Cybersecurity Report for 2020

Cybersecurity Report
for 2020

Vienna, 2021

Federal Chancellery
Republic of Austria

Federal Ministry
Republic of Austria
Interior

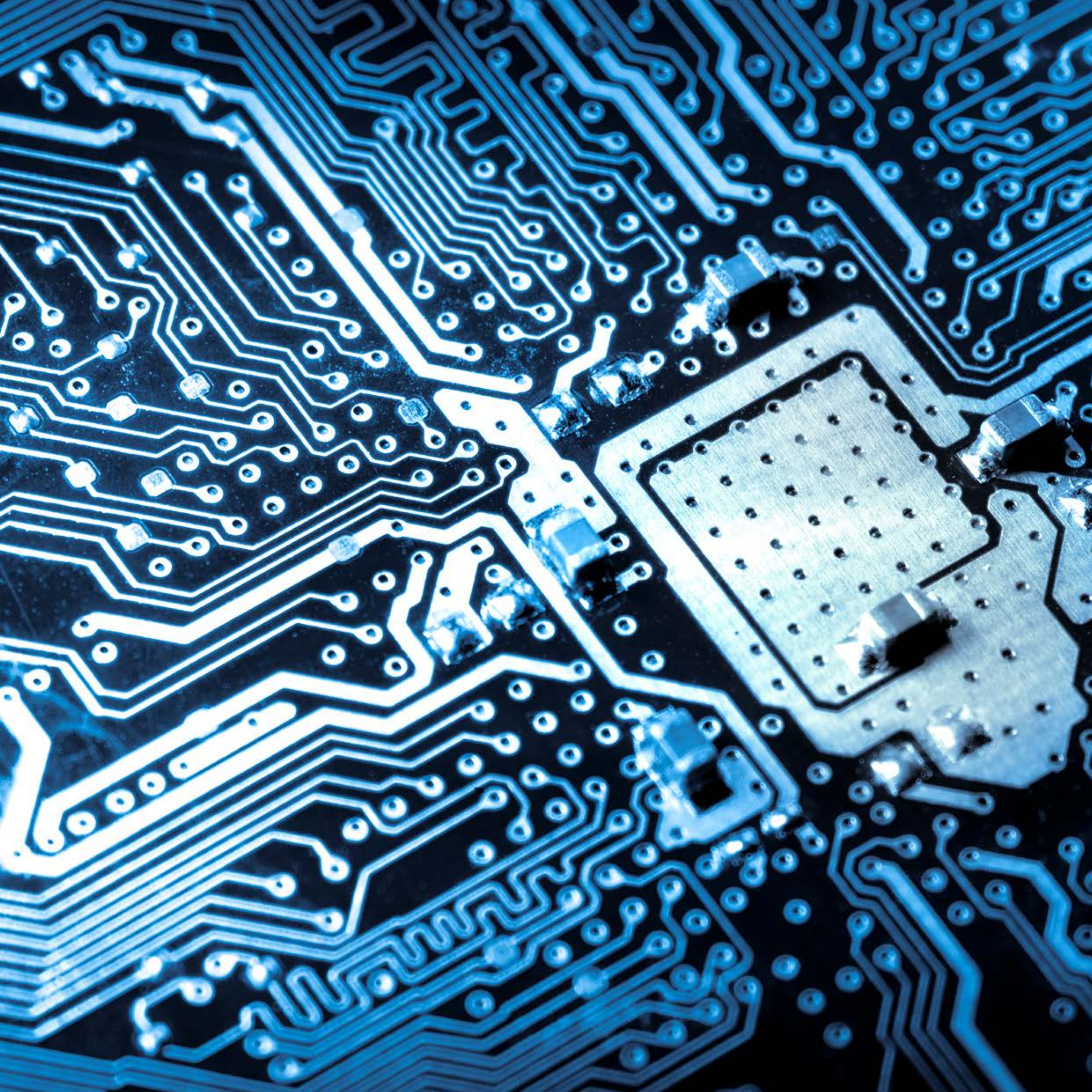
Federal Ministry
Republic of Austria
Defence

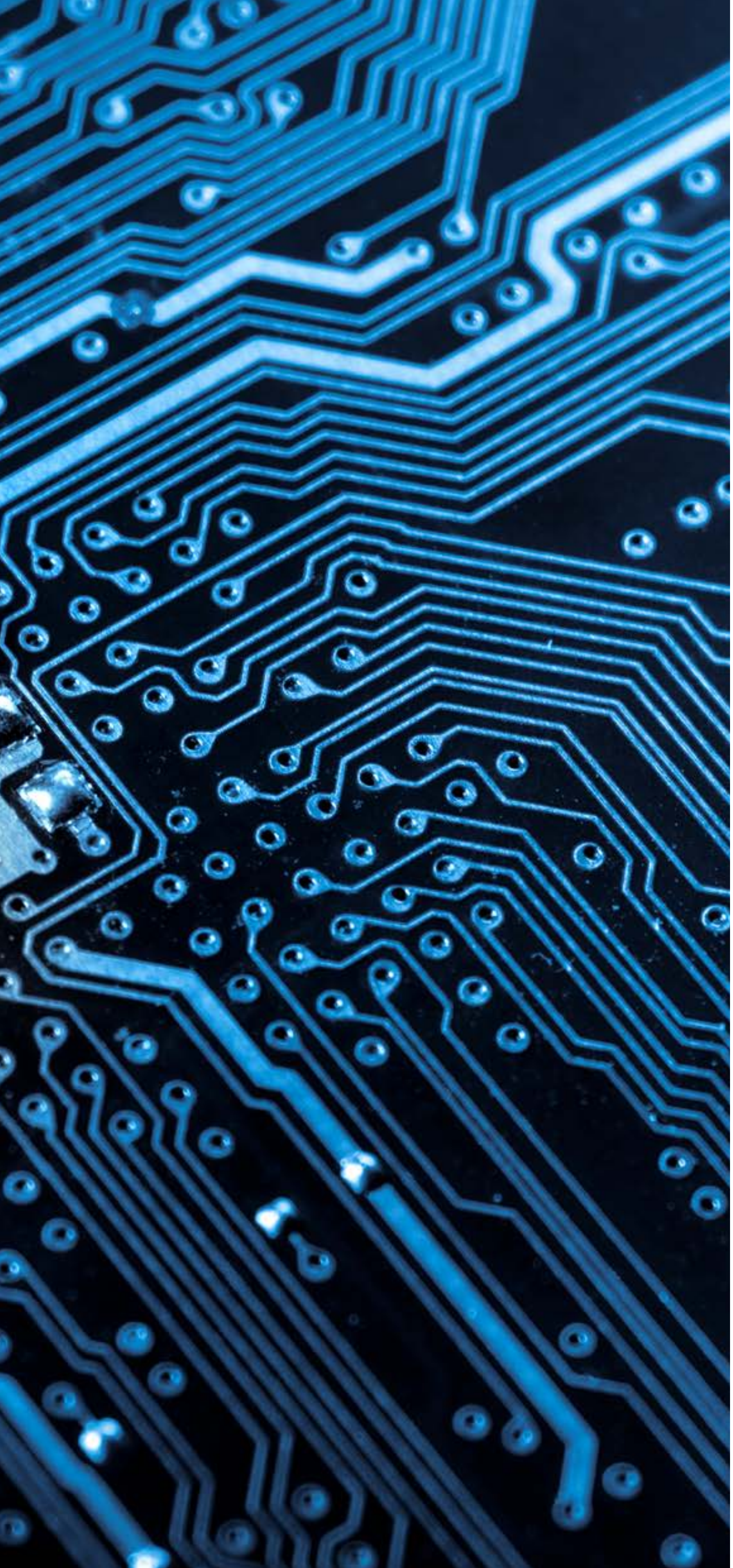
Federal Ministry
Republic of Austria
European and International Affairs

Imprint

Media owner, publisher and editor:
Austrian Federal Chancellery (Bundeskanzleramt)
Ballhausplatz 2, 1010 Vienna
bundeskanzleramt.gv.at
Photo credits: iStock
Layout: BKA Design & Grafik
Printed by: Druckerei Walla GmbH
Vienna, July 2021

Content





Editor’s note

The past year has been dominated by the pandemic. No story has been covered in as much detail, discussed so often, or had a greater influence and effect on our daily lives than the coronavirus known as Covid-19.

Indeed, you might even be tempted to assume that Covid-19 was the only important issue to arise over the last year and that there would be nothing for us to include in this Cybersecurity Report beyond the opening paragraph.

Spoiler alert: Things didn’t quite work out that way, and there are a few more pages to follow this introduction.

It may seem like an eternity ago now, but at the beginning of 2020 the Austrian Federal Ministry for European and International Affairs (BMEIA) was targeted in the biggest cyberattack ever launched against an Austrian state institution. For the first time, government-wide cybersecurity structures were activated in response to the attack. An ad hoc team consisting of experts from the Federal Ministry for European and International Affairs, the Federal Ministry of the Interior, the Federal Ministry of Defence and the Federal Chancellery, working alongside Government Computer Emergency Response Team Austria, finally succeeded in securing the BMEIA’s IT system, the components of which are distributed across the globe. This attack took place in early February, and we all assumed it would provide the highlight of the year.

In hindsight, that assumption seems almost laughable, given that the Covid pandemic had Austria and the world firmly in its grip just a few weeks later. And yet, it was the virus, not an army of Chief Information Officers (CIOs) and Chief Data Officers (CDOs) that triggered an unprecedented acceleration in digitalisation. Suddenly, working from home went from being a bespoke solution for a few exotic, self-consciously trendy companies to being the norm. Companies discovered online platforms and new media, and worked out how to use them to interact with their customers. Demand for videoconferencing exploded. Viewed in the context of this wholesale transformation, occasional data breaches at companies like Zoom were quickly dismissed as small beer.

The pandemic opened up a massive opportunity, and not just for the economy and scientific research. Austria's public administration was quick to react to new ways of working, showing considerable agility. Of course, cybercriminals showed a similar level of agility, again proving just how quickly and flexibly they can respond to changing circumstances. As luck would have it, just when we were all moving to remote working, a well-known company discovered a major security gap in Netscaler/Citrix Gateway, software that is widely used in Austria and many other countries to access networks. The consequences of this security loophole were so unpleasant that it was rather unflatteringly dubbed "Shitrix." Several more vulnerabilities were to come to light in the weeks and months that followed. 2020's cybersecurity race was by now well underway, and cybersecurity teams in Austria and around the world had their work cut out for the year to come.

Cybercriminals are often accused of having no values and no honour. Their self-appointed mouthpieces publicly countered this impression by claiming they would not target research facilities or hospitals, because they appreciated that these organisations were fighting to protect human lives. Shortly afterwards, Germany reported its first death in connection with a cyberattack. Contrary to conventional wisdom, this tragedy was not the result of criminals hacking in to an insulin pump or a pacemaker. The culprit turned out to be a seemingly innocuous hospital administration system that had been encrypted using a crypto-Trojan. When the system failed, a patient who had been admitted to accident and emergency had to be diverted to another hospital. Transferring her took extra time – time the patient couldn't afford to lose. For the time being at least, Austrian hospitals have been spared such attacks.

However, vast numbers of small and medium-sized enterprises have not been so lucky and have been subjected to a veritable flood of malicious encryption software and ransomware trojans. Moreover, while such businesses used to be able to protect themselves by simply backing up their data and implementing robust recovery procedures, today's cybercriminals are learning how to overcome these defences. They have expanded their extortionist repertoire to include threatening to publish company and personal data if the victim fails to pay the ransom.

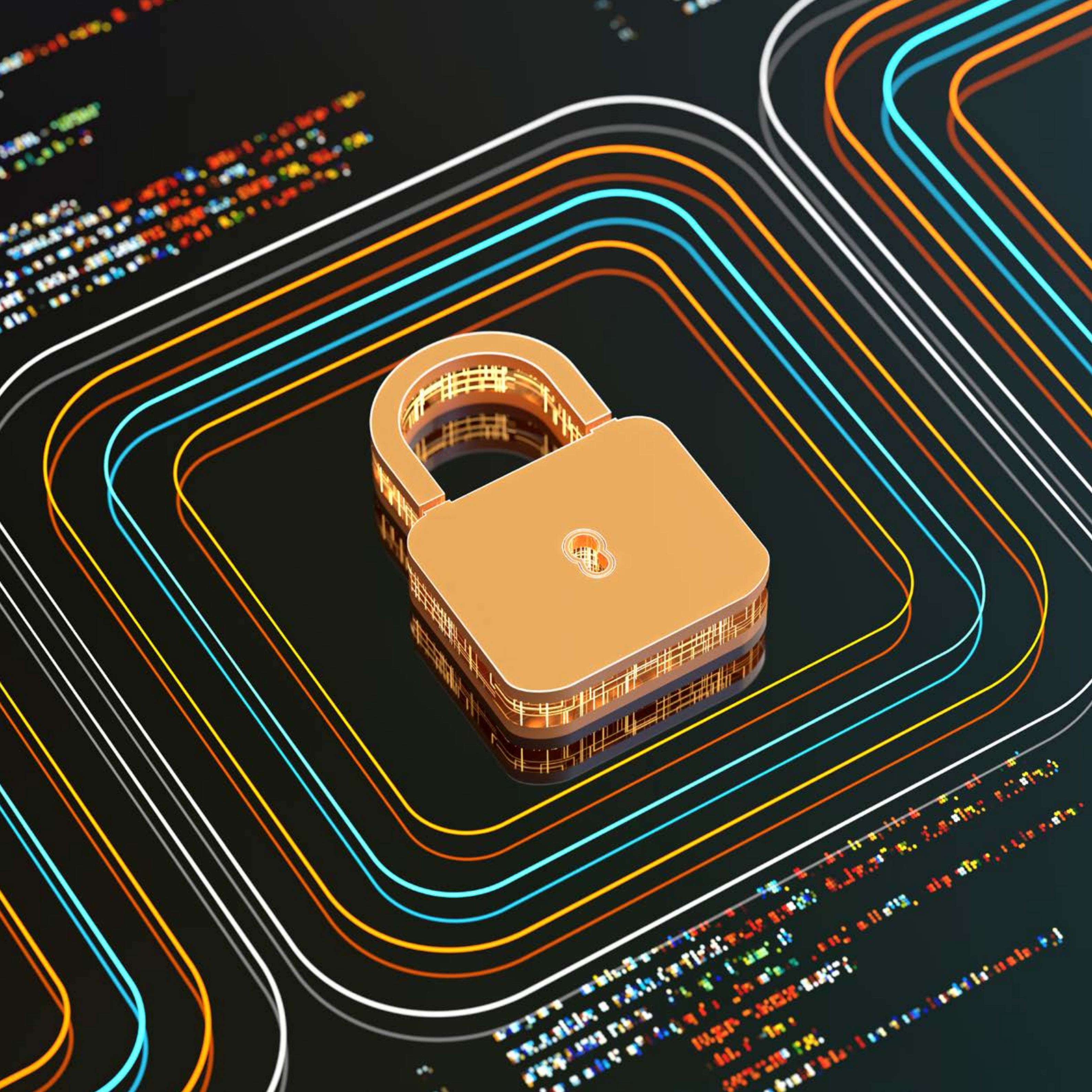
Initially, the first lockdown left the government in a state of shock. All meetings were cancelled, travel was impossible, and carrying on committee work was out of the question. However, this institutional paralysis was mercifully brief, and when the machine did get going again, it did so at an even higher tempo than before. Particularly within EU institutions, moving committees and working groups to videoconferencing has allowed meetings to be held far more frequently. This, in turn, paved the way for the new European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres to be fully established by the end of 2020, well ahead of schedule. Also this year, the EU unveiled its Cybersecurity Strategy for the Digital Decade and adopted the European Commission's proposal for a new Directive designed to ensure a high level of cybersecurity across the European Union, known as NIS 2. Officially, NIS 2 is intended to replace the existing NIS Directive adopted in 2016 with substantially improved provisions. Unofficially, it aims to turbocharge cybersecurity in the EU. As the year wore on, people even began to realise that it might be a good idea to give attendees a break from videoconferences lasting for hours at a time.

I could touch on a wide range of other topics here, and many other important events in 2020 are covered in the rest of this report. It may not have seemed like it, but 2020 was about so much more than Coronavirus, especially as far as cybersecurity was concerned.

And as if all that was not exciting enough, towards the end of the year, details began to emerge of a cyberattack that laid bare just how dependent the world is on the cyber supply chain, and how incredibly vulnerable that system is. Yet again, Christmas came and went with no time to reflect, take stock or draw breath. We could all see SolarWinds SUNBURST was not about to pass Austria by.

But that's another story for another time...

TO BE
CONTINUED...



Introduction

In accordance with Austria's Cybersecurity Strategy (ÖSCS), the Cyber Security Steering Group (CSS) is required to prepare an annual report on cybersecurity in Austria. The last such report was presented in November 2020.

The present Cybersecurity Report, covering the 2020 reporting year, builds on the content of last year's report and includes descriptions of recent developments, particularly internationally and in an operational context. The observation period of this report is 2020, although a few recent developments from 2021 are also discussed.

The aim of the report is to provide a review of the cyber threats and important national and international developments on the basis of department-specific reporting on these issues.

1
Cyber situation / threat

As digital technology increasingly penetrates almost every area of our society and daily life, it is opening up major new opportunities and possibilities. At the same time, however, this development is making society more vulnerable to cyberattacks, and more dependent on the confidentiality, availability and integrity of digital information – in short, on cybersecurity. States, groups and criminal actors are constantly finding new ways of using digital networks to engage in espionage, sabotage or other criminal activities. The technical skills of individual criminals can be more than enough to execute out a wide range of cyberattacks, with unpredictable consequences for Austria's national security.

1.1 Cybersecurity situation – operational level

1.1.1 Overview of the operational situation

The 2020 reporting period began with a cybersecurity incident affecting a government institution. In response to the attack, a cyber crisis was declared for the first time since the adoption of the Network and Information System Security Act (Netz – und Informationssystemsicherheitsgesetz – NIS Act). This led then Federal Minister of the Interior Dr Wolfgang Peschorn, to call on the government's Cyber Crisis Management staff (known by its German acronym, CKM), which in turn prompted the members of the Inner Circle of Operative Co-ordination Structure (IKDOK) to set up a staff to deal with the incident. All the bodies and operational structures involved in the incident acted in a highly professional and effective manner, and they were able to bring the crisis quickly under control. Initial measures to minimise the risks associated with the attack were taken immediately following the incident. This quick, targeted action disrupted the attacker's activities and prevented them from causing more damage. It also created the conditions for a thorough and systematic purge of the system at the beginning of February.

A cybersecurity incident at the BMEIA saw the cross-government cybersecurity structures activated for the first time

When the World Health Organization declared a pandemic in the spring of 2020, it triggered a massive increase in attempted phishing attacks and other forms of fraud. The fraudsters tried to lure their victims using pandemic-themed "bait" – a technique known as event-based social engineering. At the same time, the perimeter cybersecurity of many company and other networks dropped as they struggled to cope with the huge increase in working from home caused by social-distancing requirements and lockdowns.

All the while, perpetrators continued to develop new ways of executing ransomware and distributed denial of service (DDos) attacks throughout the reporting period. The criminals behind ransomware attacks are no longer satisfied with simply demanding a ransom to decrypt data; they are increasingly threatening to publish victims' stolen data as well.

> ” Over the last year, the Coronavirus pandemic had a major impact not just on public health and the economy, but also on cybersecurity. SARS-CoV-2 provided fertile ground for social engineering attacks and cyber fraud.

In contrast to ransomware attacks, DDoS attacks are accompanied by demands for “protection money.” DDoS attackers will often start by attacking the victim’s IT infrastructure as a “warning shot” or as “proof” of what they can do. They then threaten to take down all the victim’s online services unless they pay the blackmailers a set amount of money in a cryptocurrency of the criminals’ choice.

Increasing dependence on the cloud infrastructure and remote IT accesses that allow staff to work from home constitutes a huge risk for companies and government institutions.

Internationally, attacks are increasingly being targeted against the weakest points of networks, with criminals attacking somewhere in the cyber supply chain and using the supply chain to infect the intended target.

1.1.2 How SARS-CoV-2 has affected cyberspace

Particularly in the early stages of the pandemic, the move to working remotely from home disrupted teleworking supply chains for IT systems. Companies were often forced to lower their own cybersecurity defences to allow their employees to work away from their offices. This in turn massively increased the number of points in their systems that were vulnerable to attack and opened up new attack vectors for criminals. The threat was rendered even more acute by a security vulnerability in the RDP Gateways software needed to enable remote working, which came to light just as many businesses started working from home. This development did not lead to any major cybersecurity incidents affecting Austria’s critical infrastructure or government institutions. However, the reduced level of security associated with remote working continues to pose a high risk.

Although, at the beginning of the crisis, cybercriminals were at pains to stress that they would “refrain” from attacking targets in the health sector – a message that gained significant traction in the media – they failed to keep their promise. Both hospitals and vaccination facilities were subjected to cyberattacks and espionage, sometimes on a massive scale.

1.1.3 Advanced Persistent Threats (APTs)

Advanced persistent threats (APTs) pose a long-term and increasing threat to Austria's businesses and public administration. The primary aim behind APTs is to obtain information through economic and industrial espionage or politically motivated spying. APTs also allow attackers to sabotage computer networks in administrative bodies, production facilities and supply chains. Their consequences run the gamut from reputational damage to complete system failure.

At the turn of the year, a malware attack on the network of the Federal Ministry for European and International Affairs was uncovered following a tip-off from the Government Computer Emergency Response Team (GovCERT). As soon as the incident was identified, the incident response procedure was triggered and an initial analysis conducted by GovCERT and the Federal Agency for State Protection and Counter Terrorism (BVT)'s Cyber Security Centre (CSC). By 3 January 2020, some components of the malware had been successfully decrypted and the scale of the incident had become clear, prompting the decision to trigger the crisis mechanisms developed to deal with such major incidents.

On 7 January 2020, an operations team was stood up in response to the attack. The team was led by the Federal Ministry of the Interior (BMI), which also contributed staff from the BVT and the Cyber Crime Competence Centre (C4). They were joined by colleagues from the Federal Ministry of Defence (BMLV), including staff from the Military Computer Emergency Readiness Team (MilCERT), as well as by personnel from the Strategic Intelligence Agency (HNaA), the Armed Forces Security Agency (AbwA), the Federal Chancellery (BKA), the Government Computer Emergency Response Team (GovCERT) and the Federal Ministry for European and International Affairs (BMEIA). The team immediately set to work dealing with the specific circumstances of the incident. The BMEIA commissioned an Austrian service provider to assist, and this external contractor was integrated into the operations team.

Once a summary report had been prepared setting out the scale and severity of the incident, the clean-up phase began on 7 February 2020. This was an intensive procedure carried out at BMEIA headquarters and covering Austrian representation around the world. The BMEIA's network is both global and decentralised, operating across multiple timezones. A high proportion of its ICT equipment is made up of mobile devices. This posed particular organisational and logistical challenges as far as preparing and executing the clean-up was concerned. Nevertheless, by 9 February the clean-up had been completed successfully and largely without incident.

The nature of the attack, and the tactics, techniques and procedures (TTP) employed by the attacker were characteristic of an advanced persistent threat (APT). A criminal investigation into the incident is ongoing. In the wake of the attack, a number of measures were introduced to make the network more resilient in the long term.

1.1.4 DDoS attacks and attempted blackmail

Over the reporting period, there were several waves of distributed denial of service (DDos) attacks, particularly against banks, the financial sector, and internet service providers (ISPs). In addition to denying services, these attacks also aimed to blackmail their victims. The criminals' latest method for DDoS attacks is to target elements of the victim's system that are accessible via the internet using a low-bandwidth DDoS attack. At the same time, they send an extortion letter by e-mail, threatening the target with "far more serious" DDoS attacks if they fail to pay a certain sum in the cryptocurrency of the criminals' choice. There is no evidence to suggest that any of the low-bandwidth attacks were followed up immediately; it was only towards the end of the year that the companies that had failed to comply with the original extortion letter were attacked again. However, some of these follow-up attacks were carried out by copycat offenders who wrote their extortion letters in German using the names of well-known hacker groups (such as Fancy Bears and Lazarus).

This phenomenon can be seen worldwide and in an increasingly wide range of sectors.

The extortion letters often stick to an identical template, with only the senders' e-mail addresses and their choice of cryptocurrency (often bitcoin) varying between attacks. It is impossible to determine whether attacks of this kind are carried out by a single gang of criminals or by multiple groups of perpetrators.

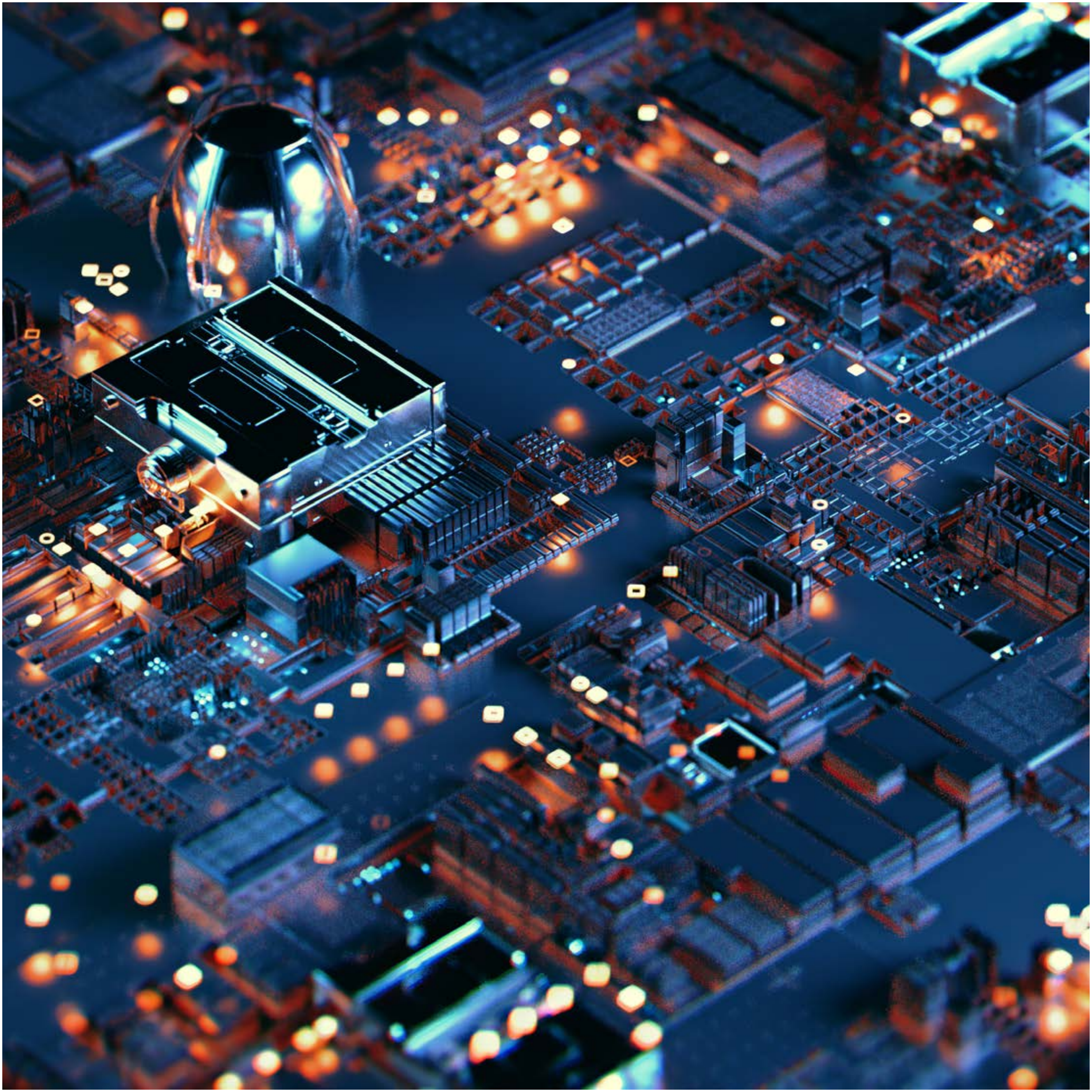
This form of digital highway robbery is expected to become even more common in the future as a result of increased interconnectivity and large numbers of poorly secured Internet of Things (IoT) devices being connected to botnets.

1.1.5 Attacks penetrating computer networks

SolarWinds: Towards the end of 2020, details emerged of a cybersecurity incident that highlighted the level of dependency within the cyber supply chain as well as exposing just how vulnerable this supply chain was in dramatic fashion. The initial incident is believed to have occurred at the American company SolarWinds, which produces software solutions for managing computer networks.

According to the reports of the incident, an attacker managed to penetrate SolarWinds' corporate network and compromise its software update infrastructure. Customers then downloaded compromised updates for the Orion software suite, as the updates still carried SolarWinds' signature. These updates then installed backdoors on the customers' systems. An initial damage assessment by SolarWinds showed that the supply chain attack could have affected as many as 18.000 targets. The victims included a number of Austrian companies, although no critical infrastructure or government institutions were affected.

The Orion software suite compromised in the attack is used by various US government offices as well as by most Fortune 500 companies. In light of this, the US Cybersecurity and Infrastructure Security Agency (CISA) issued an emergency directive following the incident, advising users not to use the platform. The attack on SolarWinds led to follow-up attacks on the US Treasury and the National Telecommunications and Information Administration (NTIA), which is part of the US Department of Commerce. The Orion software platform is not widely used in Austria.



The SolarWinds attack was not the first attack to be carried out by compromising update infrastructure, but in terms of its scope and impact it was probably the most serious security incident to have been triggered using this attack vector.

Software AG: Another serious cybersecurity incident occurred in early October 2020 when Software AG, Germany's second-largest software company, fell victim to a cyber blackmail attack. The perpetrators were able to steal data from the company network before exfiltrating it from the system and putting it beyond use. The exfiltrated data was then used to carry out follow-up attacks against Software AG customers. This unusual incident caused particular concern because Software AG produces operating technology (OT/industry 4.0) systems. These products provide the interface between software and production hardware and are usually equipped with remote maintenance accesses.

This means that the people who attacked Software AG may also have been able to steal its customers' access data. Various data stolen during the attack, including the details of Austrian companies, has been found on the TOR network, which is / has been used to publish the stolen data. The IKDOK immediately issued a warning to the Austrian firms affected, along with advice on how to mitigate the risks associated with the incident.

Cloud-based databases and storage systems: Incidents over the course of the reporting period have shown that these systems (including Amazon S3 Buckets, Redis, Elasticsearch and MongoDB) can be systematically targeted, identified and exploited by cybercriminals. The SolarWinds attack should also be viewed as an attack on a cloud-based system.

1.1.6 Ransomware

The phenomenon of ransomware was omnipresent throughout the reporting period and was responsible for major damage. In many cases it was found that the functionality of the ransomware programs used had been expanded to allow perpetrators to steal data from target networks. If victims appeared reluctant to pay the ransom demanded, they were threatened with the publication of this stolen data. The ransomware demanded usually takes account of the victim's financial circumstances, details of which can be obtained by the attackers through open-source research. In most cases, the attack vector is a combination of targeted social engineering and a Microsoft Office document, which is contaminated with malicious code before being sent to the victim in an e-mail.

1.1.7 Other malicious code

Following a pause lasting several months, the **Emotet** malware program became active once again in the summer of the reporting period, triggering another global wave of malspam. It soon became clear that the program's capabilities had been significantly improved during its hiatus. Preventing Microsoft Office from running macros or ensuring that only trusted and signed macros can be executed is one of the main lines of defence against Emotet. Office documents containing macros are effectively executable files and are comparable with .EXE files from a technical security standpoint. Emotet passes itself off as legitimate by embedding itself in existing e-mail communications, thus prompting the victim to download and open malicious files.

The code used in Emotet can also download additional malicious code modules once a device has been infected. These modules may include ransomware, data extraction / theft tools, or software that connects the infected machine to a botnet.

1.1.8 Vulnerabilities

Yet again, numerous critical vulnerabilities were identified in the course of this reporting period. Some of the most challenging for Austria's businesses and government institutions are described below.

CITRIX/NetScaler: The publication of the exploit codes for CITRIX/NetScaler on 10 January 2020 was followed by numerous attacks on private companies and state authorities. These attacks also prompted public debate on the implications for the use of Austria's new electronic file management system (known as ELAK) within government.

RDP Gateway: On 14 January 2020, Microsoft released patches to fix two critical security loopholes in RDP Gateway (CVE-2020-0609 and CVE-2020-0610). Both had the potential to facilitate remote code execution (RCE) attacks. An exploit for these vulnerabilities has been publicly available on GitHub since 23 January 2020, and the ability to use it to conduct RCE attacks has been demonstrated. However, the code used for these attacks has not been published.

Microsoft Server Message Block 3.1.1 (SMBv3): This vulnerability can be exploited via the network and allows any command to be executed with system rights. The vulnerability is also presumed to be worm-capable, meaning that any infection can spread very quickly. It affected SMBv3 clients and servers running Windows 10 1903 and 1909.

Netlogon Remote Protocol (CVE-2020-1472, alias Zerologon): Successful attackers were able to exploit this vulnerability to take control of entire Windows domains. Microsoft patched the vulnerability in August, but proof of concept for such attacks has already been published.

More critical vulnerabilities were found **in** several versions of Oracle WebLogic Server. They included a critical vulnerability that can be exploited via the internet (CVE-2020-14750) in SAP NetWeaver AS Java (CVE-2020-6287) for F5 K52145254 TMUI RCE Vulnerability (CVE-2020-5902) and Palo Alto PAN-OS (CVE-2020-2021). In December 2020 another design flaw was found in the Windows Authentication protocols in the shape of the vulnerability known as Kerberos Bronze Bit Attack (CVE-2020-17049).

As far as the cyber supply chain issues described above are concerned, there is always a trade-off between applying the update immediately (as is usually recommended) or taking the time to review the code and identify any embedded malicious code or other errors with the potential to disrupt systems before they damage the user’s network. Code reviews are always time-consuming and costly exercises, and often require existing contracts with software manufacturers to be updated.

1.1.9 Publication of data

The recent trend towards publishing data, and particularly stolen access data, is continuing unabated. The publication of personal data belonging to customers (including Austrian customers) of the IT security training company SANS was just one such 'data leak' that occurred in the course of the reporting year.

As already mentioned in the section on ransomware, DDoS attacks and other malicious codes, cybercriminals are increasingly threatening to publish stolen data (and, in some cases, carrying out these threats) to lend credibility to their demands. Such attacks affect not only their primary target, but also the target's partners right along the cyber supply chain.

1.1.10 Legacy IT infrastructure

The source code for Windows XP is suspected to have been leaked in autumn 2020 and offered for sale on an internet forum. Many older systems, including "inherited" infrastructure (also known as legacy systems), continue to use Windows XP as an operating system, often including operating technology (OT). OT faces particular challenges because it is often based on underlying operating systems for which updates are rarely, if ever, released. This poses an enormous security problem for those operating with this outdated technology. The end-of-life cycle for Microsoft's Windows XP system has been gradually scaled back since it began on 8 April 2014 and was finally wound up some time ago. In practice, this means that any vulnerabilities discovered in the operating system are no longer patched by the manufacturer. In addition, support for Microsoft's Windows 7 operating system also came to an end on 14 January 2020.

"Legacy systems" like these are often a gateway for cybercriminals. Indeed, as more and more of these outdated systems are connected to the internet and industry 4.0 (a trend that has accelerated as a result of the Covid-19 pandemic), criminals are increasingly viewing them as ideal targets. According to a report in the German magazine Heise, there are at least 100 million Windows 7 PCs still connected to the internet - 18 per cent of all Windows computers worldwide. Countless such systems are still in use in Austria, too, and they can be accessed via the internet.

1.2 Cybersecurity situation – companies and security service providers

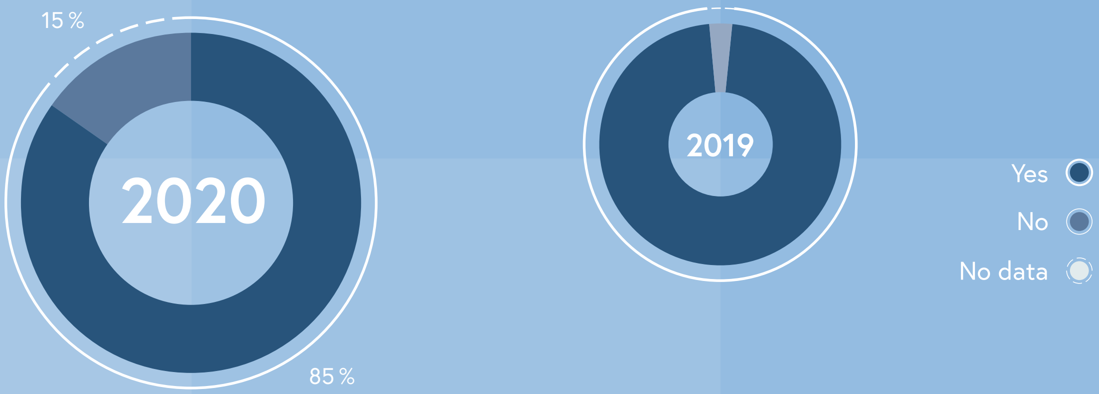
Austria's state cybersecurity bodies work closely with government institutions and operators of critical infrastructure and operators of essential services. This allows the state to retain an overview of the overall cybersecurity situation as well as to take quick action to counter any critical incidents as they arise. As in previous years, leading stakeholders were invited to contribute to this report by providing their own assessments of the latest developments, thus adding detail to the overall picture. This approach is designed to produce a reliable summary of the opportunities, threats and trends relevant to cyber in Austria and to ensure that this summary is as complete as it can possibly be.

Investments in cybersecurity helped to prevent serious IT security incidents

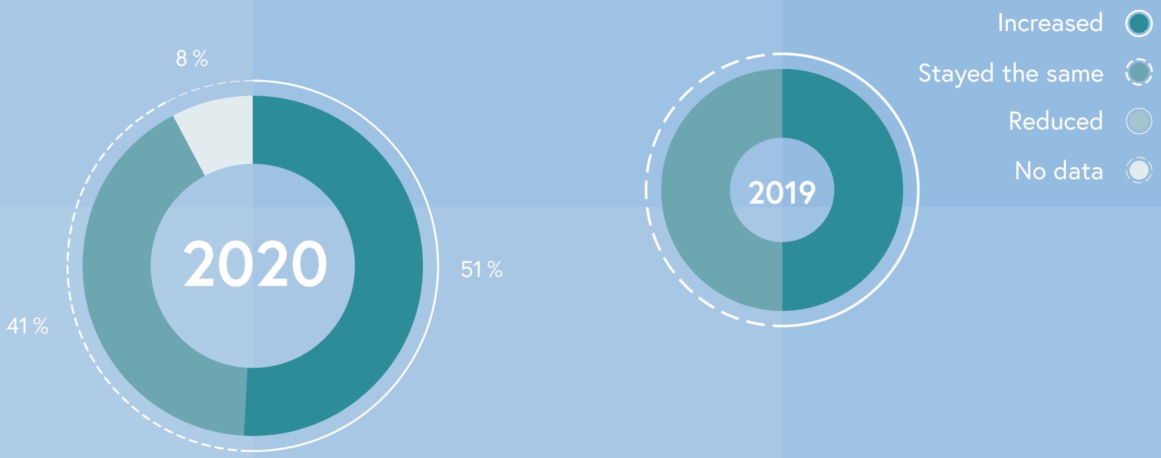
1.2.1 Companies working in critical infrastructure and government institutions

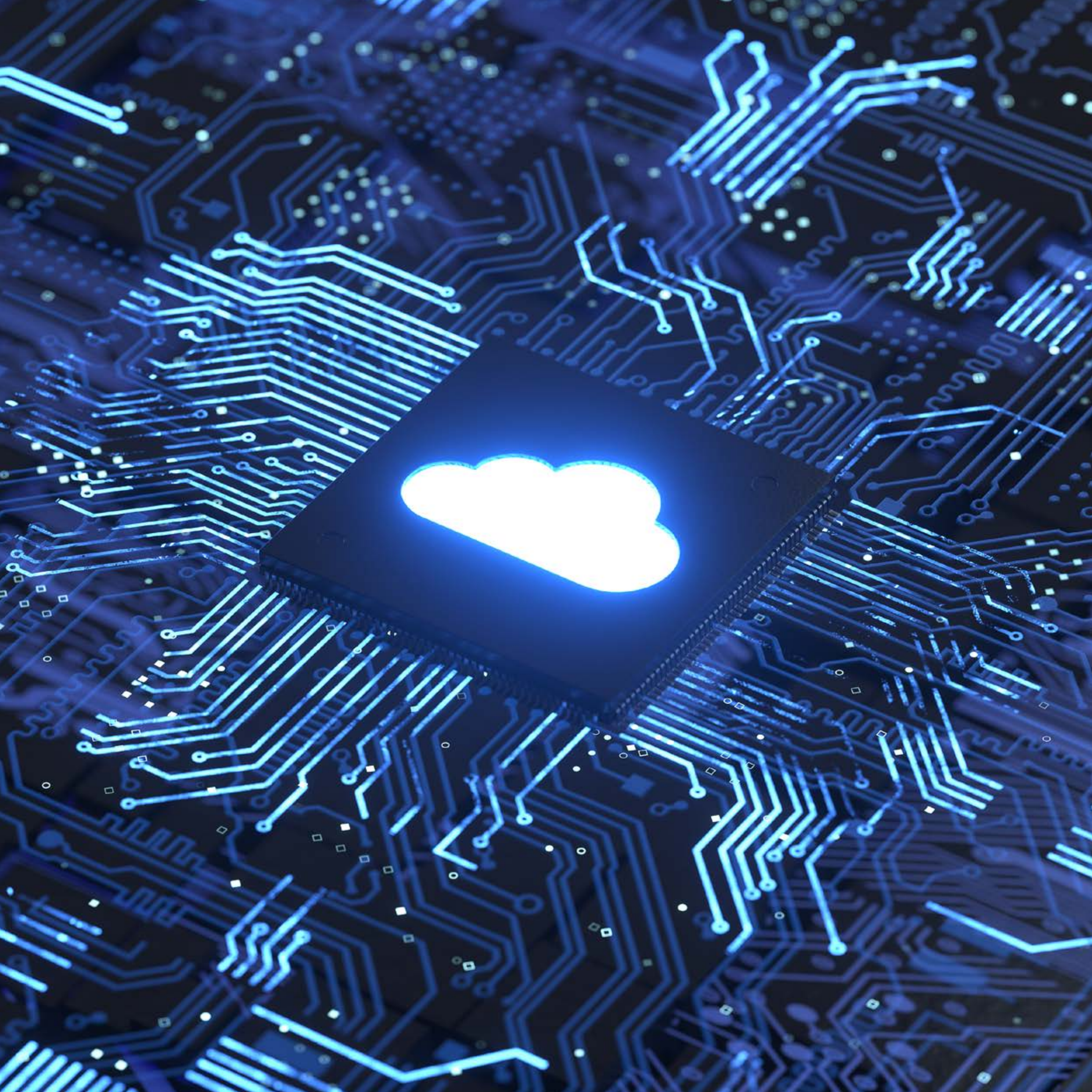
Most of the Austrian critical infrastructure companies surveyed for this report had invested in cybersecurity over the course of 2020. The proportion of companies that increased their cybersecurity budgets during the reporting period, as opposed to maintaining it at the same level as in the previous year, increased slightly. None of the companies surveyed reduced their cybersecurity budgets. Overall, the survey results confirmed the recent trend suggesting that spending on IT security is remaining broadly stable as the years go by. This investment is likely to have prevented some serious IT security incidents in 2020.

Did your company implement any new IT security measures in 2020 to make it easier to detect IT security incidents?



How did your company's IT security budget change in 2020 in comparison to 2019?





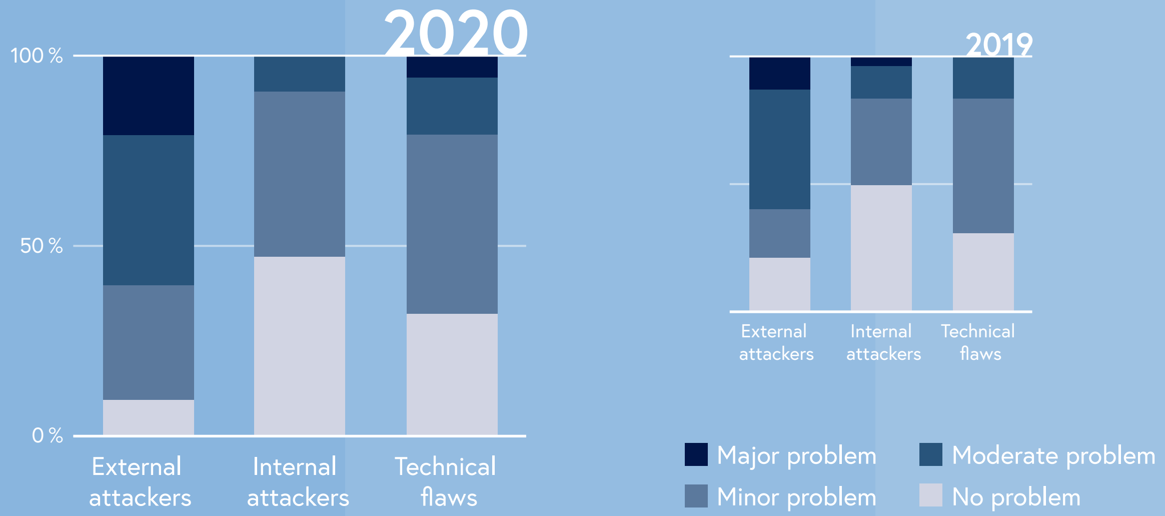
IT security measures taken by the organisations surveyed during the reporting period included stricter monitoring of on-premises and cloud systems, the implementation and expansion of security information and event management (SIEM) solutions, extended use of logging, setting up security operations centres (SOCs), the use of next-generation firewalls and next-generation mail gateways, ransomware scanning, endpoint detection, cloud access and DNS filtering, regular penetration testing and vulnerability scanning, improving Information security management systems (ISMS) and obtaining ISO 27001 certification, as well as introducing a variety of awareness-raising initiatives and staff training courses.

As in previous years, company-wide IT risk management systems, ISO 27001/27019-compliant ISMSs and training to raise awareness of IT security issues are viewed as the most effective way of avoiding security incidents and minimising the damage in the event of an attack.

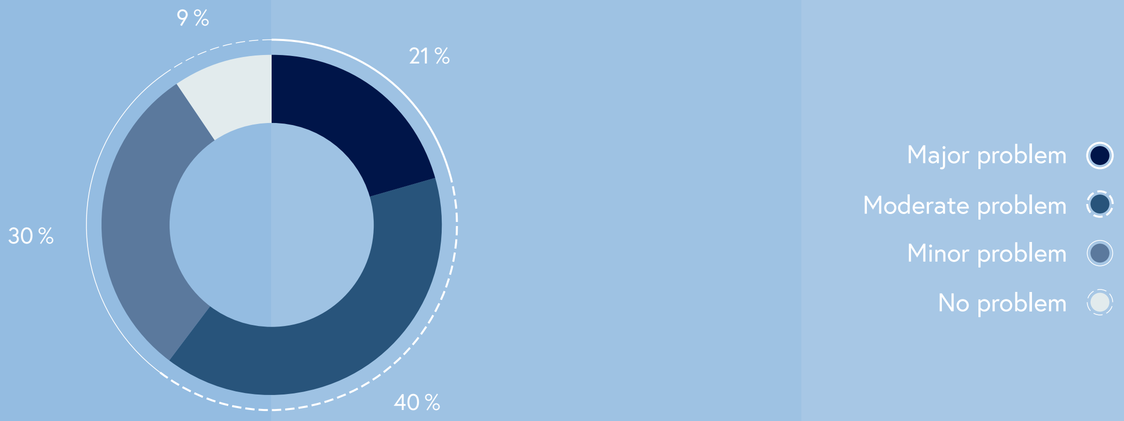
The key to success is having good cybersecurity expertise in your own team(s), which is why Austria has invested heavily in education and training

Analysis of the causes of IT security incidents in 2020 paints a comparable picture overall to that seen in 2019. It suggests that most incidents are caused by external attackers and/or technical faults. Insiders were only involved in a small number of attacks. However, there has nevertheless been a shift here in comparison to 2019, since although the risk of an insider attack or an incident caused by a technical defect is assessed as unchanged, the risk of attacks by external attackers has increased significantly. Attacks are primarily targeted against the Office environment and/or Windows devices.

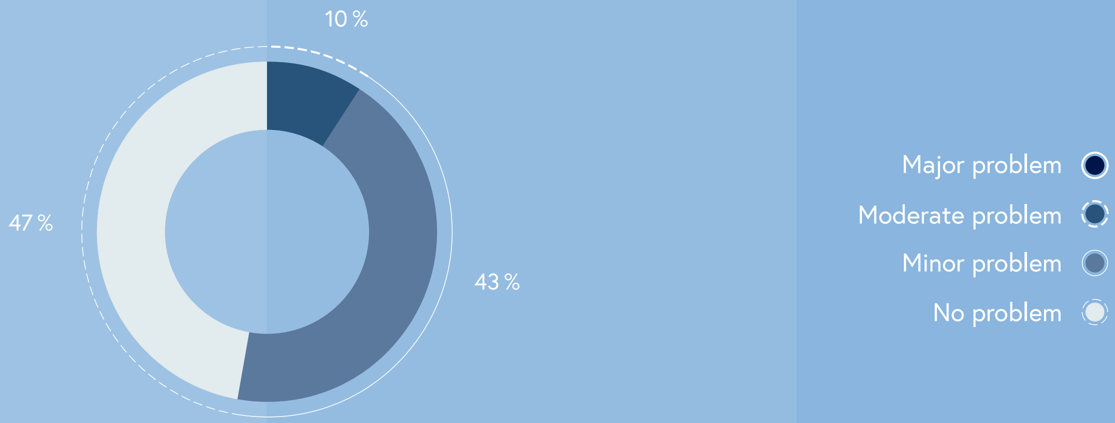
Causes of incidents



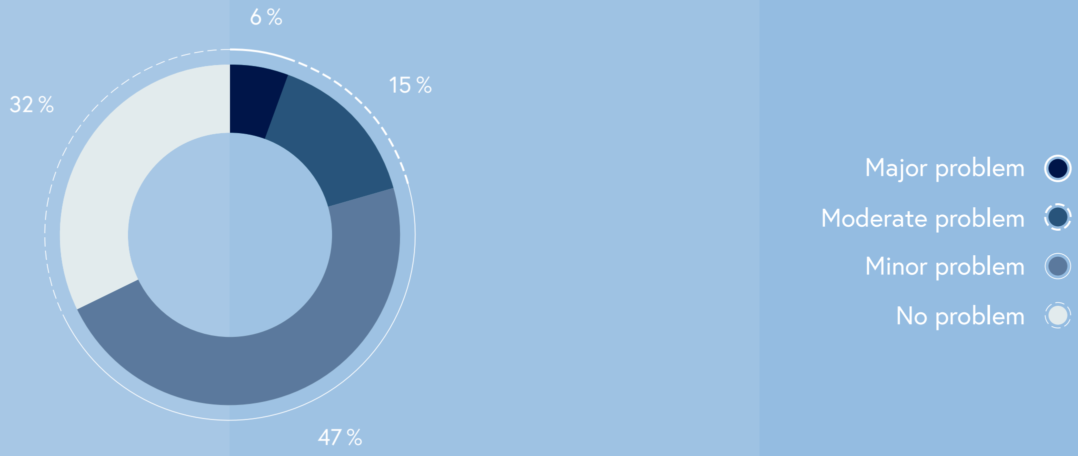
How big a problem do you think attacks by external perpetrators have been in the year 2020?



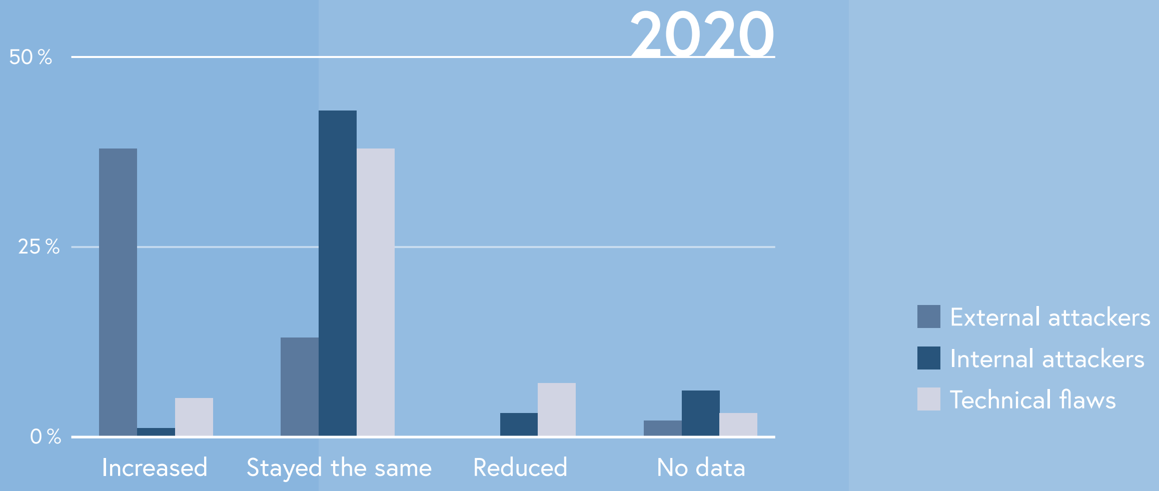
How big a problem do you think attacks by insiders have been in the year 2020?



How big a problem do you think attacks caused by technical defects have been in the year 2020?



What changes have you observed in this area in 2020 in comparison to 2019?



Feedback from “lessons learned” exercises highlights the following trends:

According to the feedback, the organisations surveyed were intensely focused on compliance with new regulatory measures, such as the European General Data Protection Regulation (GDPR) or implementing the Austrian Network and Information System Security Act (NIS Act), which came into force in 2019. As far as the technology itself was concerned, cloud computing continued to dominate their thinking. The pressure to use cloud services continues to grow, despite the fact that fundamental issues regarding data protection and data security are still to be resolved. The respondents to the survey felt that there was often no satisfactory regulatory framework in place for legal issues. In this respect, there is a major disconnect between the legal framework and reality. However, having their own cloud strategy can help companies to resolve a lot of problems before they arise in the first place. For example, companies sometimes experience severe difficulties when international software manufacturers with high market penetrations switch to “cloud first” or “cloud only” strategies. The difficulties inherent in transferring data to the United States at the same time as complying with the GDPR, an issue which is yet to be fully clarified, pose particular challenges for firms in this respect. Respondents also cited the fact there is no common, EU-wide approach to these cloud solutions as unsatisfactory. This problem rose to prominence in the course of 2020, particularly as the coronavirus took hold and use of videoconferencing systems (such as Zoom) took off.

Maintaining the ability to act independently is another challenge for companies, especially in light of the trend towards security components being managed exclusively using cloud-based systems. This development poses a variety of risks for the associated supply chain. The firms surveyed noted that hopes the GDPR would propel moves to create an independent European IT industry towards the top of the agenda have generally failed to materialise, while the American and Israeli IT industries have enjoyed major commercial success and sharp increases in profits. An increasingly impenetrable web of competence centres and centres of excellence for cybersecurity in Austria and the EU, many of which issue differing standards and recommendations on the current state of technology and other issues, has done nothing to simplify matters. The companies surveyed expressed their hopes for standardisation and consolidation in this regard.

Until very recently, cybersecurity was generally seen as only tangentially relevant to operational security. However, since the NIS Act came into force, comprehensive concepts and risk assessments have become more widespread. As part of this more holistic approach, respondents reported that business continuity management (BCM) and emergency planning had gained in importance and were increasingly being incorporated into updated strategies. In turn, this development has spurred on organisational developments related to ISMSs, and SOCs have been recognised as essential. Recent incidents within the companies surveyed have also prompted them to update their processes and/or to subject them to a variety of quality assurance procedures. This has in turn led to more Chief Information Security Officers (CISOs) being appointed within companies and to more emergency response systems being set up.

Respondents to our survey also saw incident response playbooks or security checklists as a major factor in dealing successfully with cybersecurity incidents and noted that the results of external and internal audits were also valuable in this respect. An increasing number of respondents are identifying complexity, and the specialisation it dictates, as an issue, not least because of the high number of suppliers within the IT security sector and a supply chain that is becoming ever more complicated. In light of these developments, the companies surveyed assumed that additional, dedicated resources would have to be allocated to this area in order to guarantee an appropriate level of security right along the supply chain.

Security consultants increasingly see their role as “translating” key topics for Chief Information Officers (CIOs) and IT departments, in much the same way as IT advisers explain IT issues to commercial departments. Measures to secure IT systems and maintain information security need to be treated as a top priority, and management needs to be fully committed to them. Only then can companies react to dangerous incidents appropriately and with confidence.

The sector is currently focusing even more strongly on vulnerability management and threat intelligence in an effort to close existing security loopholes quickly and identify and strengthen weaknesses in its own defences. Reducing the number of domain admins and a more granular approach to user rights are seen as the preferred means of reducing configuration errors and minimising their effects. Given this development, zero-trust systems are becoming more relevant.

Leaked passwords, lack of account lifecycle management, poor data and service in corporate IT (by service providers), failure to enforce and monitor security policies, and not implementing recommendations from security audits in a timely manner are seen as drivers of cyber risks for companies.

Respondents to our survey also noted that the sharp increase in workload associated with ever stricter compliance and documentation requirements was tying down more and more operational resources, thus reducing the effectiveness of IT security staff.

The biggest single risk factor is still considered to be people (i. e., company employees), rather than the technology itself. The companies that responded to our survey expect the requirement to raise awareness of cyber issues will increase sharply in the next few years. To meet this requirement, IT security services will have to expand beyond specific, technically focused niches to cover a comprehensive system including staff training.

Moreover, the need to raise awareness of cybersecurity issues is particularly acute at the moment, with so many staff working from home as a result of Covid-19. The use of so-called “shadow IT” (ICT infrastructure that has not been officially issued and secured by the company) at home significantly increases the risk of a cyberattack.

The companies that took part in our survey stressed the importance of securing external accesses (e. g., via 2FA) properly, as such accesses are used more frequently by staff working from home.

Despite the media hype surrounding the cyber insurance market, survey respondents felt its effect was still extremely limited, not least because of major variations in premiums and coverage. The survey also showed that respondents had no empirical experience to draw on as far as the costs and benefits of such insurance were concerned.

The companies surveyed viewed the trend towards outsourcing SOC services to professional external service providers as a positive development. Their only reservation in this regard was that it increased their dependency on third parties, which severely limited their ability to take independent action in response to incidents and especially to emergencies. Despite this, they noted that the outsourcing of security services should be assessed "in the round and not simply from an economic perspective."

Conducting regular cyber exercises within the companies surveyed at both strategic and operational level had fostered greater understanding of cybersecurity at management level, as well as improving coordination within incident response teams.

There is a current trend towards outsourcing SOC services to professional external service providers

Analysing attacks on their competitors had helped survey respondents lay the groundwork for practical action to strengthen their own security and to implement improvements to their processes and procedures. Optimising communication processes in the event of a cyberattack was cited as a particular area of focus.

Covid-19 has proved that people can work together even when they are working from home, although compliance with reporting chains and obligations was seen as particularly important in connection with home-working. Cooperating under these circumstances requires strong communication across departments and a multifaceted approach to problem-solving. Exchanging information on security incidents openly will make Austria's entire private sector economy more resilient and responsive. In order for appropriate defensive action to be taken quickly, it is crucial that attacks are reported as early as possible. Doing so requires both functioning communication structures and a high level of trust.

The shortage of skilled staff in the cybersecurity sector remains a major issue for Austrian companies, and the problem has become even more acute thanks to a combination of continuing digitalisation and the effects of the current coronavirus crisis. This lack of qualified personnel also means that urgent security-related tasks, such as checking work completed by external contractors, cannot be completed to the high standards required or cannot be carried out as thoroughly as they should be.

Widespread working from home is massively increasingly demand for secure remote access to networks

The new ways of working adopted this year also require practical and organisational changes as well as redundant internet connections and comprehensive provision of mobile workstations. In turn, these changes also give rise to new challenges in terms of administration and enforcing IT security regulations. These technical and organisational measures are increasing the workload associated with ICT security. For the staff charged with implementing the changes at technical level, it also means developing new skills to equip them for this task.

As production IT and operating technology (OT) become ever more highly networked, appropriate network plans and security concepts will have to be drawn up to support this development. Particular attention and resources should be devoted to critical OT. This should ensure that cybersecurity incidents can be quickly contained and that users can swiftly regain control over affected systems. According to the feedback from the companies surveyed, dense networks and the need to ensure that OT can continue to operate at all times, including independently of IT systems, represent a particular challenge for them. Legacy IoT – IoT devices that are no longer part of update cycles – are perceived as high risk and particularly challenging to secure.

The cyber supply chain is again on companies' radars in light of a number of recent cybersecurity incidents in this area. In evaluating the security of their supply chains, firms need to take account of their dependencies on cloud service providers at the same time as assessing how secure their suppliers, customers and partners are. In this regard, finding ways to secure the entire production chain is seen as particularly difficult, as is defining and implementing uniform security standards. Any risk assessment has to go beyond obvious dependencies associated with externally purchased IT services (such as office IT and production OT systems) to consider less obvious dependencies, such as those associated with telecoms providers. All of these factors also have to be incorporated into business continuity planning. Such planning needs to include functioning backup and restoration processes, security concepts and crisis plans, as well as individual plans for specific circumstances. In particular, there should be a clear procedure to ensure that the business can continue to operate if its critical production systems fail. Unless it is sufficiently secure, every component process along the length of the supply chain is a potential risk to all the other participants in the chain. With this in mind, the firms surveyed felt that fostering a shared understanding of cybersecurity issues was particularly important, as was the participants' determination to maintain minimum security standards at all times. However, the respondents to our survey said they often saw room for improvement in this area, particularly as far as manufacturers of production-related systems and medical devices for human use are concerned.

Companies see artificial intelligence (AI) as an opportunity to strengthen their own cybersecurity. However, they also fear it will be used by criminal actors to heighten the potential cyber threat. AI is increasing the speed at which attacks can be carried out, and AI-assisted defensive systems will be needed to counteract this development. However, companies using such systems will lose some control over their own systems and security measures, a development viewed in a negative light.

1.2.2 Leading private companies in the cybersecurity industry

Once again, the response rate to our survey of leading private cybersecurity firms was relatively low for the 2020 reporting year. Nevertheless, a few trends and lessons learned can be identified from the responses received.

Types of incident

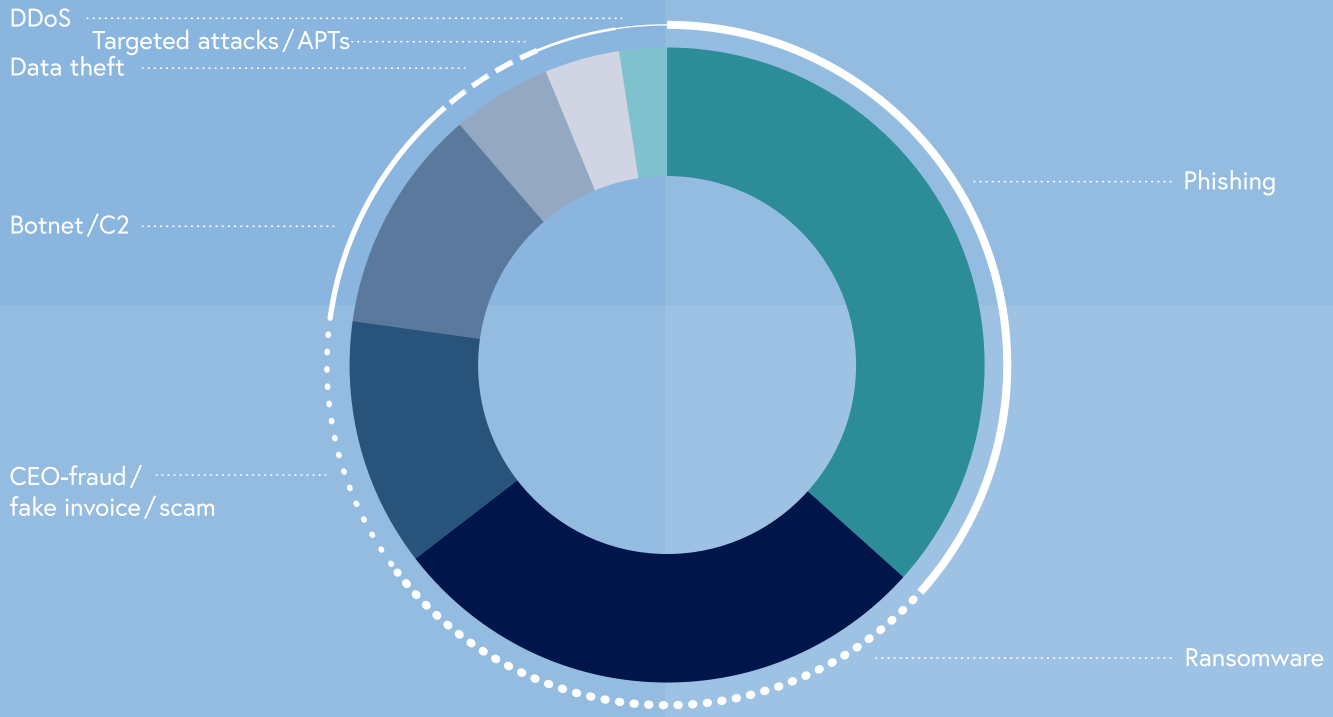
2020	SEC 01	SEC 02	SEC 03	SEC 04
Phishing	+	−	+	
Ransomware	+		+	+
CEO fraud / fake invoice / scam	+	+	−	−
Botnet / C2	−	+	=	
Data theft	+		=	
Targeted attacks / APTs	+		=	
DDoS			=	
Defacements	−		=	

Motivations for cyberattacks

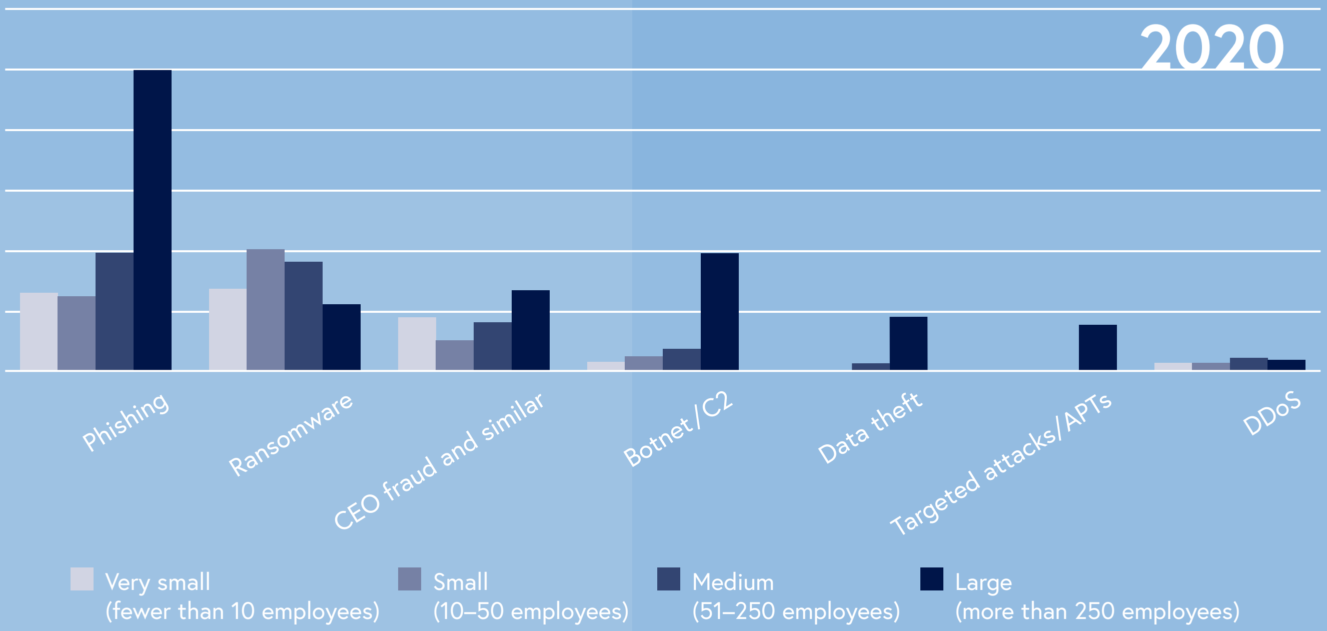
2020	SEC 01	SEC 02	SEC 03	SEC 04
Monetary / criminal	+	=	+	+
Political / “Hacktivism”	=		−	
Personal / revenge	+		−	
State / intelligence gathering	=			+
Technical flaw	=		=	

The private-sector security firms that responded to the survey reported the following types of incidents over the course of the reporting period:

Types of incident reported during the reporting period



Types of incident in the reporting period by company size



Phishing

Companies' resilience in relation to phishing attacks is still assessed as inadequate. Employees often lack the awareness required to spot targeted attacks. However, opportunities to raise awareness through training in this area are limited, and training cannot completely close down this attack vector.

According to the principle that detection and visibility is key, the ability to spot potential cybersecurity incidents within the target companies' own networks is seen as crucial for preventing phishing attacks. Users must be able not only to recognise attempted phishing, but also to identify, record and assess the damage caused by successful attacks, including account details being leaked, unauthorised access to VPN services, data loss, etc.

Ransomware

The rise of working from home has led to remote access solutions being rolled out more widely than ever before. However, this has also increased the number of potential target points for ransomware attacks. Lack of network segmentation is still a major problem in this respect. As soon as the ransomware finds a gateway, it can spread through the network and beyond, before establishing itself in multiple locations. This means attackers can access the system at any time via a range of entry points, allowing them to steal or encrypt data. Reactions to such attacks are often piecemeal, since the pressure to deal with the immediate problem leaves little time for thorough analysis. Having a comprehensive, company-wide cyber strategy in place can massively reduce the likelihood of and damage caused by successful attacks, especially if the strategy is complemented by well-drilled processes and a high level of cybersecurity awareness. This is one reason for the increasing importance of zero-trust environments.

The survey respondents cited lack of backups and business continuity strategies as the biggest single mistake companies make when dealing with ransomware threats.

CEO fraud/Business e-mail compromise (BEC)/fake invoice attacks/SCAM

These attack vectors are becoming increasingly insidious and precisely targeted, and BEC attacks are usually carried out in combination with other simultaneous attacks. However, awareness of this type of threat is perceived to be on the rise.

Botnets/C2

Without ongoing security monitoring, active bots can lurk undetected for months at a time. Outdated operating systems (legacy systems) are still in widespread use and provide the most common gateway for bots and their operators.

Data theft

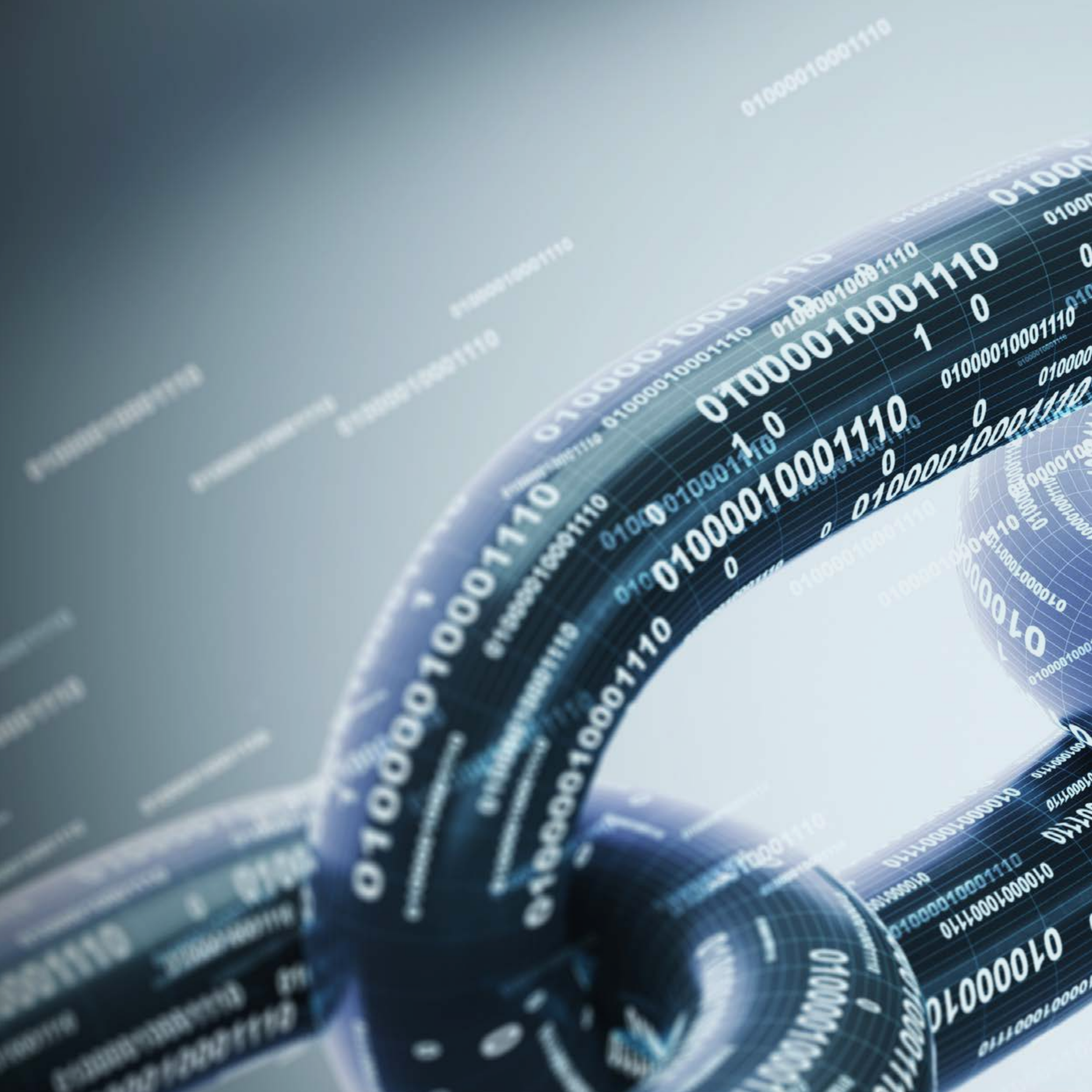
In the course of this reporting period, data theft often occurred in combination with ransomware attacks. Data theft remains a constant threat, and it should be assumed that a large number of data thefts go unreported.

Targeted attacks/APTs

The total number of targeted attacks registered by respondents to the survey is still rising, but remains relatively low. However, APT attacks are always associated with disproportionately high levels of damage.

DDoS attacks

The most effective defence against DDoS attacks is at telecoms provider level. This is where DDoS defence mechanisms should be concentrated. Where the content of a web service allows, contact delivery networks (CDNs) can provide protection against DDoS attacks and/or confine them to specific regions.


0100001000111 0
010000100011110
0100001000111 0
0100001000010

1.3 Cybercrime situation

1.3.1 Competent investigating authorities

The Austrian police authorities responsible for dealing with cybercrime in its narrowest sense, as well as for digital forensics and securing data, operate at three different levels. At national level, responsibility lies with the Cyber Crime Competence Centre (C4), which is based in Department 5 of the Criminal Intelligence Service Austria (Bundeskriminalamt). Specialist cybercrime and forensics units are also established within each of Austria's nine state police forces, operating as part of their local Criminal Police Offices (Landeskriminalämter). Finally, at district level, specially trained, uniformed police staff (known as Bezirks-IT-Ermittler or District IT Investigators) work with first responders to provide the necessary support in the event of an incident.

1.3.2 Activities

The C4, which is embedded in the Federal Ministry of the Interior, is constantly working to strength cooperation on fighting cybercrime, both at European and international level. Its primary interlocutors in this regard are Europol's European Cybercrime Centre (EC3) and INTERPOL's Digital Crime Centre (IDCC). The C4 also works closely with its partners within the European Cybercrime Task Force (EUCTF), especially as far as Operational Actions (OAs) arising from Operational Action Plans (OAPs) and the multinational Joint Investigation Teams are concerned. It also plays an active role in the European Cybercrime Training and Education Group (ECTEG), the European Multidisciplinary Platform Against Criminal Threats (EMPACT) and the G7's 24/7 Network.

Austria is fighting cybercrime by cooperating with its partners in Europe and internationally

These relationships strengthen European and international cooperation in a range of areas and were key to the success of the unit known as SOKO Clavis, for example. Tracking international cybercrime groups, conducting investigations on the dark web and monitoring cryptocurrencies is only possible as part of an international alliance.

In January 2020, just before the pandemic took hold, Vienna played host to a major international conference on cryptocurrency as part of Austria's work with its international partners.

1.3.3 Phenomena observed over the past year

The number of attacks on computer systems and ICT networks supported by malicious software rose again at the beginning of 2020. The phenomenon of criminals gaining illegal access via reused e-mail addresses, online shopping accounts, payment service providers and social media was first observed in 2019 and remained very much in evidence during this reporting year.

The beginning of the new year was marked by a spate of attempts to blackmail companies by linking pornographic images of children with the contact details and likenesses of targeted individuals. Illegal access to online accounts using leaked data also increased.

The biggest cybercrime challenges observed over the reporting period included internet fraud (many such offences were linked to Covid-19), data leaks and DDoS attacks.

Internet fraud

Generally speaking, the number of reports of internet fraud and extortion over the internet has increased very sharply in recent years. Successfully prosecuting offenders is becoming increasingly difficult as a result of increasing division of labour (the rise of 'crime as a service') and stronger networks between criminal groups, particularly as far as ransomware attacks are concerned.

Electricity customers reported falling victim to phone scams where the perpetrators correctly quoted the customer's IBAN number, the amount of their last electricity bill and other genuine details.

The midpoint of the reporting year saw an increase in CEO fraud, while in the autumn, the cyber trading fraud/investment scam reared its head again, causing millions of euros worth of damage. In this particular scam, after an initial contact by telephone, through online advertising, on social media or by e-mail, victims were pressured into investing ever more money in the scam with promises of big profits (for example through forex trading, trading binary options or investing in cryptocurrencies).

Phishing attacks are a major attack vector

With regard to phishing e-mails and websites used during the reporting period, the FinanzOnline scam is worthy of particular mention. E-mails circulating with the false sender address “finanzOnline@bmf.gv.at” promised recipients tax rebates in excess of a thousand euros each. When they followed the link, they were taken to a phishing website, which asked them to enter their credit card details and various personal information.

In addition, all major banks operating in Austria were targeted by criminals phishing for internet banking data. Mobile TANs for online banking, stolen via Android applications, were among the data collected in these attacks. A number of phishing and malware-spreading campaigns circulated over the course of the reporting year, many of them connected to Anubis malware on Android. Users were only prompted to enter their data and download a “security app” when they visited the phishing page using their Android web browser.

Trading fraud and investment scams involving cryptocurrencies were much in evidence regardless of the Covid-19 pandemic. Again, victims were promised huge profits on investments in a variety of cryptocurrencies, including bitcoin.

In late summer 2020, a number of scams surfaced using SMS messages to phish for data. A number of spam message campaigns featuring a “delivery notification” and containing internet links were in circulation during this period. When users clicked on these links, they were asked to pay “postage fees” of € 1.50; the real purpose of the messages was to collect their credit card data on behalf of the scammers.

As in previous years, the pre-Christmas period saw a seasonal spike in the number of fake online shopping sites (fake shops and phishing shops) operated by criminal gangs. There were also numerous waves of sextortion messages and e-mails designed to phish for bank details.

From mid-November onwards, a large number of attempts were made to steal users' WhatsApp accounts and to use the stolen accounts to conduct further fraud.

Covid-19-related cybercrime

The first quarter of 2020 was marked by the onset of the pandemic. A sharp increase was observed in the number of fraudulent, ostensibly Covid-19 related, websites designed for phishing or spreading malware. This increase followed the registration of several thousand new domains.

The perpetrators of these scams demanded their victims pay them USD 4,000 in bitcoin. If they failed to do so, they were told their families would be infected with coronavirus.

Malspam, phishing messages and ransomware purporting to be from parcel delivery services were among the tricks used to tempt users into downloading malware by clicking links in messages. These messages referred to changes in delivery times as a result of the pandemic. Opening the link and/or file contained in the message caused malware (including AZORult, Emotet, Nanocore RAT and Trick-Bot) to be installed on the target's computer.

There was a massive increase in the number of offences reported, which can presumably be directly linked to pandemic-related lockdowns and social-distancing measures. However, the bald figures for reported incidents are probably not representative of reality.

Generally speaking, social-distancing measures led to an increase in scams, including romance and stranded traveller scams.

There was a notable increase in cybercrime associated with the sale of disinfectants and face masks, across both fake and legitimate online shopping platforms.

Data leaks

Around the midpoint of the year, cybercriminals shifted their focus from ransomware attacks to leaking data and then demanding a ransom for its return.

DDoS attacks in the banking and financial sectors

The number of intrusions into corporate computer networks increased during this period. Unknown perpetrators were repeatedly able to extract company data and extort ransoms for its return. If the victims refused to pay, their data was published on relevant websites. The accumulation of various data leaks also led to an increase in the number of reports of accounts with online service providers (OSPs) being accessed illegally. The access data for these accounts were usually exploited by the perpetrators for fraudulent purposes. Once this data is stolen, it can often be used to carry out follow-up offences years after the original crime.

DDoS attacks

From autumn onwards, several waves of DDoS attacks were reported in Austria and beyond, targeted primarily at banks, the financial sectors and ISPs. Some of these attacks were carried out by copycats, who used the names of well-known criminal groups (such as Fancy Bears and Lazarus) in messages extorting money from victims. The attacks had bandwidths of up to 100 Gbit/s. Only in rare cases were the extortion messages followed up with further attacks, but these follow-ups used significantly higher bandwidths.

1.4 Cyber and national defence

Events in 2020 showed that, quite apart from the Covid-19 pandemic, terrorism and cyberattacks also pose an increasing risk to Austria's sovereignty and national security. The cyberattacks seen in 2020 affected large, well-known companies as well as individuals and small and medium-sized enterprises (SMEs). Austria's public administration was also a major target for cybercrime. One of the core tasks of the Austrian Armed Forces (ÖBH) is to maintain Austria's security and sovereignty, including in crisis situations, and it prepares accordingly in order to fulfil its duties under the constitution.

This is one reason why the Federal Ministry of Defence (BMLV) and the Austrian Armed Forces are paying ever more attention to defending Austria in cyberspace. Their cybersecurity remits covers measures to protect information and communications technology (ICT) and taking all necessary action to fend off attacks against military ICT systems. They are also responsible for supporting Austria's critical infrastructure in the event of a major cyber defence incident. Given their importance to Austria's national security, the BMLV and the Armed Forces are tempting targets not just for criminals or "script kiddies", but also, and above all, for state actors. State-sponsored attacks can be launched at any time without warning, meaning that preparation and training are just as important for deployments in cyberspace as it is for any other military operation. With this in mind, highly trained experts are an essential part of Austria's ICT systems, a point proved by the BMLV and the Armed Forces following the attack on the BMEIA at the beginning of the year. The BMLV made a major contribution to Austria's successful cross-governmental response to the incident by providing cyber experts from the CIS and Cyber Security Centre, the Armed Forces Security Agency (AbwA) and the Strategic Intelligence Agency (HNaA).

Terrorism and cyberattacks pose an increasing security risk

2020 will be remembered as the year of the Covid-19 pandemic, and coronavirus had a massive impact on the BMLV and the Austrian Armed Forces. The BMLV and the Armed Forces combined to provide logistical and staffing support to Austria's Covid-19 testing and vaccination drives, as well as technical support in the form of hardware, software, and technical expertise.

Like many other businesses, the government also made more use of remote working during the pandemic, which meant it had to expand its own systems for providing secure, remote ICT access. The response from the BMLV and the Armed Forces demonstrated their ability to react to current challenges, including in crisis situations.

Another dangerous development that became ever more evident over the course of 2020 was the rise of targeted attempts to influence public opinion by disinformation campaigns. This trend came very much to the fore in the run-up to the presidential election and ahead of high-profile domestic and international negotiations, but it actually had a major effect on virtually every issue to garner significant media attention during the reporting year, including the debate on Covid-19. The BMLV and the Armed Forces are engaged in intensive monitoring of the domestic and international media with a view to recognising tensions in society and taking them into account as part of the national security picture.

Although the pandemic brought with it plenty of new experiences, as far as attacks on the BMLV's ICT infrastructure were concerned, the key trends remained broadly similar to those identified in previous years. This year saw even faster growth in the number of attempts to gain unauthorised access to BMLV systems, although they were all blocked by established security measures before they could do any damage. In addition to the usual "background noise" of automated attacks and scans, increased numbers of manual or combined attacks were also detected in 2020. Cyber experts from the BMLV and the Austrian Armed Forces discovered and prevented a large number of attempted DDoS and brute-force attacks, as well as frequent phishing attacks targeted against BMLV and Armed Forces personnel. Ransomware that encrypts data on infected computers presents a major cybersecurity threat, and that threat is growing steadily. If victims of ransomware attacks refuse to pay the ransom for their sensitive data, the perpetrators threaten to publish it. However, these trends are by no means confined to the BMLV and the Austrian Armed Forces. A varied body of studies and investigations into the potential repercussions of cyberattacks has shown they have the potential to cause ever more damage and represent an ever-increasing risk. Different studies come up with different estimates of the financial impact of ransomware attacks, but they measure it in trillions of US dollars.

Almost all studies agree that the threat from cybercrime and cyber espionage is growing substantially. With this mind, it is essential that the BMLV and the Armed Forces develop and deepen the expertise required to combat the threat posed to its own systems. Over the last few years, many countries around the world have started to develop cybersecurity skills at state, military and civilian level. For example, the UK has announced it is setting up a 250-strong "cyber regiment", tasked with waging cyber and information warfare.

In addition, we can also see there is a strong international trend towards greater use of AI. More and more countries are using this technology for both offensive and defensive cybersecurity operations, and to wage hybrid war; indeed, these capabilities have already been used on many occasions against other nations or private companies. The ongoing conflict between Israel and Iran, which is increasingly being fought out in cyberspace, is just one example. For instance, in the spring of 2020, suspected Iranian hackers attempted to manipulate Israel's water supply system. Shortly afterwards, attackers believed to be based in Israel crippled an Iranian port for several days. Neither side ever confirmed that these operations took place, but this is a striking example of the potential scale of targeted, state-sponsored cyberattacks. In light of incidents like these, the BMLV and the Armed Forces are continuing their efforts to increase and bolster the security of systems across government and the state sector.

2
International developments

Austria generally campaigns at international level for a free, open and secure internet and insists that all human rights must be upheld in the virtual world. In this respect, care must be taken to maintain an appropriate balance between the public interest in prosecuting offenders and respect for fundamental human rights, including the right to freedom of expression, freedom of information, and the right to a private life and privacy.

2.1 European Union (EU)

The increasing importance of cybersecurity issues was reflected in 2020 by the way the topic was addressed within a number of international organisations and multilateral forums. These discussions featured some controversial opinions.

Measures related to foreign and security policy fall within the remit of the Federal Ministry for European and International Affairs (BMEIA), while the Federal Chancellery (BKA) is responsible for coordinating on cybersecurity issues within the EU.

2.1.1 Horizontal Working Party on Cyber Issues

The Horizontal Working Party on Cyber Issues (known as 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 activity. It sets the cyber priorities and strategic objectives of the EU as part of a comprehensive political framework, and provides a horizontal platform for work to enable harmonisation and a uniform approach to cyber policy issues.

HWP Cyber focused its work on the European Centre of Excellence for Cybersecurity and the Council Conclusions on Cybersecurity of Networked Devices

The Council's working group works closely with other related working groups, as well as with the European Commission, the European External Action Service (EEAS), Europol, Eurojust, the European Union Agency for Fundamental Rights (FRA), the European Defence Agency (EDA) and the European Union Agency for Cybersecurity (ENISA).

HWP Cyber met a total of 40 times during 2020. As in 2019, its work was focused on negotiations regarding a proposed EU regulation that would set up the European Centre of Excellence for Cybersecurity in Industry, Technology and Research, along with the Network of National Coordination Centres. In July 2020, the Croatian Council Presidency succeeded in obtaining a new mandate that allowed trialogue negotiations with the European Parliament (EP) to resume. An informal agreement was finally reached with the EP in December 2020, under the German Council Presidency. For a more detailed discussion of the content of the proposed regulation, see chapter 2.1.9.

Cyber diplomacy in 2020 concentrated on the systematic implementation of the Cyber Diplomacy Toolbox, which has been designed as a framework to allow the EU to respond jointly to malicious cyber activity. 2020 saw the toolbox used for the first time to impose cyber-related sanctions, including freezing accounts and travel restrictions (see chapter 2.1.8).

HWP Cyber prepared the “Conclusions on the Cybersecurity of Connected Devices”, which were adopted by the Council on 2 December 2020. The advent of the “internet of things” (IoT) – connecting various consumer appliances and industrial devices directly to the internet – brings with it new risks for privacy, cybersecurity and the security of information. The conclusions are intended to make Europe’s IoT industry more secure and competitive by setting the highest of standards for defensive capabilities and security measures. Horizontal legislation is expected to be drafted on the basis of the conclusions in due course.

2.1.2 NIS Cooperation Group

The NIS Cooperation Group was set up under the NIS Directive. It is intended to support and facilitate strategic cooperation and exchange of information between EU member states. The Cooperation Group is made up of representatives of the member states, the European Commission and ENISA, and is chaired by the country that holds the rotating Council Presidency.

The NIS Cooperation Group’s activities are based on work programmes, each of which is valid for two years. The first work programme for the period 2018–2020 represented the first step in shaping the NIS Cooperation Group’s working methods, building trust among member states and delivering the most urgent results required under the NIS Directive. Since then, the NIS Cooperation Group has established itself as a significant forum and point of reference for discussing cybersecurity policy within the EU. The new work programme for the period 2020 to 2022 foresees a review of the work completed thus far and an assessment of its effects, and calls on the Cooperation Group to identify potential for improvement in the future. The aims of this process are to continue to facilitate the NIS Cooperation Group's work in implementing the NIS Directive, to further operationalise exchange of information, and to allow for a strategic debate on important policy documents relevant to cybersecurity in the EU, for example in connection with 5G, AI or the IoT.

The NIS Cooperation Group held five plenary meetings in 2020, as well as 33 workstream meetings covering individual areas of its work.

2020 also saw the NIS Cooperation Group draft and publish the following reference documents, in which its work on the cybersecurity of 5G networks was a central theme:

- CG Publication 01/2020 – Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures;
- CG Publication 02/2020 – Report on Member States' progress in implementing the EU Toolbox on 5G Cybersecurity;
- CG Publication 03/2020 – Annual Report NIS Directive Incidents 2019;
- CG Publication 04/2020 – Synergies in Cybersecurity Incident Reporting.

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) emerged from the Friends of Presidency Group in 2019. The group aims to provide an overview of issues related to hybrid threats and thus to support coherence and cooperation between the EU and individual member states. Its work is focused on combating hybrid threats, making individual states and societies more resilient against those threats, improving strategic communication and fighting disinformation.

On 15 December 2020, the Council adopted the "Conclusions on strengthening resilience and countering hybrid threats, including disinformation, in the context of the COVID-19 pandemic". The conclusions were prepared by the HWP ERCHT, and the Council noted that malicious cyber activity often formed a key element of hybrid threats. It also recognised that consistently applying the EU's cyber diplomacy tools will be important when it comes to protecting against, preventing, deterring and reacting to such threats, as well when countering hybrid campaigns.

2.1.4 EU Cybersecurity Strategy for the Digital Decade

On 16 December 2020, the European Commission presented a new package of cybersecurity measures, including the EU's new cybersecurity strategy. The strategy was published in the form of a joint communication by the Commission and the EU High Representative and was designed to replace the 2013 cybersecurity strategy with a new strategic framework for cybersecurity issues across the EU.[1]

A new cybersecurity package will replace the 2013 cybersecurity strategy

[1] JOIN(2020) 18 final.

The communication aims to make Europeans safer in the digital world and notes that secure, reliable digital tools are crucial for the economy, democracy and society as a whole. With this in mind, the following specific proposals have been made:

- Improve the resilience of critical infrastructure and items connected to networks.
- Develop and expand operational capabilities with a view to preventing, deterring and reacting to cyberattacks.
- Work together with international partners for a global, open, stable and secure cyberspace in which international law, human rights, basic freedoms and democratic values are respected.

A number of specific initiatives in connection with these proposals were pursued in 2020, specifically:

- NIS: Work started on revising the NIS Directive on the basis of the Commission's proposal of 16 December 2020. The new NIS Directive (known as NIS 2) aims to ensure a uniformly high level of cybersecurity across the EU. For a detailed description of its content, see chapter 2.1.5.
- IoT: The EU plans to present legislation in late 2021 that will build on the Conclusions on the Cybersecurity of Networked Devices, published on 2 December 2020. The legislation will aim to establish a mandatory minimum level of IT security for all devices connected to the internet.
- 5G: Measures to implement the 5G toolbox should be finalised by the end of the second quarter of 2021. The annex to the joint communication also lists a number of additional measures and targets in this regard, including securing convergent national approaches in order to reduce risk across the EU, supporting continuous capacity-building efforts and the exchange of expertise, and strengthening the resilience of the supply chain and other strategic EU security targets.

- Cybersecurity within EU institutions: Proposals were drafted for an information security directive and common cybersecurity rules to apply to all EU institutions, facilities and agencies.

The Commission and the High Representative are determined to implement the new cybersecurity strategy in the next few months of 2021. It is now down to the European Parliament and the Council to scrutinise and approve the proposed NIS 2 Directive and the proposed directive on the resilience of critical infrastructure, which was published alongside the NIS 2 Directive on 16 December 2020 as part of the new cybersecurity package. As soon as the proposals have been approved and formally adopted, the member states will have 18 months in which to implement them.

2.1.5 NIS 2 Directive

NIS 2 directive will further improve cybersecurity within the EU

The European Commission presented its cybersecurity package on 16 December 2020. In addition to a new EU cybersecurity strategy, the package included a number of other proposals, including one for a new directive regarding measures designed to ensure a uniformly high level of cybersecurity throughout the European Union (the NIS 2 Directive, also referred to simply as “NIS 2”). NIS 2 is intended to replace and substantially improve the previous directive, which dates from 2016, while continuing to pursue the same fundamental objectives. The specific aims behind the new directive are to improve cybersecurity capabilities within the EU, facilitate closer cooperation between member states, and make public and private-sector organisations more resilient against cyber threats. The directive is intended to increase the overall level of cybersecurity within the EU, specifically by adopting the following measures:

- Member states will be required to adopt national cybersecurity strategies and to nominate responsible authorities, central points of contact and the members of their respective Computer Security Incident Response Teams in Europe (CSIRTs).

- Companies should be made more resilient against cyberattacks across all relevant sectors of the economy. All public and private-sector organisations across the single market performing essential functions in the economy and society as a whole (referred to in NIS 2 as “essential and important services”) will be required to take appropriate cybersecurity measures, specifically by setting up a cybersecurity management system. They will also be required to report all IT security incidents and cyber threats.
- Sectors within the single market that are already covered by the current NIS Directive will be encouraged to take further action to make them more resilient. This aim is to be achieved by continuously aligning the de facto scope of application, security requirements and reporting requirements in relation to IT security incidents, as well as the rules governing supervision and enforcement at national level and the capabilities of the relevant authorities within individual member states.
- Both member states’ ability to produce joint situation reports and their collective capabilities in terms of preparing for and reacting to incidents should be strengthened by taking action to foster trust between the relevant authorities and improve information exchange. The new directive will also set out rules and procedures to be followed in the event of a wide-ranging cyberattack or crisis (i. e. cybersecurity crisis management procedures). NIS 2 will introduce an additional duty to set out a national framework for managing cybersecurity crises and will provide for the establishment of a European Cyber Crises Liaison Organisation Network [EU-CyCLONe]. This network has been designed to support coordinated efforts to deal with large-scale cybersecurity incidents and crises and to ensure regular exchanges of information between member states and EU bodies.

NIS 2 is being dealt with within the European Parliament's Committee on Industry, Research and Energy (ITRE) and in the European Council's Horizontal Working Party on Cyber Issues (see chapter 2.1.1). It is expected that the NIS 2 directive will be transposed into national law within 18 months of its entry into force.

2.1.6 EU Cybersecurity Certification Framework (Cybersecurity Act)

The Cybersecurity Act, which came into force back in 2019, introduced a number of new measures, including a European certification framework for cybersecurity. This framework sets out a mechanism by which Europe-wide cybersecurity certification schemes can be created. In the future, this European cybersecurity certification framework is intended to be used as evidence that ICT products, services and processes assessed under the framework are in compliance with the framework's security requirements. Providers and operators will be able to opt in to cybersecurity certification for ICT products, services and processes on a voluntary basis, and cybersecurity certificates issued under the framework will be recognised across the EU. By demonstrating that a given product fulfils certain security-related functions or complies with set security requirements, cybersecurity certification has the potential to significantly increase trust in ICT products, services and processes, thus ensuring that the digital single market functions as it should.

The European Cybersecurity Certification Group (ECCG) was established by the Cybersecurity Act and began work in 2019. It is made up of representatives of national cybersecurity certification authorities or other relevant national authorities. Austria is represented in the ECCG by its national CIO (the Federal Ministry of Digital and Economic Affairs – BMDW) and its Strategic NIS Office (the BKA). The ECCG held six plenary sessions in 2020 and at least four additional sub-group meetings.

2020 also saw the Stakeholders Cybersecurity Certification Group begin its work (SCCG). This group is chaired jointly by the European Commission and ENISA and is made up of representatives of academic institutions, consumer organisations, conformity assessment bodies, companies, trade associations and other bodies, including standardisation authorities. The role of the SCCG is to provide advice on strategic issues related to cybersecurity certification.

EUCC will regulate the security of cloud services

The European Commission asked ENISA to draw up a system for cybersecurity certification back in 2019. This system is known as the European Union Common Criteria Scheme (EUCC) and is intended as the successor to the current Senior Officials Group Information Systems Security (SOG-IS) and Mutual Recognition Agreement (MRA). The EUCC provides for cybersecurity certification for ICT products. The EUCC is based on the Common Criteria and the Common Methodology for Information Technology Security Evaluation and the corresponding standards, specifically ISO/IEC 15408 and ISO/IEC 18045. The official consultation on the draft EUCC took place in July 2020, marking a significant milestone in the development of the European cybersecurity certification framework.

Having drafted the EUCC, on 21 November 2019 ENISA was commissioned to draw up an additional framework for cybersecurity certification, known as the European Union Cybersecurity Certification Scheme on Cloud Services (EUCS), with a view to regulating the security of cloud services. The overall objective is to harmonise security standards for cloud services with EU regulations, international standards, industry best practice and existing certification regimes in EU member states. A draft of the EUCS was presented for public consultation in December 2020, another milestone for cybersecurity in Europe. The EUCS provides for a horizontal, technology-based programme that will ensure a high level of cybersecurity at every stage of the cloud supply chain and provide a solid foundation for sector-specific cybersecurity schemes. It is envisaged that the programme will be applicable to all types of cloud services (ranging from infrastructure right through to applications) and include transparency requirements on issues such as where data is stored and processed.

2.1.7 Cybersecurity for 5G networks

The security of fifth-generation mobile technology (more commonly known as “5G”) was again a major focus for cybersecurity authorities in 2020.

Following the completion of a range of preparatory work in 2019, including drafting a national risk analysis for Austria, reviewing existing national security measures and taking part in a coordinated EU-wide risk analysis, work on and around the issue of 5G cybersecurity continued right from the beginning of 2020.

For example, the report entitled “Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures” (hereinafter referred to as the “Toolbox”) was published on 29 January 2020. The Toolbox identifies and posits various “risks” (which were previously identified as part of the EU-wide risk analysis in 2019), “mitigating measures” (which are subdivided into strategic and technical measures) and “supporting actions” available to member states in their efforts to make their networks more secure.

Member states were given until 15 May 2020 to implement the proposals included in the Toolbox.

The ordinance that implemented these proposals in Austria was the Telekom-Netzsicherheitsverordnung 2020 (Telecom Network Security Ordinance 2020, known by its German acronym TK-NSiV2020). It was issued by Austrian regulator Rundfunk und Telekom Regulierungs-GmbH (RTR) and entered into force on 4 July 2020 following a consultation period. This regulation applied all the technical measures set out in the Toolbox.

On 24 July 2020, the “Report on Member States’ progress in implementing the EU Toolbox on 5G Cybersecurity” was published. It took stock of the progress member states had made in implementing the 5G Toolbox and the difficulties that had become apparent during this process. The report features four examples of the way Austria implemented the requirements in RTR’s TK NSiV, as described above.

In 2020, a sub-work stream was formed from the existing NIS Cooperation Group on 5G cybersecurity recommendations. Although preparations to establish the group had begun back in 2019, it was not until 25 May 2020 that the sub-group actually met for the first time. The "Sub-Group on 5G Standardisation and Certification Policy" began its work by collecting and categorising existing standards and went on to use them to draw up a certification framework in accordance with the Cyber Security Act. There were four meetings of this working group in 2020, all of which were held virtually.

In addition to activities under the auspices of NIS Cooperation Group, the second Prague 5G Security Conference was held virtually on 23 and 24 September 2020. Delegates at the conference were introduced to the "Prague repository", a database containing national best practice and legislation on network security from every country contributing to the scheme.

5G Toolbox to be implemented by the second quarter of 2021

Work to update Austria's national risk analysis for the telecoms sector was completed in November of the reporting year. The update was carried out in a public-private partnership in a series of primarily virtual meetings, organised by RTR.

As described above, 5G is also one of the ongoing projects included in the EU's "Cybersecurity Strategy for the Digital Decade", which was published on 16 December 2020. Implementation of the 5G toolbox at national level is expected to have been completed by the second quarter of 2021, along with a number of other measures. The strategy also lists a number of additional measures and objectives; implementing these measures and achieving the objectives will require a significant effort by member states over the course of 2021.

2.1.8 Cyber diplomacy

Significant steps were taken over the course of 2020 with a view to implementing the EU's Cyber Diplomacy Toolbox, which is designed to act as a framework for a joint EU diplomatic response to malicious cyber activity. In May 2019, the Council adopted a sanctions regime that allowed it to impose sanctions against individuals and entities (but not states) by freezing their bank accounts and applying travel restrictions. 2020 saw sanctions imposed for the first time, with eight individuals and four entities being listed. Some of the measures included in the Cyber Diplomacy Toolbox can be imposed without the malicious behaviour in question being firmly attributed to a specific perpetrator. A number of the options available to the EU when responding to cyberattacks are exercised publicly, such as Council conclusions and declarations. For example, in February 2020, the EU issued a declaration regarding major cyberattacks against essential infrastructure in Georgia. This was followed by a separate declaration in April 2020 on cyberattacks aiming to exploit the Covid-19 pandemic.

Cyber Diplomacy Toolbox: key steps towards implementation completed in 2020

A large proportion of cyber diplomacy activity at EU level depends on agreeing EU-wide positions and strategies on cyber issues and applying them internationally. These positions and strategies are particularly key for working with the United Nations (UN). Two standard-setting exercises have been running at UN level since 2019, and 2020 marked the beginning of preparations for drafting a UN convention on cybercrime (for further details, see section 2.2 on the United Nations). The new EU Cybersecurity Strategy of 16 December 2020 is heavily focused on the concept of digital sovereignty, which is itself embedded in the European Commission's work programme as an objective. For the first time, cyber diplomacy has been assigned a key role in the geopolitical posture adopted by the European Commission and the EU's External Action Service, which reflects the fact that setting standards for new technologies and in cyberspace has long been a source of geopolitical conflict. Moreover, the exponential rise in attacks against EU bodies by state-sponsored actors has increased polarisation within the international community on cybersecurity-related issues. The EU's vision of a global, open internet is incorporated into the EU's ambition to play a leading role on cybersecurity at both regional and international level, thus ensuring that new technology focuses on individuals and protecting their privacy and that it is used both legally and ethically.

2.1.9 Network of National Coordination Centres and European Competence Centre

On 12 September 2018, the European Commission presented a draft regulation on setting up a European Cyber Security Centre of Excellence, creating a network of national coordination centres and establishing a cybersecurity competence community[2]. This proposal constituted concrete action to implement the joint communication entitled "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", which was released jointly by the European Commission and the High Representative for Foreign Affairs in September 2017.

The network of national coordination centres and the European Cybersecurity Industrial, Technology and Research Competence Centre have been designed to support existing EU initiatives and to develop new European cyber capabilities.

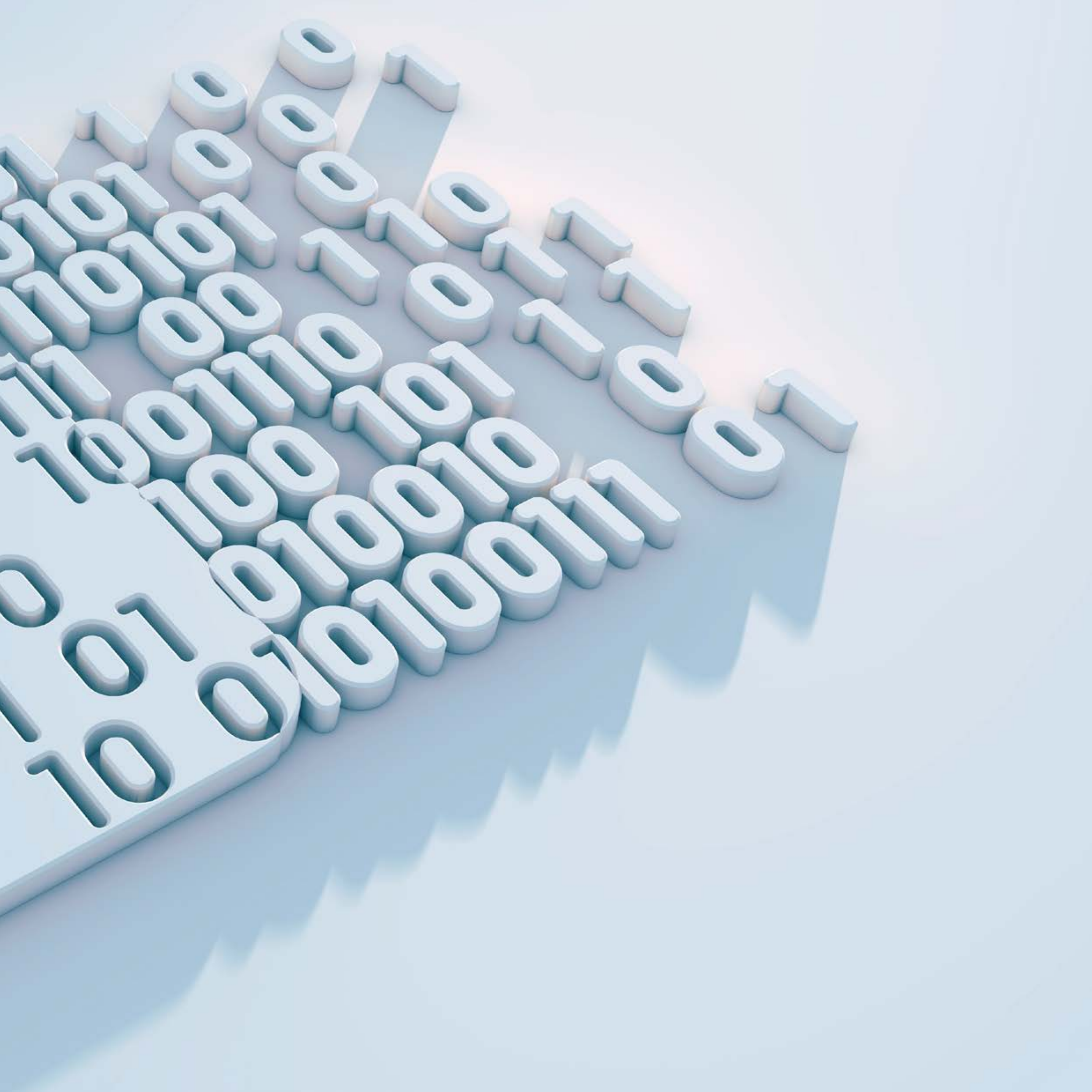
The way funds earmarked for cybersecurity between 2021 and 2027 are used in practice will be coordinated with the European Competence Centre as part of the Digital Europe and Horizon Europe programmes. The European Competence Centre will support the competence community and the network of national coordination centres, as well as driving research and innovation in cybersecurity. It will also arrange joint investments by the EU, its member states and industry. The European Competence Centre will be based in Bucharest.

[2] COM (2018) 630

Each EU member state will be asked to nominate a national coordination centre to represent it in the network of national coordination centres. Each national centre will work to encourage the development of new cybersecurity capabilities and skills, while the network will look to identify and support the most important cybersecurity projects taking place within member states.

At the same time, the competence community will create a large, open and varied group of cybersecurity stakeholders. This group will be composed of scientific experts and representatives from across the private and public sectors, including civilian and military authorities.

For an update on the negotiations, see chapter 2.1.1.



2.2 United Nations (UN)

Cybersecurity was first discussed at the United Nations within the First Committee (Disarmament and International Security) during the UN General Assembly (UNGA) of 1998. UNGA has devoted more time and focus to the issue in the years since. States discuss cybersecurity within this UN framework with a view to minimising the risks to international security resulting from the use of cyberspace. Negotiations thus far have succeeded in defining four priority action areas, all of which are particularly important in terms of establishing and enforcing a framework of international standards for cyberspace. The four areas are:

- international law;
- non-binding standards of responsible behaviour by states;
- confidence-building measures (CBMs); and
- capacity-building.

The cybersecurity-related bodies established by General Assembly resolutions back in 2018 continued to deliberate in the course of 2020, as did two parallel but nominally independent cybersecurity mechanisms: the Open-Ended Working Group (OEWG), which is open to all UN member states, and the Group of Governmental Experts (GGE), which brings together experts from 25 countries. However, the Covid-19 pandemic caused some delays and postponements. Austria played an active part in discussions via the OEWG, at the same time as passively monitoring the proceedings of the GGE, of which Austria is not a member.

The OEWG had been due to complete its work in 2020, but this date had to be pushed back to 2021 due to the coronavirus. This decision provided some additional time for further discussions, which was used to hold a range of informal consultations designed to lay the groundwork for negotiating and potentially approving a final report in March 2021.

In the autumn, while mandated discussions over plans to embed cybersecurity further at institutional level within the UN were continuing in the OEWG, Russian and China tabled a draft resolution to set up another OEWG to carry on the work completed by the original OEWG, with the support of several other UNGA member states. Despite Austria, all EU member states and other like-minded countries being united in their opposition to the proposal, the motion was adopted, meaning that a new OEWG will begin work in 2021 as soon as the existing OEWG is wound down. The mandate for the new OEWG runs until 2025. It remains to be seen how this new OEWG will respond to the proposal to establish an Action Plan on cybersecurity, an initiative that has the support of 50 countries including Austria.

While there have been some agreements on individual issues surrounding areas like capacity-building and what confidence-building measures ought to look like, major differences of opinion remain within the international community, particularly regarding the extent to which international law should be applicable to cyberspace.

UNIDIR Conference on the Future of UN Cybersecurity Processes

The importance of international cybersecurity is also reflected in the UN Secretary-General's disarmament agenda, which was launched in 2018. In the associated implementation plan, two areas for action are dedicated to cybersecurity. One of them is focused on resolving conflicts peacefully, while the other calls for developing standards in cyberspace to be strengthened. Over the course of 2020, nations continued to make progress towards implementing the changes required to achieve these aims.

The work to implement the disarmament agenda is supported by the United Nations Office for Disarmament Affairs (UNODA), as are the activities of the GGE and the OEWG. The United Nations Institute for Disarmament Research (UNIDIR) contributes to the international debate on cybersecurity by publishing scientific studies, as well as by hosting an annual conference on cyber-stability. 2020's conference was devoted to discussing the future of UN cybersecurity mechanisms.

2020 also marked the first time the issue of cybersecurity was discussed in detail within the UN Security Council. The debate arose as part of a series of events held under Estonian chairmanship in May 2020.

The High-level Panel on Digital Cooperation (HLPDC) was convened in 2018 and tasked with drawing up recommendations to strengthen cooperation between governments, the private sector, civil society, international organisations, the scientific community, technical experts and other relevant stakeholders in the digital world. It produced its first report last year. Also in 2020, UN Secretary-General António Guterres introduced a new selection process for nominating a "Tech Envoy", a post intended to promote the issue of cybersecurity at institutional level. We will need to wait until 2021 to see how much influence the Tech Envoy will have and how they manage to embed their priorities within the UN system.

Cybersecurity was also a major theme of the 15th Internet Governance Forum (IGF), which was held in November 2020. The need to ensure secure access to the internet during the Covid-19 pandemic was one of the key topics under discussion at the event. Delegates identified a lack of trust from governments, the private sector and individuals in technology and the companies providing it as a particularly critical issue. This led them to call for digital policies that took account of the uncertainties of the internet.

The International Telecommunications Union (ITU) is working at the UN in Geneva to draw up guidelines for the use of its Global Cybersecurity Agenda (GCA), which aims to bolster trust and certainty in the information society. Some Western countries have been very critical of the GCA. The recommendation included in the draft guidelines that legally binding regulations to resolve global cybersecurity issues should be drawn up by the ITU has proved controversial among member states and is likely to remain so.

Cybercrime has quickly developed into a global and extremely profitable form of criminal activity. The UN Office on Drugs and Crime (UNODC) in Vienna remains an indispensable part of the global machinery for fighting cybercrime. Assistance for affected member states is provided on the basis on a comprehensive study published in 2013[3] and is concentrated in the following three areas:

- Improving the way cybercrime is investigated, prosecuted and judged, particularly as regards sexual exploitation and child abuse.
- Promoting an integrated, cross-governmental approach to cybercrime, including national coordination, data collection and effective legal frameworks to deter cybercrime and combat it effectively over the long term.
- Strengthening cooperation between governments, prosecuting authorities and the private sector at both national and international level, as well as boosting public awareness.

At the operational level, UNODC's cybercrime department is delivering new initiatives for use in school and university education systems. UNODC has shown an interest in using the comic book Der Online-Zoo (The Online Zoo) as part of these initiatives. The book is published by Internet Service Providers Austria and is already being used in Austrian schools.

The Intergovernmental Expert Group (IEG) on cybercrime was set up in 2010 and held its sixth meeting in 2020, when it sat virtually for the first time. The IEG was unable to resolve the issue of whether the existing Budapest Convention should be expanded to cover cybercrime or whether a new cyber convention would have to be negotiated. In the end, delegates decided to continue the IEG's deliberations on fundamental issues

[3] http://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf

and developments relating to cybercrime and to discuss national legislative frameworks, examples of best practice, technical assistance and international cooperation.[4]

Cybercrime was also a central theme of the 29th meeting of UNODC's Commission on Crime Prevention and Criminal Justice (CCPCJ), held in spring 2020. Together with Canada and Colombia, Austria presented a resolution on cybercrime, which the Commission adopted by general consensus.

In addition to the discussions on cybersecurity in the First Committee of the UN General Assembly, cybercrime has also been discussed at the Security Council, with Russia having first raised the issue back in 2018. It had been proposed that the UN Secretary-General present a report on the cybercrime situation on the basis of General Assembly resolution A/RES/73/187. Along with the rest of the EU and other like-minded Western countries, Austria opposed this resolution, noting that cybercrime was dealt with within the UN as part of the Intergovernmental Expert Group (IEG). However, Russia insisted on taking the discussion on cybercrime into the General Assembly and on starting negotiations on a new UN convention to combat cybercrime. EU member states continue to view any attempt to negotiate instruments of this nature – which are governed by international law – in the absence of international consensus, without making thorough preparations, and without taking into account existing instruments (such as the Budapest Convention) as problematic.

At the 74th session of the UN General Assembly, delegates voted to adopt resolution A/RES/74/247, which provided for the establishment of an ad hoc committee (AHC) to draft the new convention. Again, EU member states and other like-minded countries opposed the resolution, pointing out that it duplicated existing UN mechanisms (such as the IEG on cybercrime). Austria led the negotiations on Resolution A/RES/74/247

[4] CCPCJ Res 26/4 (https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_26/CCCPJ_Res_Dec/CCPCJ-RES-26-4.pdf)

on behalf of the EU. The key issues at stake in this negotiation were, and are, Austria's foreign policy objectives in this area. They are: the desire to root the new negotiation process in Vienna by strengthening the role of UNODC's head office, establishing a consensual approach to the conduct of negotiations, and mandating a transparent, inclusive negotiation process in which non-governmental organisations are also involved.

At the 41st session of the UN Human Rights Council, held in June 2019, Austria was among the main sponsors (together with South Korea, Brazil, Denmark, Morocco and Singapore) of a resolution on "New and emerging digital technologies and human rights" (A/HRC/Res/41/11). The resolution was adopted by consensus. The Advisory Committee of the Human Rights Council was commissioned to prepare a study on digital technologies and their repercussions for human rights, with a view to opening up a broad debate on the challenges and potential benefits the rapid development of digital technologies (and particularly of AI) might bring from a human rights standpoint. The report was published in January 2021, and the main sponsors of the original resolution plan to submit another one to the Human Rights Council in June 2021.

The resolution on the safety of journalists (A/HRC/RES/45/18), which Austria also introduced during the 45th session of the UN Human Rights Council in September 2020, was the first to condemn deliberately and completely shutting down the internet as a violation of human rights standards.

2.3 NATO

As a military and political alliance with a strong focus on security and common defence, NATO has been dealing with the defence-related aspects of cybersecurity since it adopted its current strategic concept in 2010. It recognised cyberspace as a distinct domain for defence purposes in 2016, and space was given similar recognition in 2019. As a NATO partner country, Austria cooperates closely with the Alliance. At a technical level, Austria takes part in meetings of the NATO-C3 (Consultation, Command and Control) Board, as well as discussions on relevant smart-defence projects. In 2020, this cooperation focused on preventing cyberattacks and warning of Covid-19 disinformation, among other issues.

The Austrian Federal Ministry of Defence (BMLV) has posted an officer to NATO's Co-operative Cyber Defence Center of Excellence (CCDCoe) in Tallinn since 2013. The aim of Austria's collaboration with NATO is to improve cyber defence capabilities. Austrian government departments are making extensive use of the range of courses NATO offers in this area, as well as the opportunities our relationship with NATO provides to compare Austria's capabilities against those of other countries in NATO exercises. In addition, Austria also posts a member of staff from the Federal Ministry of Defence to the European Centre of Excellence for Countering Hybrid Threats in Helsinki, an organisation 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) plays a dual role in international cybersecurity policy. On the one hand, it encourages the implementation of decisions passed at UN level. This support is particularly evident in the capacity-building work it facilitates via its executive structures, and specifically through its Secretariat, which is based in Vienna, and its wider network of field missions. On the other hand, the OSCE has emerged as a pioneer when it comes to developing confidence-building measures (CBMs) in cyberspace. The approval of the 16 CBMs designed by the OSCE represents the most ambitious global attempt yet to strengthen international cooperation on cybersecurity. The measures are intended to minimise the tensions that can arise between OSCE member states on the use of cyberspace by encouraging exchange of information, establishing communication channels and improving capacity. The OSCE's work also focused on upholding and strengthening human rights in cyberspace.

The informal working group on cyber (Cyber IWG) is primarily responsible for the continued design and implementation of confidence-building measures (CBMs). The work of Cyber IWG is informed by the OSCE's underlying definition of security, and the OSCE's approach to cyber issues takes political, military, economic and human-rights aspects into account. In 2020, the Cyber IWG continued its work as part of the "Adopt a CBM" initiative, through which states or groups of states drive forward the implementation of confidence-building measures. Important steps in this regard include the establishment of a network of points of contact, regular checks of communication channels, and preparations for effective cooperation in the event of a cyber crisis. Along with Belgium and Estonia, Austria has committed itself to driving implementation of CBM 14 on public-private-partnerships.

In addition to Cyber IWG's work on cybersecurity at an institutional level, successive OSCE chairs have also put the issue on the agenda for their respective terms. This has in turn established a precedent that OSCE chairpersons-in-office hold regular cybersecurity conferences; 2020's conference was held virtually as a result of the pandemic. Participants in the conference examined the joint work of all significant stakeholders, including states, international organisations, private companies and individuals, in securing a stable cyber environment. The meeting also provided an opportunity for discussions on the role of private stakeholders and gender equality in the cyber industry.

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 operating under the umbrella of the Organisation for Economic Co-operation and Development (OECD)'s "Committee on Digital Economy Policy". The working party aims to draw up evidence-based directives for digital security, as well as practical guidelines designed to build confidence in the digital transformation and support the resilience, continuity and security of critical activity. It is primarily focused on managing digital security risks with the potential to threaten economic and social activities, and on making digital products and services more secure. To this end, it draws on expertise from OECD members and partner countries, businesses, civil society and the technical internet community. The WPSDE meets in Paris twice a year and organises workshops and conferences. Within the Austrian government, coordination with this working group is the responsibility of the Federal Chancellery (BKA).

In 2020, the group's focus was on improving the security of smart products and addressing vulnerabilities. It outlined a number of overarching principles and recommendations for political action, building on previous case studies and a comprehensive analysis of the value chain and lifecycle for smart products. The second report aims to raise awareness among policymakers of the importance of a responsible approach to "vulnerability management", defined as detecting, managing and handling digital security vulnerabilities in products and information systems, and disclosing details of them in a coordinated fashion. Both strands of work represent important groundwork for a planned revision of the OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity, which dates back to 2015.

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

2.6 Council of Europe

The core of the Council of Europe's activities in the field of cybersecurity is the Convention on Cybercrime (also known as the Budapest Convention). The Convention was first adopted in 2001 and has proved significant well beyond the boundaries of Europe. Colombia ratified the Convention in 2020, the 65th country to do so. The Convention's primary purpose is to pursue a shared criminal justice policy to protect society from cybercrime and specifically to encourage the necessary statutory regulations and cooperation at international level.

Work to implement the Convention is supported by capacity-building projects, which are coordinated by the Cybercrime Programme Office of the Council of Europe (C-PROC) from its head office in Bucharest. The Council of Europe is also involved in various other projects, such as advising on relevant legislative measures and providing support for the training of judges and public prosecutors. It supports the "iProceeds 2" project in South-Eastern Europe, which focuses on the profits of cybercrime, the "Cyber South" project in North Africa, and "GLACY+", a global project delivered in cooperation with INTERPOL. Its latest project, known as "Cyber East", aims to improve the structures of the Eastern Partnership, and is funded by the EU's European Neighbourhood Instrument.

Negotiations are currently underway on a second additional protocol to the Budapest Convention that will deal with international legal assistance and the associated need to access data across borders. It is expected that the Council of Europe will work closely with the EU on the relevant documents, which are currently being drawn up.

"Guidance Notes" on the Budapest Convention have been drafted and published since 2012, with a view to facilitating the effective application and implementation of the Convention by its signatories. The last such note considered the issue of interference in elections.

The Council of Europe's "Octopus Conferences" serve as an important cybercrime platform for experts and organisations alike. The latest conference was held in 2019 and was dedicated to evidence in cyberspace and the ongoing discussions regarding the Second Additional Protocol to the Budapest Convention.

Other Council of Europe instruments include the Council of Europe Convention on Data Protection (ETS 108), which was updated in 2018, and the Lanzarote Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, which makes a major contribution to protecting children online.

2.7 Computer Security Incident Response Teams Network (CSIRTs Network)

In summer 2016, the European Parliament and the European Council adopted EU Directive 2016/1148 (the NIS Directive), which in turn established the CSIRTs Network (CNW) and its remit. The CSIRTs Network includes representatives of the CSIRTs of the member states (pursuant to Article 9 of the NIS Directive) and of CERT-EU. The European Commission (EC) participates in the CSIRTs Network as an observer, while ENISA manages its administration and actively supports cooperation between national CSIRTs. Austria's nominated participants in the CSIRTs network are GovCERT Austria, CERT.at and the Austrian Energy CERT (AEC).

The network operates primarily online, with most communication being done through a web portal, mailing lists and an instant messaging system. CNW meetings provide opportunities for exchanges of information on the services and activities of the CSIRTs and the potential for cooperation between them. Information is also exchanged voluntarily on significant security incidents, and attendees discuss insights into network and information security gained from exercises. The CNW's main tasks are to develop and strengthen trust between member states and promote rapid and effective operational collaboration between them, thus providing for a uniform high level of security in all the EU's networks and information systems.

Its first meeting in 2020 was held in February and took place face-to-face in Stockholm. The pandemic dictated that the other two (which had been scheduled to take place in Zagreb and Bonn respectively) had to be held as videoconferences. The European emergency exercise "Cyber Europe 2020", originally planned for June, also had to be cancelled. The exercise had been due to target the health sector, which could not spare the capacity at the same time as responding to the coronavirus pandemic. Instead, a "capture the flag" event was held in parallel to the latest CNW meeting, combining technical puzzles with a quiz on CNW joint working processes.

On 19 March 2020, with Covid-19 having reached pandemic proportions, CNW was put in "alert cooperation mode", producing weekly summaries of the cybersecurity situation within the EU in relation to the pandemic. As it transpired, networks had few problems coping with the transition to working from home and remote learning, there were hardly any significant attacks on the healthcare sector, and the network was not in a position to assist in tackling reports of Covid-related fraud. The CNW therefore resumed its normal operations on 6 May 2020.

As part of the European Commission's MeliCERT 2 project, the requirement for the CNW toolbox was reassessed in summer 2020, under the leadership of CERT.at. On 5 March 2020, the CSIRTs network submitted its official report (as required under the NIS Directive) to the Cooperation Group for the second time.

2.8 Other committees and forums

WTO eCommerce

E-commerce negotiations continued at the World Trade Organisation on the basis of the Joint Statement Initiative on eCommerce. The discussions covered a variety of topics, including the trade implications of cybersecurity issues.

Freedom Online Coalition

The Freedom Online Coalition is an informal grouping of states originally founded by the Netherlands in December 2011. Its members, including Austria, are committed to ensuring that human rights are respected online across the globe. At the 8th Freedom Online Conference, held in Accra, Ghana, between 5 and 7 February 2020, delegates adopted a declaration on the human rights impact of cybersecurity laws, practices and policies.

3 National actors

3.1 Cyber Security Centre (CSC)

Despite facing constant challenges, the CSC, which is based in the Austrian Ministry of Defence, managed to consolidate its position both in organisational terms and as far as the content of its work was concerned, as well as successfully expanding its staff.

Since the NIS Act came into force, the BMI has been charged with implementing it at operational level, while responsibility for strategic matters has remained with the BKA. In light of this division of labour, 2020 was marked by a number of measures designed to implement the technical and organisational procedures required for the BMI to carry out its new operational role as an authority under the NIS Act and the ordinance that codified this new role in law.

A number of measures were also taken to prevent cybercrime, including talks and events designed to raise awareness of the issue within government institutions and companies working in critical infrastructure.

In addition, CSC held regular ICT security training sessions for its own staff and other government departments.

3.2 Cyber Crime Competence Centre (C4)

3.2.1 Competent investigating authorities

The police authorities responsible for dealing with cybercrime, digital forensics and data security in Austria operate at three different levels. At national level, responsibility lies with the C4, which is based in Department 5 of the Criminal Intelligence Service Austria (Bundeskriminalamt). Specialist cybercrime and forensics units have been established within each of Austria's nine federal state police forces, operating as part of their local Criminal Police Offices (Landeskriminalämter). At district level, specially trained, uniformed police staff (known as Bezirks-IT-Ermittler or District IT Investigators) work with first responders to provide the necessary support in the event of an incident.

3.2.2 Activities

International cooperation on cybercrime:

The C4, which is embedded in the Federal Ministry of the Interior, is constantly working to strength cooperation on fighting cybercrime, both at European and international level. Its primary interlocutors in this regard are Europol's European Cybercrime Centre (EC3) and INTERPOL's Digital Crime Centre (IDCC). The C4 also works closely with its partners within the European Cybercrime Task Force (EUCTF), especially as far as Operational Actions (OAs) arising from Operational Action Plans (OAPs) and the multinational Joint Investigation Teams are concerned. It also plays an active role in the European Cybercrime Training and Education Group (ECTEG), the European Multidisciplinary Platform Against Criminal Threats (EMPACT) and the G7's 24/7 Network, as well as helping to organise the annual New Technology Conference attended by Austrian, German and Swiss representatives.

These relationships and initiatives strengthen cooperation within Europe in various different areas, including on combating ransomware, as well as contributing to the success of the unit formerly known as SOKO Clavis, and a number of international cybercrime investigations. They also help to develop specialist experience on the dark web, cryptocurrencies, vehicle forensics and training.

3.3 CIS and Cyber Security Centre (CISCSC)

The CIS and Cyber Security Centre is part of the Austrian Joint Service Support Command (Kommando Streitkräftebasis). It serves as the Austrian Armed Forces' centre of excellence for information and communication technology, cyber defence and military geoscience. The CIS and Cyber Security Centre has a total of 12 offices across seven of Austria's federal states, covering information and communications technology, cyber defence, electronic warfare and military geoscience for combat deployments, exercises and peacetime operations.

One of its core tasks is to provide interoperable, secure and innovative services and ICT for use in Austria and abroad, and to enable effective administration. Its role means that the CIS and Cyber Security Centre is constantly confronted with cyber, information-related and hybrid threats, and needs to be able to react to threats during deployments and in the course of normal operations. In doing so, the CIS and Cyber Security Centre secures the ability of the Austria Armed Forces to lead in the cyber domain and helps it to maintain information superiority.

3.3.1 Military Cyber-Centre (MilCyZ)

The Military Cyber-Centre (MilCyZ) is part of the CIS and Cyber Security Centre, and is the division of the Austrian Armed Forces charged with acting against threats and attacks from cyberspace against its military ICT systems and networks. The MilCyZ is responsible for planning and delivering the complete cybersecurity systems and components required to protect its own systems, as well as for defending the Austrian Armed Forces in the event of a cyberattack. These systems are constantly being developed and adapted to take account of the latest threats. When MilCyZ expertise is combined with observations, assessments and work to identify vulnerabilities in the Austrian Armed Forces' current technology, ICT systems and components, the result is a complete picture of Austria's military cybersecurity position. In order to monitor all the military's ICT systems and ensure they are secure enough to be deployed within the Austrian Armed Forces, systems and components are audited to identify design flaws and structural weaknesses in technology, products, components and systems.

In order to ensure the military systems are protected, the MilCyZ must cover every aspect of cybersecurity consistently and in detail. This task is reflected in the MilCyZ's remit and tasking. Its duties include:

- selecting, introducing and operating ICT security components (e. g. firewalls, endpoint protection, antivirus systems, etc.);
- reporting on the overall military cybersecurity position and adapting the content and presentation of this reporting as appropriate to meet the needs of its customers;
- forensics and malware analysis;
- auditing the Austrian military's ICT systems and networks;
- information and cyber risk management;
- protecting information and military ICT systems via a central Security Operations Centre (SOC);
- providing rapid response teams to protect Austria's military infrastructure.

3.3.2 Military Computer Emergency Readiness Team (milCERT)

The Austrian Armed Forces' milCERT is located within the MilCyZ. It is essential to ensure that sufficiently technical and human resources are available to identify, contain and fend off cyberattacks and to detect preparations for attacks before they can be carried out in the first place. The ability to grasp and represent the current cybersecurity situation is a crucial component of that capability. In order to obtain the most accurate and up-to-date information on cybersecurity incidents and the latest insights, milCERT is in constant dialogue with its partners at national and international level. It coordinates the response in the event of an IT security incident and provides advance warning of security vulnerabilities.

3.3.3 Electronic warfare

As part of Austria’s defence against cyberattacks, MilCyZ is also responsible for providing services in the field of electronic warfare. In doing so, it lays the technical groundwork that allows it to protect its own systems and defend external systems attack. The aim of its work in this area is to gain and maintain superiority in combat, to fulfil its duties as part of national and international alliances, and to increase the survivability of Austria forces in the field.

3.4 Austrian Armed Forces Security Agency (AbwA)

The work carried out by the Austrian Armed Forces in cyberspace is referred to under the umbrella term “cyber defence.” The Austrian Armed Forces Security Agency contributes to this work by providing its expertise and intelligence accesses. It produces situation reports on cyberspace drawing together information from across government and from intelligence sources, and analyses it to provide a basis for assessing appropriate measures to counter cyber threats. This work is combined with other activities to provide a permanently high level of security for military ICT infrastructure.

3.5 Austrian Strategic Intelligence Agency (HNaA)

As Austria’s strategic foreign intelligence service, the Austrian Strategic Intelligence Agency (HNaA) is tasked with obtaining information on activity outside Austria, analysing it, and providing intelligence products to the highest levels of Austria’s political and military leadership. This also means monitoring events and developments of intelligence interest in cyberspace, which constitute part of the overall intelligence picture. By identifying cyber threats, the HNaA makes a major contribution to decision-making on cyber-defence measures and whether threats can be attributed to specific actors.

3.6 GovCERT, CERT.at and Austrian Energy CERT

Under the provisions of Austria's NIS Act, GovCERT Austria responds to computer emergencies within the public administration and is part of IKDOK. Its strategic operations are based within the BKA and its operational services are provided as part of a public-private partnership with CERT.at. GovCERT functions as Austria's point of contact for public administration networks and is in close dialogue with various international organisations and interlocutors, including the European GovCERT Group and the Central European Cybersecurity Platform (CECSP).

CERT.at has been acting as Austria's national computer emergency team since March 2019, in accordance with the NIS Act. CERT.at sees itself as a point of contact for all ICT incidents in Austria with a security dimension. It is renowned as a reliable and widely recognised information hub for Austrian organisations and companies in the cybersecurity sector.

The Austrian Energy CERT (AEC) is an industry-specific Computer Emergency Response Team (CERT) for the Austrian energy industry. In 2020 it was accredited as the sector-specific computer emergency team for the energy sector under the NIS Act. The main tasks of the AEC are geared towards strengthening IT security expertise within the energy sector and making it more resilient against cyberattacks. In addition to managing security incidents, the AEC is also responsible for handling day-to-day queries and security reports, providing training sessions, taking part in international cybersecurity exercises and helping to draft technical security plans for the electricity and gas sectors. The AEC also acts as the single point of contact in the event of security incidents affecting the energy sector at home and abroad, ensuring rapid communication and coordinating the work of IT security experts and authorities within the energy industry.

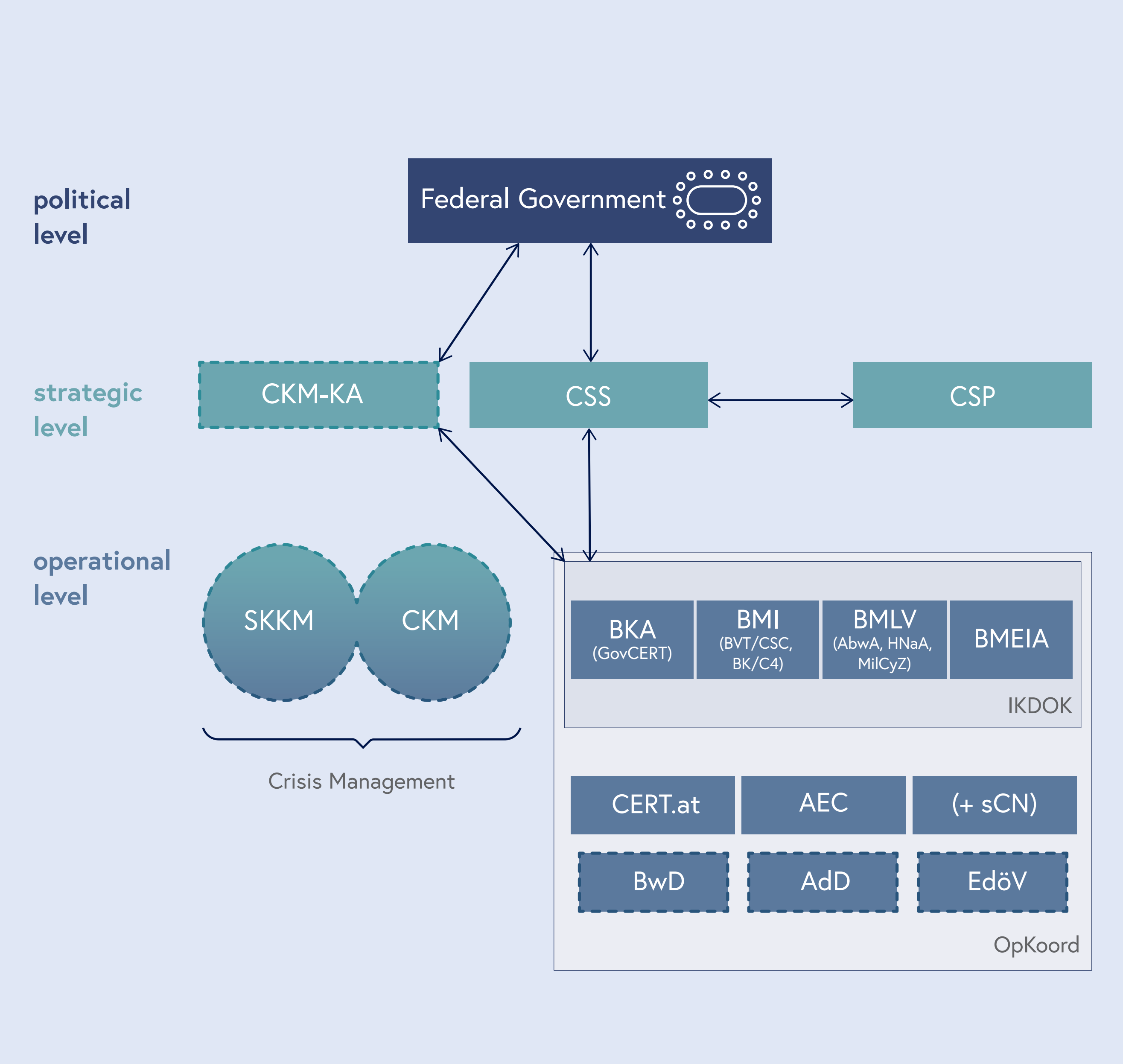
The three CERTs work together to exercise their responsibilities under Section 14 of the NIS Act, thus meeting the requirements set out in the European Directive on the Security of Network and Information Systems (NIS) and the recommendations of the European Union Agency for Network and Information Security (ENISA) for increasing IT security in critical infrastructure. They also represent Austria within the EU's CSIRTs Network. All three CERTs work primarily on security threats and incidents, either under agreements with relevant bodies or on the basis of their own research. All three also carry out work to prevent cybersecurity incidents, including early detection of potential threats and raising public awareness, as well as providing advice and support as required and requested. The remits of the CERTs were codified when the NIS Directive was transposed into Austrian law as the NIS Act (NIS-Gesetz). Among other provisions, the law places operators of essential services and digital service providers under an obligation to report serious security incidents. These mandatory reports are sent by affected parties to defined, sector-specific recipients (sector-specific computer emergency teams) and then forwarded to the BMI and/or the CSC, which is part of the BVT. The same procedure also applies to voluntary reporting, with the exception that voluntary reports can be anonymised by the sector-specific CERTs before they are forwarded to the CSC. Unless the reporting organisation is a member of IKDOK in its own right, incident reports from organisations within the public administration are sent to GovCERT, which forwards them on as appropriate. GovCERT can issue early warnings, alerts, recommendations for action and notifications. It also provides general technical support as part of the initial response to security incidents, analyses risks, incidents and security vulnerabilities, and assesses the overall cybersecurity situation. To enable GovCERT to fulfil its role as a report's authority, the NIS Act provides for an industry or sector-specific CERT to be set up for each of the sectors covered by the Act. Where specific sectors do not yet have CERTs of their own, the duties normally assigned to the computer emergency team and the reporting authority are carried out by CERT.at.

3.7 Office for Strategic Network and Information System Security

The Office for Strategic Network and Information System Security, often referred to as the “Strategic NIS Office” is based in the BKA. It was able to continue its work in 2020 with considerable success, despite the difficult circumstances engendered by the Covid-19 pandemic. For example, the AEC was officially certified and authorised as the first suitable sector-specific computer emergency team to be established under the NIS Act, marking an important milestone. Substantial progress was also made towards identifying the operators of essential services on the basis of the NIS Act. The NIS Office was also involved in a wide range of other activities in 2020, particularly as part of its work representing Austria within the NIS Cooperation Group and other strategic EU and global bodies dealing with the security of network and information systems. The NIS Office has been working closely with a variety of interlocutors, including with the relevant authorities and regulators on issues relating to the security of 5G networks, and actively took steps to provide relevant information to the public throughout 2020. The English translations of the NIS Act and the accompanying NIS Ordinance, which can be found on nis.gv.at, are worthy of particular mention in this regard. The NIS Office also worked together with the BMI to publish the third edition of NIS Fact Sheet 8/2018 (“Mapping-Tabelle von IKT-Sicherheitsstandards und Cyber Security Best Practices”) on the NIS website, as well as the second edition of NIS Fact Sheet 7/2019 (“Qualifizierte Stellen”).

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
GovCERT	Government Computer Emergency Response Team Austria
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


political level
Federal Government
strategic level
CKM-KA
CSS
CSP
operational level
SKKM
CKM
Crisis Management
BKA (GovCERT)
BMI (BVT/CSC, BK/C4)
BMLV (AbwA, HNaA, MilCyZ)
BMEIA
IKDOK
CERT.at
AEC
(+ sCN)
BwD
AdD
EdöV
OpKoord

4
National structures

4.1 Inner Circle of the Operative Coordination Structure (IKDOK)

The NIS Act came into force on 29 December 2018. The Act transposed the EU's NIS Directive in relation to cybersecurity into Austrian law, as well as providing an essential foundation for inter-ministerial cooperation on the issue within the Austrian government. One immediate result of the advent of the NIS Act was the creation of a permanent structure for cooperation at operational level (known as Op-Coord). This body incorporates an inter-ministerial structure for operational cooperation on network and information systems security, known as the Inner Circle of the Operative Cooperation Structure (IKDOK). While the Op-Coord itself is primarily tasked with assessing the overall security situation, taking account of voluntary and mandatory incident reports, the IKDOK is responsible for recording and assessing the overall risk, incident and security incident picture and for providing support to the Cyber Crisis Management Committee's Coordination Committee (CKM).

In the event of a crisis, the IKDOK assumes the role of a direct interface with the government-wide CKM, supported by the Op-Coord. In terms of the mechanisms and processes to be applied in such a crisis, the CKM will be guided by the tried and tested procedures used by Austria's Crisis and Disaster Management Agency (SKKM). The IKDOK and the CKM had their mettle tested at the beginning of this reporting period when a government institution was attacked (for full details, see section 1.1.1 above). They succeeded in fending off the attack before any permanent damage could be done and went on to coordinate and carry out a purge of the affected network.

The IKDOK is composed of representatives of the BMI (CSC, C4), the BMLV (AbwA, HNaA, CIS and Cyber Security Centre), the BKA (GovCERT) and the BMEIA. The IKDOK is chaired by the CSC and the Cyber Defence Centre. The IKDOK produces a monthly IKDOK and an Op-Coord situation picture, which is made available to the respective target group.

4.2 CERT Verbund Austria

CERT VERBUND AUSTRIA

The CERT Verbund Austria was founded in 2011 to bring together all the Austrian CERTs operating at the time across government and the private sector. It is intended to pool the available resources in order to exploit shared expertise as effectively as possible. Participation in CERT Verbund Austria is voluntary. All members of the group, which is jointly led by its members and operates on the basis of cooperation between them, commit to taking part in regular exchanges of information and experience, helping to identify and provide core expertise, and supporting CERTs across all sectors of the economy.

One of the differences between a ‘traditional’ IT security team and a CERT is that readiness to communicate and work with third parties is an essential requirement for a CERT. Part of a CERT’s role is to act as an interface with outside stakeholders, network, and work together with other teams. At international level, CERTs are organised within FIRST (Forum of Incident Response and Security Teams), while in Europe they fall under the TF-CSIRT and EU CSIRTs networks.

The main focus of CERT Verbund Austria’s work is to improve cooperation between the different Austrian CERTs, alongside promoting CERT activity within Austria. The reason for this emphasis on cooperation is that a comprehensive network of CERTs is recognised as one of the most effective tools for securing networked information and communications systems, as confirmed by the steady growth in the number of CERTs, CSIRTs, Security Operations Centres (SOCs) and cyber defence teams within Austrian companies and the close partnerships that have been forged between them.

The procedures introduced in 2019 proved themselves to be fundamentally effective during the coronavirus pandemic of 2020 and required only minor improvements. CERT Verbund Austria’s first meeting of 2020 was held in person, but all other meetings were moved online due to Covid-19.

Since the organisation was set up, its membership has grown to 16 teams and it has held 44 separate meetings. Its members are also in constant dialogue via secure communication channels.

Cyber Sicherheit
Plattform

4.3 Cyber Security Platform (CSP)

The CSP is a central platform for dialogue and cooperation between businesses, science and the public administration. It fosters the exchange of experience and information on cybersecurity, with a particular focus on the security of critical infrastructure. The CSP also advises and supports the Cyber Security Steering Group (CSS) on strategic cybersecurity issues. Since it was set up in 2015, the platform has established itself as a model of its kind, and numerous cybersecurity initiatives have been launched under its umbrella. The results of the platform's work play an important role in shaping Austrian national cybersecurity policy.

2020 saw the staging of the CSP's 10th workshop. The event focused on the implementation of the NIS Act, developments within the EU (including the review of the NIS Directive) and cyber diplomacy, and delegates also provided reporting on the current cybersecurity situation.

4.4 Austrian Trust Circle (ATC)

The Austrian Trust Circle (ATC) is a national initiative designed to facilitate exchange of information on cybersecurity and related incidents at a technical level. Its work is targeted at all sectors of Austria's strategic infrastructure, as well as the public administration. The ATC was founded in 2011 by CERT.at with the support of the Federal Chancellery. It consists of a series of sector-specific security information exchanges and is aimed at companies and organisation running Austria's critical infrastructure and relevant government authorities. CERT.at and the AEC, in cooperation with GovCERT Austria and the BKA respectively, provide a formal framework for exchanging practical information and joint working across the security sector.

The ATC's primary objectives are:

- to create a basis of trust allowing joint action in the event of a major incident;
- facilitating networking and exchange of information within and between sectors involved in critical infrastructure, as well as with the government;
- exchanging contacts between CERTs and participating companies organisations and authorities;
- helping sectors involved in critical infrastructure to help themselves on IT security;
- establishing operational contacts with the CERTs, for example
  - regarding reporting and handling;
  - security incidents within organisations;
  - establishing contacts with BKA experts in the event of a crisis.

Regular meetings within the individual sectors were sporadic in 2020 as a result of the coronavirus pandemic, but dialogue between sectors and the government is encouraged through a two-day annual conference. ATC activity was limited in 2020 as a result of the coronavirus pandemic.

4.5 ICT security portal

The ICT security portal at onlinesicherheit.gv.at is an inter-ministerial initiative launched in cooperation with Austrian business. It is a central internet portal for issues related to security in the digital world. The portal is a strategic measure, set up as part of Austria's national ICT security strategy and the cybersecurity strategy (ÖCSC). It aims to create and strengthen a culture of cybersecurity in Austria over the long term by raising awareness of related issues among its target audience and providing them with tailored recommendations for action.

The range of information and services available via the portal is continuously expanding, and regular editorial meetings are held with the 40 organisations involved in the project, including federal ministries, the governments of Austria's federal states, state authorities, universities, technical colleges, research institutes, companies, associations and representative bodies. It provides access to the latest reports and warnings, important information and advice for cybersecurity beginners and experts alike.

Over the course of 2020 the ICT Security Portal published 133 news articles, as well as details of 43 publications and 70 events. In addition, a number of contributions are published on a selected topic each month. In 2020, these topics included IT security and private WiFi networks (April) and Austria's contributions to European Cybersecurity Month" (ECSM) in October, and inspired a total of 44 specialist articles. There is also a dedicated section on the portal for information related to the coronavirus pandemic, which will continue to be updated as the situation develops. Pieces published in this section so far have covered topics ranging from IT security when working from home to details of the latest cyber-fraud scams.

The ICT Security Portal was also restructured in October 2020, improving usability and making it the first specialist website to reflect the federal government's new cooperate identity.

ICT Security Portal user statistics for 2019/2020
Figures correct as of 31 December2020):

Visits in 2019

~249,000

(+20% compared to 2018)

Visits in 2020

~323,000

(+30% compared to 2019)

Visits per day (peaks, Mon–Thu)

Av. 900/day

Visits per day during the "Covid peak" (mid-March to mid-May)

Av. 1,300/day

5
Cyber exercises

As a result of the coronavirus pandemic, almost all national and international exercises planned for 2020 were cancelled to protect the health of the participants. The BMLV/Austrian Armed Forces took part in just two exercises all year.

Crossed Swords 2020

As every year, Crossed Swords 2020 was organised and run by NATO's Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE).

The purpose of the exercise was to get penetration testers, forensic experts and special operations working together in a single team to meet the objectives and technical challenges set for them in a virtual cyber environment. The Austrian Armed Forces again sent a delegation to take part in the exercise with a view to improving their expertise in penetration testing – a key skill for detecting attacks against their own IT systems. The opportunity to exchange experiences with specialists from other countries was also particularly appreciated.

5.1 Common Roof

As in previous years, this exercise saw representatives from Austria, Germany and Switzerland come together to construct a joint, multinational mission network and defend it against cyber threats. Alongside standardised (or still-to-be-standardised) ICT management processes, the event also focused on ICT security procedures and the ICT services involved in implementing them. The network components of the multinational network were monitored and controlled by a multinational Networks Operation Cell (NOC). The exercise strengthened ties with Germany and Switzerland, and operational systems were tested successfully.

Exercises are crucial for increasing resilience across the government and state bodies

6
Summary/outlook

6.1 The BMEIA incident and its consequences across government

The attack on the Federal Ministry for European and International Affairs' computer networks at the beginning of 2020 was the largest and most extensive attack to date on an Austrian government ministry. It saw the cross-governmental crisis mechanisms provided for under the Network and Information System Security Act called into action for the first time (for full details, see section 1.1.3). All the bodies and operational structures involved in the incident acted in a highly professional and efficient manner, and they were able to bring the situation under control quickly. At the same time, the processes set out in the Network and Information System Security Act and the Austria's Cybersecurity Strategy largely proved both targeted and effective.

In the course of investigations following the attack, the Federal Chancellery coordinated work on a lessons learned document, which aimed both to identify measures to increase cybersecurity across the board (and particularly within the federal government) and to make the Austrian government as a whole more resilient against cyberattacks. The measures identified as part of this process were subsequently adopted for implementation following a joint decision by the ministries' General Secretaries. They also provide a foundation on which minimum standards for cybersecurity can be set and implemented.

The first concrete action taken in this regard was to strengthen Government Computer Emergency Response Team Austria by placing it under a new, improved contract and ensuring it is available 24 hours a day, seven days a week, 365 days a year. Steps have also been taken to appoint Chief Security Officers within government ministries and other government bodies, thus ensuring that standardised structures are in place across government departments in the event of a crisis.

Ministries across government perceive dealing with cybersecurity issues as an ongoing process. The experience gained in dealing with the incident is proving useful as we make continual adjustments to Austria's security structures and processes. These adjustments are founded upon a risk-based approach and are gradually making the Austria's government machinery more and more secure.

Republic of Austria

Cybersecurity