# Bericht Cybersicherheit 2020

# Bericht Cybersicherheit 2020

Wien, 2020

Bundeskanzleramt

Bundesministerium
Inneres

Bundesministerium
Landesverteidigung

Bundesministerium
Europäische und internationale
Angelegenheiten

**Impressum**

Medieninhaber, Verleger und Herausgeber:
Bundeskanzleramt
Ballhausplatz 2, 1010 Wien
bundeskanzleramt.gv.at
Fotonachweis: iStock
Layout: BKA Design & Grafik
Druck: XXX
Wien, September 2020

## Inhalt

# Einleitung

Die Österreichische Strategie für Cybersicherheit (ÖSCS) legt fest, dass durch die Cyber Sicherheit Steuerungsgruppe (CSS) ein jährlicher Bericht zur Cybersicherheit in Österreich erstellt wird. Der letzte Bericht wurde im Mai 2019 vorgelegt.

Der aktuelle Bericht Cybersicherheit 2020 baut auf den Inhalten des letztjährigen Berichtes auf und ergänzt diesen um aktuelle Entwicklungen mit Schwerpunkte in den Bereichen internationale und operationelle Entwicklungen. Beobachtungszeitraum ist das Jahr 2019, einzelne aktuelle Entwicklungen im Jahr 2020 haben Eingang gefunden.

Zielsetzung des Berichtes ist eine zusammenfassende Darstellung der Cyberbedrohungen und wesentlicher nationaler und internationaler Entwicklungen. Grundlage dazu sind ressortspezifische Berichte zur Thematik.

# 1
# Cyberlage / Bedrohung

Die zunehmende Durchdringung nahezu aller Bereiche der Gesellschaft und des täglichen Lebens mit digitaler Technologie bietet erhebliche Chancen und Möglichkeiten. Gleichzeitig wird die Gesellschaft dadurch aber auch angreifbarer und abhängiger von der Vertraulichkeit, Verfügbarkeit und Integrität von digital verarbeiteten und gespeicherten Informationen, mit anderen Worten: Von der Sicherheit im Cyberraum. Staaten, Gruppierungen, aber auch kriminellen Akteuren eröffnen sich immer neue Wege, die digitale Vernetzung für Spionage, Sabotage oder andere kriminelle Aktivitäten nutzbar zu machen. Dabei können schon die Fähigkeiten einzelner krimineller Individuen genügen, um Cyberangriffe mit im Vorfeld nicht abschätzbaren Folgen für die Sicherheit Österreichs durchzuführen.

## 1.1 Lage Cybersicherheit – operative Ebene

Der Berichtszeitraum 2019 zeigte eine weitere Zunahme von monetär oder staatlich-strategisch motivierten Angriffen. Darunter fielen vor allem solche mittels Ransomware, mit einer steigenden Tendenz zu spezialisierten Ransomware-Angriffen (Targeted Ransomware). Weiterhin kam es zu einer Steigerung der Anzahl von Fällen des Datendiebstahls mittels Advanced Persistent Threats (APTs). Deren Auftreten und Bewältigung wird im Allgemeinen öffentlich mit größter Zurückhaltung kommuniziert. Die Attribuierung[1] ist schwierig sowie potentiell fehleranfällig und wird daher oftmals nicht kommuniziert. Im Bereich von DDoS-Angriffen kam es im Berichtszeitraum ebenfalls zu einer leichten Zunahme.

Zunahme von monetär oder staatlich-strategisch motivierten Angriffen

Darüber hinaus wurden Fälle von CEO-Fraud bekannt. Ihre Effektivität blieb weitgehend begrenzt – trotz konstant hohem Angriffsvolumen waren nur die wenigsten Angriffe erfolgreich. Dies ist auf eine erhöhte Sensibilisierung der Endnutzer bei Behörden und Unternehmen zurückzuführen.

Risiken für Unternehmen mit Abhängigkeiten von Cloud-Infrastrukturen und digitalen Lieferketten steigen. So ist mit vermehrten Angriffen auf Unternehmensdaten in der Cloud auch in nächster Zukunft zu rechnen.

Durch mögliche Kompromittierungen der Supply-Chain, also der bösartigen Fälschung vermeintlich sicherheitsfördernder Software-Updates, sind insbesondere auch mittelständische Unternehmen einer zunehmenden Gefährdung ausgesetzt.

1 Zuordnung oder Zurechnung

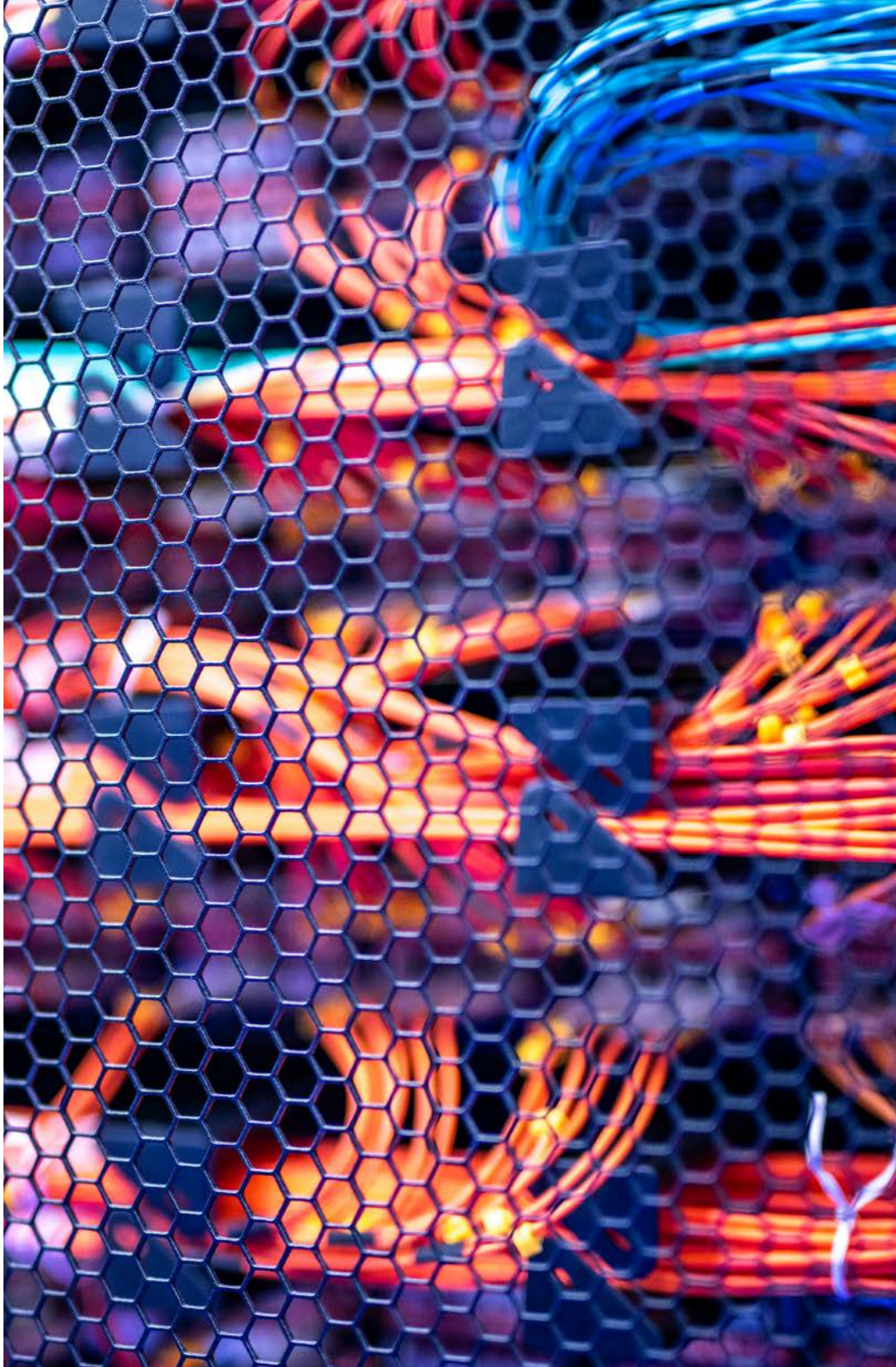
**In enger Zusammenarbeit konnten im ‚Inneren Kreis der operativen Koordinierungsstruktur' (IKDOK) neben reaktiven Maßnahmen zum Schutz und zur Stärkung der Resilienz vermehrt Früherkennungsmechanismen zur Anwendung gebracht werden.**

Bedrohungen durch mögliche Wahlmanipulationen nahmen im Berichtszeitraum eine besondere Stellung ein, darunter die Europawahlen 2019 und die Nationalratswahl 2019. Zum Schutz der Widerstandsfähigkeit des demokratischen Systems durch freie, faire und sichere Wahlen wurden von Seiten der Sicherheitsbehörden verschiedene Maßnahmen getroffen:

- eine Risikoanalyse des Wahlprozesses mit betroffenen Stakeholdern,
- die zielgerichtete Minimierung organisatorischer und technischer Risiken,
- die Durchführungen von Awareness-Schulungen zum Thema Cybersicherheit bei Bundes- und Landeswahlbehörden sowie
- der Vorortdienst des Cyber Security Centers (CSC) bei Wahlbehörden an Wahltagen.

In enger Zusammenarbeit konnten im „Inneren Kreis der operativen Koordinierungsstruktur“ (IKDOK) neben reaktiven Maßnahmen zum Schutz und zur Stärkung der Resilienz vermehrt Früherkennungsmechanismen zur Anwendung gebracht werden.

Auf Ebene der Europäischen Union (EU) ist der Cybersecurity Act mit 27. Juni 2019 (unter anderem mit EU-weit geltendem europäischen Zertifizierungsrahmen für die Cybersicherheit von Produkten, Verfahren und Diensten) in Kraft getreten. Mit der Cyberdiplomacy Toolbox wurde eine einheitliche Vorgehensweise für die Attribuierung von Cyberangriffen ausgearbeitet. Darüber hinaus ist die Etablierung eines europäischen Netzwerks nationaler Kompetenzzentren (NCCC) angedacht.



### 1.1.1 EMOTET

Im Jahr 2019 konnte eine massive Zunahme bei der Verbreitung der Schadsoftware EMOTET festgestellt werden. Diese Malware kann auf bestehende E-Mail-Konversationen zugreifen und authentisch wirkende „maßgeschneiderte" E-Mails als Antworten auf eingelangte Korrespondenz verschicken. Ab dem vierten Quartal setzte eine zusätzliche Verschärfung ein, als cyberkriminelle Täter versuchten, die mittlerweile auf EMOTET besser abgestimmten Maßnahmen (Antivirensoftware und generelle Policies) auf den Zielsystemen zu umgehen. Man setzte hierbei weniger auf den klassischen Ansatz, das Opfer durch Öffnen infizierter E-Mail-Anhänge den Schadcode aktivieren zu lassen, sondern verleitete zum Anklicken eines direkt im erhaltenen E-Mail-Text platzierten Links. Solche Links sahen legitimen Adressen täuschend ähnlich, waren aber bösartiger Natur und führten das Opfer zu einem Server, von dem aus EMOTET den Angriff automatisch startete. Die solcherart kompromittierten Systeme verursachten eine weitere Spam-Welle und damit zusätzliche hohe Infektionszahlen. In Österreich waren zahlreiche Unternehmen unterschiedlicher Größe, darunter Betreiber kritischer Infrastrukturen und verfassungsmäßige Einrichtungen betroffen.

### 1.1.2 Ransomware

Einhergehend mit der EMOTET-Welle kam es zu zahlreichen „erfolgreichen" Ransomware-Angriffen mit teilweise erheblicher Schadenswirkung. Darunter waren nicht nur solche, die auf Breite und Masse hin abzielen und ohne spezifische Vorauswahl und Aufklärungsmaßnahmen von Seiten der Angreifer unternommen wurden. Vielmehr wurden auch Ransomware-Angriffe beobachtet, die eine gezielte Opferauswahl vornahmen und die eine Einschleusung von Schadcodes in Zielsysteme mittels „maßgeschneidertem" Spear-Phishing zum Ziel hatten. Dies geschah unter anderem mittels Ryuk, einem der prominentesten Vertreter von Targeted Ransomware, die auch Betreiber kritischer Infrastrukturen und öffentliche Institutionen befällt und die über EMOTET verteilt wird. Die Höhe der anschließenden Geldforderung richtete sich dabei nach der wirtschaftlichen Potenz der jeweiligen Opfer, deren Hintergrund zuvor von Täterseite entsprechend ausgeforscht worden war. Insgesamt hat die Gefahr der missbräuchlichen Verwendung von sensiblen Unternehmensinformationen für Angriffe mittels Social Engineering-Techniken

(z. B. Spear-Phishing) zugenommen. Gründe dafür sind unter anderem die bestehenden Offenlegungspflichten für Unternehmen, bisweilen überschießende Informationspolitik der Unternehmen selbst oder aber auch (unintendierte) Indiskretionen von Mitarbeiterinnen und Mitarbeitern in Sozialen Medien.

### 1.1.3 DDoS (ÖBB, Gemeinde Wien)

Im Jahr 2019 waren die ÖBB und die Gemeinde Wien verstärkt DDoS-Agriffen ausgesetzt. Da Bekennerschreiben und auch monetäre Forderungen an die Opfer ausblieben, liegen zu konkreten Motiven keine Erkenntnisse vor. Betroffen waren unter anderem Teile der ÖBB Online-Verkaufsinfrastruktur sowie das Wahlkartenamt der Gemeinde Wien vor den Wahlen zum EU-Parlament im Mai 2019. Rechtzeitig getroffene Gegenmaßnahmen auf Zielseite trugen entscheidend zur Eindämmung der DDoS-Angriffe bei, sodass Totalausfälle wichtiger Dienste vermieden werden konnten.

### 1.1.4 EU-Wahl

Bereits im vorvergangenen Jahr hatte sich die NIS-Kooperationsgruppe der Thematik angenommen und dazu mit Juli 2018 ein „Compendium on Cyber Security of Election Technology“ veröffentlicht.[2] Die Bundesbehörden legten sowohl im Vorfeld zur EU-Wahl Ende Mai 2019 als auch während ihres Verlaufs ein besonderes Augenmerk auf den korrekten und ungestörten Ablauf sowie die Aufrechterhaltung der Cybersicherheit. Dies geschah durch entsprechende Sensibilisierung der wahldurchführenden Organe einerseits, als auch durch ein Monitoring der verwendeten Cyberinfrastruktur andererseits. Eine eigens zum Zweck der Abwehr hybrider Bedrohungen eingesetzte Taskforce hatte zur Aufgabe, mögliche Beeinflussung durch ausländische staatliche Akteure zu erfassen und geeignete Gegenmaßnahmen im Bedarfsfall einzuleiten. Darüber hinaus wurde durch das Europäische Parlament (EP) in Brüssel zur Erhöhung der Awareness sowie zur Überprüfung von Prozessen eine Übung durchgeführt (siehe Kapitel 5.4 und 5.5).

---

2 https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

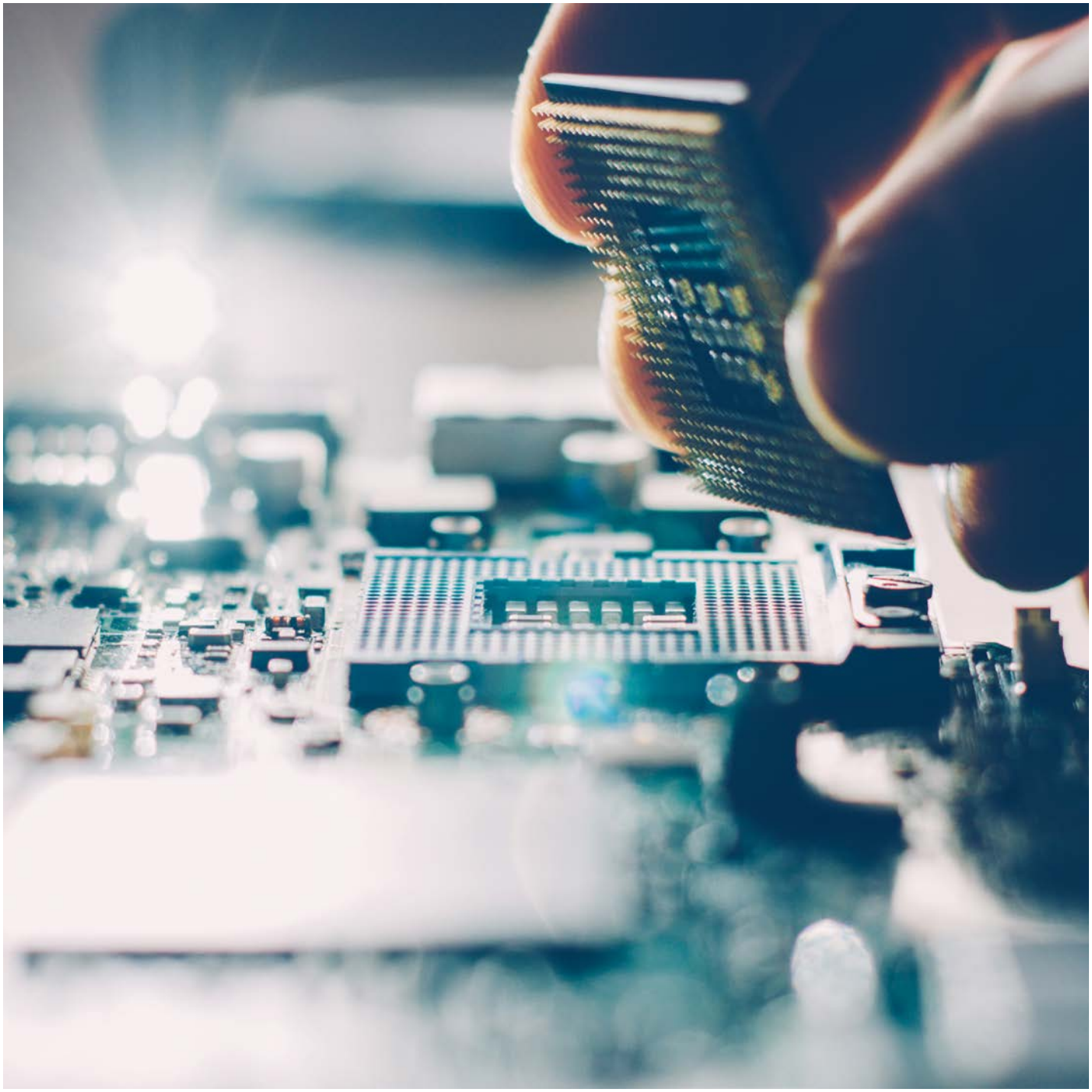
### 1.1.5 Schwachstellen (BLUEKEEP [RDP], Foreshadow, PDF-Signatur)

Im Berichtszeitraum wurden erneut zahlreiche Softwareschwachstellen erkannt. Von diesen sind speziell BLUEKEEP, Foreshadow und eine Validierungsschwäche bei elektronischen Signaturen zu erwähnen, da es sich hierbei um als kritisch einzustufende Schwachstellen handelt.

**BLUEKEEP** ist eine im Remote-Desktop-Protocol-Dienst (RDP) von Microsoft-Windows enthaltene Lücke, die einen Fernzugriff auf Computer mit Windows-Betriebssystemen ermöglicht. Kurz nach Bekanntwerden der Schwachstelle lag die Zahl anfälliger Computer in Österreich im vierstelligen Bereich. Zeitnahe Informationsmaßnahmen halfen bei der effektiven Eindämmung des bestehenden Risikos.

**Foreshadow** ist eine Lücke, die virtualisierte Umgebungen (meist Cloud-Dienste) betrifft und das unberechtigte Ausführen von Codes ermöglicht. Durch einen Designfehler in Intel-Prozessoren können Programme auf für sie eigentlich nicht zugängliche Speicherbereiche zugreifen. Neben der im Jahr 2018 bekannt gewordenen Lücke Meltdown/Specter handelt es sich bei Foreshadow somit um eine weitere innerhalb der Intel-Prozessoren-Architektur vorhandene Schwachstelle.

**PDF-Signaturen** ermöglichen die rechtssichere elektronische Unterschrift von Formularen im PDF-Format. Die im Berichtszeitraum 2019 festgestellte Schwäche bei der Signatur machte es Angreifern möglich, den Inhalt von PDF-Dateien unberechtigterweise zu ändern, ohne die PDF-Signatur an sich zu verletzen. Damit war die Authentizität und Integrität nicht mehr gewährleistet und das gesamte System der elektronischen und dokumentarischen Zuverlässigkeit untergraben. Es erfolgte eine umgehende Benachrichtigung der in Österreich potentiell betroffenen Stellen.



### 1.1.6 Eindringen in Computernetzwerke

Im Verlauf des Berichtsjahres kam es zu Angriffen mit partiellem Datenabfluss auf die Netzwerkinfrastruktur österreichischer Parteien sowie eines Ministeriums. Bei zwei österreichischen Parteien wurden im Zeitraum Juli bis August 2019 unberechtigte Zugriffe festgestellt. Die offenbar aus diesen Zugriffen beschafften Informationen fanden anschließend den Weg in die Öffentlichkeit.

Der um den Jahreswechsel stattgefundene Angriff auf das Netzwerk des Bundesministeriums für europäische und internationale Angelegenheiten (BMEIA) stellte den bisher größten und umfangreichsten Cyberangriff auf ein Ministerium in Österreich dar. Er führte erstmalig zur Aktivierung der im Netz- und Informationssystemsicherheitsgesetz (NISG) vorgesehenen gesamtstaatlichen Krisenmechanismen. Die Erstreaktion wurde sofort nach Bekanntwerden von Unregelmäßigkeiten eingeleitet.

Nach Erkennen der Dimension des Vorfalls wurden mit dem Inneren Kreis der operativen Koordinierungsstruktur (IKDOK) und dem Cyberkrisenmanagement Koordinationsausschuss (CKM KA) die vorgesehenen Krisenmechanismen für derartige Vorfälle initiiert. Ein operatives Einsatzteam bestehend aus Vertreterinnen und Vertretern des Bundesministeriums für Inneres (BMI), des Bundesministeriums für Landesverteidigung (BMLV), des Bundesministeriums für europäische und internationale Angelegenheiten (BMEIA) und des Bundeskanzleramtes (BKA) inkl. GovCERT, wurde unter Leitung des Cyber Security Centers (CSC) aufgestellt. Die ersten Risikominimierungsmaßnahmen erfolgten zeitnah, die Vorfallsbehandlung setzte sich über den Jahreswechsel hinaus fort.

### 1.1.7 Advanced Persistent Threats (APTs)

APTs stellen sowohl für die öffentliche Verwaltung als auch für Unternehmen in Österreich eine permanente Bedrohung dar, auch wenn die Anzahl der erkannten Fälle im Vergleich zu Angriffen mit Ransomware oder EMOTET deutlich geringer ausfällt. Während letztere

von Cyberkriminellen zur Geldbeschaffung eingesetzt werden, dienen APTs vorrangig der Beschaffung von Informationen im Kontext von Wirtschafts- und Industriespionage oder politisch motivierter Ausspähung. Darüber hinaus erlauben APTs den Angreifern Computernetzwerke in Produktions- und Lieferketten zu sabotieren. Dies kann bis zur vollständigen Unbrauchbarkeit der Systeme – etwa durch Datenlöschung (Wiping) oder Zufügen physischer Schäden – führen.

Im Frühjahr 2019 wurde in den Medien bekannt, dass die EU-Delegation in Moskau Ziel eines als APT einzuschätzenden Angriffs geworden war.

Zu Jahresbeginn 2019 konnte ein Angriff auf das COREU/CORTESY-Netzwerk der EU unterbunden werden. Dieses von EU-Mitgliedstaaten genutzte Netzwerk dient dem Austausch von Dokumenten im Zusammenhang mit der „Gemeinsamen Außen- und Sicherheitspolitik" (GASP). In Österreich konnte ein APT-Angriff auf eine verfassungsmäßige Einrichtung (siehe 1.1.6) rechtzeitig erkannt und somit Schäden verhindert werden. Dieser Angriff stand jedoch nach bisherigen Erkenntnissen nicht im Zusammenhang mit den beiden zuvor genannten EU-Fällen.

### 1.1.8 Veröffentlichung von Zugangsdaten im Internet

Zu Jahresbeginn 2019 wurde eine umfangreiche Sammlung von Login-Daten (Credentials) im Internet veröffentlicht, von der auch zahlreiche österreichische Internet-User betroffen waren. Der später als „Collection #1–5" bezeichnete Leak bestand aus insgesamt fünf nacheinander veröffentlichten Tranchen mit einem Gesamtumfang von mehr als 1,3 Milliarden Zugangsdaten aus unterschiedlichen Quellen. Obwohl es sich bei diesem Datenleak nur um einen von zahlreichen ähnlichen im genannten Berichtszeitraum handelte, stellte er doch aufgrund seiner Größe einen vorläufigen Höhepunkt dar. Durch rechtzeitige Information konnte nach derzeitigem Kenntnisstand zumindest bei betroffenen staatlichen Stellen größerer Schaden abgewendet werden.

## 1.2 Lage Cybersicherheit – Unternehmen und Sicherheitsdienstleister

Staatliche Stellen können im Rahmen ihrer Tätigkeit lediglich einen Ausschnitt der in Österreich vorliegenden Situation überblicken und sind auf die Kooperation mit Bedarfsträgern angewiesen. Deshalb wurden zur Erstellung des vorliegenden Berichtes auch in diesem Berichtsjahr wieder Unternehmen der kritischen Infrastruktur und verfassungsmäßige Einrichtungen sowie führende private Unternehmen aus der Cybersecurity-Branche eingeladen, aus eigener Perspektive zum Informationsaufkommen beizutragen und mit Expertise zu unterstützen. Auf diese Weise wird ein valides und weitestgehend vollständiges Bild der Cyberlage in Österreich am ehesten möglich. Dabei liegt das Augenmerk nicht primär auf konkreten Vorfällen, sondern auf Trends und Entwicklungen im Sinne einer abstrahierenden Überblicksdarstellung.

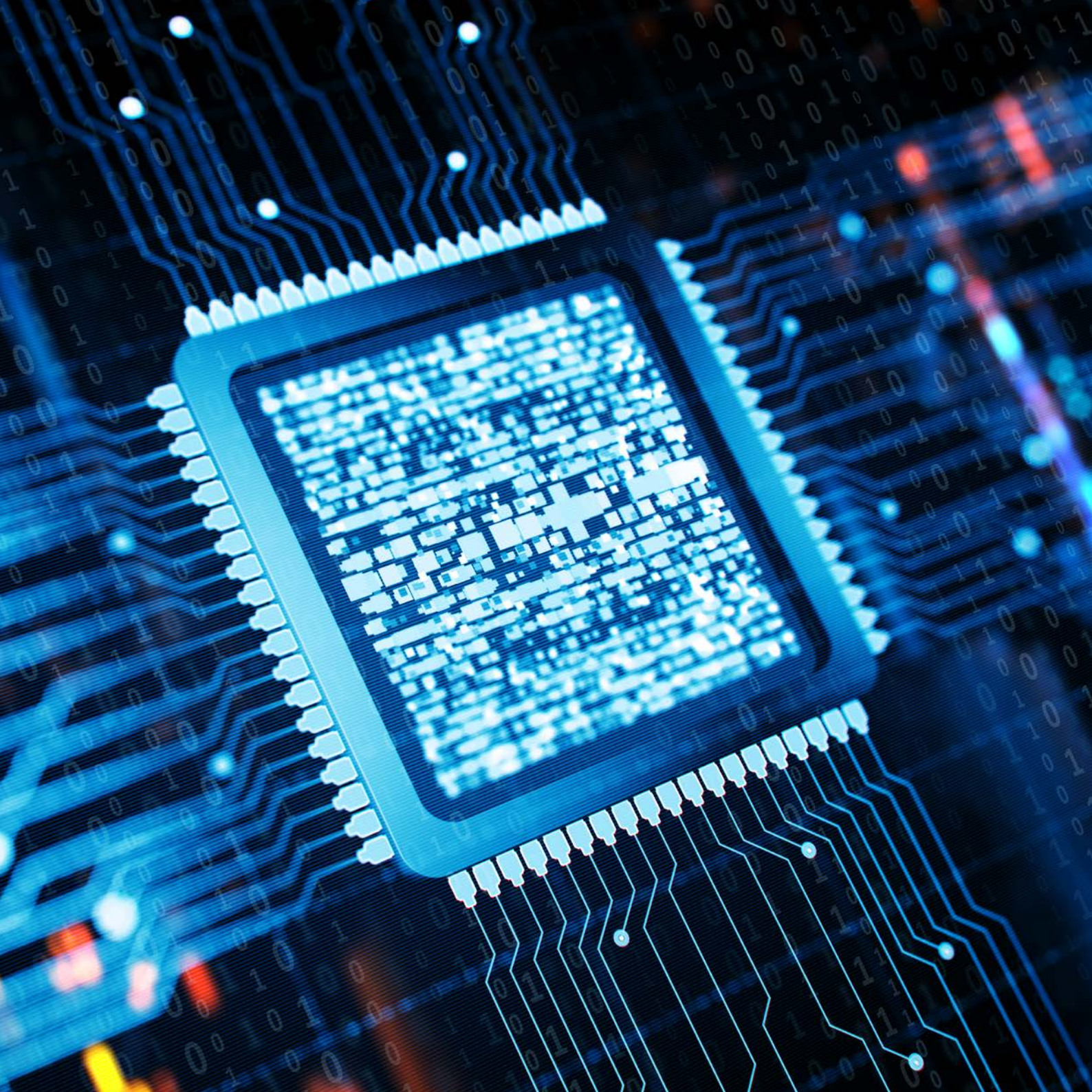
**50 %**
der befragten Unternehmen erhöhten das Budget für Cybersicherheit

### 1.2.1 Unternehmen der kritischen Infrastruktur und verfassungsmäßige Einrichtungen

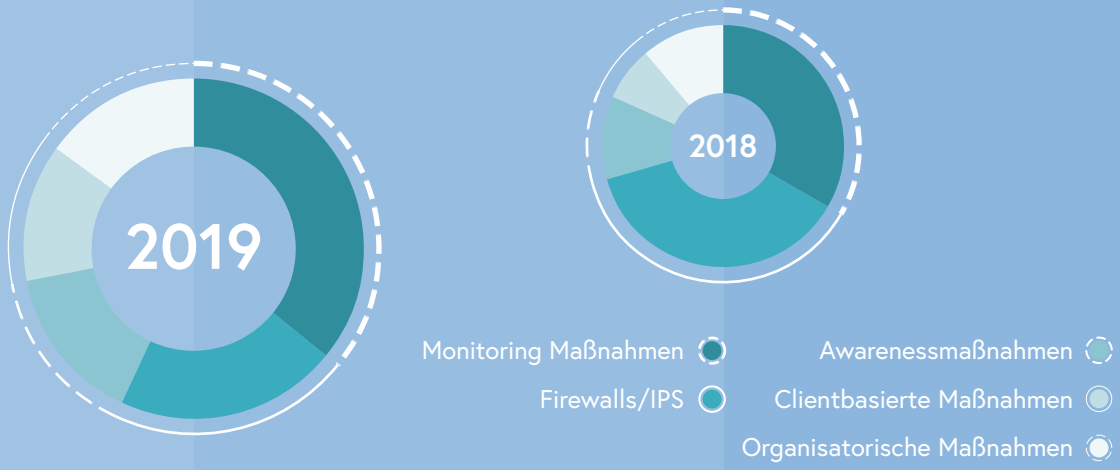
Im Berichtsjahr 2019 tätigten alle befragten österreichischen Unternehmen der kritischen Infrastruktur erneut Investitionen im Bereich der Cybersicherheit. Es konnte ein ausgeglichenes Verhältnis von Firmen, die ihr Budget für den Berichtszeitraum erhöht hatten, gegenüber solchen Firmen, die das Budget auf Vorjahresniveau hielten, festgestellt werden. Im Gegensatz zur letzten Berichtsperiode meldete diesmal keine Firma ein vermindertes Budget für Cybersicherheit. Insgesamt zeichnet sich in Bezug auf die Ausgaben für IT-Sicherheit eine Stabilisierung auf hohem Niveau ab.

## Entwicklung des zur Verfügung stehenden Cybersicherheitsbudgets

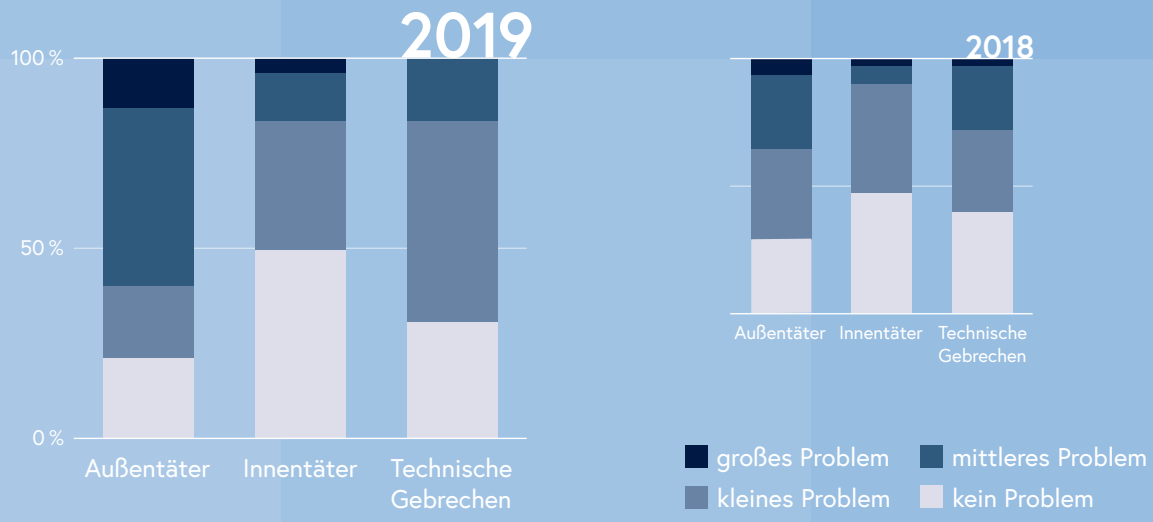

## Zusätzliche IT-Sicherheitsmaßnahmen



## Getroffene Maßnahmen für die Cybersicherheit




## Vorfallsursachen



Einhergehend mit steigenden Budgets ergriffen rückmeldende Firmen und Organisationen nahezu zur Gänze (über 96 %) zusätzliche IT-Sicherheitsmaßnahmen. Das erhöhte Sicherheitsbewusstsein dürfte nicht zuletzt auf die zeitgleiche Ausgestaltung staatlicher Rahmenbedingungen zurückzuführen sein. So wurde zur Schaffung eines hohen gemeinsamen Sicherheitsniveaus unter Betreibern wesentlicher Dienste und Anbietern digitaler Dienste mit Jahresbeginn 2019 das Netz- und Informationssystemsicherheitsgesetz (NISG) erlassen. Darüber hinaus hat Österreich 2018 das Datenschutzgesetz (DSG) an die neue Datenschutz-Grundverordnung (DSGVO) angepasst, welche erweiterte gesetzliche Auflagen an die IT-Sicherheit vorsieht.

## Trend zum aktiven Monitoring der Firmennetzwerke

Die im IT-Bereich getroffenen Sicherheitsmaßnahmen umfassten dabei Monitoring, den Betrieb von Firewalls/IPS, die Durchführung von Awarenesstrainings, clientbasierte sowie Maßnahmen organisatorischer Natur. Der auffälligste Unterschied im Vergleich zum Vorjahr zeigt sich in einer deutlichen Steigerung beim Einsatz von Firewalls/IPS. Hier hat der technische Fortschritt einerseits skalierbare und einfach konfigurierbare Produkte verfügbar gemacht, aber auch die effektive Abwehrfähigkeit der Systeme erhöht.

Unabhängig davon setzte sich aber unter den Firmen und Organisationen der Trend fort, dass man sich nicht mehr allein auf eine „Abschottung“ (durch Firewalls) verlässt, sondern mit Maßnahmen eines aktiven Monitorings Angreifer identifiziert, die bereits in das eigene Netz eingedrungen sind. Dies sieht die Suche nach aktuellen Bedrohungen für die jeweilige Organisation und in einem zweiten Schritt die gezielte Überprüfung des eigenen Systems nach Infektionen vor. Begleitend dazu wurden vielerorts vorbereitende Maßnahmen zur Analyse von Sicherheitsvorfällen mit forensischen Methoden getroffen.

In vielen Fällen wurden Awarenessmaßnahmen entweder neu eingeführt oder bestehende Maßnahmen gestärkt und ihr Output unter der Maßgabe von „Lessons Learned“ als effektiv und teilweise unverzichtbar zur Prävention von einer Vielzahl von Cyberangriffen gewertet. Zu solchen Maßnahmen zählten neben Fachvorträgen auch simulierte Phishing-

oder Ransomware-Attacken. Parallel dazu gaben Unternehmen auch an, dass die in der Vergangenheit getroffenen Maßnahmen 2019 Erfolg zeigten und Angriffsversuche und Angriffe im Vorfeld erkannt werden konnten. Darüber hinaus bauten viele der Befragten Security Information and Event Management Systeme (SIEM) sowie Security Operations Center (SOC) auf.

Im Berichtsjahr 2019 wurden durch eine Vielzahl der Unternehmen organisatorische Maßnahmen getroffen, darunter die Etablierung strengerer Policies für Passwörter oder eine Anpassung der Unternehmensprozesse.

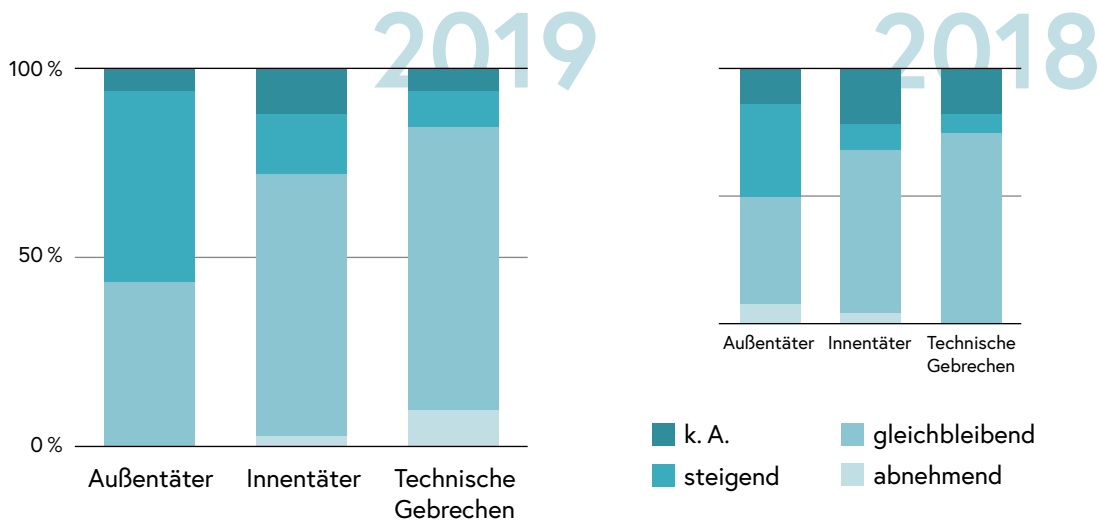
Hier zeichnet sich ebenfalls ein Zusammenhang mit den als „Lessons Learned" bezeichneten Rückmeldungen ab: Diesen zufolge beschäftigen sich befragte Organisationen 2019 zunehmends mit neuen regulatorischen Maßnahmen wie der DSGVO oder der Umsetzung des mit 2019 in Kraft getretenen NISG.

## Gefährdung durch Innentäter nimmt zu

Die Einschätzung von Vorfallsursachen zeigt auch für 2019 im Großen und Ganzen ein dem voranliegenden Berichtsjahr vergleichbares Bild. Demnach sind primär Außentäter oder technische Gebrechen Vorfallsverursacher, Innentäter waren bei einer geringen Anzahl von Vorfällen involviert. Allerdings sind im Vergleich zu 2018 leichte Verschiebungen dahingehend zu verzeichnen, dass die Gefährdung durch Außentäter eher zurückgeht, die Gefährdung durch Innentäter jedoch eher zunimmt. Die Gefahr eines technischen Gebrechens wird als zunehmend problematisch eingeschätzt.

Betrachtet man die Angaben zum Trend, so wurden 2019 alle Vorfallsursachen als steigend angegeben – wenn auch mit geringeren Steigerungsraten gegenüber dem Vorjahr. Dieses Zusammenspiel könnte in Bezug auf Außentäter darauf zurückzuführen sein, dass durch die gesteigerten Abwehrmaßnahmen insbesondere im Bereich Ransomware und Phishing das Angriffsvolumen zwar zunimmt, aber immer mehr dieser Angriffe auch im Vorfeld erkannt beziehungsweise abgewehrt werden können.

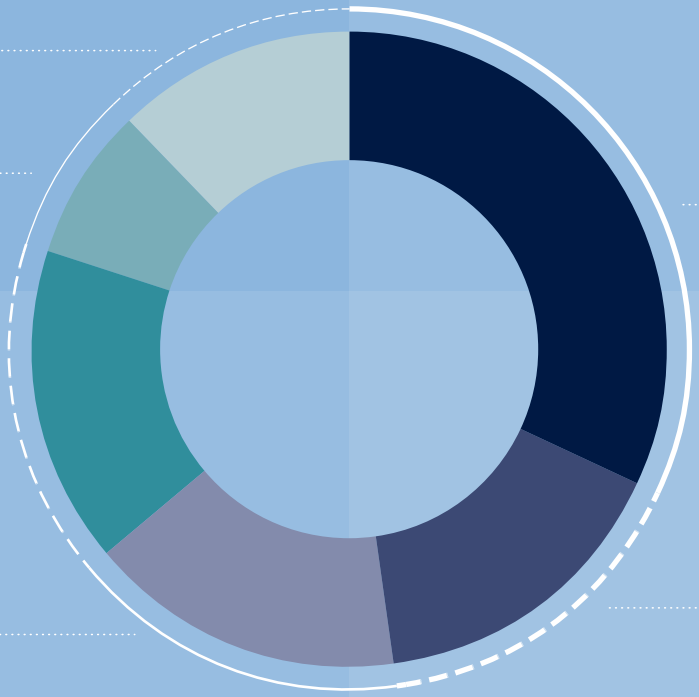
**Vorfallsursachen Trends**




Zu den generellen Entwicklungen in der IT-Sicherheitsbranche zeigt sich außerdem auch für 2019 eine erneute Ausweitung von Cloud Computing. Allerdings wird dieser Trend von den befragten Unternehmen zunehmend mit Skepsis betrachtet. Mit der steigenden Abhängigkeit von externen Anbietern geht ein – mitunter auch nur gefühlter – Kontroll- und Hoheitsverlust über die eigenen Daten einher. Lokale (On-Premis) Lösungen werden durch Cloudlösungen zunehmend aggressiver vertrieben – langfristig werden sich diese auch durchsetzen. Die zunehmende Alternativlosigkeit von Cloudlösungen sorgt für eine nicht zu unterschätzende Resignation seitens der Befragten.

Andere Trends (Regulatorische Maßnahmen, Internet of Things, Artificial Intelligence, Distributed Denial of Service, Social Engineering) fallen gegenüber der Cloud-Thematik mit deutlichem Abstand zurück.

## Generelle Trends 2019



### 1.2.2 Führende private Unternehmen aus der Cybersecurity-Branche

Die Befragung von führenden privaten Unternehmen aus dem Bereich der Sicherheitsdienstleister wies auch für das Berichtsjahr 2019 eine vergleichsweise geringe Rücklaufquote auf.[3] Aus den eingegangenen Beantwortungen zur Erhebung lassen sich aber dennoch einige Trends ableiten:

#### Trends bei bearbeiteten Vorfallsart

| 2019 | | 2018 | |
|---|---|---|---|
| + | DDoS | - | DDoS |
| + | Ransomware | + | Ransomware |
| + | Phishing | = | Phishing |
| + | CEO-Fraud / Fake Invoice / SCAM | - | CEO-Fraud / Fake Invoice / SCAM |
| + | Targeted Attack / APTs | = | Targeted Attack / APTs |
| + | Datendiebstahl | + | Datendiebstahl |
| + | Botnet / C2 | = | Botnet / C2 |
| – | Defacements | = | Defacements |

#### Trends bei bearbeiteten Motivationen

| 2019 | | 2018 | |
|---|---|---|---|
| + | Monetär | + | Monetär |
| + | Politisch | - | Politisch |
| + | Persönlich / Rache | = | Persönlich / Rache |
| + | Staatlich | + | Staatlich |
| + | Technisches Gebrechen | - | Technisches Gebrechen |

3 Dank ergeht insbesondere an die Firmen Alpha Strike Labs GmbH, Kapsch BusinessCom AG und SEC Consult Unternehmensberatung GmbH für ihre Antworten.

## Zunahme von Spionage mittels APTs

Insgesamt wurde bei Vorfallsarten eine Zunahme in allen Bereichen gemeldet. Lediglich im Bereich der Defacements kam es 2019 zu einem Rückgang. Hinsichtlich der Motivation gab es 2019 ebenfalls eine Zunahme in allen Bereichen. Insbesondere die gemeldete Zunahme politisch motivierter Vorfälle (Spionage) muss mit einiger Sorge zur Kenntnis genommen werden, da es sich hier um Vorfälle mit Einsatz von APTs handeln dürfte. Diese haben nicht nur ein hohes Schadenspotential, sondern dürften aufgrund der hohen Dunkelziffer im Berichtsjahr 2019 einen noch höheren Anteil am Prozentsatz ausmachen.

Vor allem kleinere und mittlere Unternehmen melden für das Jahr 2019 einen hohen Anteil an in die Breite gestreuten Angriffen – also Ransomware und Phishing. Mit steigender Größe des Unternehmens gewinnen zielgerichtete Angriffe zum Zwecke der Industriespionage oder auch der Störung des Betriebes mittels DDoS an Relevanz.

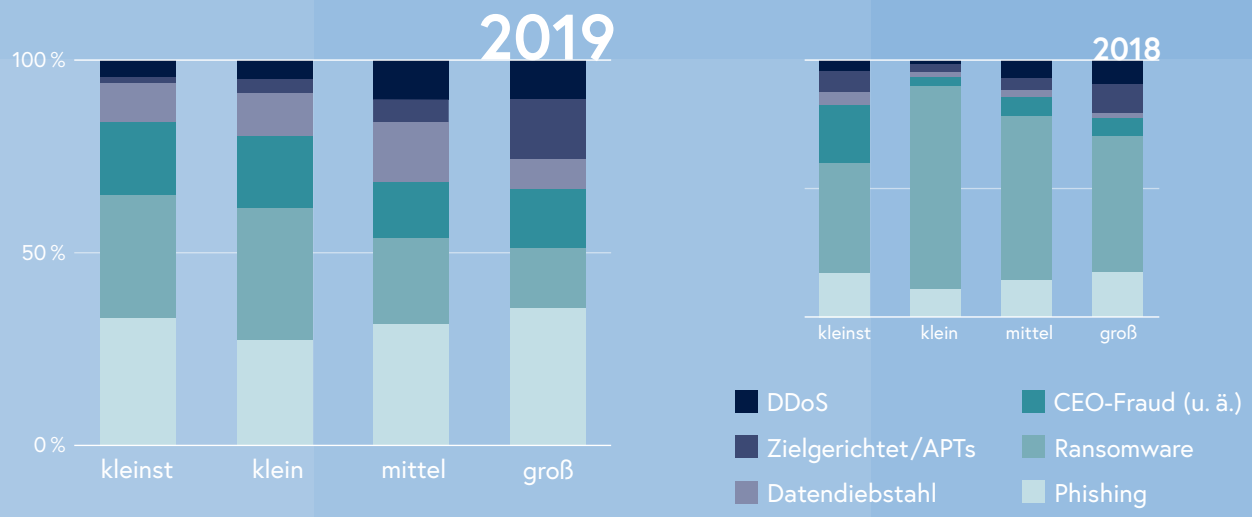
Im Hinblick auf die offenbar am stärksten im Zunehmen begriffenen Vorfallsarten sind auch die entsprechenden „Lessons Learned“ und Erkenntnisse der führenden privaten Unternehmen aus der Cybersecurity-Branche von großer Relevanz.

Im Jahr 2019 kam es erneut zu einem Ansteigen erkannter Versuche von Ransomware-Angriffen. Insgesamt dürfte seitens der Firmen und Organisationen das Problembewusstsein zugenommen haben und vermehrt in Präventionsmaßnahmen (technischer und nicht-technischer Natur) investiert worden sein. Dies zeigt sich vor allem darin, dass gerade Kleinstunternehmen (<10 MA), welche im Vorjahr noch wenig Ransomware-Angriffe gemeldet hatten, nun auch stärker in der Statistik vertreten sind. Benutzerschulungen im Bereich der Awareness und simulierte Phishing-Angriffe, aber auch neue Methoden in der Erkennung von Schadsoftware konnten hier viele Angriffe im Vorfeld abwehren, wobei große Unternehmen – aufgrund der ihnen zur Verfügung stehenden Kapazitäten – weiterhin Vorreiter bleiben.

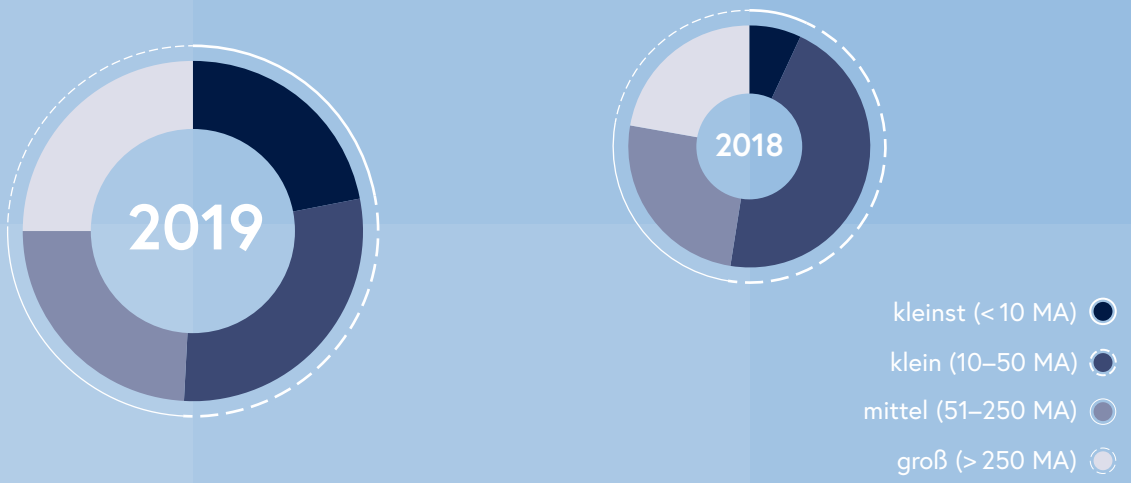
## Sicherheitsdienstleister ziehen positive Bilanz

Bei Phishing-Angriffen zogen Sicherheitsdienstleister eine durchwegs positive Bilanz; obwohl insgesamt eine Zunahme von Angriffen verzeichnet wurde, waren nur die wenigsten Angriffe erfolgreich.

## Vorfallsarten nach Unternehmensgröße




## Angriffe mittels Ransomware



Dabei zeigt sich für den Jahresverlauf 2019 ein deutlicher Rückgang im Bereich von Großunternehmen: Dies dürfte auf entsprechende Sensibilisierung der Mitarbeiterinnen und Mitarbeiter sowie dem Wirksamwerden anderer Sicherheitsmaßnahmen zurückzuführen sein. Demgegenüber haben Kleinstunternehmen (<10 MA) einen Aufholbedarf: 2019 wurden mehr Vorfällen mit Phishing gemeldet als im Vorjahr. Die Situation bei kleinen und mittleren Unternehmen hingegen scheint sich stabilisiert zu haben.

Angriffe mittels CEO-Fraud/Fake Invoice/SCAM konnten auch im Berichtsjahr 2019 festgestellt werden. Sie gingen mitunter mit tatsächlichen Hacking-Angriffen im Vorfeld einher. Die im Zuge dessen erbeuteten Informationen wurden alsdann zum „eigentlichen" Betrugsversuch verwendet. Bei Großunternehmen war dabei ein Rückgang des Volumens gegenüber 2018 zu verzeichnen, wohl auch weil Unternehmen und ihre Belegschaft in diesem Bereich mittlerweile stärker sensibilisiert sind und geeignete Prozesse eingerichtet wurden. Dagegen nahm die Zahl der Angriffe auf Kleinstunternehmen (<10 MA) deutlich zu. Hier dürfte der Nachholbedarf an Schutzmaßnahmen ungleich höher sein. Kleine und mittlere Unternehmen hingegen konnten die Lage weitgehend stabilisieren.

DDoS-Angriffe auch auf Unternehmen mit weniger als zehn Mitarbeitern

Im Bereich der zielgerichteten Angriffe/APTs (mit dem Schwerpunkt in der Informationsgewinnung) hat es im Berichtsjahr 2019 eine deutliche Zunahme bei großen Unternehmen gegeben. Dieser ging mit einem unverkennbaren Rückgang in den übrigen Unternehmensgrößen (kleinst, klein und mittel) einher. Gründe dafür könnten in einer verstärkten Fokussierung der Angriffsstrategie auf nunmehr große Unternehmen, oder aber in verbesserten Möglichkeiten großer Unternehmen bei der Angriffsentdeckung liegen.

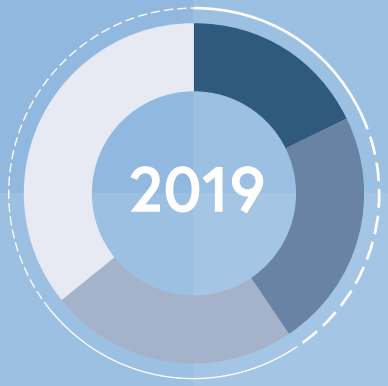
Auch DDoS-Angriffe nahmen im Berichtsjahr von Neuem zu. Hier erwies sich neben der eigentlichen Abwehr vor allem eine unklare Zuordnung auf Täter und deren Motivlage als großes Problem. In diesen oft politisch oder anders aktionistisch gesteuerten Kampagnen, sind naturgemäß mittlere und vor allem große – aus dem öffentlichen Diskurs bekannte – Unternehmen betroffen. Auffällig ist aber, dass im Berichtsjahr 2019 eine Zunahme von DDoS-Angriffen auch auf kleine und sogar Kleinstunternehmen (>10 MA) zu verzeichnen ist.

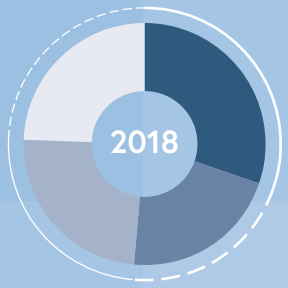
## Angriffe mittels Phishing



kleinst (< 10 MA)
klein (10–50 MA)
mittel (51–250 MA)
groß (> 250 MA)

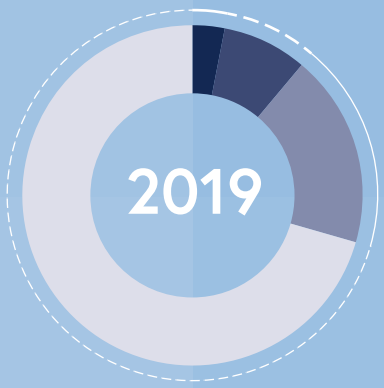
## Angriffe mittels CEO-Fraud / Fake Invoice / SCAM

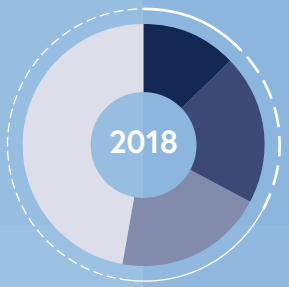



kleinst (< 10 MA)
klein (10–50 MA)
mittel (51–250 MA)
groß (> 250 MA)

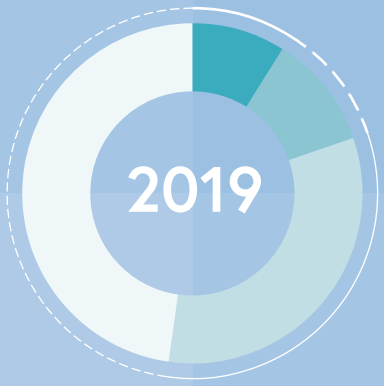
## Zielgerichtete Angriffe/APTs

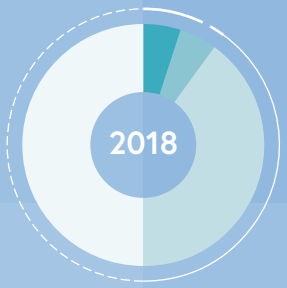



kleinst (< 10 MA)
klein (10–50 MA)
mittel (51–250 MA)
groß (> 250 MA)

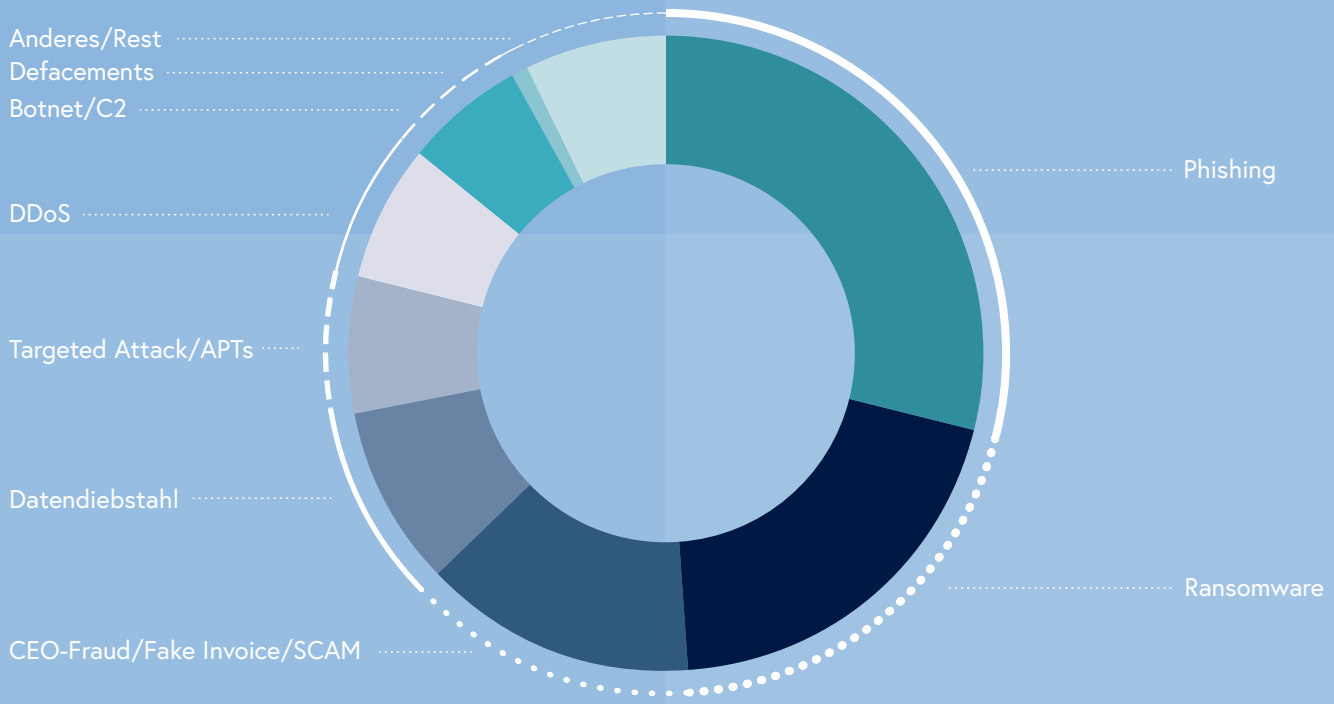
## Angriffe mittels DDoS



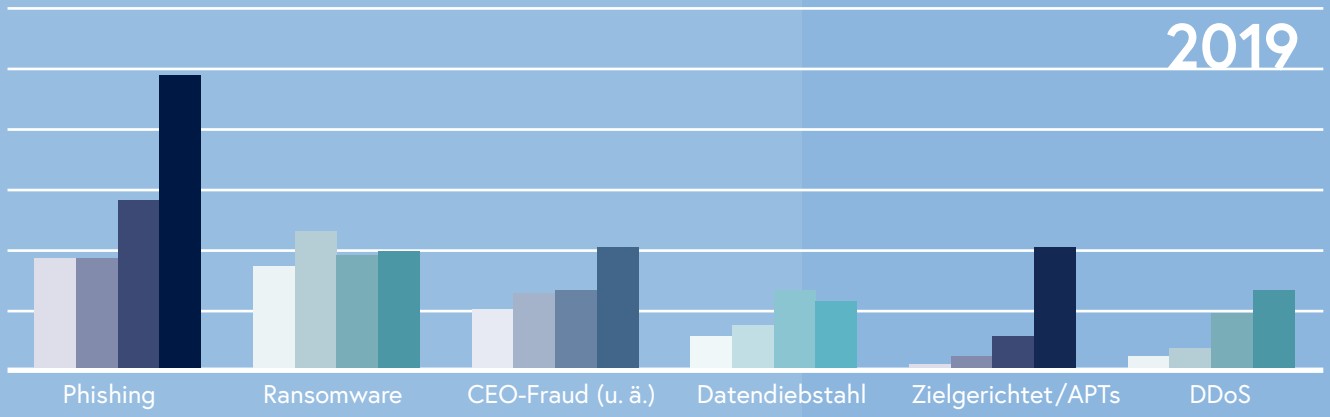



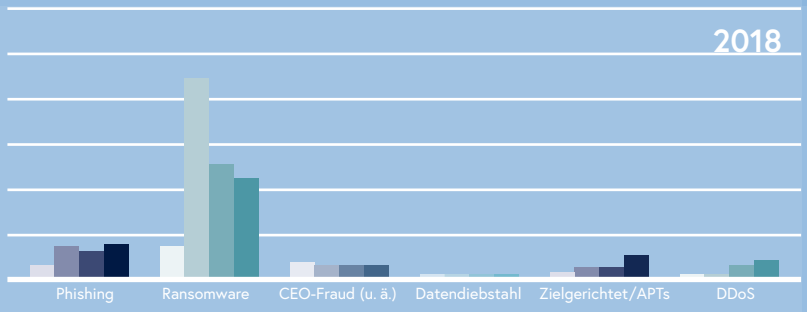

kleinst (< 10 MA)
klein (10–50 MA)
mittel (51–250 MA)
groß (> 250 MA)

## Angriffsarten 2019

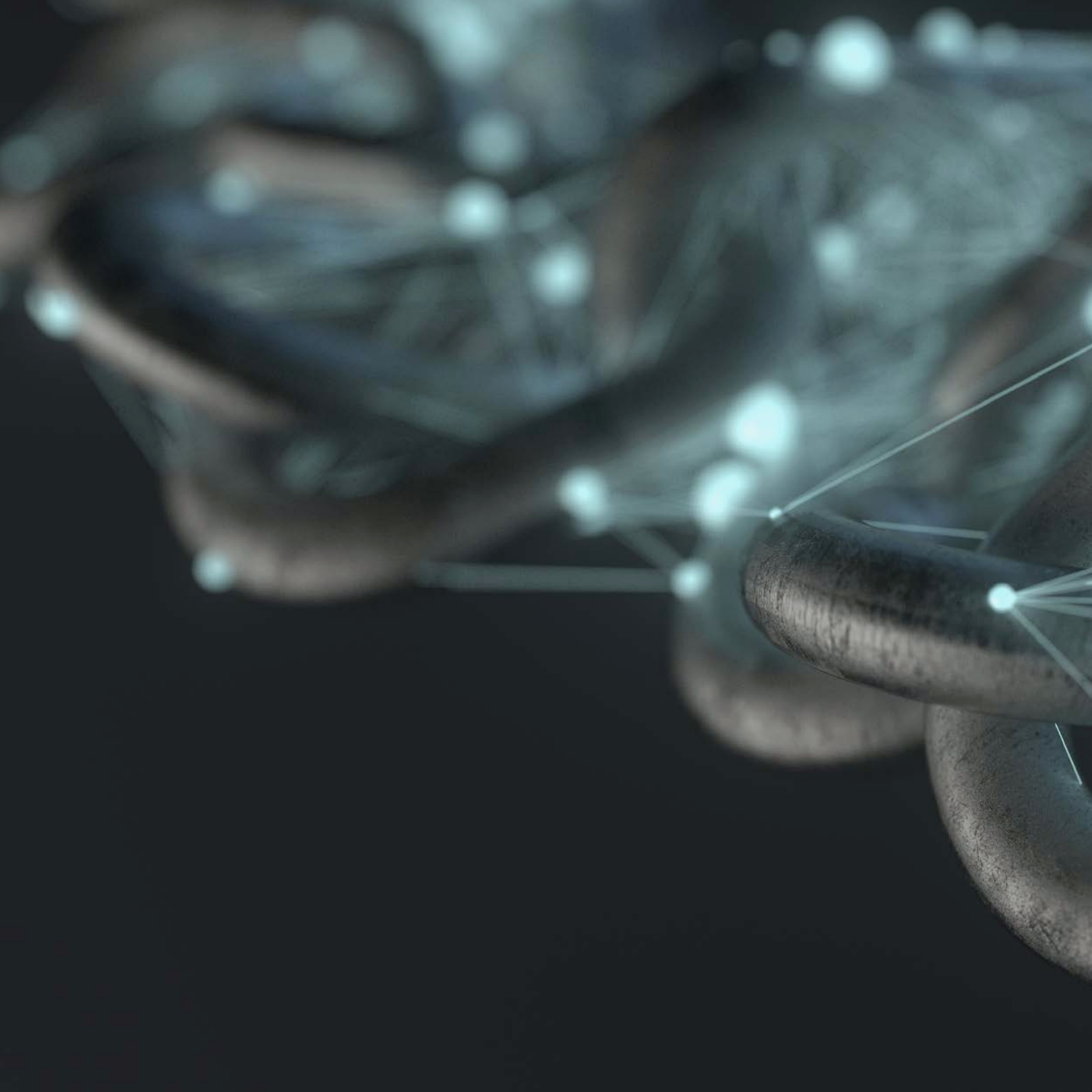


## Bedrohungen nach Unternehmensgröße




- kleinst (< 10 MA)
- klein (10–50 MA)
- mittel (51–250 MA)
- groß (> 250 MA)



## 1.3 Lage Cybercrime

Die Betrachtung der vorläufigen polizeilichen Kriminalstatistik lässt mit über 13.000 angezeigten Delikten in den ersten sechs Monaten des Jahres 2019 eine Steigerung von etwa 50 Prozent gegenüber dem Vergleichszeitraum von 2018 erkennen. Die genauen Deliktszahlen wurden mit der kriminalpolizeilichen Kriminalstatistik im Frühjahr 2020 veröffentlicht. Eine tiefergehende Analyse und Beschreibung der kriminalpolizeilichen Phänomene erfolgt mit dem jährlichen Cybercrimereport des Bundeskriminalamtes.

Der Begriff Cybercrime umfasst:

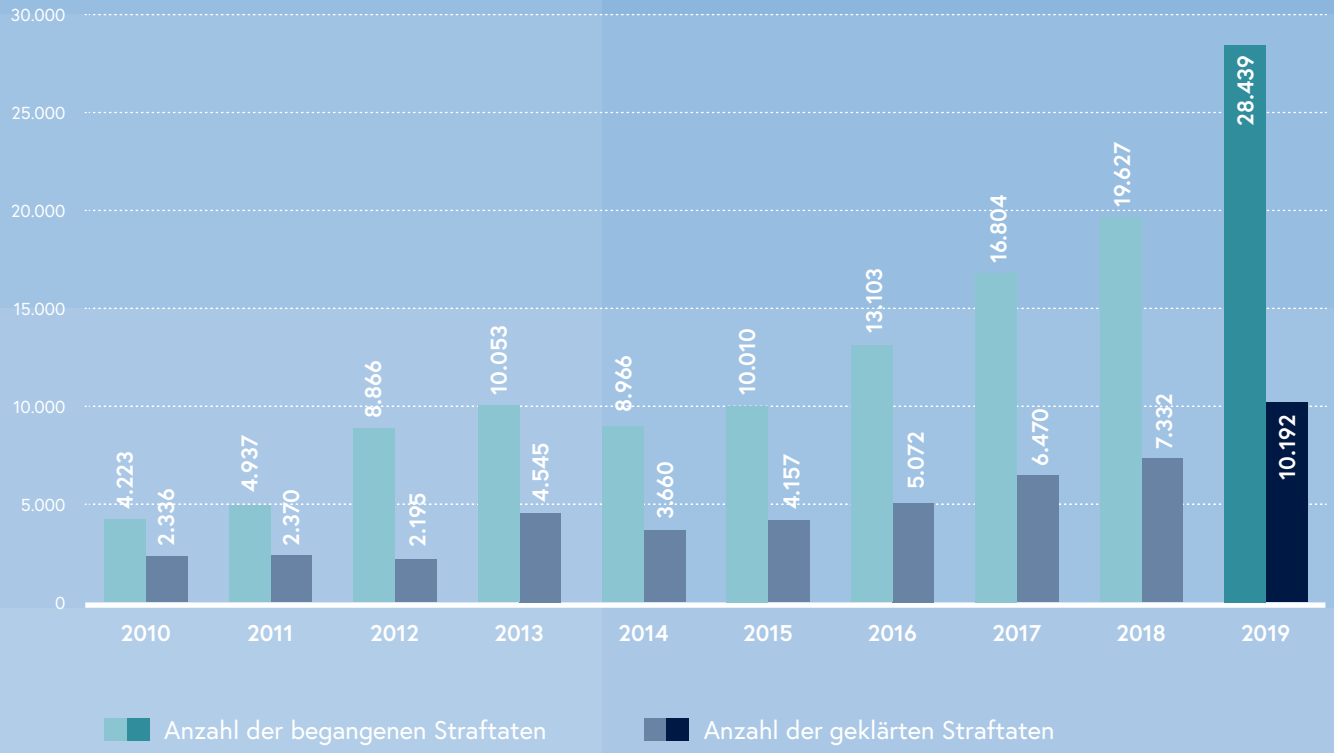
- Angriffe auf Daten und Computersysteme „Cybercrime im engeren Sinn";
- Internetbetrug;
- sonstige Formen von Kriminalität, bei denen nicht die Computersysteme selbst das Ziel darstellen, sondern diese lediglich als Tatbegehungsmittel für klassische Delikte zum Einsatz kommen „Cybercrime im weiteren Sinn".

### 1.3.1 Internetbetrug

Täglich zehn neue Fake- und Phishing-Shops

Den zahlenmäßig größten Faktor stellt der Internetbetrug dar. Dieser ist auch maßgeblich für den letztjährigen Anstieg der Delikte im Bereich der Cyberkriminalität verantwortlich. Hier konnte für das erste Halbjahr ein Anstieg der Delikte von einem Drittel angenommen werden. Mit der fortschreitenden Digitalisierung verlagern sich Betrugsdelikte immer mehr ins Internet. Für die Täter ist es ein Leichtes, aufgrund technischer Anonymisierung sowie Verschleierung der Finanzflüsse Betrugshandlungen unerkannt und damit „sicher" durchzuführen. Zusätzlich können durch den weltweiten Zugang zum Internet immer mehr Menschen als potentielle Opfer angesprochen werden. Häufig verwendete Betrugsmethoden sind das Versenden von Gewinnversprechen via E-Mail und Bestellbetrügereien mittels sogenannter Fake-Webshops. Es konnten rund 200 neue falsche Online Shops, vorwiegend im Technik- und Bekleidungsbereich erkannt werden, welche jedoch auf wenige Tätergruppierungen zurückzuführen sind. In der Vorweihnachtszeit 2019 konnte eine Verdoppelung mit durchschnittlich bis zu zehn Fake- und Phishing-Shops

## Entwicklung Cybercrime



pro Tag beobachtet werden. Ebenso wurden zahlreiche Betrugsfälle durch das Verwenden falscher Identitäten und Kontaktdaten bei Bestellungen im Internet, durch Kontaktaufnahme per Telefon, E-Mail oder über Soziale Medien registriert. Häufige Vorgehensweise war neben der Vortäuschung von Liebesbeziehungen das Angebot besonders lukrativer Geschäftsmodelle und vermeintlich technische Unterstützungsleistungen (sogenannter Tech Support Scam). Im Mai 2019 wurden die ersten Fälle von versuchtem CEO-Fraud via WhatsApp gemeldet. Im Herbst kam es zu einem exponentiellen Anstieg von Angriffen auf Facebook und Instagram, indem alte, von Vorbesitzern nicht mehr genutzte, aber von Tätern recycelte Accounts, verwendet wurden.

Social Engineering maßgeblicher Angriffsvektor

Social Engineering blieb im letzten Jahr demnach maßgeblicher Angriffsvektor.

### 1.3.2 Cybercrime im engeren Sinn

Im Bereich des Cybercrime im engeren Sinn waren 2019 die Anzeigen im Vergleichszeitraum des ersten Halbjahres um etwa 60 Prozent angestiegen. Darunter fallen Straftaten, bei denen Angriffe auf Daten oder Computersysteme unter Ausnutzung der Informations- und Kommunikationstechnik begangen werden. Beispiele dafür sind der widerrechtliche Zugriff auf ein Computersystem oder die Datenbeschädigung. Von Mai bis Juni wurden sehr viele Anzeigen wegen widerrechtlichen Finanztransaktionen von meist privaten Bankkonten gemeldet. Ab Juni wurden technische Sicherheitslücken (wie beispielsweise RDP-Schwachstellen bei Microsoft-Produkten) zu einer großen Bedrohung für Unternehmen und Institutionen, welche Systemaktualisierungen nicht zeitnahe durchführten. Gegen Jahresende wurden massiv Angriffe auf unzureichend gesicherte Telefonanlagen (VoIP-Anlagen) durchgeführt. Die Täter nutzten vor allem arbeitsfreie Zeiten, um in die Telefonanlagen von Unternehmen einzudringen. Danach wurden in einem programmierten Callcenter-Modus teure Mehrwertnummern oder Fraudulent Carrier angerufen.

Aufgrund der großen Anzahl von Datenleaks in den Jahren 2018 und 2019 wurden massenhaft personenbezogene Daten im Internet veröffentlicht, beziehungsweise im Darknet zum Kauf angeboten. Die widerrechtlichen Zugriffe mit den so erlangten Zugangsdaten stiegen massiv an. Des Weiteren wurden bei Organisationen kritischer Infrastruktur

Phishing-Angriffe registriert, die durch geänderte Outlook-Mail-Regeln die eingehenden Nachrichten an externe Adressen weitergeleitet hatten.

Im ersten Quartal fielen auch vermehrt Spam-Phishing-Kampagnen auf die DNS-Infrastruktur an, die mit verbesserter Version des EMOTET-Schadcodes auch gezieltere Angriffe auf öffentliche Einrichtungen begingen. Im Laufe des Jahres blieb die Bedrohung vor allem für kleine und mittlere Unternehmen bestehen. Mit diesem Trojaner verschafft sich der Täter in der Regel den Zugriff zum IT-System des Opfers, wobei erst nach einigen Tagen oder Wochen die Daten von weiteren Geräten im Netz verschlüsselt werden.

Für das Folgejahr lässt sich, wie für 2019, bereits absehen, dass die Straftäter weiterhin vermehrt DDoS-Attacken mittels Crime-as-a-Service nutzen. Diese zielen aber nicht auf Breitenwirkung ab, sondern sind vielmehr zielgerichteter Aktivismus, um die Verfügbarkeit bestimmter Webseiten einzuschränken.

### 1.3.3 Sonstige Kriminalität im Internet

Der dritte Teilbereich der „sonstigen Kriminalität im Internet“ verzeichnete im ersten Halbjahr 2019 eine Steigerung von etwa 140 Prozent. Der Grund dafür liegt in der zunehmenden Verlagerung klassischer Strafrechtsdelikte ins Internet. Gleichzeitig werden sogenannte „Crime-as-a-Service“-Leistungen im Darknet angeboten. Dabei handelt es sich vorwiegend um Hackingtools oder Erpressungstrojaner. Ebenso wurde ein vermehrter Vertrieb von Falschgeld, Kinderpornographie, Kreditkartendaten und gefälschten Urkunden wahrgenommen. Durch die im Darknet angebotenen Dienste steigen vor allem Erpressungen mit Ransomware und Massenerpressungsmails, meist begleitet von Geldforderungen in Bitcoin, sehr stark an. Im Laufe des Jahres gingen die Täter immer zielgerichteter gegen ihre Opfer vor und mit einer technischen Kompromittierung von durchschnittlich vierzehn Tagen auch viel aufwendiger und angepasster in ihren Methoden. So wurden sogar Erpressungssummen an vermeintliche Einkommen der Opfer angepasst. In diesem Zusammenhang hatte bereits zu Jahresbeginn eine eigene „ARGE-Erpressungsmail“ im Cyber Crime Competence Center (C4) des Bundeskriminalamtes ihre Arbeit aufgenommen, um derartige modi operandi künftig zentral bearbeiten zu können.

**‚sonstige Kriminalität im Internet'
verzeichnete im ersten Halbjahr 2019
eine Steigerung von etwa 140 %**


F4
Delete
Home
Esc
Page Down
Del
7 Home
Page Up
W
8
Num Lock
F10

## 1.4 Cyberlage Landesverteidigung

Neben den physischen Domänen Land, Luft, Meer und Weltraum hat durch die technologischen Entwicklungen und die globale digitale Vernetzung vor allem der Cyberraum als immaterielle Domäne im militärischen Bereich massiv an Bedeutung gewonnen.

### Durchsetzung strategischer Zielsetzungen erfolgt auch im Cyberraum

In keinem militärischen Konflikt der Gegenwart und Zukunft, aber auch im „Graubereich" zwischen Krieg und Frieden „Hybride Konflikte", wird auf das Erzielen von Wirkung im Cyberraum verzichtet. Besonders hervorzuheben ist, dass im Cyberraum die Attribuierung von defensiven und offensiven Handlungen verschleiert werden kann. Das kann die (verdeckte) Durchsetzung strategischer und militärstrategischer Zielsetzungen zusätzlich begünstigen.

Für das Bundesministerium für Landesverteidigung (BMLV) bedeutet dies, sich im Sinne der Kernaufgabe des Österreichischen Bundesheeres (ÖBH), festgelegt im § 2 lit.a. Wehrgesetz, bestmöglich auf die militärische Landesverteidigung im Cyberraum auszurichten und darauf vorzubereiten. Das umfasst sowohl alle Maßnahmen der Informations- und Kommunikationstechnologie-Sicherheit (IKT), als auch alle Maßnahmen zur Abwehr von Cyberangriffen auf die militärischen IKT-Systeme.

Aufgrund der gegenwärtigen Gesamtsituation des ÖBH ist dieses zum Schutz im Cyberraum vorrangig auf militärische IKT-Systeme ausgerichtet.[4]

Generell können aus den Erfahrungswerten des vergangenen Jahres folgende Trends abgeleitet werden:

- Steigende Anzahl an automatisierten Angriffen auf Netzwerkebene;
- Professionellere, großflächiger angelegte Social Engineering-Angriffe via E-Mail.

---

4 Bericht „Unser Heer 2030"

## Border Protection

Aus den Daten der Sicherheitssysteme des BMLV lassen sich bisher bekannte Trends unverändert fortführen. So konnte auf Netzwerkebene in den Sicherheitseinrichtungen weiterhin ein wachsender Anstieg an Zugriffen beobachtet werden, die durch eigene Sicherheitsmaßnahmen geblockt wurden. Diese werden vor allem durch automatisierte Angriffe und Scans verursacht. Zusätzlich wurden zunehmend manuelle Eingriffe in Kombination mit automatisierten Angriffen beobachtet. Wie bereits im Jahr 2019 ist auch für das kommende Jahr mit einem weiteren Anstieg in dieser Form zu rechnen.

## Angriffe per E-Mail

Im Vergleich zur vorhergehenden Zeitperiode konnten mehr großflächig angelegte Angriffe über E-Mail-Anhänge, wie z. B. mit dem weit verbreiteten EMOTET-Schadcode, festgestellt werden. Zusätzlich wurde ein Anstieg personalisierter Angriffe beobachtet.

mit weiterem Anstieg von Angriffen muss gerechnet werden

### Ausblick

In der Zukunft wird mit einem weiteren Anstieg an automatisierten Angriffen, vermehrt in Kombination mit manuellen Angriffen, gerechnet. Die Trendannahme, vor allem beim Angriffsvektor E-Mail in Richtung automatisierter Personalisierung, hat sich bestätigt und ist auch für das nächste Jahr anzunehmen. Dies bedeutet, dass die Angreifer sich nicht nur als bekannte Services (Bank, Post, Rechnungszustellungen, etc.) ausgeben, sondern auch deutlicher Bezug auf das Unternehmen sowie die Personen selber nehmen bzw. verstärkt nehmen werden.

Aufgrund der gegenwärtigen Gesamtsituation des ÖBH kann eine zukünftige, rechtzeitige Früherkennung bzw. Unterstützung zur Abwehr durch das ÖBH nicht sichergestellt werden[5].

---

5 Bericht „Unser Heer 2030“

# 2 Internationale Entwicklungen

In den letzten Jahren wurden Fragen der Cybersicherheit von zahlreichen internationalen Organisationen und multilateralen Foren aufgenommen und teilweise sehr kontroversiell diskutiert. Die relevanten außen- und sicherheitspolitischen Maßnahmen werden vom BMEIA koordiniert. Im Bereich der Europäischen Union (EU) wird das Thema Cybersicherheit vom Bundeskanzleramt (BKA) koordiniert.

Die rasanten Entwicklungen im Bereich der Cybersicherheit werfen eine Reihe fundamentaler Fragen in Bezug auf das Völkerrecht, insbesondere auf das Humanitäre Völkerrecht sowie Grund- und Menschenrechte, auf. Im Allgemeinen setzt sich Österreich auf internationaler Ebene für ein freies, offenes und sicheres Internet ein, wobei die Ausübung aller Menschenrechte auch im virtuellen Raum gewährleistet werden muss. Dabei muss auf ein angemessenes Gleichgewicht zwischen den Interessen der Strafverfolgung und der Achtung grundlegender Menschenrechte, wie dem Recht auf freie Meinungsäußerung und Informationsfreiheit sowie dem Recht auf Privatleben und Privatsphäre, geachtet werden.

## 2.1 Europäische Union (EU)

### 2.1.1 Horizontal Working Party on Cyber Issues

Die Horizontal Working Party on Cyber Issues „HWP Cyber“ oder auch Horizontale Arbeitsgruppe für Cyberangelegenheiten genannt, wurde im Jahr 2016 eingerichtet und ist für die Koordinierung der Arbeit des Rates der EU zu Angelegenheiten im Cyberrraum, insbesondere für die Cyberpolitik und die gesetzgeberischen Aktivitäten, zuständig. Sie legt die Cyberprioritäten und strategischen Ziele der EU als Teil eines umfassenden politischen Rahmens fest und gewährleistet eine horizontale Arbeitsplattform, die eine Harmonisierung und ein einheitliches Vorgehen in Fragen der Cyberpolitik ermöglicht.

Die Ratsarbeitsgruppe arbeitet eng mit anderen verwandten Arbeitsgruppen wie der Europäischen Kommission (EK), dem Europäischen Auswärtigen Dienst (EAD), Europol, Eurojust, der European Union Agency for Fundamental Rights (FRA), der European Defence Agency (EDA) und der ENISA zusammen.

Schwerpunkte in der HWP Cyber waren das Europäische Kompetenzzentrum für Cybersicherheit und die Weiterentwicklung der diplomatischen Reaktion der EU auf böswillige Cyberaktivitäten.

Im Jahr 2019 fand die HWP Cyber zu insgesamt 35 Sitzungen zusammen. Einen Schwerpunkt der Arbeit bildeten dabei die Verhandlungen zum EU-Verordnungsvorschlag zur Einrichtung des Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung und des Netzes nationaler Koordinierungszentren, die nach Vorlage am 12. September 2018 unter österreichischem Vorsitz aufgenommen wurden. Unter rumänischem Vorsitz konnten ein Mandat erreicht werden und zwei Triloge mit dem Europäischen Parlament (EP) stattfinden. Jedoch konnten die Verhandlungen vor Ende der Legislaturperiode des EP nicht mehr abgeschlossen werden. Die HWP Cyber arbeitet seither an einer neuen Fassung des Verhandlungsmandats. Zum näheren Inhalt des Verordnungsvorschlags siehe Kapitel 2.1.7.

Im Bereich der Cyberdiplomatie stand die Weiterentwicklung der gemeinsamen diplomatischen Reaktion der EU auf böswillige Cyberaktivitäten „Cyber Diplomacy Toolbox“ im Vordergrund. Hierzu fand Ende November eine Table-Top-Exercise „CYBER-DIPLO TTX 19“

statt. Das Erreichen einer gemeinsamen EU-Position hinsichtlich internationaler Entwicklungen von Cybersicherheit wie beispielsweise im VN-Kontext oder hinsichtlich des Cybersanktionenregimes, konkrete Schritte im Rahmen der Cyber Diplomacy Toolbox, bzw. Diskussionen zur Attribuierung, standen im Fokus.

Ferner wurden die von der HWP Cyber vorbereiteten „Schlussfolgerungen des Rates über Cybersicherheitskapazitäten und deren Aufbau in der EU" vom Rat (Allgemeine Angelegenheiten) am 19. März 2019 angenommen.

### 2.1.2 NIS-Kooperationsgruppe

Die durch die NIS-Richtlinie eingesetzte NIS-Kooperationsgruppe dient der Unterstützung und Erleichterung der strategischen Zusammenarbeit sowie des Informationsaustausches zwischen den Mitgliedstaaten. Die NIS-Kooperationsgruppe setzt sich aus Vertretern der Mitgliedstaaten, der EU-Kommission und der ENISA zusammen, wobei der Vorsitz von der jeweiligen Ratspräsidentschaft gehalten wird.

Die NIS-Kooperationsgruppe nimmt ihre Aktivitäten auf der Grundlage von zweijährigen Arbeitsprogrammen wahr. Nach wie vor bilden hierbei Aktivitäten im Zusammenhang mit der Umsetzung der NIS-Richtlinie einen Schwerpunkt. Doch setzte sich auch 2019 der Trend fort, wonach die NIS-Kooperationsgruppe umfassendere Fragen der Cybersicherheitspolitik behandelt. So wurde bereits im Jahr 2018 der „Work Stream on Cyber Security of Election Technology" eingerichtet, dessen Ergebnis von der NIS-Kooperationsgruppe im Juli 2018 angenommen wurde (CG Publication 03/2018 – Compendium on cyber security of election technology). Die flexible Struktur der NIS-Kooperationsgruppe erlaubte es, dass neben „NIS- bzw. Cyberbehörden" auch andere inländische Behörden teilnehmen konnten, um sich zusammen mit den NIS- bzw. Cyberbehörden dieses Themas anzunehmen. Am 26. März 2019 veröffentlichte die EU-Kommission die Empfehlung zu Cybersicherheit der 5G-Netze, welche der NIS-Kooperationsgruppe die maßgebliche Operationalisierungsrolle zuwies.

Zu den Hauptergebnissen der NIS-Kooperationsgruppe gehören weiterhin unverbindliche Leitlinien für die Mitgliedstaaten. So wurden auch im Jahr 2019 Referenzdokumente von der NIS-Kooperationsgruppe erarbeitet und veröffentlicht. Einen Schwerpunkt bildete hierbei die Arbeit zum Thema Cybersicherheit von 5G-Netzen. Daneben wurde ein umfangreiches Referenzdokument über die Umsetzung der NIS-Richtlinie im Sektor Energie angenommen. Bei den veröffentlichten Referenzdokumenten handelt es sich konkret um:

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

Die NIS-Kooperationsgruppe beschäftigt sich zunehmend mit umfassenderen Fragen der Cybersicherheitspolitik, z.B. zum Thema Cybersicherheit von 5G-Netzen.

Die NIS-Kooperationsgruppe traf sich im Jahr 2019 zu vier Plenarsitzungen und zu mehr als 16 Sitzungen im Rahmen von Work Streams. Es wurden 2019 ein Work Stream über den Sektor Digitale Infrastruktur sowie ein weiterer über die Sicherheit von 5G-Netzen eröffnet. In Fortsetzung der unter österreichischem Vorsitz erstmals verwirklichten Idee fanden die strategisch orientierte NIS-Kooperationsgruppe und das operativ tätige CSIRTs Netzwerk im Rahmen der Plenarsitzungen zu weiteren Back-to-Back-Meetings zusammen, um einen Austausch über die wichtigsten Themen der beiden Gruppen zu ermöglichen.

### 2.1.3 Horizontal Working Party on Enhancing Resilience and Countering HybridThreats

Die Horizontal Working Party on Enhancing Resilience and Countering HybridThreats oder Horizontale Arbeitsgruppe zur Stärkung der Resilienz und zur Abwehr hybrider Bedrohungen (HWP ERCHT) ist 2019 aus einer „Friends of Presidency Group“ entstanden.

Ziel der Arbeitsgruppe ist es, einen horizontalen Überblick über Fragen im Zusammenhang mit hybriden Bedrohungen zu bieten, um die Kohärenz und die Zusammenarbeit zwischen der EU und ihren Mitgliedstaaten zu unterstützen. Der Fokus der Arbeit liegt

auf der Abwehr von hybriden Bedrohungen, der Stärkung der Resilienz von Staaten und der Gesellschaft gegenüber solcher Bedrohungen, der Verbesserung der strategischen Kommunikation und der Bekämpfung von Desinformation.

Am 10. Dezember 2019 nahm der Rat der EU Schlussfolgerungen zu „zusätzlichen Anstrengungen zur Stärkung der Resilienz und zur Abwehr hybrider Bedrohungen“ an. In diesen Schlussfolgerungen werden im Kontext der Umsetzung der neuen Strategischen Agenda für den Zeitraum 2019–2024 Prioritäten festgelegt. Hierzu zählt unter anderem der Schutz der Gesellschaften, der Bürgerinnen und Bürger und der Freiheiten sowie der Sicherheit der Union vor hybriden Bedrohungen. Erreicht werden soll dies durch die Förderung eines umfassenden Sicherheitsansatzes mit besserer Koordinierung, mehr Mitteln und besseren technischen Kapazitäten. Der Ansatz soll auf der umfangreichen Arbeit aufbauen, die in verschiedenen Politikbereichen bereits geleistet wurde, unter anderem auch im Rahmen der sicherheits- und verteidigungspolitischen Zusammenarbeit. Ferner nahm der Rat zur Kenntnis, dass böswillige Cyberaktivitäten Teil einer hybriden Bedrohung sein können und unterstrich die Bedeutung der NIS-Richtlinie.

### 2.1.4 EU-Zertifizierungsrahmen (Cybersecurity Act)

Der Cybersecurity Act trat am 27. Juni 2019 in Kraft.

Mit dem Inkrafttreten des Cybersecurity Act am 27. Juni 2019 wurde unter anderem ein Europäischer Zertifizierungsrahmen für die Cybersicherheit geschaffen. Der Europäische Zertifizierungsrahmen für die Cybersicherheit legt einen Mechanismus fest, mit dem europäische Schemata für die Cybersicherheitszertifizierung geschaffen werden. In weiterer Folge soll dieser bescheinigen, dass nach einem solchen Schema bewertete IKT-Produkte, -Dienste und -Prozesse den festgelegten Sicherheitsanforderungen genügen. Diese sollen es erlauben, die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von gespeicherten, übermittelten oder verarbeiteten Daten, Funktionen oder Diensten, die von diesen IKT-Produkten, -Diensten und -Prozessen angeboten oder über diese zugänglich gemacht werden, während deren gesamten Lebenszyklus zu schützen.

In Zusammenarbeit mit den Mitgliedstaaten und Stakeholdern arbeitet die EU-Kommission an dem sogenannten fortlaufenden Arbeitsprogramm der Union für die Europäische Cybersicherheitszertifizierung, in dessen Rahmen die strategischen Prioritäten für künftige europäische Schemata für die Cybersicherheitszertifizierung festgelegt werden sollen.

Die Europäische Gruppe für die Cybersicherheitszertifizierung (European Cybersecurity Certification Group – ECCG) wurde durch den Cybersecurity Act eingesetzt und nahm die Arbeit mit ihrer ersten formellen Sitzung am 18. September 2019 auf. Die ECCG setzt sich aus Vertretern der nationalen Behörden für die Cybersicherheitszertifizierung oder Vertretern anderer einschlägiger nationaler Behörden zusammen. Österreich wird in der ECCG durch den CIO des Bundes (BMDW) und das strategische NIS-Büro (BKA) vertreten.

### 2.1.5 Cybersicherheit von 5G-Netzen

Die Sicherheit der als „fünfte Generation des Mobilfunknetzes“ (5G) betitelten Technologie stand 2019 im Fokus der Aufmerksamkeit von Cybersicherheitsbehörden.

Das EU-Parlament forderte die EU-Kommission und die Mitgliedstaaten in der Entschließung vom 12. März 2019 zu Sicherheitsbedrohungen im Zusammenhang mit der zunehmenden technologischen Präsenz Chinas in der EU auf, Maßnahmen auf Unionsebene zu ergreifen. Ferner wird in der Strategischen Perspektive EU-China (Gemeinsame Mitteilung der Hohen Vertreterin der Union für Außen- und Sicherheitspolitik vom 12. März 2019) betont, dass ein gemeinsamer Ansatz der EU hinsichtlich der Sicherheit von 5G-Netzen erforderlich ist, um einen Schutz vor potenziell schwerwiegenden Auswirkungen auf die Sicherheit kritischer digitaler Infrastrukturen zu gewährleisten. Der Europäische Rat sprach sich schließlich in seinen Schlussfolgerungen vom 22. März 2019 dafür aus, dass die EU-Kommission Empfehlungen für ein abgestimmtes Vorgehen bei der Sicherheit von 5G-Netzen geben solle.

In diesem Sinne veröffentlichte die EU-Kommission am 26. März 2019 eine Empfehlung über die Cybersicherheit von 5G-Netzen, welche insbesondere folgende Maßnahmen empfiehlt:

- die Durchführung einer nationalen Risikoanalyse mit dem Fokus auf 5G-Netzwerke;
- die Überprüfung der gesetzten nationalen Maßnahmen;
- eine verstärkte Zusammenarbeit auf EU-Ebene und die Durchführung einer EU-weit koordinierten Risikoanalyse und
- die Schaffung eines gemeinsamen Instrumentariums von Maßnahmen zur Risikominimierung.

Im Bereich der Cybersicherheit wurde zum Thema 5G erstmals eine koordinierte europäische Risikobewertung, die auf Risiko-analysen aller Mitgliedstaaten aufbaut, durchgeführt.

Als erster Schritt wurde, die Empfehlung umsetzend, eine nationale Risikoanalyse hinsichtlich der möglichen Gefahren, die sich durch den neuen Standard ergeben, erstellt. Zu diesem Zweck wurde die bereits bestehende nationale Risikoanalyse hinsichtlich der Risiken, die sich aus dem neuen Standard ergeben, aktualisiert. Zur Unterstützung der Mitgliedstaaten wurde ein eigener Work Stream im Rahmen der NIS-Kooperationsgruppe ins Leben gerufen. Die Nationale Risikoanalyse wurde fristgerecht im Juli 2019 an die EK und an ENISA übermittelt.

Bereits am 9. Oktober 2019 erschien die koordinierte europäische Risikobewertung (CG Publication 02/2019 – Risk assessment of 5G networks) mit der Prämisse, die Basis einer zukünftigen Toolbox zu bilden. In dieser koordinierten Risikobewertung wurde ein europäischer Überblick, basierend auf den gemeinsamen Elementen der einzelnen Risikoanalysen der Mitgliedstaaten, geschaffen. Identifiziert wurden dabei die größten Gefahren für 5G-Netze, die wichtigsten Bedrohungsakteure, die wichtigsten Assets und ihr Sensibilitätsgrad, die Hauptschwachstellen und Hauptrisiken und die damit verbundenen Szenarien.

Im November 2019 wurde die „ENISA Threat Landscape for 5G networks“ veröffentlicht, die einen tiefgehenden Einblick in die Gefahren und Herausforderungen bietet, die im Zusammenhang mit 5G-Netzen zu bewältigen sein werden. Dabei wurde vor allem ein technischer Überblick über die 5G-Architektur, die Identifizierung wichtiger Assets

(Asset-Diagramm), die Bewertung von 5G-Bedrohungen (Bedrohungstaxonomie), die Identifizierung der Gefährdung von Vermögenswerten (Bedrohungs-Asset-Mapping) und eine erste Bewertung der möglichen Motive der Bedrohungsagenten gegeben.

Der Rat der EU nahm am 3. Dezember 2019 Schlussfolgerungen „zur Bedeutung von 5G für die europäische Wirtschaft und zur Notwendigkeit der Begrenzung der Sicherheitsrisiken im Zusammenhang mit 5G" an, denen zufolge die EU und die Mitgliedstaaten unter anderem ein besonderes Augenmerk auf die Förderung der Cybersicherheit von 5G-Netzen richten müssen.

### 2.1.6 Cyberdiplomatie

Die EU nahm 2019 ein Cybersanktionenregime an.

Bei der Cyber Diplomacy Toolbox (Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten) wurden 2019 wichtige Erweiterungen zur praktischen Umsetzung vorgenommen. Im Mai 2019 nahm der Rat ein Cybersanktionenregime an, mit dem zukünftig gegen Einzelpersonen und Entitäten (nicht Staaten) mit Kontoeinfrierungen und Reisebeschränkungen vorgegangen werden kann. Im Bereich Cybersicherheit mangelt es an internationalen Verträgen oder Organisationen, auf welchen man aufbauen könnte – von daher war hier Grundlagenarbeit zu leisten. Ein weiteres Schwergewicht der Arbeiten lag auf der Erarbeitung von Möglichkeiten der Zurechnung von Cyberangriffen und einer koordinierten europäischen Vorgangsweise bei schweren Vorfällen auf Grundlage der Cyber Diplomacy Toolbox. Attribuierung ist grundsätzlich eine souveräne, politische Entscheidung jedes Mitgliedstaates. Eine Zurechnung ist nicht für alle in der Cyber Diplomacy Toolbox enthaltenen Maßnahmen eine Voraussetzung. Ein Teil der Maßnahmen, mit denen die EU auf Cyberangriffe reagieren kann, sind öffentlich, z. B. Ratsschlussfolgerungen oder Erklärungen.

Im Bereich Cybersicherheit mangelt es an internationalen Verträgen.

Ein wichtiger Teil der Cyberdiplomatie auf EU-Ebene umfasst die Erarbeitung gemeinsamer Positionen und Strategien zu Cyberthemen auf internationaler Ebene, vor allem bei den Vereinten Nationen, wo 2019 hiezu zwei parallele Normensetzungsprozesse begonnen haben (siehe Kapitel 2.2).

### 2.1.7 Netz nationaler Koordinierungszentren und Europäisches Kompetenzzentrum

Die EU-Kommission legte am 12. September 2018 den Entwurf für eine Verordnung zur Einrichtung des Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung und des Netzes nationaler Koordinierungszentren zur Einrichtung der Kompetenzgemeinschaft für Cybersicherheit[6] vor. Der Vorschlag erging als eine konkrete Maßnahme zur Umsetzung der gemeinsamen Mitteilung der EU-Kommission und der Hohen Vertreterin vom September 2017 für Maßnahmen zur Erhöhung der Abwehrfähigkeit, der Abschreckung und der Abwehr gegen Cyberattacken und zur wirksamen Erhöhung der Cybersicherheit in der EU.

Das Netz von nationalen Koordinierungszentren sowie das Europäische Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung unterstützt bereits bestehende EU-Initiativen und baut neue europäische Kapazitäten im Cyberbereich auf.

Mit einem Europäischen Kompetenzzentrum soll die Verwendung der für Cybersicherheit bestimmten Mittel für die Jahre 2021–2027 aus den Programmen „Digitales Europa“ und „Horizont Europa“ koordiniert werden. Das Zentrum wird das Netz nationaler Koordinierungszentren und die Kompetenzgemeinschaft unterstützen und Forschung und Innovation im Bereich Cybersicherheit vorantreiben. Ferner wird es gemeinsame Investitionen der EU, der Mitgliedstaaten und der Industrie organisieren.

Bei dem Netz nationaler Koordinierungszentren soll jeder Mitgliedstaat ein nationales Koordinierungszentrum benennen, das sich für die Entwicklung neuer Cybersicherheitskapazitäten und den weiteren Kompetenzausbau einsetzen wird. Das Netz wird zur Ermittlung und Unterstützung der relevantesten Cybersicherheitsprojekte in den Mitgliedstaaten beitragen.

---

6 Siehe COM (2018) 613

Die Kompetenzgemeinschaft wiederum wird eine große, offene und vielseitige Gruppe von Interessensträgern im Bereich Cybersicherheit aus der Wissenschaft sowie dem privaten und dem öffentlichen Sektor, einschließlich Zivil- und Militärbehörden schaffen.

Zum Verhandlungsstand siehe Kapitel 2.1.1.

### 2.1.8 Aktionsplan gegen Desinformation

Zunahme gezielter Desinformations-kampagnen gegen die EU

Das Recht auf freie Meinungsäußerung ist ein zentraler Wert der EU. Für offene demokratische Gesellschaften ist entscheidend, dass Bürgerinnen und Bürger Zugang zu qualitätsgesicherten und überprüfbaren Informationen haben und sich somit zu verschiedenen politischen Themen eine Meinung bilden können. Derzeit können sich EU-Bürgerinnen und Bürger an 25 öffentlichen Debatten zu politischen Prozessen beteiligen, sich hierzu informieren und ihren Willen zum Ausdruck zu bringen. Die bewusste, umfassende und systematische Verbreitung von Desinformation kann zu Bedrohungen für die demokratischen Prozesse sowie für öffentliche Güter wie Volksgesundheit, Umwelt und Sicherheit führen.

Im Vorfeld der Wahlen zum Europäischen Parlament (EP) wurde mit einer Zunahme ständiger gezielter Desinformationskampagnen gegen die EU, ihre Organe und ihre Politik gerechnet. Die schnelle Veränderung der eingesetzten Instrumente und Techniken macht eine ebenso schnelle Weiterentwicklung der Reaktion darauf erforderlich. Insgesamt setzen staatliche Akteure zunehmend Desinformationsstrategien ein, um gesellschaftliche Debatten zu beeinflussen, Spaltungen herbeizuführen und in die demokratischen Entscheidungsfindungen einzugreifen.

Aus diesem Grund nahm das EK-Kollegium am 5. Dezember 2018 einen Aktionsplan gegen Desinformation an. Der Aktionsplan sieht verschiedene Maßnahmen in den folgenden vier Bereichen vor:

- Ausbau der Fähigkeiten der Organe der Union Desinformation zu erkennen, zu untersuchen und zu enthüllen;
- koordinierte und gemeinsame Maßnahmen gegen Desinformation;
- Mobilisierung des Privatsektors bei der Bekämpfung von Desinformation und
- Sensibilisierung der Gesellschaft und Ausbau ihrer Widerstandsfähigkeit.

Die Maßnahmen zu den Bereichen zeigten Wirkung: In der gemeinsamen Mitteilung der Europäischen Kommission und der Hohen Vertreterin der Europäischen Union für Außen- und Sicherheitspolitik, Federica Mogherini, vom 14. Juni 2019 über die Umsetzung des Aktionsplanes wurde festgestellt, dass Versuche, die Wahlen zum EP zu beeinflussen, aufgrund des koordinierten Vorgehens verhindert werden konnten.

## 2.2 Vereinte Nationen (VN)

Im 1. Komitee (Abrüstung und internationale Sicherheit) der Generalversammlung der Vereinten Nationen (VN-GV) wurde Cybersicherheit erstmalig 1998 behandelt. Seitdem beschäftigen sich die VN-GV mit zunehmender Intensität mit der Thematik. Die Staaten verfolgen in diesem Rahmen das Ziel, die aus der Nutzung des Cyberraumes entstehenden Risiken für die internationale Stabilität zu minimieren. Im Zuge der Verhandlungen gelang es, vier prioritäre Handlungsbereiche zu identifizieren, die für die Etablierung und Durchsetzung eines internationalen Normengerüstes für den Cyberraum besondere Relevanz besitzen:

- Völkerrecht,
- nicht-bindende Normen verantwortungsvollen staatlichen Handelns,
- Vertrauensbildende Maßnahmen (VBM) und
- der Aufbau von Kapazitäten.

### Zwei eigenständige Verhandlungsformate durch die VN-GV zum Thema Cybersicherheit eingerichtet

2019 gelangten die Cybersicherheitsprozesse im Kontext der VN-GV in eine neue Phase. Der lange Zeit prekäre politische Konsens zwischen „westlichen" Staaten einerseits, Russland und einigen gleichgesinnten Staaten andererseits, zerfiel 2018, weshalb es zur Einrichtung zweier eigenständiger Verhandlungsformate durch die VN-GV kam. Dies ist einerseits eine Group of Governmental Experts (GGE) sowie eine Open-ended Working Group (OEWG). Die GGE wird bereits zum sechsten Mal eingesetzt und ist mit 25 nominierten Expertinnen und Experten besetzt, während die OEWG erstmalig eingerichtet wurde und allen Mitgliedstaaten offen steht. Sowohl die GGE als auch die OEWG hielten 2019 ihre ersten Sitzungen ab. Die Staaten waren erstmalig aufgefordert, substantiell Position gegenüber den beiden Gruppen zu beziehen. Österreich unterstützte die Einrichtung der GGE und nahm aktiv an den Diskussionen im Rahmen der OEWG teil. Für die weitere Arbeit wird es relevant sein, ob und in welchem Ausmaß sich zwischen GGE und OEWG eine effektive Aufgabenteilung etabliert.

Die inhaltlichen Differenzen zwischen den Staaten, vor allem die Frage nach der genauen Anwendbarkeit des Völkerrechts, blieben auch 2019 bestehen.

Neben der VN-GV befassen sich weitere VN-Organe mit dem Erhalt der Stabilität der Cybersicherheit. Zentrales Referenzdokument dafür bildet die 2018 verabschiedete Abrüstungsagenda des Generalsekretärs der Vereinten Nationen (VN). Im dazugehörigen Implementierungsplan sind zwei Aktionsbereiche der Cybersicherheit gewidmet; einer bezieht sich auf die friedliche Konfliktbeilegung, der andere auf die Stärkung sich entwickelnder Normen im Cyberraum. 2019 wurden die dahingehenden Implementierungsmaßnahmen durch die Staaten fortgesetzt.

## Künstliche Intelligenz als Thema der 41. Tagung des Menschenrechtsrats

Im Rahmen der 41. Tagung des VN-Menschenrechtsrats im Juni 2019 brachte Österreich als einer der Hauptsponsoren (neben Südkorea, Brasilien, Dänemark, Marokko und Singapur) erstmals eine Resolution zum Thema „Neue und aufkommende Technologien und Menschenrechte“ (A/HRC/Res/41/11) ein, die im Konsens angenommen werden konnte. Darin wird der beratende Ausschuss mit der Ausarbeitung einer Studie zum Thema beauftragt – dies mit dem Ziel, im VN-MRR einen breiten Diskurs über menschenrechtliche Herausforderungen und Potentiale im Zusammenhang mit der rasanten Entwicklung digitaler Technologien (insbesondere im Bereich der künstlichen Intelligenz (KI) anzustoßen.

Die von Österreich im September 2019 im Rahmen der 42. Sitzung des VN-MRR erneut eingebrachte Resolution zum Recht auf Privatsphäre im digitalen Zeitalter (A/HRC/Res/42/15) konnte wieder im Konsens angenommen werden. Diese Resolution legte den Schwerpunkt auf das Thema KI und Privatsphäre und der Ansicht, dass ohne adäquate Schutzmechanismen bei der Entwicklung und Nutzung von KI, Risiken für den Menschenrechtsschutz entstehen würden. Auch werde das Recht auf Privatsphäre gefährdet, wenn die für KI notwendigen Datenmengen unreguliert für Gesichtserkennung, Scoring oder Profiling von Individuen eingesetzt würden.

Der Bericht des High-level Panel on Digital Cooperation (HLPDC) ist ein Gremium für digitale Zusammenarbeit, welches im Jahr 2018 einberufen wurde, um Empfehlungen zur Stärkung der Zusammenarbeit zwischen Regierungen, dem Privatsektor, der Zivilgesellschaft, internationalen Organisationen, der Wissenschaft, der technischen Gemeinschaft und anderen relevanten Stakeholdern im digitalen Raum vorzulegen.

In der Empfehlung Nummer 4 „Vertrauen, Sicherheit und Stabilität", wird die Entwicklung eines „Global Commitment on Digital Trust and Security" vorgesehen. Eine Kerngruppe interessierter Stakeholder soll Möglichkeiten für das Follow-Up dieser Empfehlung vorschlagen. Daraufhin gründeten Microsoft, Hewlett-Packard und Mastercard im Oktober 2019 das „Cyber Peace Institute" in Genf, mit dem Ziel, die Stabilität des Cyberspace zu verbessern, indem sie nichtstaatliche Opfer von Cyberangriffen unterstützt, die Verantwortungslücke schließt und internationales Recht und Normen vorantreibt, die verantwortungsvolles Verhalten im Cyberspace fördern. „Safety, Security, Stability & Resilience" war eines der drei Themenschwerpunkte des heurigen Internet Governance Forums (IGF), welches von 25. bis 29. November 2019 in Berlin stattfand. Im Mittelpunkt der Diskussion standen Normen für den Bereich Cybersicherheit, die sich vermehrt auf die Rolle des privaten Sektors, als auf das Verhalten von Staaten im Cyberspace konzentrierte.

Im Kontext der VN in Genf arbeitet die Internationale Fernmeldeunion (ITU) weiter an Verbesserungen ihrer „Global Cybersecurity Agenda", die darauf abzielt, das Vertrauen und die Sicherheit in der Informationsgesellschaft zu stärken, aber von westlichen Staaten teilweise sehr kritisch gesehen wird.

Cyberkriminalität hat sich rasch zu einer globalen und äußerst profitablen Verbrechenssparte entwickelt. Das VN-Büro für Drogen- und Verbrechensbekämpfung (UNODC) in Wien stellt weiterhin einen unverzichtbaren Bestandteil in der effektiven weltweiten

Bekämpfung von Cyberkriminalität dar. Die 2013 veröffentlichte umfassende Studie[7] konzentriert sich dabei in seiner Hilfeleistung für betroffene Mitgliedstaaten auf folgende drei Schwerpunkte:

- Verbesserung der Ermittlung, Strafverfolgung und Beurteilung von Cyberkriminalität, vor allem im Bereich sexueller Ausbeutung und Kindesmissbrauch im Internet;
- Förderung eines integrierten und regierungsweiten Ansatzes, einschließlich nationaler Koordinierung, Datenerhebung und wirksamer rechtlicher Rahmenbedingungen zur nachhaltigen Bekämpfung und effektiven Abschreckung von Cyberkriminalität;
- Stärkung der nationalen und internationalen Kooperation zwischen Regierungen, Strafverfolgungsbehörden und der Privatwirtschaft, sowie Stärkung des öffentlichen Bewusstseins.

Auf operativer Ebene setzt die UNODC Cyber Crime Abteilung neue Initiativen im Bereich der Schul- und Universitätsbildung um. In diesem Zusammenhang zeigt UNODC Interesse an dem von Internet Service Providers Austria (ISPA) erstellten Comic-Buch „Der Online-Zoo“, das ebenso im Schulunterricht eingesetzt wird.

UNODC in Wien unverzichtbarer Bestandteil in der weltweiten Bekämpfung von Cyberkriminalität

Die 2010 im Bereich Cyberkriminalität eingerichtete Intergouvernementale Expertengruppe (IEG) trat im März 2019 zum insgesamt fünften Mal zusammen. Die Streitfrage, ob eine neue Cyber-Konvention ausgehandelt oder die Budapest-Konvention ausgeweitet werden soll, konnte nicht gelöst werden. Final wurde der Beschluss gefasst, die Diskussionen der IEG über grundlegende Themen und Entwicklungen betreffend Cyberverbrechen

7 http://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf

fortzuführen und sich über nationale Gesetzgebung, Best Practice Beispiele, technische Hilfe und internationale Zusammenarbeit auszutauschen.[8]

2019 lancierte Russland eine Resolution zu Cybercrime in der VN-Generalversammlung, die die Schaffung einer eigenen Arbeitsgruppe zur Ausarbeitung eines neuen völkerrechtlichen Vertrags zu Cybercrime vorsieht. Cyberkriminalität war auch ein wichtiges Thema der 28. Tagung der Kommission für Verbrechensverhütung und Strafrechtspflege (CCPCJ)[9] im Mai 2019. Österreich legte dabei gemeinsam mit Kanada und Kolumbien eine Resolution mit dem Schwerpunkt Cybercrime vor, die im Konsens angenommen werden konnte.

Die Internationale Atomenergie-Organisation (IAEO) behandelte das Thema Cybersicherheit von Kernanlagen und Kernmaterial im Jahr 2019 weiterhin prioritär. Für ein IAEO-Forschungsprojekt errichtete das Austrian Institute of Technology (AIT) eine spezielle virtuelle IT-Trainings- und Simulationsplattform, die auf hochsensible industrielle Steuerungssysteme ausgelegt ist.

Unterstützt wird die Umsetzung der Abrüstungsagenda sowie die Arbeit der United Nations Group of Governmental Experts (GGE) und der Open-ended Working Group (OEWG) durch das Büro der VN für Abrüstungsfragen (United Nations Office for Disarmament Affairs – UNODA). Das Institut der VN für Abrüstungsforschung (United Nations Institute for Disarmament Research – UNIDIR) trägt mit der Veröffentlichung wissenschaftlicher Publikationen zu den internationalen Cybersicherheitsdiskussionen bei. Darüber hinaus veranstaltet UNIDIR jährlich eine Konferenz zur Cyberstabilität.

---

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

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

## 2.3 NATO

Als militärisch-politisches Bündnis mit einem starken Fokus auf Sicherheit und gemeinsame Verteidigung befasst sich die NATO spätestens seit der Verabschiedung ihres geltenden strategischen Konzepts von 2010 und der Anerkennung des virtuellen Raumes als eine Domäne im Jahr 2016 sowie des Weltraums als eine weitere Domäne im Jahr 2019 mit den Verteidigungsaspekten von Cybersicherheit. Österreich kooperiert hier als Partnerland eng mit der NATO und beteiligt sich auf technischer Ebene an Sitzungen des NATO-C3 (Consultation, Command and Control) Boards sowie jenen im Zusammenhang mit einschlägigen Smart Defence-Projekten.

Seit 2013 kooperiert das BMLV mit der NATO durch die Entsendung eines Offiziers an das Center of Excellence in Tallinn. Ziel der Zusammenarbeit ist die Steigerung der Fähigkeiten zur Cyberverteidigung. Das dadurch zugängliche Kursangebot wird durch die österreichischen Ressorts umfassend in Anspruch genommen und die angebotenen Übungen zur Überprüfung der nationalen Fähigkeiten im internationalen Vergleich genutzt. Ergänzend stellt Österreich auch einen Mitarbeiter des BMLV für das „European Centre of Excellence for Countering Hybrid Threats“ in Helsinki, an dem sich auch die NATO beteiligt, ab.

## 2.4 Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE)

Als größte regionale Sicherheitsorganisation der Welt befindet sich die Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) im Bereich der internationalen Cybersicherheitspolitik in einer Doppelrolle. Einerseits unterstützt sie die Umsetzung der auf Ebene der VN getroffenen Beschlüsse, insbesondere den Kapazitätenaufbau,

durch ihre exekutiven Strukturen und das Netz an Feldmissionen. Andererseits übernahm die OSZE bei der Ausarbeitung Vertrauensbildender Maßnahmen (VBM) im Cyberraum eine Vorreiterrolle. Die Annahme der 16 VBM mit dem Ziel, durch den Austausch von Informationen, die Etablierung von Kommunikationskanälen und den Aufbau von Kapazitäten zwischenstaatliche Spannungen, die aus der Nutzung des Cyberraumes entstehen, zwischen den teilnehmenden Staaten der OSZE zu minimieren, stellt global gesehen den ambitioniertesten Versuch zur Steigerung der internationalen Kooperation im Feld der Cybersicherheit außerhalb der VN dar.

Für die Weiterentwicklung und Implementierung der VBM vorrangig zuständig ist die Informelle Arbeitsgruppe zu Cyber (Cyber-IWG). Das der OSZE zugrundeliegende Sicherheitsverständnis leitet auch die Arbeit der Cyber-IWG: Die Thematik wird unter Berücksichtigung politisch-militärischer, wirtschaftlicher und menschenrechtlicher Aspekte behandelt. 2019 setzte die Cyber-IWG ihre Aktivitäten im Rahmen der „adopt a CBM (Confidence Building Measure)"-Initiative fort, im Zuge derer Staaten oder Staatengruppen die Umsetzung der VBM vorantreiben. Wichtige Schritte in diesem Zusammenhang sind die Einrichtung eines Netzwerkes von Kontaktpersonen, regelmäßige Überprüfungen der Kommunikationskanäle sowie die Sicherstellung einer effektiven Zusammenarbeit im Falle einer Cyberkrise.

Neben der institutionalisierten Behandlung der Thematik durch die Cyber-IWG setzen seit einigen Jahren die jeweiligen Vorsitzstaaten der OSZE die Cybersicherheit auf ihre Vorsitzagenda. So hat es sich etabliert, dass regelmäßig Cybersicherheitskonferenzen durch den jeweiligen OSZE-Vorsitz abgehalten werden. 2019 fand diese unter slowakischem Vorsitz statt. Die Konferenz thematisierte aktuelle Entwicklungen im Bereich der internationalen Cybersicherheitspolitik und bot erstmalig Gelegenheit zum Austausch zwischen der OSZE und der auf Ebene der VN eingerichteten GGE.

## 2.5 Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD)

Die „Working Party on Security in the Digital Economy“ (WPSDE) ist eine von vier Arbeitsgruppen unter dem „Committee on Digital Economy“ der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD). Ziel ist die Entwicklung evidenzbasierter Richtlinien für digitale Sicherheit und praktischer Leitlinien, um Vertrauen in die digitale Transformation aufzubauen und die Widerstandsfähigkeit, Kontinuität und Sicherheit kritischer Aktivitäten zu unterstützen. Der Schwerpunkt liegt auf dem Management digitaler Sicherheitsrisiken für wirtschaftliche und soziale Aktivitäten und auf der Verbesserung von Sicherheit bei digitalen Produkten und Dienstleistungen. Dabei wird auf die Expertise aus OECD- und Partnerländern, Wirtschaft, Zivilgesellschaft und der technischen Internet-Community gesetzt, um Ansätze für die Zukunft zu erarbeiten. Die WPSDE trifft sich zweimal im Jahr in Paris und organisiert Workshops und Konferenzen, die in verschiedenen Gastgeberländern stattfinden. In Österreich nimmt das BKA die inhaltliche Koordination für diese Arbeitsgruppe wahr.

Ende 2019 wurde die „OECD Recommendation on Digital Security of Critical Activities“ verabschiedet, die eine Empfehlung aus 2008 ersetzt. Anstatt eines rein technischen wird ein wirtschaftlicher und sozialer Risikomanagementansatz für digitale Sicherheit verfolgt. Darüber hinaus beschäftigte sich die Arbeitsgruppe 2019 mit der Förderung eines verantwortungsvollen Managements und der Offenlegung von Sicherheitslücken sowie der Verbesserung der digitalen Sicherheit von Produkten. Diesbezüglich wird beispielsweise eine Liste der global existierenden IoT-Zertifizierungen erarbeitet.

## 2.6 Europarat

Den Kern der Aktivitäten des Europarates im Bereich Cybersicherheit bildet die Konvention zu Cyberkriminalität „Budapest-Konvention“ aus 2001, die mit aktuell 64 Ratifikationen (darunter 2019 San Marino, Ghana, Peru) eine Bedeutung weit über Europa hinaus erlangt hat. Hauptzweck ist die Verfolgung einer gemeinsamen Strafrechtspolitik zum Schutz der Gesellschaft vor Cyberkriminalität, insbesondere durch entsprechende gesetzliche Regelungen und die Förderung internationaler Zusammenarbeit.

Die Umsetzung der Konvention wird über kapazitätsbildende Projekte unterstützt, die durch ein Cybercrime-Programmbüro des Europarates in Bukarest (C-PROC) koordiniert werden, wie z. B. Beratung bei einschlägigen Legislativmaßnahmen, Hilfe bei der Ausbildung von Richtern und Staatsanwälten, ferner das „iProceeds“ in Südosteuropa mit Fokus auf Erträgen aus Cyberkriminalität, das „Cyber South“ in Nordafrika sowie das weltweit agierende und in Zusammenarbeit mit Interpol durchgeführte Projekt „GLACY+“. Im Jahr 2019 wurden diese Projekte durch das „Cyber East“-Projekt ergänzt, das finanziert durch das Europäische Nachbarschaftsinstrument in der Östlichen Partnerschaft Unterstützung leistet.

Derzeit laufen die Verhandlungen für ein Zweites Zusatzprotokoll zur Budapest-Konvention, das sich mit internationaler Rechtshilfe und dem damit verbundenen grenzüberschreitenden Zugang zu Daten befassen wird. Eine enge Zusammenarbeit mit der EU, im Hinblick auf dort derzeit in Entwicklung befindliche relevante Dokumente, ist vorgesehen. Im Juli 2019 wurde außerdem ein Leitfaden zur Budapest-Konvention „Guidance Notes“ zur Thematik „election interference“ erarbeitet. Derartige Leitfäden haben das Ziel, die effektive Anwendung und die Umsetzung der Konvention zu erleichtern.

Zu den weiteren Instrumenten des Europarats zählt die 2018 modernisierte Datenschutzkonvention des Europarates (ETS 108) sowie die Lanzarote-Konvention zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch, die einen wesentlichen Beitrag zum Online-Schutz von Kindern leistet. Die sogenannte „Octopus-Konferenz" befasste sich 2019 mit Beweismitteln im Cyberspace und der Arbeit am Zweiten Zusatzprotokoll zur Budapest-Konvention.

## 2.7 Computer Security Incident Response Teams-Netzwerk (CSIRTs-Netzwerk)

Im Sommer 2016 wurde durch das EP und den Rat der EU die EU-Richtlinie 2016/1148 (NIS-Richtlinie) erlassen und durch selbige auch das CSIRTs-Netzwerk (CNW) geschaffen, sowie deren Tätigkeitsbereich festgelegt. Das CSIRTs-Netzwerk setzt sich aus Vertretern der CSIRTs der Mitgliedstaaten (gemäß Artikel 9 der NIS-Richtlinie) und des CERT-EU zusammen. Die Europäische Kommission (EK) nimmt als Beobachter am CSIRTs-Netzwerk teil. Die ENISA führt die Sekretariatsgeschäfte und unterstützt aktiv die Zusammenarbeit zwischen den CSIRTs. Die Teilnehmer Österreichs im CSIRTs--Network sind das GovCERT Austria, CERT.at und das CERT der Energiewirtschaft (Austrian Energy CERT – AEC). Das Netzwerk arbeitet primär online: Die Kommunikation erfolgt über ein Webportal, Mailinglisten und ein Instant Messaging System. Bei den Treffen des CNW findet ein Informationsaustausch zu den Diensten, Tätigkeiten und Kooperationsfähigkeiten der CSIRTs statt, ebenso werden von Vertretern der CSIRTs der Mitgliedstaaten auf freiwilliger Basis Informationen zu einzelnen Sicherheitsvorfällen ausgetauscht und bereitgestellt, sowie aus Übungen zur Sicherheit von Netz- und Informationssystemen gewonnene Erkenntnisse erörtert. Zentrale Aufgabe des CNW ist der Auf- und Ausbau von Vertrauen zwischen den Mitgliedstaaten und die Förderung der raschen und wirksamen operativen Zusammenarbeit zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der EU. 2019 fanden Treffen des CNW in Brüssel, Bukarest und Helsinki statt. Darüber hinaus wurden im Vorfeld der

Europawahl 2019 die Prozesse (Standard Operating Procedures – SOPs) des CNWs im Rahmen einer Übung getestet. Aufgrund des österreichischen Vorsitzes in der zweiten Jahreshälfte 2018 war der „standing representative" Österreichs eingeladen, sich auch 2019 an der Governance des Netzwerkes zu beteiligen. Aktiv mitgearbeitet wurde in der Arbeitsgruppe „Tooling" des CNW, wo es unter anderem auch um das Projekt MeliCERTes geht, mit dem die EU-Kommission einen Werkzeugkasten für die CNW Mitglieder in Auftrag gegeben hatte. Dieses Projekt wird 2020 unter direkter Einbindung von CERT.at fortgeführt.

## 2.8 Andere Gremien und Foren

Neben den bereits genannten Foren beteiligt sich Österreich an einer Reihe weiterer internationaler Zusammenarbeitsgremien im Bereich der Cybersicherheit.

Zu diesen zählen:

- Die „Freedom Online Coalition" – diese Koalition, der auch Österreich seit der Errichtung auf Initiative der Niederlande im Dezember 2011 angehört, ist eine informelle Vereinigung von Staaten, die sich weltweit für die effektive Umsetzung der Menschenrechte online einsetzt. 2019 wurde die Schweiz das 31. Mitglied. Im Mai veröffentlichte die Koalition eine gemeinsame Erklärung zur Wahrung des zivilgesellschaftlichen Raums online.
- Die „Central European Cyber Security Platform" (CECSP) ist eine Kooperationsplattform der Länder (und der CERTs/teilweise milCERTs) der Visegrad-Staaten (Ungarn, Tschechien, Slowakei und Polen) und Österreich, welche im Jahr 2013 auf Initiative von Tschechien und Österreich ins Leben gerufen wurde. Österreich hatte im Jahr 2019 den Vorsitz der CECSP inne.
- Das Global Forum on Cyber Expertise (GFCE) ist eine globale Plattform, die 2015 gegründet wurde. Österreich ist seit 2017 Mitglied.

- Das Internet Governance Forum (IGF), das aus dem Weltgipfel zur Informationsgesellschaft (WSIS) hervorging, fand in Berlin statt. Von diesem Treffen, das stark auf die Zivilgesellschaft und den Privatsektor ausgerichtet ist, gibt es bisher keine konkreten Abschlussdokumente. Der im Rahmen des IGF Paris 2018 lancierte „Pariser Appell zu Vertrauen und Sicherheit im Cyber Space“ wurde 2019 weitergeführt. Der Appell ist als politische Plattform zur Zusammenarbeit zwischen Staaten, Unternehmen und Zivilgesellschaft konzipiert und soll dazu dienen, dass alle Beteiligten ihr Bekenntnis zu Prinzipien, wie Einhaltung der internationalen Rechtslage im Cyberraum, bekräftigen. Alle EU-Mitgliedstaaten unterstützen diese Initiative.
- Die Europäische Cyber Sicherheitsorganisation (ECSO) wurde im Jahr 2016 von der EU (vertreten durch die EK) und Akteuren des Cybersicherheitsmarkts in Form einer vertraglichen öffentlich-privaten Partnerschaft (cPPP) für Cybersicherheit gegründet. ECSO ist sowohl eine Implementierungsmaßnahme der EU-Cybersicherheitsstrategie aus dem Jahr 2013 als auch eine Umsetzungsinitiative der EU-Strategie für einen digitalen Binnenmarkt. Sie ist eine „Vereinigung ohne Gewinnerzielungsabsicht“, die sich vollständig selbst finanziert. Zu den Mitgliedern zählen europäische Großunternehmen, KMUs, Forschungszentren, Hochschulen sowie lokale, regionale und nationale Verwaltungen aus der EU und dem Europäischen Wirtschaftsraum (EWR), der Europäischen Freihandelsassoziation (EFTA) und den mit dem Programm Horizont 2020 assoziierten Ländern. Mehrere österreichische Organisationen und Forschungseinrichtungen sind Mitglieder und nehmen an den verschiedenen Gremien und Arbeitsgruppen der ECSO teil. Das BKA trat der ECSO am 22. März 2017 bei und nahm fortan an den ECSO-Treffen der öffentlichen Verwaltung, der sogenannten ECSO-NAPAC-Group (National Public Authority Representatives Commitee), teil.

# 3
# Nationale Akteure

## 3.1 Cyber Security Center (CSC)

Das im Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) angesiedelte Cyber Security Center (CSC) konnte sich trotz anhaltender Herausforderungen in organisatorischer und inhaltlicher Hinsicht, auch in diesem Berichtsjahr weiter etablieren. Mit der Umwandlung des CSC von einem Referat in eine eigenständige Abteilung kamen eine Reihe neuer Aufgaben hinzu. Um diese erfüllen zu können, wurde eine erste Ausweitung des Personalbestands in Angriff genommen.

Zu Jahresbeginn 2019 trat das NISG in Kraft. Seitdem obliegt die operative Umsetzung dem Verantwortungsbereich des BMI (strategische Aufgaben verbleiben weiterhin im BKA). Damit wurde die Abteilung Cybersicherheit im Bundesamt für Verfassungsschutz und Terrorismusbekämpfung zur operativen NIS-Behörde aufgewertet. Aus diesem Grund war das Berichtsjahr von Maßnahmen der Gründung und der Umsetzung von organisatorischen und technischen Notwendigkeiten in Bezug auf die zusätzliche neue Aufgabe geprägt. Dies betraf vor allem den Erlass einer entsprechenden Netz- und Informationssystemsicherheitsverordnung (NISV) des BKA mit Regelungen zu Sektoren, Sicherheitsvorfällen und Sicherheitsvorkehrungen, sowie die Ausarbeitung einer Verordnung über qualifizierte Stellen (QuaSteV) des BMI.

Darüber hinaus wurde im CSC eine eigene Lagebeobachtung etabliert, die eine regelmäßige und umfassende Lagedarstellung zur Cybersicherheit in Österreich vornimmt und die Lagebilder an die Stakeholder kommuniziert. Schließlich wurde der Bereich der Cyberprävention fortgesetzt. Neben laufenden Awareness-Vorträgen und Veranstaltungen der Bewusstseinsbildung bei Unternehmen der kritischen Infrastruktur und bei verfassungsmäßigen Einrichtungen durch das CSC werden regelmäßig vielfältige Schulungsmaßnahmen zur IKT-Sicherheit für das eigene, sowie für andere Ressorts durchgeführt.

# 3.2 Cyber Crime Competence Center (C4)

## 3.2.1 Zuständige Ermittlungsbehörden

Die sowohl für Cyberkriminalität im engeren Sinne, als auch für digitale Forensik und Datensicherung in Österreich zuständigen Polizeibehörden sind auf drei Ebenen tätig. Auf Bundesebene und als übergeordnete Organisation ist das C4 in der Abteilung 5 des Bundeskriminalamtes Österreich angesiedelt. In jeder der neun Landespolizeidirektionen sind spezialisierte Assistenzbereiche für den Cybercrime- und Forensik-Bereich als Teil der Landeskriminalämter etabliert. Auf Bezirksebene arbeiten speziell ausgebildete, uniformierte Polizeibedienstete (Bezirks-IT-Ermittler), die den ersteinschreitenden Beamtinnen und Beamten (First Responder) die notwendige Unterstützung bieten können.

## 3.2.2 Tätigkeiten

**Internationale Kooperation im Bereich Cybercrime:**

Im „Cyber Crime Competence Center“ (C4) des Bundesministeriums für Inneres werden laufend Maßnahmen gesetzt, um den europäischen und internationalen Austausch im Bereich der Bekämpfung von Cyberkriminalität zu intensivieren. Dies betrifft vornehmlich die Zusammenarbeit mit dem European Cybercrime Centre (EC3) von Europol sowie mit INTERPOL’s Digital Crime Center (IDCC), die Leitungsfunktionen und Mitarbeit bei Operational Actions (OAs) aus den Operational Action Plans (OAPs) im Rahmen der European Cybercrime Task Force (EUCTF), die Beteiligung an multinationalen Joint Investigation Teams (JIT), die Mitarbeit in der European Cybercrime Training and Education Group (ECTEG), die Beteiligung an der European Multidisciplinary Platform Against Criminal Threats (EMPACT), die Mitveranstaltung des jährlichen DACH-Symposiums „Neue Technologien“, sowie die Beteiligung am G7-24/7-Netzwerk.

Diese Kooperationen stärken die europäische und internationale Zusammenarbeit in vielen Bereichen, darunter die Bekämpfung von Ransomware, die erfolgreiche Arbeit der ehemaligen SOKO Clavis, verschiedene internationale Cybercrime-Ermittlungen, Spezialisierungen im Bereich Darknet und Kryptowährungen, sowie KFZ-Forensik und Ausbildung.

## 3.3 IKT und Cybersicherheitszentrum (IKT&CySihZ)

Im Zuge der Heeresgliederung 2019 wurde das ehemalige Kommando Führungsunterstützung und Cyber Defence, welches bis dato in virtueller Form aufgebaut wurde, aufgelöst. Die Kernkompetenzen blieben weitgehend bestehen und werden in den nachfolgenden Kompetenzbereichen näher beschrieben.

### 3.3.1 Militärisches Cyberzentrum (MilCyZ)

Das MilCyZ als Teil des IKT&CySihZ ist jene Stelle im Österreichischen Bundesheer (ÖBH), die bei der Abwehr von Bedrohungen oder Angriffen aus dem Cyberraum gegen die eigenen IKT-Systeme und -Netze wirksam wird.

Um diesen Schutz aufrecht zu erhalten, ist es essentiell, eine durchgängige und konsequente Abdeckung aller Aspekte der Cybersicherheit aufzuweisen. Dies spiegelt sich im nachfolgend aufgelisteten Aufgaben- und Kompetenzbereich des MilCyZ wider:

- Auswahl, Einführung und Betrieb von IKT-Sicherheitskomponenten (z. B. Firewall, End-Point-Protection – Virenschutz etc.);
- Erstellung eines Cyberlagebilds;
- Forensik;
- Auditieren[10] der eigenen IKT-Systeme und -Netze;
- Cybersicherheitsmanagement;
- Cybertruppenübungsplatz;
- Elektronische Kampfführung (Eigenschutz und Assistenzleistung).

10 Regelmäßige Überprüfung/Revision, um etwaige Schwachstellen frühzeitig zu erkennen.


0
30
40
50
60
70
80
90

### 3.3.2 Eigenschutz

Dem militärischen Cyberzentrum obliegt die Planung und Implementierung der Cybersicherheitssysteme und -komponenten für den Eigenschutz sowie die Verteidigung des ÖBH gegen Cyberangriffe. Diese Systeme werden laufend weiterentwickelt und an die aktuelle Bedrohungslage angepasst. In Kombination mit Beobachtungen, Bewertungen und Maßnahmen über Schwachstellen bei aktuellen Technologien, IKT-Systemen und Komponenten des ÖBH, kann ein vollständiges Lagebild zur Cybersicherheit erstellt werden. Um fortlaufend alle IKT-Systeme auf ihre sicherheitstechnische Eignung für den Einsatz im ÖBH überprüfen zu können, werden mit System- und Komponenten-Audits konzeptionelle und strukturelle Schwächen in Technologien, Produkten, Komponenten und Systemen frühzeitig erkannt.

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

Für den Fall eines bevorstehenden oder laufenden Cyberangriffs müssen ausreichende technische und personelle Kapazitäten zur Erkennung, Eindämmung und Abwehr zur Verfügung stehen. Unverzichtbarer Bestandteil dafür ist die Fähigkeit zur Erfassung und Darstellung der aktuellen Cyberlage. Um möglichst genaue und aktuelle Informationen zu Cybersicherheitsvorfällen und aktuellen Erkenntnissen zu erhalten, steht das milCERT in ständigem Austausch mit nationalen und internationalen Partnerorganisationen. Es koordiniert die Maßnahmen beim Auftreten von IT-Sicherheitsvorfällen und warnt rechtzeitig vor Sicherheitslücken.

### 3.3.4 Cybertruppenübungsplatz

Da hochspezialisierte Kräfte nur begrenzt verfügbar sind, ist eine mit den Konzepten und Verfahren akkordierte Ausbildung und ein entsprechendes Training der Angehörigen der Armee erforderlich. Im Rahmen des Cybertruppenübungsplatzes (Cyber Range) werden Übungen im Cyberumfeld koordiniert und Forschungsprojekte zusammen mit wissenschaftlichen Einrichtungen erarbeitet. Dabei werden aktuelle Cybersicherheitstrends analysiert und in die Cyberverteidigungsverfahren des ÖBH eingearbeitet.

### 3.3.5 Informationssicherheit

Zur Ergänzung der technischen und taktischen Fähigkeiten müssen Informationssicherheit, cyberspezifische Risiken und das Zusammenwirken mit österreichischen und internationalen Partnern gemanagt werden. Das militärische Cybersicherheitszentrum betreibt ein umfassendes IKT- und Cyberrisikomanagement, eingebettet in ein Information Security Management System und vertritt das ÖBH in nationalen und internationalen Zulassungsbehörden. Für einen sicheren Informationsaustausch führt das ÖBH Sicherheitszulassungen und -Audits von Systemen auf Basis nationaler und internationaler Sicherheitsvorschriften durch.

### 3.3.6 Elektronische Kampfführung

Als Teil der Cyberverteidigung ist das Zentrum auch für die Leistungserbringung im Fachbereich „Elektronische Kampfführung“ verantwortlich. Dabei werden die technischen Grundlagen bereitgestellt, welche für den Eigenschutz und bei Assistenzleistungen für die Verteidigung fremder Systeme notwendig sind. Das Ziel ist die Gewinnung und Erhaltung der eigenen Führungsüberlegenheit, die Auftragserfüllung im nationalen und multinationalen Verbund und die Erhöhung der Überlebensfähigkeit der Truppe.

## 3.4 Abwehramt (AbwA)

Das Abwehramt (AbwA) leistet ebenso einen wichtigen Beitrag zur Cyberverteidigung. Unter dem Begriff Cyberverteidigung werden alle Anstrengungen des ÖBH im Cyberraum als Gesamtes verstanden. Das AbwA unterstützt diese Anstrengungen, indem es ein Lagebild zur Verfügung stellt, in welchem gesamtstaatliche und auch nachrichtendienstliche Informationen aus und über den Cyberraum zusammengeführt, analysiert und für die Beurteilung von Gegenmaßnahmen herangezogen werden. Durch diese und weitere Maßnahmen soll permanent ein hohes Maß an Sicherheit der militärischen IKT-Infrastruktur gewährleistet werden.

Darüber hinaus wird die im deutschsprachigen Raum größte IKT-Sicherheitskonferenz jährlich vom AbwA veranstaltet. Diese Konferenz dient primär der Erhöhung des Sicherheitsbewusstseins und ist als eines der zentralen Awarenessprojekte des ÖBH zu sehen.

## 3.5 Heeresnachrichtenamt (HNaA)

Als strategischer Auslandsnachrichtendienst trägt das Heeresnachrichtenamt (HNaA) vor allem durch Darstellung des strategischen Kontexts bei großangelegten Cybervorfällen zum gesamtstaatlichen Cyberlagebild bei. Neben dem rechtzeitigen Erkennen von Cyberbedrohungen aus dem Ausland, erlauben von ihm beschaffte Informationen über Absichten und Fähigkeiten internationaler Cyberakteure eine wesentliche Beitragsleistung zur Attribuierung und damit zur Entscheidungsfindung der obersten politischen und militärischen Führung, unter anderem bezüglich einzuleitender Gegenmaßnahmen.

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

GovCERT Austria

Das GovCERT ist nach dem NISG das Computer-Notfallteam der öffentlichen Verwaltung und auch Teil des bereits genannten IKDOK. Das GovCERT stellt den CERT Point of Contact für Österreich in Bezug auf die Netze der öffentlichen Verwaltung dar und ist daher mit entsprechenden internationalen Organisationen und Ansprechpartnern wie der European GovCERT Group oder der Central European Cyber Security Platform eng vernetzt. Das im BKA angesiedelte GovCERT arbeitet eng mit CERT.at in Form einer Public-Private-Partnership zusammen.

CERT.at

CERT.at ist das österreichische nationale Computer Emergency Response Team (CERT), das seit 2008 gemeinsam mit GovCERT als Kooperation des BKA mit der nic.at GmbH (der Registry von „.at“) betrieben wird. Seit März 2019 nimmt CERT.at auch die Rolle des nationales Computer-Notfallteams gemäß NISG wahr. CERT.at versteht sich als Kontaktpunkt für sicherheitsrelevante IKT-Ereignisse in Österreich und dient als vertrauenswürdige und anerkannte Informationsdrehscheibe innerhalb österreichischer Organisationen und Unternehmen im Bereich der Cybersicherheit.

AUSTRIAN ENERGY CERT

Das Austrian Energy CERT (AEC) ist ein brancheneigenes CERT (Computer Emergency Response Team) für die österreichische Energieindustrie. 2019 war das AEC noch nicht als sektorenspezifisches Computer-Notfallteam laut NISG akkreditiert, da die Energieversorger selber noch nicht als „Betreiber wesentlicher Dienste“ identifiziert waren. Dieser formale Schritt wird 2020 erfolgen. Das AEC ist ein wichtiger Baustein bei der Erhöhung der Resilienz der Energiewirtschaft gegenüber Cyberattacken. Die Hauptaufgaben des AEC dienen der Stärkung der IT-Sicherheitskompetenz des Energiesektors. Zu diesen Aufgaben gehört das laufende Security Incident Management, also die Bearbeitung von täglich eingehenden Anfragen und Sicherheitsmeldungen, die Durchführung von Schulungstätigkeiten, die Teilnahme an internationalen Cybersicherheitsübungen oder

die Mitarbeit bei der Erstellung technischer Sicherheitskonzepte für die Elektrizitäts- und Erdgaswirtschaft. Darüber hinaus erfüllt das AEC die Rolle des Primäransprechpartners (Single Point of Contact) bei nationalen und internationalen Security Incidents im Energiesektor. Somit wird neben der schnellen und effizienten Kommunikation auch die Koordination der IT-Sicherheitsexpertinnen und -experten und Behörden innerhalb der Branche gewährleistet.

Gemeinsam erfüllen die drei CERTs die Aufgaben gemäß §14 NISG und decken damit Vorgaben der europäischen Richtlinie für Netz- und Informationssicherheit (NIS) sowie die Empfehlungen der Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) für die Erhöhung der IT-Sicherheit bei kritischen Infrastrukturen ab. Diese drei CERTs stellen auch die österreichischen Mitglieder des CSIRTs-Netzwerk der EU.

Alle drei CERTs werden in erster Linie bei akuten Sicherheitsbedrohungen und -ereignissen aktiv. Dies geschieht durch Verständigung von betroffenen Stellen oder auf Basis eigener Recherchen. Darüber hinaus führen alle drei auch vorbeugende Maßnahmen wie Früherkennung, Öffentlichkeitsarbeit, Beratung und Unterstützung im Anlassfall auf Anfrage durch.

Mit der Umsetzung der NIS-Richtlinie in nationales Recht durch das NISG wurden die Aufgabenbereiche für die CERTs festgeschrieben. So sieht das Gesetz in der Umsetzung unter anderem für Betreiber wesentlicher Dienste sowie Anbieter digitaler Dienste eine Meldeverpflichtung für schwerwiegende Sicherheitsvorfälle vor. Diese verpflichtenden Meldungen werden von den Betroffenen an bestimmte, sektorenspezifische Meldestellen (sektorenspezifische Computer-Notfallteams) gesendet und von dort an das CSC weitergeleitet. Auf freiwillige Meldungen trifft dies ebenfalls zu, allerdings können diese

Meldungen vor der Weiterleitung an das CSC von den Sektor-CERTs anonymisiert werden. Für die Einrichtungen der öffentlichen Verwaltung nimmt das GovCERT die Entgegennahme und Weiterleitung solcher Meldungen vor, falls die Einrichtung nicht im IKDOK vertreten ist. Zusätzlich kann das GovCERT auch Frühwarnungen, Alarmmeldungen, Handlungsempfehlungen und Bekanntmachungen vornehmen, erste allgemeine technische Unterstützung bei der Reaktion auf einen Sicherheitsvorfall leisten, um Risiken, Vorfälle und Sicherheitsvorfälle zu beobachten, zu analysieren sowie die Lage zu beurteilen.

Das NISG sieht zur Wahrnehmung dieser Meldestellenfunktion die Existenz eines solchen Sektor-CERTs in jedem Sektor vor. Diese CERTs erfüllen neben der Meldestellenfunktion eine Vielzahl weiterer CERT-Aufgaben für die Organisationen ihres Sektors.

Für den Fall, dass ein Sektor noch über kein eigenes Sektor-CERT verfügt, werden die Aufgaben des Computer-Notfallteams und die der Meldestelle durch das nationale Computer-Notfallteam (CERT.at) wahrgenommen.

## 3.7 Büro für strategische Netz- und Informationssystemsicherheit

Informationssysteme mit den zugehörigen Diensten spielen eine zentrale Rolle in der heutigen Gesellschaft. Für wirtschaftliche und gesellschaftliche Tätigkeiten ist es von entscheidender Bedeutung, dass sie verlässlich und sicher sind. Um dies zu gewährleisten, wurde mit der Richtlinie (EU) 2016/1148 „NIS-Richtlinie" der erste EU-weite Rechtsakt über Cybersicherheit verabschiedet.

Die NIS-Richtlinie wurde in Österreich mit dem am 29. Dezember 2018 in Kraft getretenen „NIS-Gesetz" umgesetzt (Netz- und Informationssystemsicherheitsgesetz, kurz: NISG, BGBl. I Nr. 111/2018). Das NISG überträgt dabei Aufgaben, die sich aus der NIS-Richtlinie ergeben, auf bestehende Strukturen und regelt Zuständigkeiten für die mit der Umsetzung betrauten Behörden sowie deren Befugnisse. In diesem Zusammenhang nimmt der Bundeskanzler die strategischen und der Bundesminister für Inneres die operativen Aufgaben wahr. Im Anwendungsbereich des Gesetzes befinden sich Einrichtungen mit einer hohen Bedeutung für das Funktionieren des Gemeinwesens, weshalb ihre Netz- und Informationssysteme besonders schutzbedürftig sind. Dies betrifft zum einen Einrichtungen in den sieben Sektoren Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasserversorgung und Digitale Infrastruktur, zum anderen Einrichtungen, die bestimmte digitale Dienste zur Verfügung stellen sowie Einrichtungen der öffentlichen Verwaltung.

Auf Grundlage des NISG nahm das Büro für strategische Netz- und Informationssystemsicherheit „strategisches NIS-Büro", welches im BKA als Teil der Abteilung I/8 (Cyber Security, GovCERT, NIS Büro und ZAS) angesiedelt und für bestimmte Angelegenheiten im Zusammenhang mit der Umsetzung der gesetzlichen Verpflichtung aus der NIS-Richtlinie zuständig ist, seine Arbeit auf.

Als ein erster Meilenstein kann diesbezüglich die im April 2019 auf Antrag erfolgte bescheidmäßige Feststellung der Eignung und Ermächtigung von CERT.at als nationales Computer-Notfallteam im Sinne des NISG genannt werden.

Ein weiterer Meilenstein erfolgte, als die auf Basis des NISG erlassene „NIS-Verordnung" (Netz- und Informationssystemsicherheitsverordnung, kurz: NISV, BGBl. II Nr. 215/2019) am 18. Juli 2019 in Kraft trat. In dieser Verordnung legte der zuständige Kanzleramtsminister im Bundeskanzleramt im Einvernehmen mit dem Bundesminister für Inneres verschiedene essentielle Sachverhalte aus dem NISG näher fest. Dazu gehören nähere Regelungen zu den Sektoren, wobei insbesondere die wesentlichen Dienste und die Kriterien für die Parameter zu Sicherheitsvorfällen „Meldeschwellenwerte" definiert wurden. Ferner wurden in der NISV Kategorien und Maßnahmen hinsichtlich der Sicherheitsvorkehrungen für Betreiber wesentlicher Dienste festgelegt.

Auf Grundlage der NISV nahm das strategische NIS-Büro im August 2019 die Ermittlung der Betreiber wesentlicher Dienste in den sieben Sektoren auf. Dabei werden die Betreiber zunächst in einem Vorverfahren mit einem sogenannten „Informationsschreiben" darüber informiert, dass sie aufgrund von Daten, die dem strategischen NIS-Büro beispielsweise infolge von durchgeführten Amtshilfeverfahren vorliegen, als Betreiber wesentlicher Dienste in Frage kommen. Die Unternehmen werden dadurch einerseits über die Aufnahme der Ermittlungen informiert, sollen andererseits aber auch die Gelegenheit erhalten, sich dazu zu äußern bzw. dazu Stellung zu nehmen. Darüber hinaus werden über das Informationsschreiben mögliche grenzüberschreitende Bezüge erfragt, die in einem weiteren Ermittlungsschritt als Grundlage für die Aufnahme von Konsultationen mit anderen Mitgliedstaaten der EU verwendet werden, falls ein Betreiber wesentlicher Dienste seinen Dienst noch in einem anderen Mitgliedstaat bereitstellt. Ferner wird versucht, über die Informationsschreiben gewisse intersektorale Abhängigkeiten zu eruieren. In einem abschließenden Schritt wird auf Basis der im Vor- und Konsultationsverfahren erlangten Informationen der Bescheid erlassen, mit dem eine öffentliche oder private Einrichtung als Betreiber wesentlicher Dienste ermittelt wird.

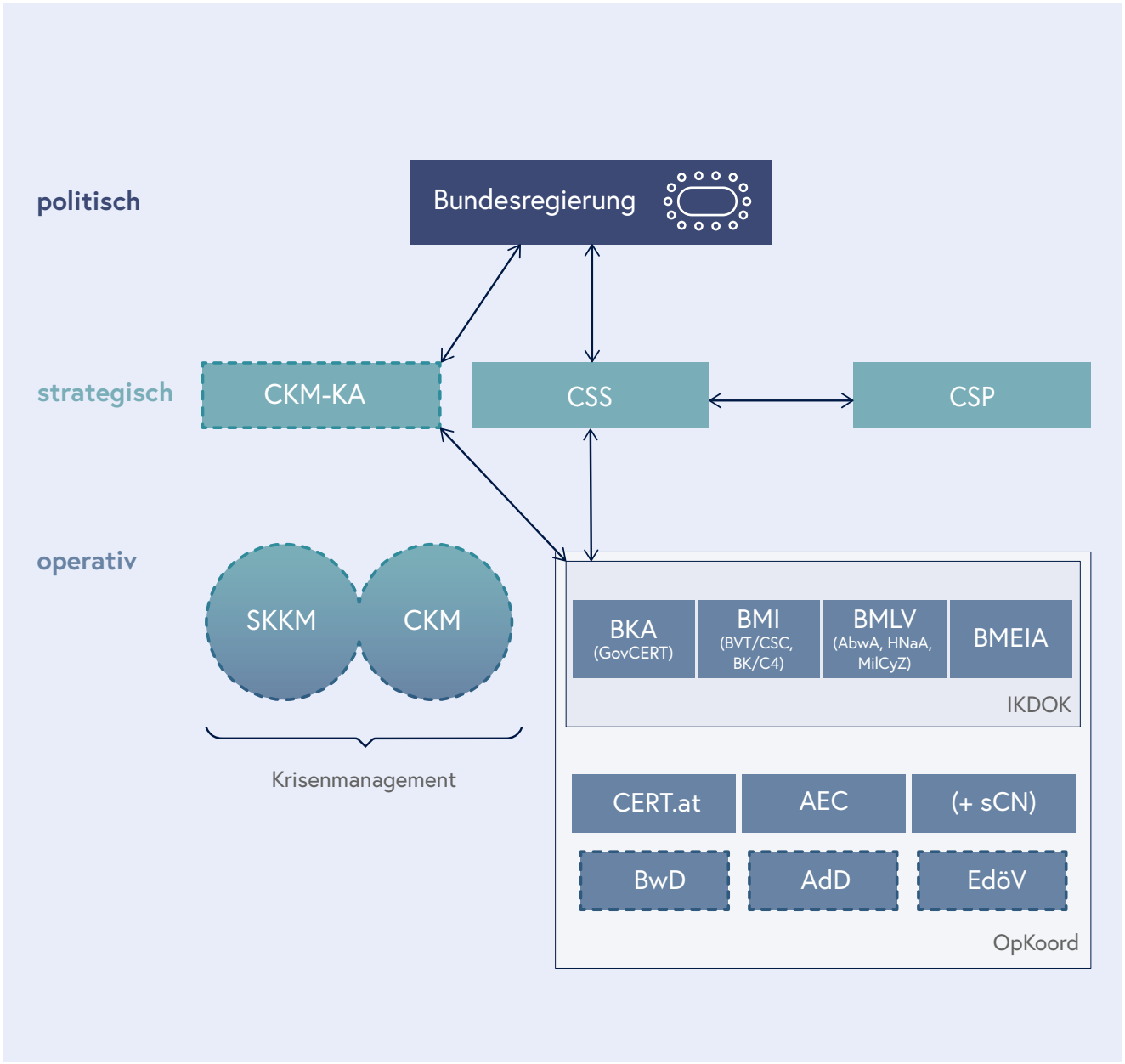
Dem strategischen NIS-Büro kommt gesetzlich weiters die Vertretung von Österreich in der NIS-Kooperationsgruppe sowie in anderen EU-weiten und internationalen Gremien für die Sicherheit von Netz- und Informationssystemen, denen strategische Aufgaben zugewiesen sind, zu. So nimmt das strategische NIS-Büro unter anderem aktiv an den Arbeiten der NIS-Kooperationsgruppe teil und leitet dort beispielsweise Work Stream 8 über Cybersicherheit im Energiesektor. Hierbei kann als Erfolg die Annahme des umfangreichen Referenzdokuments über die Umsetzung der NIS-Richtlinie im Sektor Energie (CG Publication 03/2019) durch die NIS-Kooperationsgruppe im September 2019 hervorgehoben werden. Ferner vertritt das strategische NIS-Büro Österreich unter anderem in der Rats-Arbeitsgruppe für Cyberangelegenheiten („HWP Cyber“) und der Europäischen Gruppe für die Cybersicherheitszertifizierung (ECCG).

Neben diesen gesetzlichen Aufgabenbereichen lagen weitere Tätigkeiten, die das strategische NIS-Büro im Jahr 2019 verfolgte, insbesondere im Bereich der Informationstätigkeit. So wurde gemeinsam mit dem BMI eine NIS-Website (https://nis.gv.at) ins Leben gerufen, die als Anlaufstelle im Hinblick auf die NIS-Richtlinie und das NISG fungiert und die bei der Beantwortung häufig gestellter Fragen helfen soll.

Des Weiteren wurden die Adressaten des NISG bei der Umsetzung der gesetzlichen Vorgaben unterstützt, indem vier sogenannte NIS Fact Sheets im Jahr 2019 erstellt und auf der NIS-Website zur Verfügung gestellt wurden. Der NIS Fact Sheet 1/2019 erläutert die Erwartungshaltung der Behörden im Hinblick auf die Kontaktstellen von Betreibern wesentlicher Dienste. Der NIS Fact Sheet 7/2019 bietet den qualifizierten Stellen eine Hilfestellung insbesondere im Antragsverfahren. Der NIS Fact Sheet 8/2019 erörtert die Sicherheitsmaßnahmen für Betreiber wesentlicher Dienste näher, der NIS Fact Sheet 9/2019 dient als Umsetzungsleitfaden für Einrichtungen des Bundes bei der Festlegung der wichtigen Dienste sowie der Meldekriterien.

Legende

– – – – – anlassbezogen
AbwA .....Abwehramt
AdD .....Anbieter digitaler Dienste
AEC.....Austrian Energy CERT
(=sCN für Sektor „Energie“)
BK.....Bundeskriminalamt
BKA.....Bundeskanzleramt
BMEIA ....Bundesministerium für europäische und
internationale Angelegenheiten
BMI .....Bundesministerium für Inneres
BMLV.....Bundesministerium für Landesverteidigung
BVT .....Bundesamt für Verfassungsschutz und
Terrorismusbekämpfung
BwD .....Betreiber wesentlicher Dienste
C4 .....Cyber Crime Competence Center
CERT.at ..nationales Computer-Notfallteam
CKM.....Cyberkrisenmanagement
CKM-KA....CKM-Koordinationsausschuss
CSC .....Cyber Security Center
CSP.....Cyber Sicherheit Plattform
CSS.....Cyber Sicherheit Steuerungsgruppe
EdöV.....Einrichtungen der öffentlichen Verwaltung
HNaA.....Heeresnachrichtenamt
IKDOK.....Innerer Kreis der Operativen
Koordinierungsstruktur
MilCyZ .....Militärisches Cyberzentrum
OpKoord...Operative Koordinierungsstruktur
sCN.....sektorenspezifisches Computer-Notfallteam
SKKM.....Staatliches Krisen- und
Katastrophenschutzmanagement


politisch
Bundesregierung
strategisch
CKM-KA
CSS
CSP
operativ
SKKM
CKM
Krisenmanagement
BKA
(GovCERT)
BMI
(BVT/CSC,
BK/C4)
BMLV
(AbwA, HNaA,
MilCyZ)
BMEIA
IKDOK
CERT.at
AEC
(+ sCN)
BwD
AdD
EdöV
OpKoord

# 4 Nationale Strukturen

## 4.1 Innerer Kreis der Operativen Koordinierungsstruktur (IKDOK)

Das am 31. Dezember 2018 in Kraft getretene Netz- und Informationssystemsicherheitsgesetz (NISG) sieht unter anderem die Schaffung einer Struktur zur Koordination auf der operativen Ebene „Operative Koordinierungsstruktur – OpKoord“, sowie einer interministeriellen Struktur zur Koordination auf der operativen Ebene im Bereich der Sicherheit von Netz- und Informationssystemen „Innerer Kreis der Operativen Koordinierungsstruktur – IKDOK“ vor. Während die OpKoord im Wesentlichen zur Erörterung eines gesamtheitlichen Lagebildes, das sowohl verpflichtende als auch freiwillige Meldungen enthält, eingerichtet wurde, liegen die Hauptaufgaben des IKDOK in der Erörterung und Aktualisierung des Lagebildes über Risiken, Vorfälle und Sicherheitsvorfälle sowie in der Unterstützung des Koordinationsausschusses im Cyberkrisenmanagement (CKM).

Konkret bedeutet dies, dass der IKDOK, unterstützt durch die OpKoord, im Krisenfall die direkte Schnittstelle zum gesamtstaatlichen CKM bildet. Hinsichtlich der anzuwendenden Mechanismen und Prozesse orientiert sich das CKM stark an den bereits bewährten und erprobten Abläufen des Staatlichen Krisen- und Katastrophenschutzmanagements (SKKM). Regelmäßige Cyberübungen sollen das Cyberkrisenmanagement sowie die Krisenmanagement- und Kontinuitätspläne testen.

Der IKDOK besteht gemäß NISG aus Vertretern des Bundeskanzlers (sowie des GovCERT), des Bundesministers für Inneres (das im BVT angesiedelte Cyber Security Center [CSC], das im Bundeskriminalamt angesiedelte Cyber Crime Competence Center [C4]), des Bundesministers für Landesverteidigung (Abwehramt [AbwA], Heeresnachrichtenamt [HNaA], und Militärisches Cyberzentrum [MilCyZ]) und des Bundesministers für Europa, Integration und Äußeres.

## 4.2 CERT-Verbund Austria

Um das Sicherheitsniveau der österreichischen Gesellschaft im Cyberraum weiterzuentwickeln ist es notwendig, dass das Zusammenspiel zwischen Gesellschaft, Wirtschaft und Wissenschaft weiter gefördert und ausgebaut wird. Eine wesentliche Rolle bei der Weiterentwicklung nehmen dabei die Computer Emergency Response Teams (CERTs) ein. Die inhärente Aufgabe der CERTs ist es, IKT-Systeme und digitale Netze zu schützen. Als erste Anlaufstelle für sämtliche Bereiche der Cybersicherheit kommt den Aspekten Prävention, Reaktion und Bewusstseinsbildung höchste Priorität zu. Intensiver Austausch und Vernetzung auf nationaler und internationaler Ebene stellen die Voraussetzungen für den Aufbau notwendiger Expertise dar. Im Mittelpunkt des Aufgabenbereichs des CERT-Verbund Austria stehen die Verbesserung der Zusammenarbeit zwischen den österreichischen CERTs sowie die Förderung der CERT-Aktivitäten in Österreich. Ein flächendeckendes Netz an CERTs ist das wirksamste Mittel zur Absicherung der vernetzten Informations- und Kommunikationssysteme. Eine Sichtweise, die sich in einer stetig wachsenden Anzahl von CERTs, CSIRTs, Security Operations Centers (SOC), Cyber Defence Teams etc. in den österreichischen Unternehmen bestätigt. Der CERT-Verbund-Austria wurde 2011 als Kooperation aller damals existierenden österreichischen CERTs des öffentlichen Bereichs und jenen aus den privaten Sektoren gegründet. Intention war die Bündelung der verfügbaren Kräfte zur optimalen Nutzung des gemeinsamen Know-hows zur Gewährleistung von bestmöglicher IKT-Sicherheit. Die Teilnahme am CERT-Verbund Austria ist freiwillig. Jeder einzelne Teilnehmer verpflichtet sich zu regelmäßigem Informations- und Erfahrungsaustausch, zur Identifikation und Zurverfügungstellung von Kernkompetenzen sowie zur Förderung der CERTs in allen Sektoren – im Sinne eines gemeinschaftlich geführten und auf Kooperation basierenden CERT-Verbundes – beizutragen. Seit der Gründung des CERT-Verbund Austria haben sich die aktuell 16 Mitglieder in 38 Sitzungen getroffen und sind auch außerhalb der regelmäßigen Treffen über sichere

Kommunikationsverteiler in ständigem Austausch miteinander. Um den bestehenden Teilnehmern des CERT-Verbund Austria weiterhin eine vertrauensvolle Plattform für den Informationsaustausch bieten zu können, aber auch ein geregeltes Wachstum des Verbunds zu ermöglichen, wurde 2019 die Initiative gestartet, eine Geschäftsordnung, welche die Abläufe und Prozesse innerhalb des Verbundes festschreibt, zu erstellen. Nach mehreren Iterationen konnte die Geschäftsordnung Ende 2019 verabschiedet werden.

Cyber Sicherheit Plattform

## 4.3 Cyber Sicherheit Plattform (CSP)

Die Cyber Sicherheit Plattform (CSP) stellt die zentrale Austausch- und Kooperationsplattform zwischen Wirtschaft, Wissenschaft und öffentlicher Verwaltung dar. Sie dient dem Erfahrungs- und Informationsaustausch im Bereich Cybersicherheit mit besonderem Fokus auf kritische Infrastrukturen. Darüber hinaus berät und unterstützt die CSP die Cyber Sicherheit Steuerungsgruppe (CSS) in strategischen Fragen der Cybersicherheit. Die Plattform hat sich seit ihrer Konstituierung im Jahr 2015 als ein beispielgebendes Modell etabliert und stellt ein Dach für zahlreiche Initiativen im Bereich der Cybersicherheit dar. Die Ergebnisse der Arbeiten der Plattform haben hohen Stellenwert in der Gestaltung der nationalen Cybersicherheitspolitik.

Im Jahr 2019 fanden die achte und neunte Arbeitstagung der CSP statt. Inhaltlicher Schwerpunkt in beiden Arbeitstagungen war der aktuelle Stand der Umsetzung der NIS-Richtlinie durch das nationale NISG sowie die begleitenden Verordnungen. Zahlreiche Inputs von Mitgliedern der CSP wurden aufgenommen und in den weiteren Bearbeitungen berücksichtigt.

Einen weiteren Themenschwerpunkt bildeten Fortschrittsberichte über die im Rahmen der CSP etablierten Arbeitsgruppen zu den Bereichen „Rechtliches und Regulatorisches“, „Technologien, Prozesse, Ausbildung, Forschung und Entwicklung“ sowie „betriebliches Krisenmanagement“.

Weitere im Rahmen der CSP diskutierte Themen waren der EU Cyber Security Act, das Network of Cybersecurity Competence Centers und die mögliche nationale Umsetzung sowie die Thematik 5G-Risikoanalyse. Ergänzt wurden die Diskussionen um aktuelle Informationen zum Cyberlagebild sowie zu relevanten Veranstaltungen und Initiativen im Bereich der Cybersicherheit.

Neben den umfassenden und wertvollen Diskussionen im Rahmen der beiden Arbeitstagungen wurde durch die CSP ebenso ein schriftlicher Input zur Erstellung einer aktualisierten Österreichischen Strategie für Cybersicherheit (ÖSCS 2.0) geleistet.

## 4.4 Austrian Trust Circle (ATC)

Der Austrian Trust Circle (ATC) ist eine nationale Initiative für den fachlichen Informationsaustausch bezüglich IKT-Sicherheit und Vorfälle. Zielgruppe sind alle Sektoren der strategischen Infrastruktur sowie die öffentliche Verwaltung in Österreich. Der ATC wurde im Jahr 2011 gegründet und ist eine Initiative des nationalen CERT.at mit Unterstützung des BKA. Der ATC besteht aus sektorenspezifischen Security Information Exchanges. Unternehmen und Organisationen der kritischen Infrastruktur und Behörden in Österreich werden durch den ATC adressiert. CERT.at und das Austrian Energy CERT bieten hier in Kooperation mit GovCERT Austria und dem BKA einen formellen Rahmen für praxisnahen Informationsaustausch und gemeinsame Projekte im Sicherheitsbereich.

Die wesentlichen Ziele des ATC sind:

- Das Schaffen einer Vertrauensbasis, um im Ernstfall gemeinsam agieren zu können;
- Vernetzung und Informationsaustausch in und zwischen den Sektoren der kritischen Infrastruktur und der öffentlichen Verwaltung;
- Kontaktaustausch zwischen den CERTs und den teilnehmenden Unternehmen, Organisationen und Behörden;

- Unterstützung zur Selbsthilfe in den Sektoren im Bereich IT–Sicherheit;
- Operative Kontakte zu den CERTs beispielsweise
- bei der Information über und
- bei der Behandlung von Sicherheitsvorfällen in den Organisationen;
- Operative Experten für das BKA im Krisenfall.

Neben regelmäßigen Treffen innerhalb der einzelnen Sektoren wird der Austausch zwischen den Sektoren inklusive der öffentlichen Verwaltung einmal im Jahr im Rahmen einer zweitägigen Veranstaltung gefördert. Im Jahr 2019 wurden unter anderem die Themen NIS-Umsetzung, „Client Security und Management“ sowie „Incident Response und Logdaten“, behandelt.

Besuche 2018

**206.277**

Besuche pro Woche

**~5.000 / Woche**

Besuche 2019

**248.576**

Besuche pro Tag (Spitzen MO–DO)

**Ø 820 / Tag**

## 4.5 IKT-Sicherheitsportal

Das IKT-Sicherheitsportal onlinesicherheit.gv.at ist eine interministerielle Initiative in Kooperation mit der österreichischen Wirtschaft und fungiert als zentrales Internetportal für Themen rund um die Sicherheit in der digitalen Welt.

Die Initiative verfolgt als strategische Maßnahme der Nationalen IKT-Sicherheitsstrategie und der Österreichischen Strategie für Cybersicherheit das Ziel, durch Sensibilisierung und Bewusstseinsbildung der betroffenen Zielgruppen sowie durch Bereitstellung zielgruppenspezifischer Handlungsempfehlungen die IKT- und Cybersicherheitskultur in Österreich zu fördern und nachhaltig zu stärken.

Das Informations- und Serviceangebot wird im Rahmen regelmäßiger Redaktionssitzungen mit den 39 Kooperationspartnern (Bundesministerien, Landesregierungen, Behörden, Universitäten, Fachhochschulen, Forschungsinstitute, Unternehmen, Vereine und Interessensvertretungen) laufend erweitert. Es beinhaltet aktuelle Meldungen und Warnungen, Informatives, Beratung sowie weiterführende Informationen sowohl für Einsteigerinnen und Einsteiger als auch für Expertinnen und Experten.

2019 umfassten die Aktivitäten auf dem IKT-Sicherheitsportal[11] insgesamt die Verfassung von 150 Newsartikeln, 50 Publikationseinträgen und 70 Veranstaltungseinträgen. In jedem Monat wird ein Schwerpunktthema zu aktuellen Trends festgelegt, wozu insgesamt 34 Fachbeiträge veröffentlicht wurden. Schwerpunkte waren beispielsweise zu Beginn des Jahres die Datenschutz-Grundverordnung (DSGVO) und in der Vorweihnachtszeit Sicherheitsmaßnahmen beim Online-Shopping. Im Oktober wurde zu den österreichischen Aktivitäten im Zuge des „European Cyber Security Month“ (ECSM) berichtet.

---

11 IKT-Sicherheitsportal-Auswertungen 2019/2020 (Stand: 20.1.2020)

# 5 Cyberübungen

Auch 2019 leisteten Cyberübungen einen wesentlichen Beitrag zur Erprobung festgelegter Prozesse, zur Überprüfung gesetzter Maßnahmen, sowie zur Festigung innerstaatlicher und internationaler Zusammenarbeit im Bereich der Cybersicherheit. Der Erkenntnisgewinn aus der Teilnahme an Planspielen in Form von „Lessons Learned“ ist ein ganz entscheidender Faktor bei der Erhöhung der gesamtstaatlichen Resilienz. Durch Teilnahme an verschiedenen Übungen und Planspielen konnten die staatlichen Stellen ein breites Feld von Einsatzbereichen trainieren.

## 5.1 Cyber Coin 2019

Die Finanzmarktaufsicht (FMA) lud gemeinsam mit dem Kuratorium Sicheres Österreich (KSÖ) und der Oesterreichischen Nationalbank (OeNB) zum Planspiel „Cyber Coin 2019" ein. Teilnehmer waren zehn repräsentative Kreditinstitute, deren IT-Provider, das österreichische Computer-Notfall-Team CERT sowie das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT). Bei diesem Cyberstresstest für den Finanzmarkt Österreich wurde die Reaktionsfähigkeit und Widerstandskraft des österreichischen Bankensektors auf Cyberattacken geübt. Dabei lag diesmal der Fokus auf dem Faktor Mensch. Getestet wurde insbesondere die Zusammenarbeit zwischen Kreditinstituten und der Bankenaufsicht sowie den für die Cybersicherheit in Österreich verantwortlichen Institutionen im Falle eines Hackerangriffs. Das Cyberplanspiel hat gezeigt, dass Kreditinstitute weitgehend organisatorisch gut auf Cyberangriffe vorbereitet sind, die praktische Ausgestaltung der Angriffsabwehr hat sich jedoch als sehr unterschiedlich erwiesen.

## 5.2 HELIOS 2019

Vom 13. bis 15. Mai 2019 fand im BMI die strategische Krisenübung „HELIOS 2019" statt. Teilnehmer waren rund 100 Vertreterinnen und Vertreter der Bundesministerien, der Länder, der Einsatzorganisationen sowie Betreiber kritischer Infrastrukturen. Ausgangsszenario der Übung war ein Strom-Blackout, der unmittelbare Auswirkungen auf viele Gesellschafts- und Lebensbereiche, auf verfassungsmäßige Einrichtungen und die Wirtschaft mit sich brachte. Ziel der Übung war, dass alle beteiligten Seiten erkennen konnten, wo sie ihre eigene Resilienz verbessern können, um ein hohes gesamtösterreichisches Sicherheitsniveau zu schaffen und um für einen eventuellen Ernstfall optimal aufgestellt zu sein. Die Nachfolgeübung DANTE ist für 2020 in Planung.

## 5.3 Blue OLEX 2019

Im Juli 2019 nahmen das CSC des BVT und ein Vertreter des BKA/NIS-Büro in Paris an einem hochrangigen Vernetzungstreffen europäischer NIS-Behörden samt Planspiel namens „Blue OLEX 2019“ teil. Zu diesem Treffen hatte die französische Cybersicherheitsbehörde ANSSI im Rahmen des Work Stream 7 der NIS-Kooperationsgruppe über großflächige Cybersicherheitsvorfälle eingeladen. Das BVT nimmt im Bereich der europäischen Netz- und Informationssystemsicherheit (NIS) die Funktion des österreichischen Single Point of Contact (NIS SPoC) ein und konnte hier die Kommunikation mit anderen EU-Mitgliedstaaten für den Fall von grenzübergreifenden Cybersicherheitsvorfällen üben.

## 5.4 EU ELEx19

Am 5. April 2019 fand im Europäischen Parlament in Brüssel eine Tabletop-Exercise statt, um zu testen, inwieweit die EU-Mitgliedstaaten auf Cyberangriffe, die im Zusammenhang mit den europäischen Parlamentswahlen stehen, vorbereitet sind. Weiters wurden in der Übung Erfahrungen zwischen den Mitgliedstaaten betreffend die Umsetzung einer entsprechenden Empfehlung der EK ausgetauscht. Diese sieht unter anderem vor, nationale Wahlkooperationsnetzwerke zu installieren. Dieses Kooperationsnetzwerk wurde in Österreich im November 2018 unter der Federführung der Wahlbehörde des BMI eingerichtet.

## 5.5 CyberSOPex 2019

Das EU-Netzwerk der CSIRTs hat am 15. Mai 2019, also zeitnah zur EU-Wahl, im Rahmen der Übung CyberSOPex 2019 die Prozesse für die Zusammenarbeit während eines grenzüberschreitenden Vorfalls geübt. CERT.at, als nationales CSIRT Österreichs, hat daran teilgenommen.

## 5.6 Locked Shields 2019

Bei dieser größten technischen „Life-fire“ Übung im Bereich der Cyber Defence lag der Fokus auf Defence, jedoch wurden auch begleitende Verfahren (Rechtslage „Cyber“, Öffentlichkeitsarbeit, Collaboration und Forensic) angewendet. Die Übung fand vom 8. bis 12. April 2019 in Tallinn statt und wurde durch das dortige NATO Cooperative Cyber Defence Center of Excellence (NATO CCDCoE) geführt. Dabei nahmen mehr als 1000 Soldatinnen und Soldaten und Zivilpersonen aus 25 Staaten sowie NATO- und EU-Organisationen teil. Österreich stellte sechs Übungsteilnehmerinnen und -teilnehmer direkt vor Ort in Tallinn, sowie 52 Übungsteilnehmerinnen und -teilnehmer in Wien als Blue Team (BT) in den Räumlichkeiten des MilCyZ. Bei dieser Übung wurden primär die Fähigkeiten geübt, ein wenig bekanntes Netzwerk zu schützen, Angriffe zu identifizieren und darauf geeignet zu reagieren.

Die teilnehmenden IT-Spezialistinnen und IT-Spezialisten hatten als Teams umfassende Cyberangriffe zu erkennen, die Auswirkungen zu beschränken und die Vorfälle entsprechend einheitlicher Vorgaben zu bearbeiten (z. B. rechtliche Aspekte, Informationsaustausch, forensische Analysen). Aus den Aktionen der Übungsteilnehmerinnen und -teilnehmer sollten Lösungsansätze für reale Probleme abgeleitet werden, wie die Stärkung der internationalen Zusammenarbeit durch Schaffung von Vertrauen, Verbesserung der Fähigkeit zur Durchführung ähnlicher Übungsvorhaben, Testung von Werkzeugen, dem Ausbau der Fähigkeiten im Bereich Cyber Defence und dem Ausbau der Fähigkeiten im Bereich aktiver Cyberhandlungen.

## 5.7 Common Roof 2019

Die CR19 war eine dreiwöchige Übung, die vom 23. September bis 11. Oktober 2019, verteilt in den drei Ländern der Deutschland-Österreich-Schweiz-Kooperation (D-A-CH), stattfand. Österreich war die diesjährige Lead Nation der Übung. An der CR19 nahmen circa 180 Soldatinnen und Soldaten und Zivilpersonen aus den drei D-A-CH Nationen teil, wobei Österreich durch 98 Teilnehmerinnen und Teilnehmer vertreten war.

Im Zuge der Übung wurde gemeinsam ein multinationales Mission Network aufgebaut, betrieben und gegen Cyberbedrohungen geschützt. Im Mittelpunkt standen standardisierte (bzw. teilweise noch zu standardisierende) IKT-Service-Management-Prozesse, IKT-Sicherheitsprozesse und die dabei zum Einsatz kommenden IKT-Services. Die Überwachung und Steuerung der multinationalen Netzwerkanteile übernahm eine multinationale Network Operation Cell (NOC).

## 5.8 Thor's Hammer 2019

Die Übung Thor's Hammer 19 wurde über einen Zeitraum von sechs Wochen vom 29. September bis 9. November 2019 in Australien ausgetragen. An der Ausführung waren zwölf Nationen beteiligt. Österreich entsendete 13 Personen zur Übungsteilnahme.

Übungszweck war die Testung und Weiterentwicklung von Systemen, die die Auslösung und Zündung von ferngezündeten Sprengsätzen verhindern sollen. Diese Kampfmittel stellen eine ständige Bedrohung für internationale Friedenstruppen in Einsatzräumen dar. Dabei kommen Gegenmaßnahmen im elektromagnetischen Spektrum zum Einsatz. Ein besonderer Fokus lag hierbei auf dem Wissenstransfer der internationalen Teilnehmer.

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

Bei der CWIX 19 handelte es sich um eine großangelegte Command Post Exercise (CPX) mit Schwergewicht auf Interoperabilitätstests sowie Verifizierung und Validierung (V&V) von einsatzorientierten IKT-Systemen, Services und Applikationen, die im Zeitraum vom 10. bis 27. Juni 2019 in Bydgoszcz, Polen stattfand.

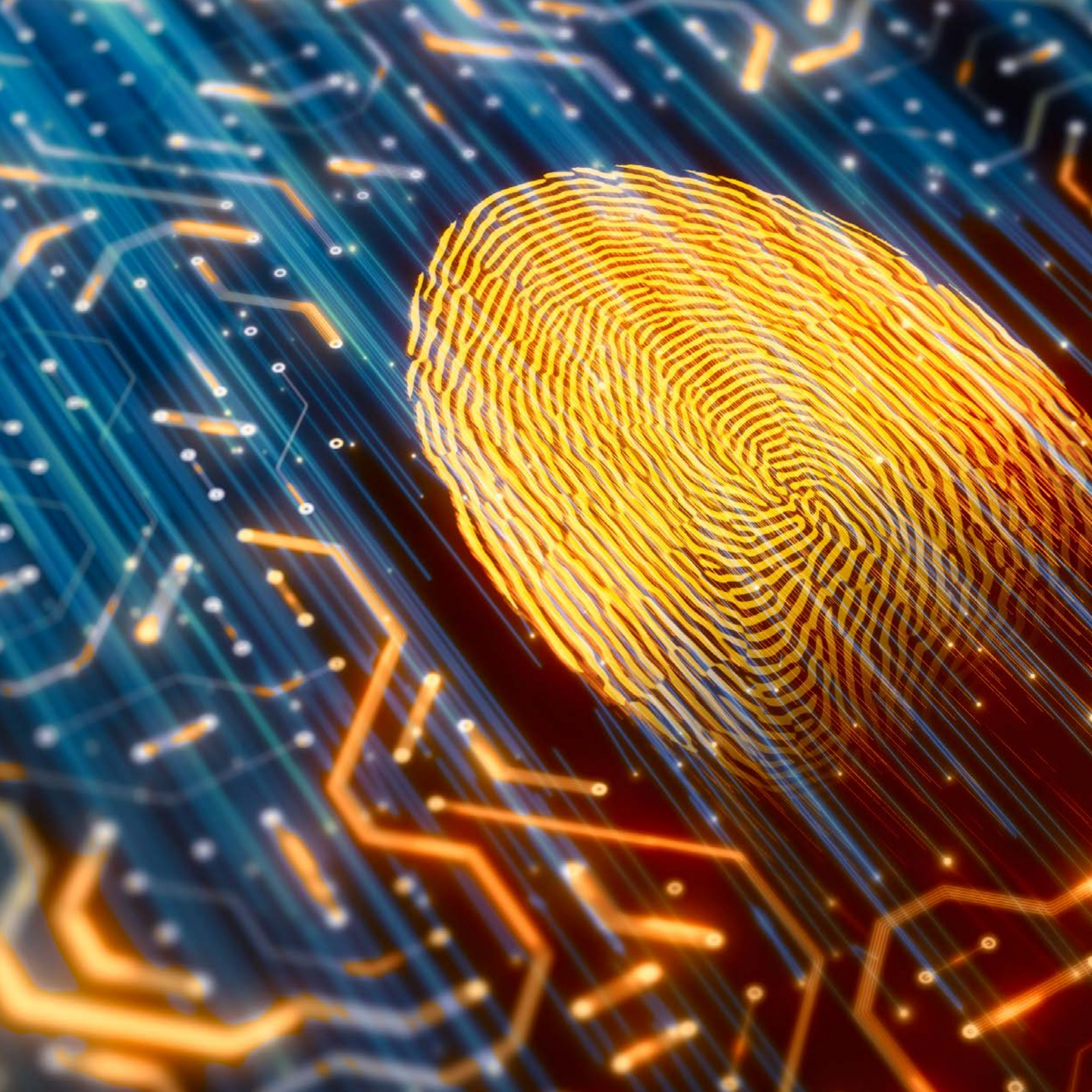
An dieser Übung nahmen knapp 1300 Soldatinnen und Soldaten und Zivilpersonen aus 36 Nationen sowie NATO-Organisationen teil. Dabei stellte Österreich 25 Teilnehmerinnen und Teilnehmer.

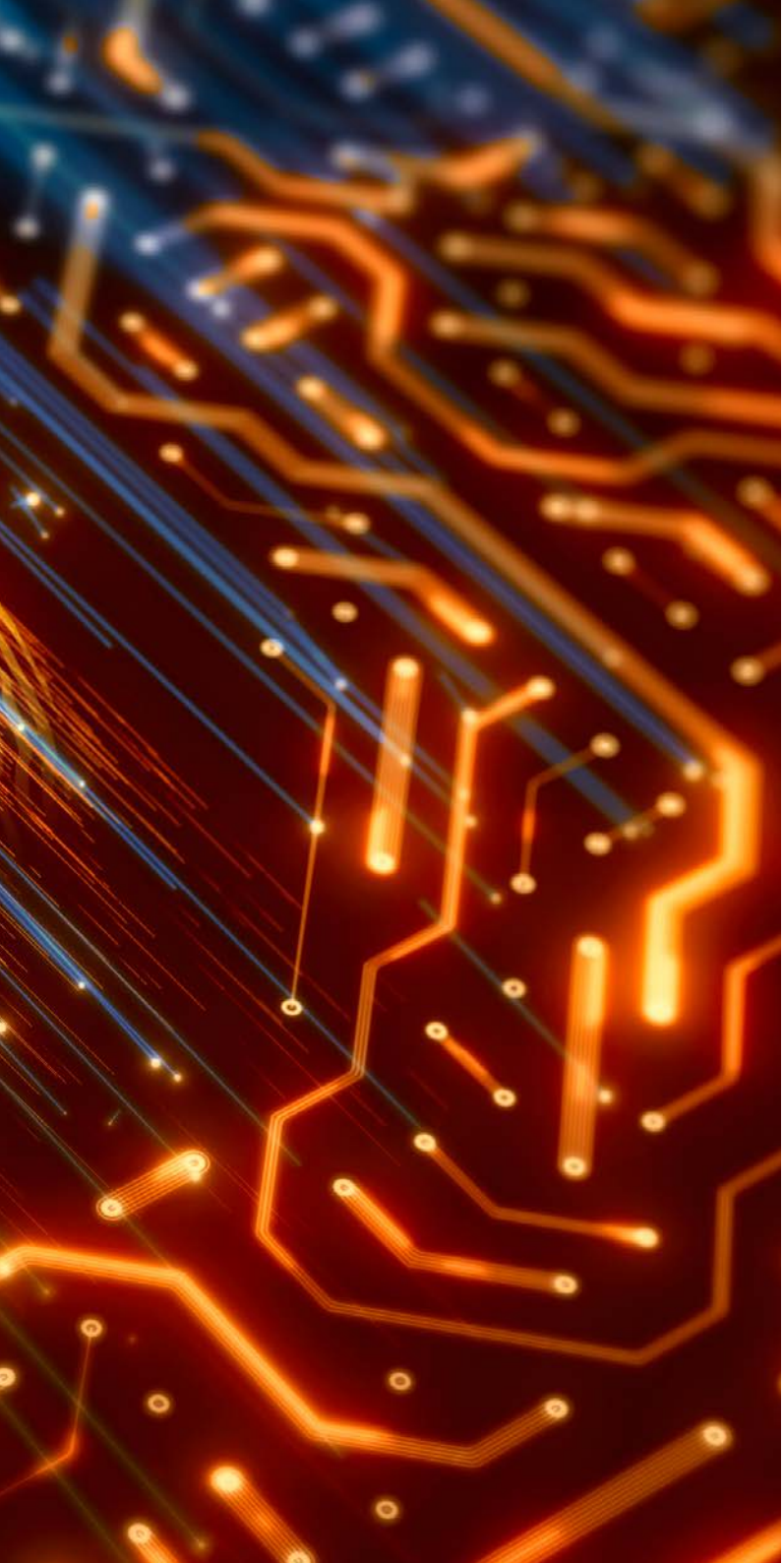
Das Hauptthema der CWIX war die wiederkehrende Interoperabilitätsübung mittels abgestimmtem Szenario. Weiters bot sich die Möglichkeit, parallel dazu zusätzliche Tests, z. B. zum Datenaustausch mit Testpartnern nach vorherigen Absprachen, durchzuführen.

## 5.10 Crossed Swords 2019

Diese technische Cyber Defence Übung fand vom 28. Jänner bis 1. Februar 2019 in Tallinn statt. Sie wurde durch das CCDCoE in Zusammenarbeit mit CERT.LV geleitet und es nahmen circa 40 Soldatinnen und Soldaten und Zivilpersonen aus 20 Staaten teil. Das BMLV stellte dabei drei Teilnehmer vom Zentrum IKT- und Cybersicherheit/MilCyZ.

Der Übungszweck bestand darin, dass Penetrationstester, forensische Experten und Special Operations Forces als gemeinsames Team arbeiteten, um die gesetzten Missionsziele und technischen Herausforderungen in einer virtuellen Cyberumgebung zu erfüllen. Der Hauptfokus lag bei der Entwicklung von taktischen Fähigkeiten in einem reaktiven Cyberverteidigungsszenario und der Bereitstellung von angemessenem Situationsbewusstsein der Teilnehmer. Ein weiteres Ziel der Teilnahme war, die vorhandenen Fähigkeiten im Penetration Testing, welches zur Überprüfung eigener IKT-Systeme benötigt wird, zu verbessern. Besondere Bedeutung kam auch dem Erfahrungsaustausch mit Spezialisten aus anderen Nationen zu.





# 6 Zusammenfassung / Ausblick

Der Berichtszeitraum 2019 war geprägt von einer weiteren Zunahme monetär oder staatlich-strategisch motivierter Angriffe. Darunter fielen vor allem Angriffe mittels Ransomware, mit einer steigenden Tendenz zu spezialisierten Ransomware-Angriffen (Targeted Ransomware). Weiterhin gibt es eine Steigerung der Anzahl von Fällen des Datendiebstahls mittels Advanced Persistent Threats (APTs). Deren Auftreten und Bewältigung wird öffentlich mit größter Zurückhaltung kommuniziert.

## Cyberangriff auf das Bundesministerium für europäische und internationale Angelegenheiten (BMEIA) aktiviert erstmalig die NIS-Krisenmechanismen

Ende des Jahres 2019 fand auf das Bundesministerium für europäische und internationale Angelegenheiten (BMEIA) ein Cyberangriff statt. Dieser stellte zweifellos einen der bisher größten und umfangreichsten Angriffe auf ein Ministerium in Österreich dar und führte erstmalig zur Aktivierung der im NISG vorgesehenen gesamtstaatlichen Krisenmechanismen. Durch die effiziente Zusammenarbeit aller Einsatzstrukturen und Gremien konnten die Krise rasch unter Kontrolle gebracht werden.

Eine anhaltend positive Entwicklung ist die in den Unternehmen steigende Awareness und Investitionen in Präventionsmaßnahmen. Dies zeigt sich auch bei Kleinstunternehmen, die im Vergleich zum Vorjahr eine ansteigende Tendenz an Ransomware-Angriffen zu verzeichnen haben und daher verstärkt Schutzmaßnahmen getroffen haben.

Vor allem Unternehmen der kritischen Infrastruktur tätigten im Jahr 2019 erneut Investitionen im Bereich der Cybersicherheit. Die zusätzlichen IT-Sicherheitsmaßnahmen und das gesteigerte Sicherheitsbewusstsein sind großteils auf die Schaffung neuer staatlicher Rahmenbedingungen mit ihren regulatorischen Maßnahmen, die Erlassung des Netz- und Informationssystemsicherheitsgesetzes (NISG) einerseits und die Datenschutz-Grundverordnung (DSGVO) andererseits, zurückzuführen.

Zudem trat die auf Basis des NISG erlassene „NIS-Verordnung“ (Netz- und Informationssystemsicherheitsverordnung, NISV) am 18. Juli 2019 in Kraft. Auf Grundlage der in der NISV festgelegten Regelungen zu Sektoren, Meldeschwellenwerte, Kategorien und Maßnahmen hinsichtlich der Sicherheitsvorkehrungen für Betreiber wesentlicher Dienste, nahm das strategische NIS-Büro im August 2019 die Ermittlung der Betreiber wesentlicher Dienste in den sieben Sektoren auf. Zu den generellen Entwicklungen in der IT-Sicherheitsbranche zeigt sich für 2019 eine erneute Ausweitung von Cloud Computing. Dieser Trend wird von den Unternehmen zunehmend mit Skepsis betrachtet, da mit der steigenden Abhängigkeit von externen Anbietern ein Kontroll- und Hoheitsverlust über die eigenen Daten einhergeht. Lokale (On-Premise) Lösungen werden durch Cloudlösungen zunehmend aggressiver vertrieben. Es ist zu erwarten, dass sich diese mittel- bis langfristig durchsetzen werden.

Auf EU-Ebene war das Jahr 2019 im Bereich der Cybersicherheit von zahlreichen bedeutenden Entwicklungen geprägt. Insbesondere mit dem Inkrafttreten des Cybersecurity Acts am 27. Juni 2019 konnte ein wichtiger Schritt sowohl zum Ausbau der Aufgabenbereiche und Fähigkeiten der ENISA sowie in Richtung der Schaffung eines einheitlichen Europäischen Zertifizierungsrahmens für die Cybersicherheit geschaffen werden. Derzeit arbeitet die EU-Kommission in enger Zusammenarbeit mit den Mitgliedstaaten und anderen Stakeholdern an dem sogenannten fortlaufenden Arbeitsprogramm der Union an der europäischen Cybersicherheitszertifizierung zur konsequenten Umsetzung des Cybersecurity Acts.

Der europäische Cybersecurity Act schafft einen einheitlichen Zertifizierungsrahmen.

Die europäische Cyber Diplomacy Toolbox führt ein Cybersanktionenregime ein.

Im Bereich der Cyberdiplomatie stand die Weiterentwicklung der gemeinsamen diplomatischen Reaktion der EU auf böswillige Cyberaktivitäten „Cyber Diplomacy Toolbox“ im Vordergrund, wobei insbesondere das im Mai 2019 angenommene Cybersanktionenregime hervorzuheben ist.

Ein bedeutendes Ereignis auf EU-Ebene im Jahr 2019 waren die Wahlen zum Europäischen Parlament (EP) und dessen reibungsloser Ablauf. Dazu wurden bereits im Vorfeld gezielte Maßnahmen gegen Desinformationskampagnen gegen die EU gesetzt. Ein Ergebnis ist der im Dezember 2018 verabschiedete Aktionsplan gegen Desinformation, der eine Reihe von Maßnahmen zur Bekämpfung von Desinformation vorsieht. Die Bilanz des Aktionsplans war durchaus erfreulich, denn die gesetzten Maßnahmen zeigten Wirkung und aufgrund des koordinierten Vorgehens konnten etliche Versuche, die Wahlen zum EP zu beeinflussen, verhindert werden.

Die 5G-Thematik bzw. die als Sicherheit der „fünften Generation des Mobilfunknetzes“ (5G) betitelte Technologie stand 2019 nicht nur im Fokus zahlreicher Debatten auf EU-Ebene, sondern ist ebenso ein prioritäres Thema in Österreich. Anfang des Jahres 2020 wurde die 5G-Toolbox (Cybersecurity of 5G networks, EU Toolbox of risk mitigating measures) von der EK vorgestellt, die es nun national umzusetzen gilt.