during the IGF Paris in 2018, was continued in 2019. The Call is designed as a political platform for collaboration between states, companies and civil society and aims to support all of those involved in their commitment to principles such as compliance with the international legal position in cyberspace. All EU member states support this initiative.
- The European Cyber Security Organisation (ECSO) was founded by the EU (represented by the EC) and actors in the cybersecurity market in 2016 in the form of a contractual Public-Private Partnership (cPPP) for cybersecurity. ECSO is both an implementation measure of the EU Cybersecurity Strategy from 2013 and an implementation initiative of the EU Strategy for a Digital Single Market. It is a “non-profit organisation” that is fully self-funded. The members include large European companies, SMEs, research centres, universities and local, regional and national administrations from the EU and the European Economic Area (EEA), the European Free Trade Association (EFTA) and countries associated with the Horizon 2020 programme. Several Austrian organisations and research facilities are members and take part in the various committees and working parties of the ECSO. The Federal Chancellery joined the ECSO on 22 March 2017 and from that point onwards took part in the ECSO public authority meetings known as the ECSO-NAPAC Group (National Public Authority Representatives Committee).









3

National  
actors

## 3.1 Cyber Security Center (CSC)

The Cyber Security Center (CSC) in the Federal Agency for State Protection and Counter Terrorism was able to further establish itself in this reporting year despite continuing challenges in terms of both organisation and content. The conversion of the CSC from a unit into a separate department brought with it a range of new tasks. The workforce was increased for the first time in order to complete these.

The NIS Act entered into force at the start of 2019. Since then, operative implementation has been the responsibility of the Federal Ministry of the Interior (strategic tasks remain with the Federal Chancellery). This made the Cyber Security Center in the Federal Agency for State Protection and Counter Terrorism an operative NIS authority. For this reason, the reporting year was shaped by measures to found and implement organisational and technical requirements relating to the additional new task. This related above all to the passing of a suitable Network and Information System Security Regulation by the Federal Chancellery with regulations on sectors, security incidents and security provisions, as well as the preparation of a Regulation on Qualified Entities by the Federal Ministry of the Interior.

Situational monitoring was also established in the CSC, providing a regular and comprehensive situation report on cybersecurity in Austria and communicating the situation reports to the stakeholders. Finally, the area of cyber prevention was continued. In addition to the ongoing awareness talks and awareness-raising events at critical infrastructure companies and constitutional facilities, the CSC regularly carries out various training measures on ICT security for its own and other departments.

## 3.2 Cyber Crime Competence Center (C4)

### 3.2.1 Competent investigating authorities

The police authorities responsible for cybercrime in the narrow sense and digital forensics and data security in Austria work over three levels. At a federal level and as a higher organisation, the C4 is located in Department 5 of the Criminal Intelligence Service Austria. Specialised areas of assistance for cybercrime and forensics are established in each of the nine provincial police directorates as part of the provincial criminal investigation departments. At a district level, specially trained, uniformed police officers (District IT Investigators) are deployed and can provide the necessary support to first responders.

### 3.2.2 Activities

#### **International collaboration in the field of cybercrime:**

In the “Cyber Crime Competence Center” (C4) of the Federal Ministry of the Interior, measures are continuously being put in place to increase the intensity of European and international exchange on the battle against cybercrime. This primarily relates to collaboration with Europol’s European Cybercrime Centre (EC3) and INTERPOL’s Digital Crime Center (IDCC), management functions and collaboration on Operational Actions (OAs) from the Operational Action Plans (OAPs) as part of the European Cybercrime Task Force (EUCTF), involvement in the multinational Joint Investigation Teams (JIT), collaboration in the European Cybercrime Training and Education Group (ECTEG), involvement in the European Multidisciplinary Platform Against Criminal Threats (EMPACT), co-hosting the annual DACH symposium on “New Technologies” and involvement in the G7-24/7 Network.

These collaborations strengthen European and international collaboration in a number of areas, including combating ransomware, the successful work of the former SOKO Clavis, various international cybercrime investigations, specialisations in the field of the dark web and cryptocurrencies and vehicle forensics and training.



### 3.3 CIS and Cyber Security Centre (CISCSC)

During the restructuring of the Austrian Armed Forces in 2019, the former support and cyber defence unit, which was previously developed in virtual form, was dissolved. The core tasks are predominantly continuing and will be described in greater detail for the following areas of competence.



#### 3.3.1 Military Cyber-Centre (MilCyZ)

The MilCyZ as part of the CISCSC is the point in the Austrian Armed Forces that defends against threats or attacks from cyberspace against the military's own ICT systems and networks.

In order to maintain this protection, it is essential that all aspects of cybersecurity are covered both thoroughly and consistently. This is reflected in the tasks and area of competence of the MilCyZ listed below:

- selection, introduction and operation of ICT security components (e.g. firewalls, end-point protection—virus protection etc.)
- creation of a cybersecurity situation report (by monitoring and assessing current technologies, ICT systems and components used by the Austrian Armed Forces),
- forensics,
- auditing<sup>10</sup> internal ICT systems and networks,
- cybersecurity management,
- cyber military training area,
- electronic warfare (self-protection and assistance).

---

<sup>10</sup> Regular reviews/revisions to identify any weak points at an early stage.



### 3.3.2 Self-protection

Responsibility for planning and implementing cybersecurity systems and components for self-protection and the defence of the Austrian Armed Forces against cyber attacks lies with the Military Cyber-Centre. These systems are constantly being developed and adapted to the current threats. A full situation report on cybersecurity can be prepared in combination with observations, assessments and measures to tackle weaknesses in current technologies, ICT systems and components used by the Austrian Armed Forces. In order to check all ICT systems for their suitability to be used in the Austrian Armed Forces on an ongoing basis, design and structural weaknesses in technologies, products, components and systems are identified early through system and component audits.



### 3.3.3 milCERT (Military Computer Emergency Readiness Team)

In the event of an imminent or ongoing cyber attack, sufficient technical and staffing capacities must be available for detection, containment and defence. An essential part of this is the ability to detect and demonstrate the current cyber situation. In order to obtain information on cybersecurity incidents and current knowledge that is as accurate and current as possible, the milCERT is constantly exchanging information with national and international partner organisations. It coordinates the measures that are carried out in the event of IT security incidents and provides warnings about any gaps in security in good time.



### **3.3.4 Cyber military training area**

Since highly specialised forces are only available to a limited extent, training on the concepts and processes and training for members of the army is needed. Exercises are coordinated in the cyber environment in the cyber military training area (Cyber Range) and research projects are developed together with scientific facilities. Current cybersecurity trends are analysed and integrated into the Austrian Armed Forces' cyber defence processes.

### **3.3.5 Information security**

Information security, cyber-specific risks and collaboration with Austrian and international partners are managed so as to supplement the technical and tactical abilities. The Military Cyber-Centre operates comprehensive ICT and cyber risk management embedded in an information security management system and represents the Austrian Armed Forces to national and international regulatory authorities. The Austrian Armed Forces carry out security authorisations and audits of systems based on national and international security regulations to ensure the secure exchange of information.

### **3.3.6 Electronic warfare**

As part of cyber defence, the centre is also responsible for the provision of services in the field of electronic warfare. The technical basics needed for self-protection and the provision of assistance for the defence of foreign systems are provided. The aim is to obtain and maintain combat superiority, to carry out jobs as a national or multinational group and to increase the viability of the force.



### 3.4 Austrian Armed Forces Security Agency (AbwA)

The Austrian Armed Forces Security Agency (AbwA) also makes an important contribution to cyber defence. The term cyber defence is understood to mean all of the efforts made by the Austrian Armed Forces in cyberspace as a whole. The Austrian Armed Forces Security Agency supports these efforts by preparing a situation report analysing national and intelligence information from and about cyberspace and uses it to assess countermeasures. These and additional measures aim to ensure a permanently high level of security in the military ICT infrastructure.

The largest ICT security conference in the German-speaking world is also organised annually by the Austrian Armed Forces Security Agency. This conference primarily serves to increase awareness of security and is one of the Austrian Armed Forces' main awareness projects.



### 3.5 Austrian Strategic Intelligence Agency (HNaA)

As a strategic foreign intelligence service, the Austrian Strategic Intelligence Agency (HNaA) primarily contributes to the national cyber situation report by representing the strategic context in large-scale cyber incidents. In addition to the prompt detection of cyber threats from abroad, information it has obtained about the intentions and abilities of international cyber agents makes an important contribution to attribution and therefore to decision-making by the highest level of political and military leadership, among other things with regard to any countermeasures.

### 3.6 GovCERT, CERT.at and Austrian Energy CERT

According to the NIS Act, GovCERT is the public administration computer emergency team and part of the above-mentioned IKDOK. GovCERT is the CERT Point of Contact for Austria in terms of the public administration networks and is therefore closely linked to appropriate international organisations and contacts such as the European GovCERT Group and the Central European Cyber Security Platform. GovCERT, which comes under the Federal Chancellery, works closely with CERT.at in the form of a public-private partnership.

 GovCERT Austria

CERT.at is the Austrian national Computer Emergency Response Team (CERT), which has been operated together with GovCERT as a cooperation of the Federal Chancellery with nic.at GmbH (the registry of “.at”) since 2008. Since March 2019, CERT.at has also taken on the role of the national computer emergency team according to the NIS Act. CERT.at is a contact point for security-related ICT events in Austria and is a trusted and recognised information hub within Austrian organisations and companies in the field of cybersecurity.



The Austrian Energy CERT (AEC) is an industry-specific CERT (Computer Emergency Response Team) for the Austrian energy industry. In 2019, the AEC was not yet accredited as a sector-specific computer emergency team according to the NIS Act, since the energy suppliers themselves were not yet identified as “operators of essential services”. This formal step will follow in 2020. The AEC is an important component of the increase in the resilience of the energy economy to cyber attacks. The main tasks of the AEC are to strengthen the IT security skills of the energy sector. These tasks include ongoing security incident management, in other words the handling of queries that come in each day and security reports, carrying out training sessions, participating in international



cybersecurity exercises and collaborating on the development of technical security concepts for the electricity and natural gas industry. The AEC also takes on the role of single point of contact for national and international security incidents in the energy sector. In addition to rapid and efficient communication, coordination between IT security experts and authorities within the industry is also ensured.

Together, the three CERTs carry out the tasks according to Section 14 of the NIS Act and therefore meet the requirements of the European Directive on Security of Network and Information Systems (NIS) and the recommendations of the European Union Agency for Network and Information Security (ENISA) for increasing IT security in critical infrastructures. These three CERTs are also the Austrian members of the EU CSIRTs Network.

All three CERTs primarily work actively on acute security threats and events. This happens by communicating with areas that are affected or on the basis of its own research. All three also out preventative measures such as early detection, PR work, advice and support on request as the need arises.

The transposition of the NIS Directive into national law in the form of the NIS Act set out the remit of the CERTs. This law provides, among other things, for an obligation to report serious security incidents on the part of operators of essential services and providers of digital services. These compulsory reports are sent by those affected to certain, sector-specific reporting point (sector-specific computer emergency teams) and from there forwarded to the CSC. This also applies to voluntary reports, although these reports can be anonymised by the sector CERTs before they are forwarded to the CSC.

GovCERT receives reports of this type for public administration facilities and forwards them on if the facility is not represented in IKDOK. In addition to this, GovCERT can also issue early warnings, alarms, recommendations for action and notifications and provide initial general technical support when responding to security incidents to monitor and analyse risks, incidents and security incidents and to assess the situation.

The NIS Act provides for a sector CERT of this type in each sector to carry out this function of being a reporting point. In addition to the reporting point function, these CERTs carry out a large number of additional CERT tasks for the organisations in their sector.

If a sector still does not have its own sector CERT, the tasks of the computer emergency team and the reporting are carried out by the national computer emergency team (CERT.at).



### 3.7 Office for Strategic Network and Information System Security

Information systems with the associated services play a key role in modern society. It is critical that they are reliable and safe for economic and social activities. In order to ensure this, the first EU-wide legal act on cybersecurity was passed in the form of Directive (EU) 2016/1148 “NIS Directive”.

The NIS Directive was transposed into the “NIS Act” (Network and Information System Security Act, Federal Law Gazette I No. 111/2018), which entered into force in Austria on 29 December 2018. The NIS Directive transfers tasks arising from the NIS Directive to existing structures and regulates responsibilities for authorities responsible for their implementation and their powers. In this context, the Federal Chancellor carries out the strategic tasks and the Federal Minister of the Interior carries out the operative tasks. The law covers facilities which are very important for the functioning of the community, which is why their network and information systems are particularly worthy of protection. On the one hand this relates to facilities in the seven sectors of energy, traffic, banking, financial market infrastructures, healthcare, drinking water supply and digital infrastructure, and on the other to facilities which provide certain digital services and public administration facilities.

The Office for Strategic Network and Information System Security (“Strategic NIS Office”), which is housed within the Federal Chancellery as part of department I/8 (Cyber Security, GovCERT, NIS Office and ZAS) and is responsible for issues linked to the transposition of the legal obligation from the NIS Directive started its work on the basis of the NIS Act.

A first milestone here is the official assessment of the suitability and authorisation of CERT.at as a national Computer Emergency Response Team in the sense of the NIS Act, which was carried out following an application in April 2019.

A further milestone was achieved when the “NIS Regulation” (Network and Information System Security Regulation, Federal Law Gazette II No. 215/2019) passed on the basis of the NIS Act entered into force on 18 July 2019. In this Regulation, the competent Chancellery Minister in the Federal Chancellery in coordination with the Federal Minister of the Interior set out a great deal of essential content from the NIS Act in greater detail. This included more detailed regulations of the sectors, with the essential services and the criteria for the parameters of security incident “reporting thresholds” in particular being defined in greater detail. The NIS Regulation also sets out categories and measures relating to security precautions for operators of essential services.

On the basis of the NIS Regulation, the Strategic NIS Office included the determination of the operators of essential services in the seven sectors in August 2019. The operators were initially informed in an “information letter” that they could be considered to be operators of essential services on the basis of the data available to the Strategic NIS Office as a result of administrative assistance procedures which were carried out, for example. The companies were informed about the start of investigations, but were also given the opportunity to make a statement/give an opinion on this. The information letter was also used to ask about possible cross-border connections which could be used as the basis for the start of consultations with other EU member states in a further investigation step if an operator of essential services also provides their services in another member state. An attempt is also being made to determine certain intersectoral dependencies through the information letters. In a final step and on the basis of the information obtained in the preliminary and consultation procedure, a decision is made regarding whether a public or private facility should be classed as an operator of essential services.



Under the law, the Strategic NIS Office is also responsible for the representation of Austria in the NIS Cooperation Group and other EU-wide and international committees for the security of network and information systems to which strategic tasks are allocated. The Strategic NIS Office, among other things, takes an active role in the work of the NIS Cooperation Group, where it manages Work Stream 8 on cybersecurity in the energy sector, for example. The acceptance of the extensive reference document on the implementation of the NIS Directive in the energy sector (CG publication of March 2019) by the NIS Cooperation Group in September 2019 can be highlighted as a particular success. The Strategic NIS Office also represents Austria in the Council's Horizontal Working Party on Cyber Issues (HWP Cyber) and the European Cybersecurity Certification Group (ECCG).

In addition to these tasks set out by the law, the Strategic NIS Office carried out other activities in 2019, particularly in the field of information. Together with the Federal Ministry of the Interior, an NIS website was created (<https://nis.gv.at>), which acts as a point of contact with regard to the NIS Directive and the NIS Act and aims to help answer frequently asked questions.

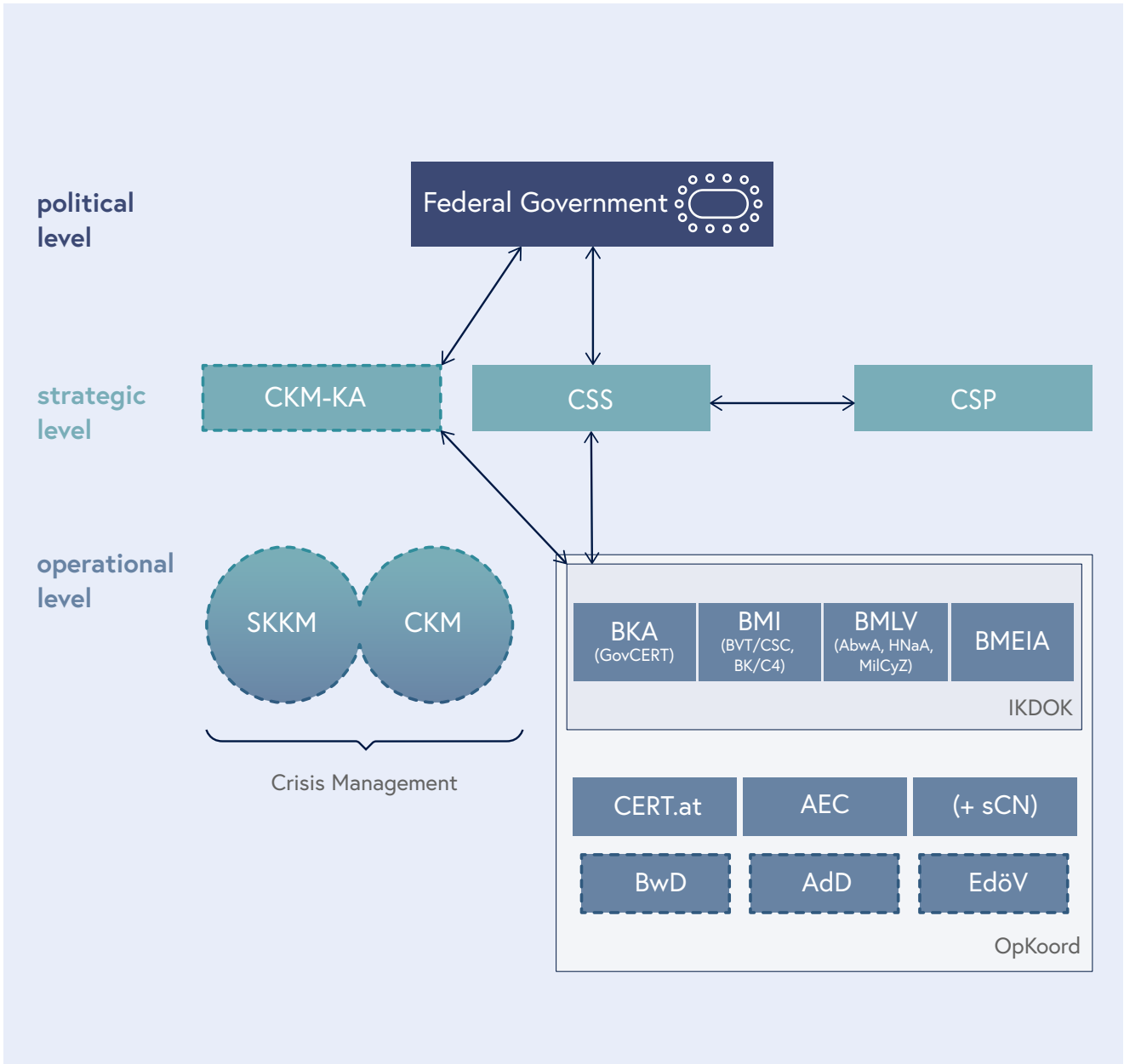
The target group of the NIS Act was also supported in its implementation of the legal requirements through the creation of four "NIS Fact Sheets" in 2019 which were made available on the NIS website. NIS Fact Sheet 1/2019 explains the authorities' expectations for the contact points for operators of essential services. NIS Fact Sheet 7/2019 offers qualified facilities support on the application process in particular. NIS Fact Sheet 8/2019 explains the security measures for operators of essential services in greater detail, while NIS Fact Sheet 9/2019 serves as an implementation guideline for federal facilities on identifying essential services and the reporting criteria.

## Legend

----- event-related

AbwA ..... Austrian Armed Forces Security Agency  
AdD ..... Digital Service Providers  
AEC..... Austrian Energy CERT  
(= sector-specific CSIRT for sector energy)  
BK..... Criminal Intelligence Service Austria  
BKA..... Federal Chancellery  
BMEIA ..... Federal Ministry for European and  
International Affairs  
BMI ..... Federal Ministry of the Interior  
BMLV..... Federal Ministry of Defence  
BVT ..... Federal Agency for State Protection  
and Counter Terrorism  
BwD ..... Operator of Essential Services  
C4 ..... Cyber Crime Competence Center  
CERT.at ..... the national CSIRT

CKM..... Cyber Crisis Management  
CKM-KA..... Cyber Crisis Management  
Coordination Committee  
CSC ..... Cyber Security Center  
CSP..... Cyber Security Platform  
CSS..... Cyber Security Steering Group  
EdöV..... Entities of Public Administration  
HNaA..... Austrian Strategic Intelligence  
Agency  
IKDOK..... Inner Circle of the Operative  
Coordination Structure  
MilCyZ ..... Military Cyber-Centre  
OpKoord..... Operative Coordination Structure  
sCN..... Sector-specific CSIRT  
SKKM..... State Crisis and Catastrophe  
Protection Management





4

# National structures

## 4.1 Inner Circle of the Operative Coordination Structure (IKDOK)

The Network and Information Systems Security Act (NIS Act), which entered into force on 31 December 2018, provides, among other things, for the creation of a structure for coordination at an operative level “Operative Coordination Structure – OpKoord” and an interministerial structure for coordination at an operative level in the field of the security of network and information systems (“Inner Circle of the Operative Coordination Structure – IKDOK”). While OpKoord was essentially set up to discuss a overall situation report that also includes both compulsory and voluntary reporting, the main tasks of the IKDOK include discussing and updating the situation report to include risks, incidents and security incidence and supporting the coordination committee with Cyber Crisis Management (CKM).

Specifically, this means that IKDOK, supported by OpKoord, forms the direct interface with the general government Cyber Crisis Management team (CKM) in the event of a crisis. In terms of the mechanisms and processes to be used, the CKM relies strongly on the tried and tested processes of State Crisis and Catastrophe Protection Management (SKKM). Regular cyber exercises aim to test cyber crisis management and crisis management and continuity plans.

As defined in the Network and Information Systems Security Act, the Inner Circle of the Operative Coordination Structure (IKDOK) is an inter-ministerial structure for coordination at the operational level regarding the security of network and information systems. It is composed of representatives of the Federal Chancellor (including the Governmental CERT [GovCERT]), the Federal Minister of the Interior (Cyber Security Center [CSC] and Cyber Crime Competence Center [C4]), the Federal Minister of Defence (Austrian Armed Forces Security Agency [AbwA], Austrian Strategic Intelligence Agency [HNaA] and Military Cyber-Centre [MilCyZ]) and the Federal Minister for Europe, Integration and Foreign Affairs.

## 4.2 CERT Verbund Austria

The interaction between society, the economy and science needs to be further promoted and expanded to further increase the level of security of Austrian society in cyberspace. A key role in this increase is played by the Computer Emergency Teams (CERTs). It is the inherent job of the CERTs to protect ICT systems and digital networks. The aspects of prevention, reaction and awareness-raising are the highest priorities and the first point of contact for all areas of cybersecurity. An intensive exchange of information and networking at a national and international level are both required to develop the necessary expertise. The focus of the remit of the CERT Verbund Austria is improving collaboration between Austrian CERTs and promoting CERT activities in Austria. A comprehensive network of CERTs is the most effective way of protecting the networked information and communication systems. This is a perspective which is confirmed by the constant increase in CERTs, CSIRTs, Security Operations Centers (SOC), Cyber Defence Teams etc. in Austrian companies. The CERT Verbund Austria was founded in 2011 as a collaboration between all of the Austrian CERTs that existed at the time from the public sphere and the private sector. The intention was to bring together all of the available forces to make the best possible use of joint expertise to ensure the best possible ICT security. Participation in the CERT Verbund Austria is voluntary. Each individual participant commits to exchange information and experience on a regular basis, to identify and provide core competencies and to contribute to the promotion of the CERTs in all sectors in the sense of a community-led and cooperation-based CERT Verbund. Since the CERT Verbund Austria was founded, the 16 current members have met 38 times and constantly exchange information with one another outside of the regular meetings via secure communication distributors. In order to continue to offer the existing participants in the CERT Verbund Austria a trustworthy platform for information exchange but also to enable regulated growth of the Association, an initiative was launched in 2019 to create rules or procedure which set out the procedures and processes within the Association. Following several iterations, the rules of procedure were finally able to be passed in late 2019.

## 4.3 Cyber Security Platform (CSP)

The Cyber Security Platform (CSP) is the central exchange and cooperation platform between the economy, science and public administration. It is used to exchange experience and information on cybersecurity, with a particular focus on critical infrastructures. The CSP also advises and supports the Cyber Security Steering Group (CSS) on strategic issues of cybersecurity. Since it was set up in 2015, the platform has become an exemplary model and is an umbrella for numerous cybersecurity initiatives. The results of the work done by the platform are important when it comes to shaping national cybersecurity policy.

The eighth and ninth CSP workshops took place in 2019. The focus of both workshops was on the current status of the implementation of the NIS Directive by means of the national NIS Act and the accompanying regulations. Numerous inputs from members of the CSP were recorded and taken into account in the further revisions.

Another thematic focus was progress reports on the working parties established under the CSP on the areas of “legal and regulatory issues”, “technologies, processes, training, research and development” and “operational crisis management”.

Other topics discussed as part of the CSP were the EU Cyber Security Act, the Network of Cybersecurity Competence Centers and the possible national implementation, and the subject of 5G risk analysis. The discussions were supplemented with current information on the cyber situation and relevant events and initiatives in the field of cybersecurity.

In addition to the comprehensive and valuable discussions during both workshops, the CSP also made a written input to the creation of an updated Austrian Cybersecurity Strategy (ÖSCS 2.0).



## 4.4 Austrian Trust Circle (ATC)

The Austrian Trust Circle (ATC) is a national initiative for the technical exchange of information on ICT security and incidents. The target groups are all sectors of strategic infrastructure and public administration in Austria. The ATC was founded in 2011 and is an initiative of the national CERT.at with the support of the Federal Chancellery. The ATC consists of sector-specific Security Information Exchanges. The ATC addresses companies and organisations responsible for critical infrastructure and authorities in Austria. CERT.at and Austrian Energy CERT in collaboration with GovCERT Austria and the Federal Chancellery offer a formal framework for a practical exchange of information and joint projects in the field of security.

The main objectives of the ATC are:

- creating a foundation of trust so serious cases can be addressed together,
- facilitating networking and information exchange within and between the critical infrastructure sectors and public administration,
- exchanging contacts between the CERTs and the participating companies, organisations and authorities,
- supporting self-help in the sectors in the field of IT security,
- operative contacts with the CERTs for example
  - on information about and
  - on the handling of security incidents in the organisations,
- operative experts for the Federal Chancellery in the event of a crisis.

In addition to the regular meetings within the individual sectors, exchange between the sectors including public administration is promoted once a year at a two-day event. In 2019, the topics of NIS implementation, client security management and incident response and log data were addressed.

visits 2018

**206.277**

visits per week

**~5.000 / week**

visits 2019

**248.576**

visits per day (peaks Mon-Thurs)

**Ø 820 / day**

## 4.5 ICT security portal

The ICT security portal [onlinesicherheit.gv.at](https://onlinesicherheit.gv.at) is an interministerial initiative in cooperation with the Austrian economy and acts as a central internet portal for topics related to security in the digital world.

As a strategic measure of the national ICT security strategy and the Austrian National Cybersecurity Strategy, the initiative aims to promote and sustainably strengthen the ICT security and cybersecurity culture in Austria by sensitising the affected target groups and raising awareness with them and by providing target group-specific recommendations for action.

The information and services on offer are constantly being expanded during regular editorial meetings with the 39 cooperation partners (federal ministries, state governments, authorities, universities, technical colleges, research institutes, companies, associations and advocacy groups). It includes current reports and warnings, informative materials, advice and further information for both beginners and experts.

In 2019, the ICT security portal<sup>11</sup> wrote 150 news articles, 50 publication records and 70 event records. Each month a main topic on current trends is chosen, with a total of 34 specialist articles being published. The focus at the start of the year, for example, was the General Data Protection Regulation (GDPR) and before Christmas it was the security measures behind online shopping. In October, there was a report on activities carried out by Austria for the “European Cyber Security Month” (ECSM).

---

11 ICT security portal assessments 2019/2020 (version of 20 January 2020)







5

# Cyber exercises

Cyber exercises also made a significant contribution to testing defined processes, checking measures set and strengthening domestic and international collaboration on cybersecurity in 2019. The knowledge obtained from participating in the simulation games in the form of “lessons learned” was a key factor in increasing overall national resilience. The state bodies were able to be trained on a wide range of different applications by participating in various exercises.



## 5.1 Cyber Coin 2019

The Austrian Financial Market Authority together with the Kuratorium Sicheres Österreich (KSÖ) and the Oesterreichische Nationalbank (OeNB) invited participants to the simulation game “Cyber Coin 2019”. The participants were ten representative credit institutions, their IT providers, the Austrian Computer Emergency Response Team (CERT) and the Federal Agency for State Protection and Counter Terrorism. This cyber stress test of the Austrian financial market practised the reactivity the resistance of the Austrian banking sector to cyber attacks. This time, the focus was on the human factor. Collaboration between credit institutions and the banking supervision and the institutions responsible for cybersecurity in Austria were tested for their response to a hacker attack. The cyber simulation game showed that credit institutions are broadly well organisationally prepared for cyber attacks, but the practical design of the defence against the attack varied considerably.

## 5.2 HELIOS 2019

The strategic crisis exercise “HELIOS 2019” took place from 13 to 15 May 2019. The participants were around 100 representatives of the federal ministries, the provincial states, the emergency services and operators of critical infrastructures. The starting scenario for the exercise was a power cut involving direct effects on several areas of society and life, constitutional facilities and the economy. The aim of the exercise was for all of the parties involved to identify where they could improve their own resilience to create a high overall level of security in Austria and be optimally positioned for any serious incident. The follow-up exercise, DANTE, is being planned for 2020.



### **5.3 Blue OLEX 2019**

In July 2019, the CSC of the Federal Agency for State Protection and Counter Terrorism and a representative of the Federal Chancellery/NIS Office in Paris took part in a high-ranking networking event of European NIS authorities along with a simulation game called “Blue OLEX 2019”. The French cybersecurity authority ANSSI invited participants to this meeting as part of Work Stream 7 of the NIS Cooperation Group on large-scale cybersecurity incidents. In the field of European Network and Information System Security (NIS), the Federal Agency for State Protection and Counter Terrorism takes on the role of the Austrian Single Point of Contact (NIS SPoC) and was able to practise communicating with other EU member states in the event of cross-border cybersecurity incidents.

### **5.4 EU ELEx19**

A tabletop exercise was carried out at the European Parliament in Brussels on 5 April 2019 to test the extent to which EU member states were prepared for cyber attacks linked to the European parliamentary elections. Experience relating to the implementation of the corresponding recommendations of the EC was also exchanged during the exercise. This provides for installing national election cooperation networks, among other things. This cooperation network was set up in Austria in November 2018 under the leadership of the Federal Ministry of the Interior election authorities.

### **5.5 CyberSOPex 2019**

The EU network of CSIRTs practised the processes for collaboration during a cross-border incident on 15 May 2019, in other words shortly before the EU elections, as part of the CyberSOPex 2019 exercise. CERT.at took part as Austria’s national CSIRT.

## 5.6 Locked Shields 2019

The focus of this, the largest technical “life-fire” exercise in cyber defence, was on defence, but supportive processes (legal position on “cyber”, PR work, collaboration and forensics) were also used. The exercise took place from 8 to 12 April 2019 in Tallinn and was led by the NATO Cooperative Cyber Defence Center of Excellence (NATO CCDCoE) there. More than 1000 soldiers and civilians from more than 25 countries, NATO and EU organisations took part. Austria sent six people to participate in Tallinn and had a further 52 exercise participants in Vienna as the Blue Team (BT) in the MilCyZ.

This exercise primarily practised the skills of protecting a less familiar network, identifying attacks and reacting appropriately to these.

As teams, the participating IT specialists had to identify cyber attacks, limit the effects of these and handle the incidents in line with uniform specifications (e.g. legal aspects, exchange of information, forensic analyses). The aim was to use the actions taken by the exercise participants to derive solutions to real problems, to strengthen international collaboration by creating trust, to improve the ability to carry out similar exercise projects, to test tools, to expand cyber defence skills and to improve active cyber negotiation skills.

## **5.7 Common Roof 2019**

CR19 was a three-week exercise that took place from 2 September to 11 October 2019 across the three countries of Germany, Austria and Switzerland. Austria was the lead nation for the exercise in 2019. Around 180 soldiers and civilians from the three countries took part in CR19, with Austria represented by 98 participants.

Over the course of the exercise, a multinational mission network was developed and operated and used to protect against cyber threats. The focus was on standardised (or in some cases still to be standardised) ICT service management processes, ICT security processes and the ICT services used. The monitoring and control of the multinational network elements was carried out by a multinational Network Operation Cell (NOC).

## **5.8 Thor's Hammer 2019**

The Thor's Hammer 19 exercise was carried out over a period of six weeks from 29 September to 9 November 2019 in Australia. Twelve countries were involved. Austria sent 13 people to take part in the exercise.

The purpose of the exercise was to test and further develop systems which aim to prevent the triggering and ignition of explosive devices which are ignited remotely. These weapons are a constant threat to international peacekeeping forces on missions. Countermeasures in the electromagnetic spectrum are used against these weapons. There was a particular focus on transfer of knowledge to the international participants.

## **5.9 Coalition Warrior Interoperability eXploration, eXperimentation, eXamination eXercise (CWIX) 2019**

CWIX19 was a large-scale Command Post Exercise (CPX) with a focus on interoperability tests and verification and validation (V&V) of mission-oriented ICT systems, services and applications that took place from 10 to 27 June 2019 in Bydgoszcz, Poland.

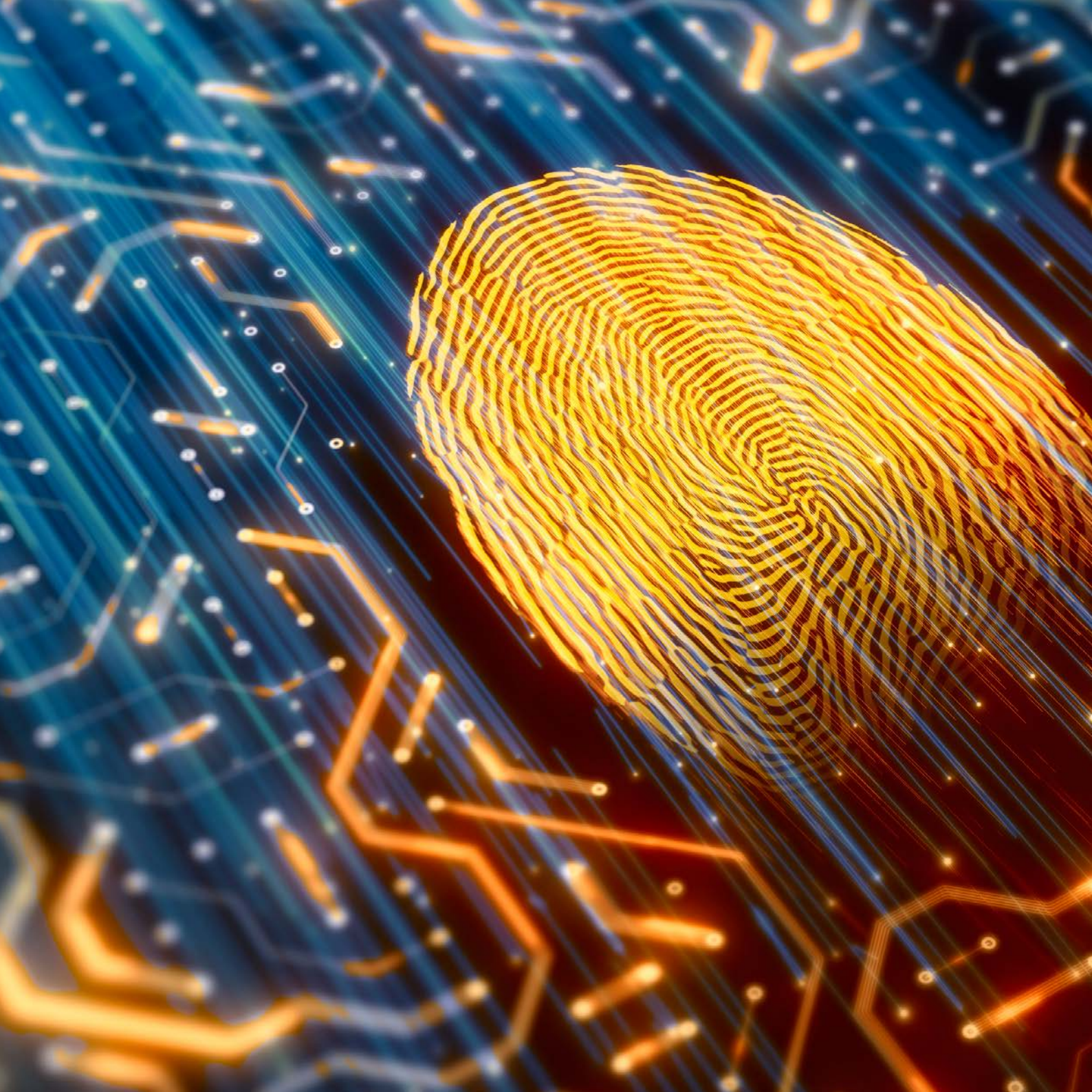
Around 1300 soldiers and civilians from more than 36 countries and NATO organisations took part in the exercise. Austria sent 25 participants.

The main topic of CWIX was the recurring interoperability exercise using tailored scenarios. There was also an option to exchange data with test partners following prior discussion in parallel to the additional tests.

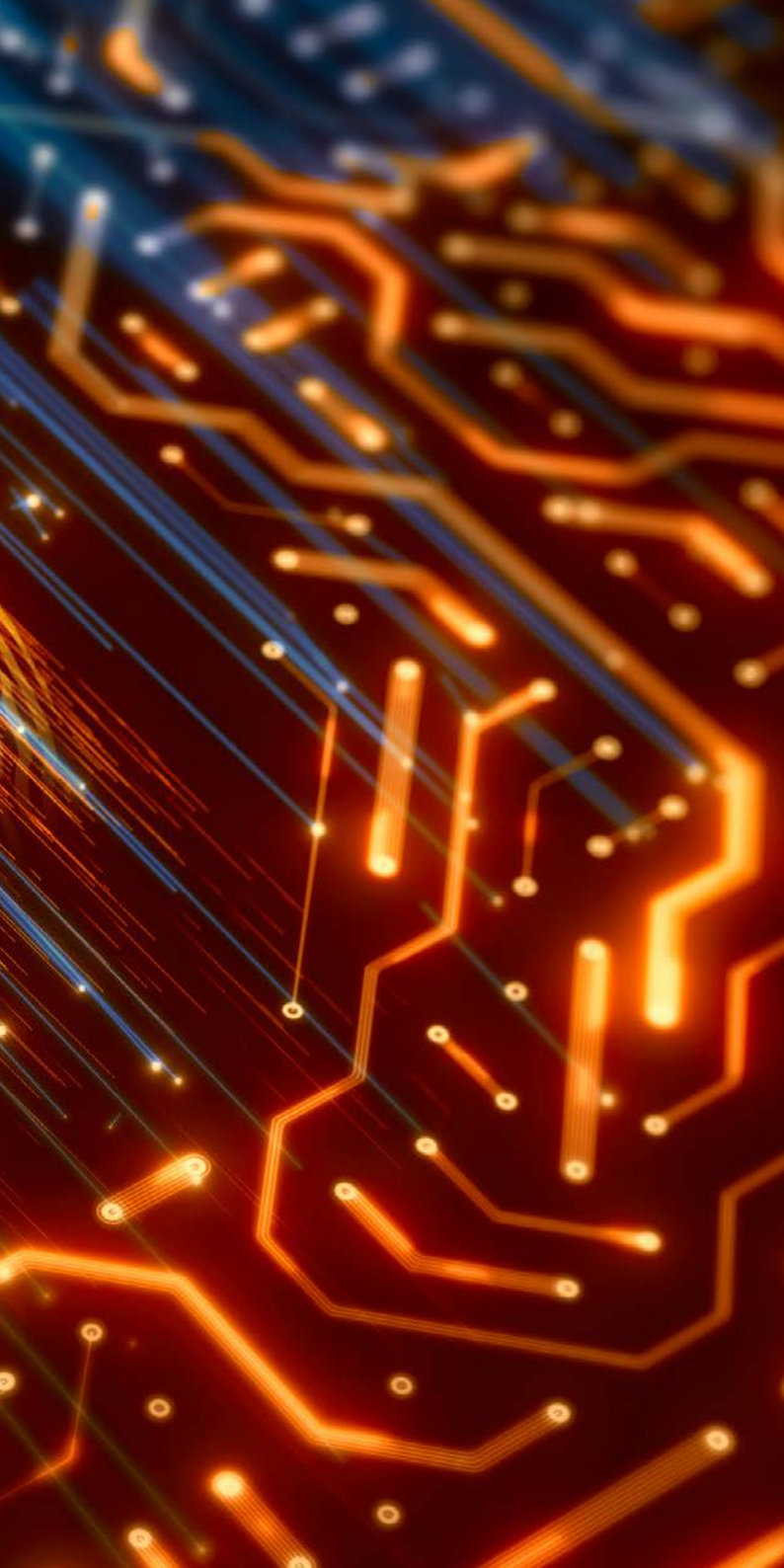
## **5.10 Crossed Swords 2019**

This technical cyber defence exercise took place from 28 January to 1 February 2019 in Tallinn. It was run by the CCDCoE in collaboration with CERT.LV, and around 40 soldiers and civilians from 20 countries took part. The Federal Ministry of Defence sent three participants from the CIS and Cyber Security Centre / MilCyZ.

The purpose of the exercise was for penetration testers, forensic experts and special operations forces to work together as a team to achieve the mission objectives and overcome the technical challenges in a virtual cyber environment. The main focus was on developing tactical skills in a reactive cyber defence scenario and making the participants suitably aware of the situation. Another goal of participation was to improve existing skills in penetration testing, which is needed to check ICT systems. The exchange of experience with specialists from other countries was particularly important.









6

Summary /  
outlook

The 2019 reporting period was shaped by a further increase in monetary or state-supported, strategically motivated attacks. This primarily included attacks carried out using ransomware, with an increased tendency towards targeted ransomware. There has also been an increase in the number of cases of data theft using Advanced Persistent Threats (APTs). Companies are extremely reticent about communicating the occurrence and management of these.

Cyber attack on the Federal Ministry for European and International Affairs (BMEIA) activates NIS crisis mechanisms for the first time

There was a cyber attack on the Federal Ministry for European and International Affairs at the end of 2019. This was without doubt one of the largest and most extensive attacks on a ministry in Austria to date and led to the activation of the national crisis mechanisms provided for in the NIS Act for the first time. Thanks to the efficient collaboration of all operational structures and committees, the crisis was quickly able to be brought under control.

There has been a lasting positive development in increasing awareness and investments in prevention measures in companies. This can also be seen in very small companies, who suffered more ransomware attacks compared to the previous year and therefore took increasing protective measures.

It was critical infrastructure companies in particular which made new investments in the field of cybersecurity in 2019. The additional IT security measures and the increased awareness of security are mainly due to the creation of new state framework conditions with regulatory measures, the passing of the Network and Information System Security Act and the General Data Protection Regulation (GDPR).

The “NIS Regulation” (Network and Information System Security Regulation) passed on the basis of the NIS Act entered into force on 18 July 2019. On the basis of the regulations on sectors, reporting thresholds, categories and measures for security precautions for operators of essential services set out in the NIS Regulation, the Strategic NIS Office included the determination of operators of essential services in the seven sectors in August 2019. In terms of general developments in the IT security industry, there was once again an expansion in cloud computing in 2019. This trend is viewed with increasing scepticism by companies as rising dependence on external providers is associated with a loss of control and sovereignty over a company’s own data. Local (on-site) solutions are being replaced more aggressively by cloud solutions. These are expected to become established in the medium to long term.

At an EU level, 2019 was shaped by numerous significant developments. An important step both in terms of expanding the remit and abilities of ENISA and in the direction of the creation of a standardised European certification framework for cybersecurity was able to be taken in particular with the entry into force of the Cybersecurity Act on 27 June 2019. The European Commission is currently working closely with the member states and other stakeholders on what is known as the Union’s continuing work programme on European cybersecurity certification for the consistent implementation of the Cybersecurity Act.

The European  
Cybersecurity Act  
creates a uniform  
certification  
framework.

The European  
Cyber Diplomacy  
Toolbox introduces  
a cyber sanctions  
regime.

In the field of cyber diplomacy, the focus was on the further development of the EU's joint diplomatic response to malicious cyber activities ("Cyber Diplomacy Toolbox"). The cyber sanctions regime which was adopted in May 2019 should be highlighted in particular.

A significant event at an EU level in 2019 was the European Parliament elections, which ran smoothly. Targeted measures were taken in advance against disinformation campaigns against the EU. One result of this is the Action Plan against Disinformation, which was passed in December 2018 and provides for a range of measures to combat disinformation. The result of the Action Plan was decidedly gratifying, as the measures used were effective and as a result of the coordinated approach numerous attempts to influence the European Parliament elections were able to be prevented.

The topic of 5G or the security of the technology known as the "fifth generation of the mobile network" (5G) was not just the focus of numerous debates at an EU level, it was also a priority topic in Austria. The 5G Toolbox (Cybersecurity of 5G networks, EU Toolbox of risk mitigating measures) was presented by the European Commission in early 2020 and now needs to be implemented at a national level.



 Republic of Austria

 Cybersecurity