Bericht Cybersicherheit für das Jahr 2022

Bericht Cybersicherheit für das Jahr 2022

Wien, 2023

Bundeskanzleramt

Bundesministerium
Inneres

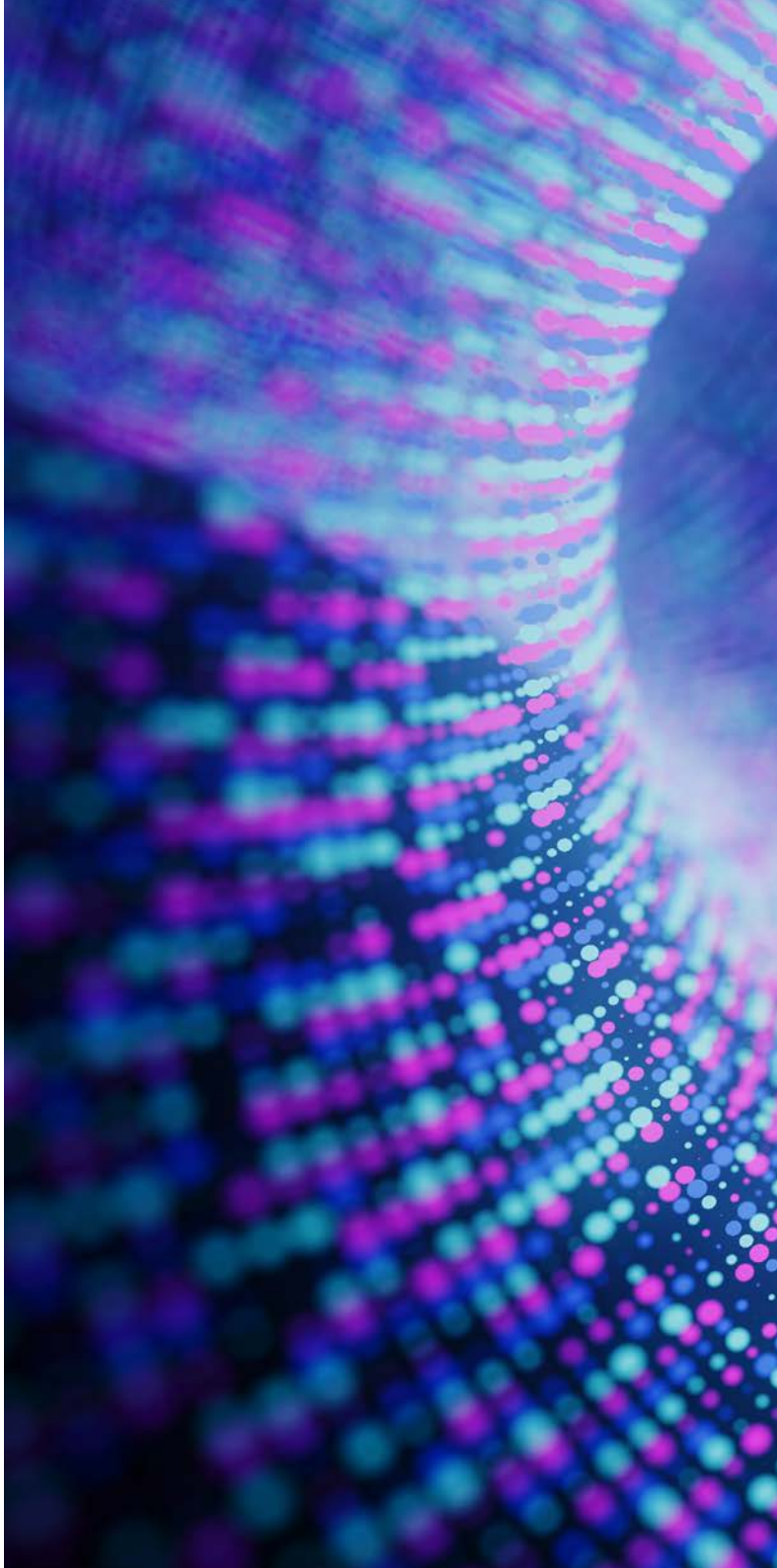
Bundesministerium
Landesverteidigung

Bundesministerium
Europäische und internationale
Angelegenheiten

Impressum

Medieninhaber, Verleger und Herausgeber:
Bundeskanzleramt
Ballhausplatz 2, 1010 Wien
bundeskanzleramt.gv.at
Fotonachweis: iStock
Layout: BKA Design & Grafik
Wien, Dezember 2023

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 November 2022 vorgelegt.

Der aktuelle Bericht Cybersicherheit für das Jahr 2022 baut auf den Inhalten des letztjährigen Berichtes auf und ergänzt diesen um aktuelle Entwicklungen mit Schwerpunkten in den Bereichen internationale und operationelle Entwicklungen. Beobachtungszeitraum ist das Jahr 2022, einzelne aktuelle Entwicklungen im Jahr 2023 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 Steigerung der digitalen Widerstandsfähigkeit Österreichs und die Gewährleistung von Cybersicherheit in der digitalen Welt insgesamt sind sowohl für unseren Wohlstand als auch für unsere Sicherheit von großer Bedeutung.

Für Österreich ist Cybersicherheit daher eine der obersten Prioritäten und eine gemeinsame Herausforderung für Staat, Wirtschaft, Wissenschaft und Gesellschaft.

1.1 Lage Cybersicherheit – operative Ebene

1.1.1 Operatives Lagebild – Überblick

Neben den weiter anhaltenden Auswirkungen der Corona-Pandemie begann im Februar 2022 der russische Angriffskrieg gegen die Ukraine und rückte aufgrund von russischen Cyberangriffen das Wort „Cyberkrieg" ins mediale Rampenlicht.

Abseits des Kriegs war Österreich ein verstärktes Opfer von Ransomwareangriffen auf Universitäten, verfassungsmäßige Einrichtungen, kleine und mittlere Unternehmen (KMUs) sowie Großunternehmen. Zumeist wurden die Systeme der Betroffenen verschlüsselt und damit einhergehend Lösegeld gefordert. Gruppierungen wie *„BlackCat"* und *„Vice Society"* bekannten sich zu Taten in Österreich. Der Umfang des Datendiebstahls war je nach Betroffenen unterschiedlich und reichte von der Einschränkung diverser IT-Services bis hin zum Verlust von sensiblen (personenbezogenen) Daten.

Österreich ein verstärktes Opfer von Ransomware-angriffen

Im Juli 2022 wurde bekannt, dass österreichische Unternehmen Ziel von Spionageangriffen waren. Industriespionage ist nicht nur für die betroffenen Unternehmen nachteilig, sondern stellt auch eine Gefährdung der nationalstaatlichen Cybersicherheit dar. Das Erkennen und die Abwehr derartiger Angriffe erfordert einen erhöhten Ressourceneinsatz sowie einen verstärkten Fokus auf die zur Anwendung kommenden Taktiken, Techniken und Prozeduren (TTPs).

1.1.2 Krieg in der Ukraine

Schon vor – vor allem aber mit – dem Beginn des russischen Angriffskriegs gegen die Ukraine kam es zu Cyberangriffen gegen ukrainische Einrichtungen. So wie schon bei dem Vorfall NotPetya im Jahr 2017 wurden dadurch Auswirkungen auf europäischer Ebene befürchtet, die Cyberabwehrmaßnahmen in EU-Mitgliedstaaten notwendig machen könnten. Im Fall von NotPetya verschlüsselte die angewandte Sabotage-Schadsoftware IT-Infrastrukturen in der Ukraine und gelangte über internationale IT-Firmennetze auch ins Ausland, wo sie einen Schaden in Milliardenhöhe verursachte.

In Österreich wurden die Einschätzung der Bedrohungslage und die sich daraus abzuleitenden Vorbereitungen in Abstimmung mit den im Inneren Kreis der Operativen Koordinierungsstruktur (IKDOK) vertretenen staatlichen Organisationen vorgenommen. Noch vor der Invasion wurde ein Sonderlagebild an die IT-Sicherheitsvertreterinnen und -vertreter der kritischen Infrastrukturen und verfassungsmäßigen Einrichtungen übermittelt, um vor potentiellen Szenarien bei einem Angriff Russlands zu warnen. Die in Europa feststellbaren Auswirkungen in der Cyberdomäne entsprachen den erwarteten Szenarien, wobei Österreich von diesen fast gänzlich verschont geblieben ist. Die einzige bekannte Ausnahme waren mehrere DDoS-Angriffe im Dezember 2022 von einer oder mehreren prorussischen Hackergruppierungen, welche IT-Netzwerkkomponenten von kritischen Infrastrukturen und verfassungsmäßigen Einrichtungen für je ein bis zwei Tage überlasteten. In weiterer Folge wurden diese Vorfälle als „Erfolge“ auf Telegram-Kanälen veröffentlicht. Diese Vorfälle zogen jedoch keinen bleibenden Schaden nach sich. Vorbereitete Prozesse und Vorgänge konnten gleichzeitig umgesetzt und verbessert werden.

1.1.3 Ransomware

Der größte Ransomware bedingte Vorfall im Jahr 2022 war der Angriff der Gruppierung „*BlackCat*“ auf die IT-Systeme der Landesregierung Kärnten. Dies hatte zur Folge, dass ein Großteil der internen Systeme nicht mehr funktionstüchtig war und somit viele Dienstleistungen des Landes den Bürgerinnen und Bürgern temporär nicht mehr zur Verfügung standen. Die Angreifenden versuchten weiters durch das Veröffentlichen von gestohlenen personenbezogenen Daten, die Landesregierung zur Zahlung eines Lösegelds zu zwingen.

Bei Ransomware handelt es sich um Erpressungssoftware, die ein IT-System sperren kann und anschließend ein Lösegeld für die Freigabe fordert. ‚*Ransom*‘ ist der englische Begriff für ‚Lösegeld‘.

Herausforderung für die Aufgaben des Gesamtstaates

Es ist damit zu rechnen, dass derartige Vorfälle auch zukünftig eine Herausforderung für die Aufgaben des Gesamtstaates und dessen Verpflichtungen gegenüber den Bürgerinnen und Bürgern darstellen werden. Ransomware ist in den letzten Jahren zu einer zunehmend verbreiteten und lukrativen Bedrohung geworden. Ein Faktor, der zum Wachstum von Ransomware beiträgt, ist die zunehmende Raffinesse der Angriffe. Die Tragweite von Ransomware hat sich von der einfachen Verschlüsselung einiger weniger Dateien zu komplexen und gezielten Angriffen entwickelt, die ganze Netzwerke und Systeme verschlüsseln können. Darüber hinaus hat es der Aufstieg der Kryptowährungen für Angreifende einfacher gemacht, Zahlungen anonym zu erhalten. Neben den technischen Fortschritten entwickelten sich die dahinterstehenden kriminellen Gruppen zu regelrecht professionellen Firmen, welche eine sogenannte „*Software as a Service*“ (SaaS) an Partnerinnen und Partner anbieten, um damit Opfernetzwerke angreifen und die Daten erfolgreich bis zur Zahlung als „Geisel“ halten zu können.

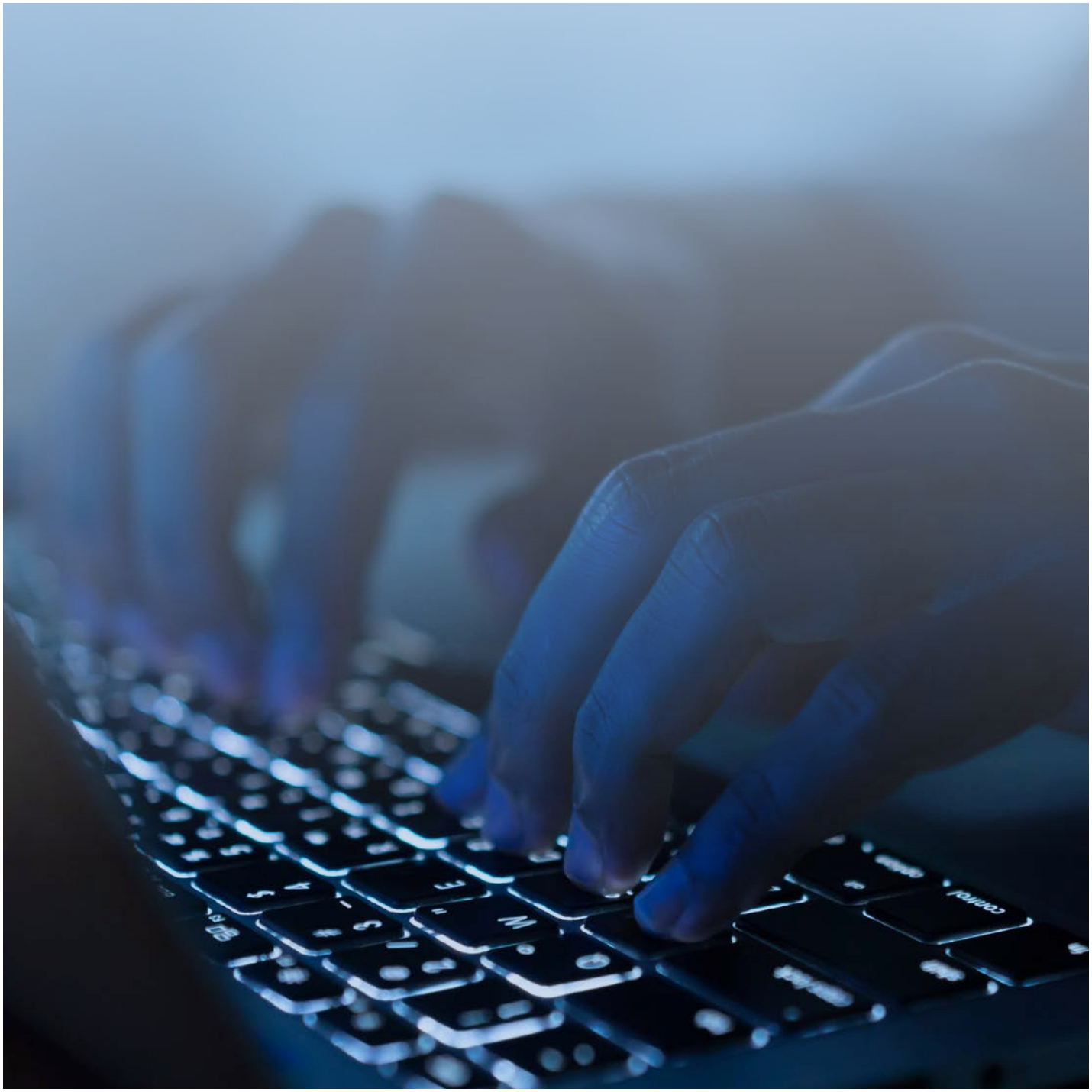
1.1.4 Private Sector Offensive Actor (PSOA)

Die letzten Monate und Jahre waren von dem bekanntgewordenen Einsatz von Überwachungs- und Spähsoftware geprägt:

Die Spionagesoftware ‚Pegasus' eines israelischen Unternehmens führte zu zahlreichen Opfern, deren mobile Endgeräte durch den Einsatz dieser Schadsoftware ausgespäht wurden. Das Europäische Parlament setzte nach Bekanntwerden der Vorfälle im Jahr 2022 einen Untersuchungsausschuss zum Einsatz von ‚Pegasus' und ähnlicher Überwachungs- und Spähsoftware ein.

Die Gefährdung, die von Software mit Spionagefunktionalität ausgeht, beschränkt sich also nicht nur auf kriminelle Gruppierungen und unrechtmäßige Eingriffe staatlicher Akteure, sondern findet mitunter auch aus wirtschaftlichen oder juristischen Motiven ihre Anwendung. Somit erhöht sich der Kreis potentieller Opfer und diese PSOAs werden zunehmend zu einer Gefährdung der gesamtstaatlichen Cybersicherheit.

Die in diesem Geschäftssektor tätigen Unternehmen sind finanziell in der Lage, sich auf verschiedenen Dark- und Greymarkets mit entsprechenden 0-Day- und n-Day-Schwachstellen zu versorgen und diese in ihre Spionageprodukte zu integrieren. Das Herausfordernde an diesen Schwachstellen ist, dass es sich dabei um, der Allgemeinheit und den Herstellenden unbekannte, Schwachstellen handelt, gegen die es in der Folge auch keine direkten Verteidigungsmaßnahmen gibt.



‚*Private Sector Offensive Actor*' ist der englische Begriff für offensive Akteure des Privatsektors. Damit werden Cyberaktivitäten von Privaten beschrieben, die durch den Verkauf von Softwarelösungen, das Ausspähen von beispielsweise Regimekritikerinnen und -kritikern, Menschenrechtsverteidigerinnen und -verteidigern, Journalistinnen und Journalisten und anderen Personen möglich machen.

1.2 Lage Cybersicherheit – Unternehmen und Sicherheitsdienstleister

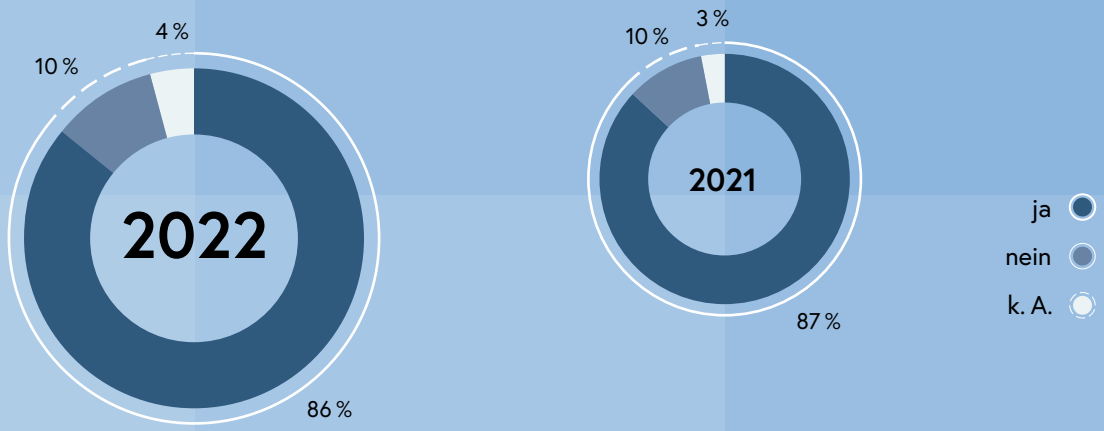
Staat arbeitet bei Lagebilderstellung mit kritischer Infrastruktur zusammen

Staatliche Stellen arbeiten im Bereich der Lagebilderstellung und -beurteilung nach dem Kooperationsmodell mit Bedarfstragenden zusammen: Zur Erstellung des vorliegenden Berichtes wurden auch in diesem Berichtsjahr wieder Unternehmen der kritischen Infrastruktur, verfassungsmäßige Einrichtungen sowie führende private Unternehmen aus der Cybersicherheitsbranche eingeladen, aus eigener Perspektive zum Informationsaufkommen beizutragen und mit ihrer Expertise zu unterstützen. Auf diese Weise wird ein weitestgehend vollständiges Bild der Cyberlage in Österreich erstellt. Dabei liegt das Augenmerk nicht nur auf konkreten Vorfällen, sondern auch auf Trends und Entwicklungen im Sinne einer abstrakten Überblicksdarstellung.

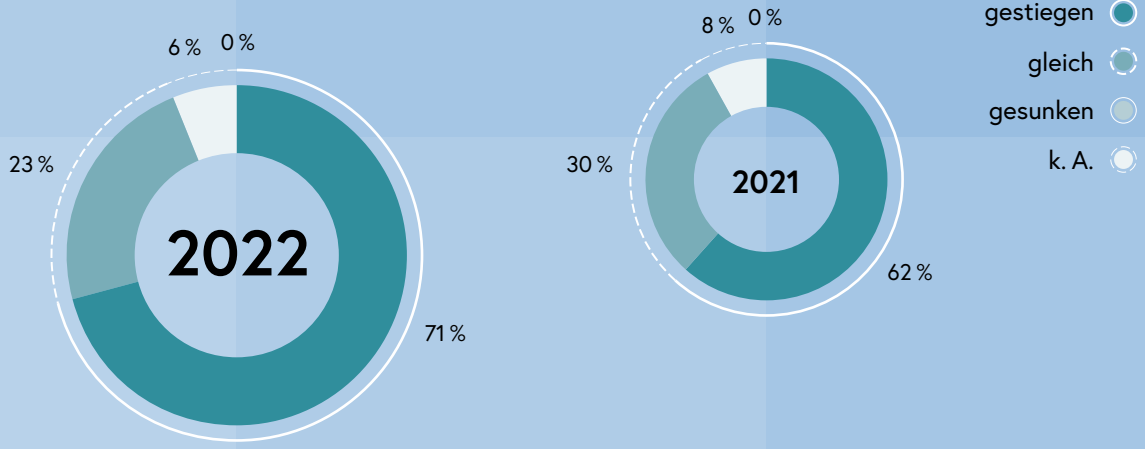
1.2.1 Lageeinschätzung Unternehmen der kritischen Infrastruktur und verfassungsmäßige Einrichtungen

Im Berichtsjahr 2022 wurden wie schon in den Vorjahren bei der Mehrheit der befragten österreichischen Unternehmen der kritischen Infrastruktur Investitionen im Bereich der Cybersicherheit getätigt. Kein Unternehmen verminderte das Budget für Cybersicherheit, der Großteil investierte mehr in Cybersicherheit. Insgesamt bestätigt sich der Trend, die Ausgaben für IT-Sicherheit auf einem hohen Niveau zu halten. Durch diese Investitionen konnten mutmaßlich schwerwiegende IT-Sicherheitsvorfälle verhindert werden.

Wurden in Ihrer Firma 2022 neue Cybersicherheitsmaßnahmen implementiert, welche die Erkennbarkeit von IT-Sicherheitsvorfällen erhöhen können?



Wie hat sich in Ihrer Firma im Jahr 2022 das für Cybersicherheit zur Verfügung stehende Budget gegenüber dem Jahr 2021 verändert?



Auch im Berichtszeitraum stieg das Budget für Cybersicherheit im vergleichbaren Ausmaß bei allen befragten Unternehmen wie schon im Vorjahr.

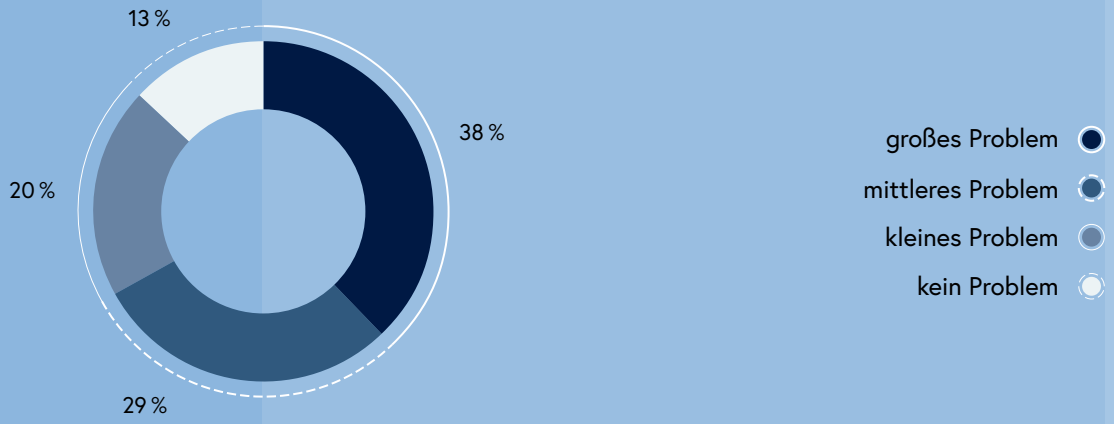
Die befragten Unternehmen haben im Berichtszeitraum eine Vielzahl an unterschiedlichen Sicherheitsmaßnahmen implementiert. Exemplarisch wurden genannt:

- Einführung von SIEM-, SOC-, EDR- oder ISMS-Lösungen
- Verbesserung von bestehenden IDS/IPS- und MDM-Lösungen, um eine bessere Struktur zur Erkennung und Abwehr von Cyberangriffen zu erreichen
- Einführung von Multi-Faktor-Authentifizierung (MFA)
- Umsetzung von *Backup*-Konzepten

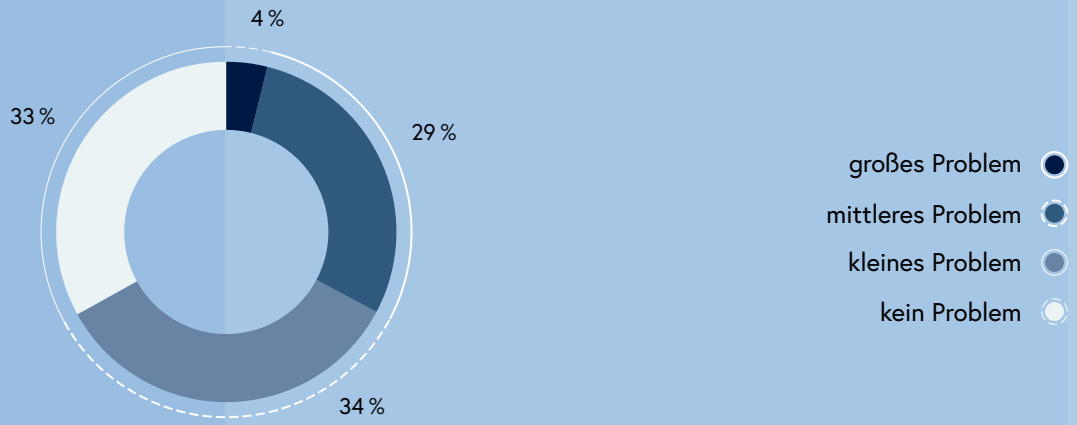
Für die kritischen Infrastrukturen und die Betreiber wesentlicher Dienste wurde auch die Einhaltung rechtlicher Vorgaben aus dem Netz- und Informationssystemsicherheitsgesetz (NISG) als ein wesentlicher Punkt angeführt.

2022 wurden primär Außentäterinnen und -tätern bei den meisten Sicherheitsvorfällen verantwortlich gemacht. Auffallend ist aber, dass mittlerweile mehr Unternehmen Innentäterinnen und -tätern als „mittleres Problem“ wahrnehmen (2021: 15 %/2022: 29 %). Auch Auswirkungen von technischen Gebrechen sind in der Wahrnehmung gestiegen und führen mit 14 % Zustimmung als „großes Problem“ für das Jahr 2022 zu einer Verdopplung im Vergleich zum Vorjahr (2021: 7 %).

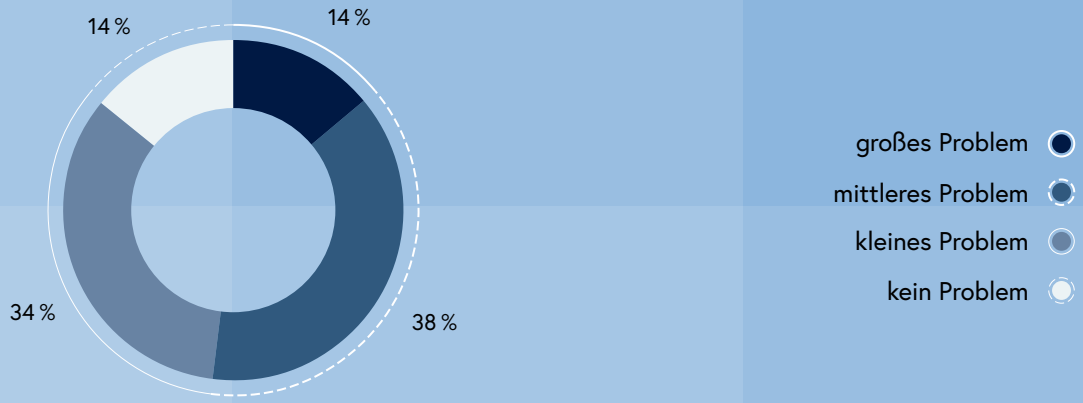
Wie beurteilen Sie die „Vorfallsursache“ für Außentäterinnen und -täter für das Jahr 2022?



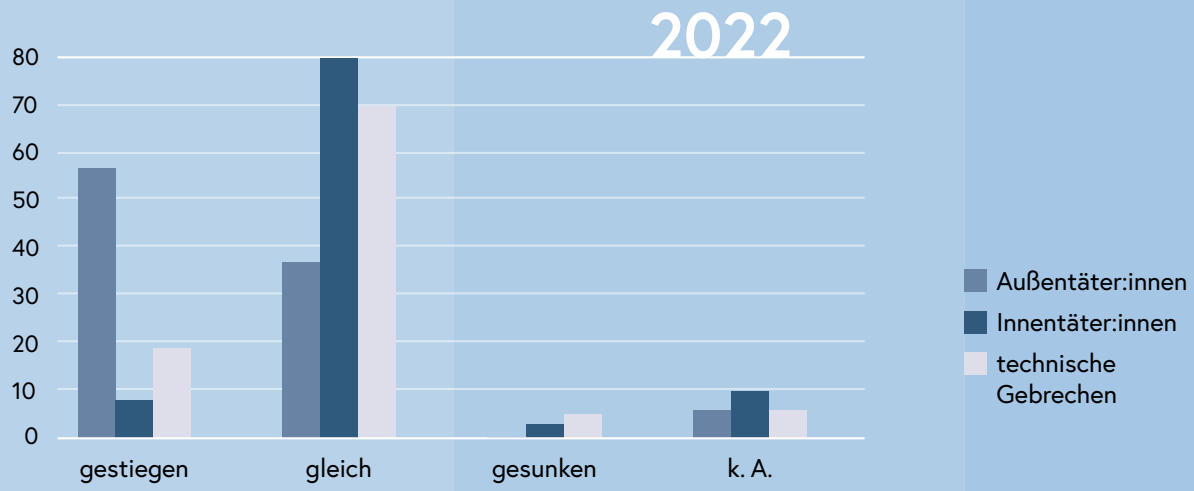
Wie beurteilen Sie die „Vorfallsursache“ für Innentäterinnen und -täter für das Jahr 2022?



Wie beurteilen Sie die „Vorfallsursache“ für technische Gebrechen für das Jahr 2022?



Und welche Trends konnten Sie 2022 diesbezüglich gegenüber 2021 beobachten?

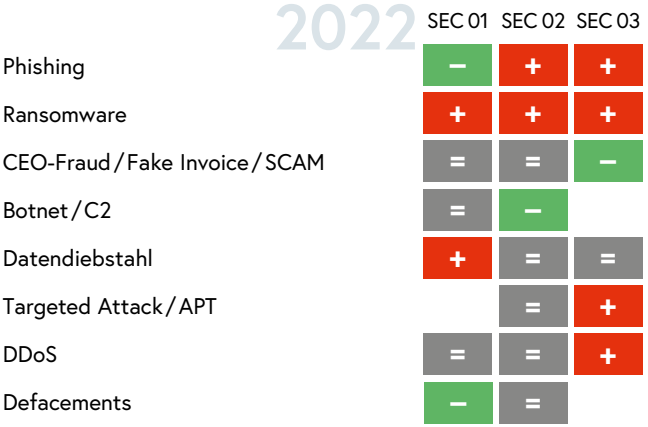


Abgefragt wurde ebenso, welche *Lessons Learned* die Unternehmen der kritischen Infrastruktur und der verfassungsmäßigen Einrichtungen im Beobachtungszeitraum gezogen hatten. Hervorgehoben wurde die wichtige Rolle von Sensibilisierungs- und Schulungsmaßnahmen von Mitarbeitenden zur Erkennung von Phishing-Nachrichten und Social-Engineering-Angriffen.

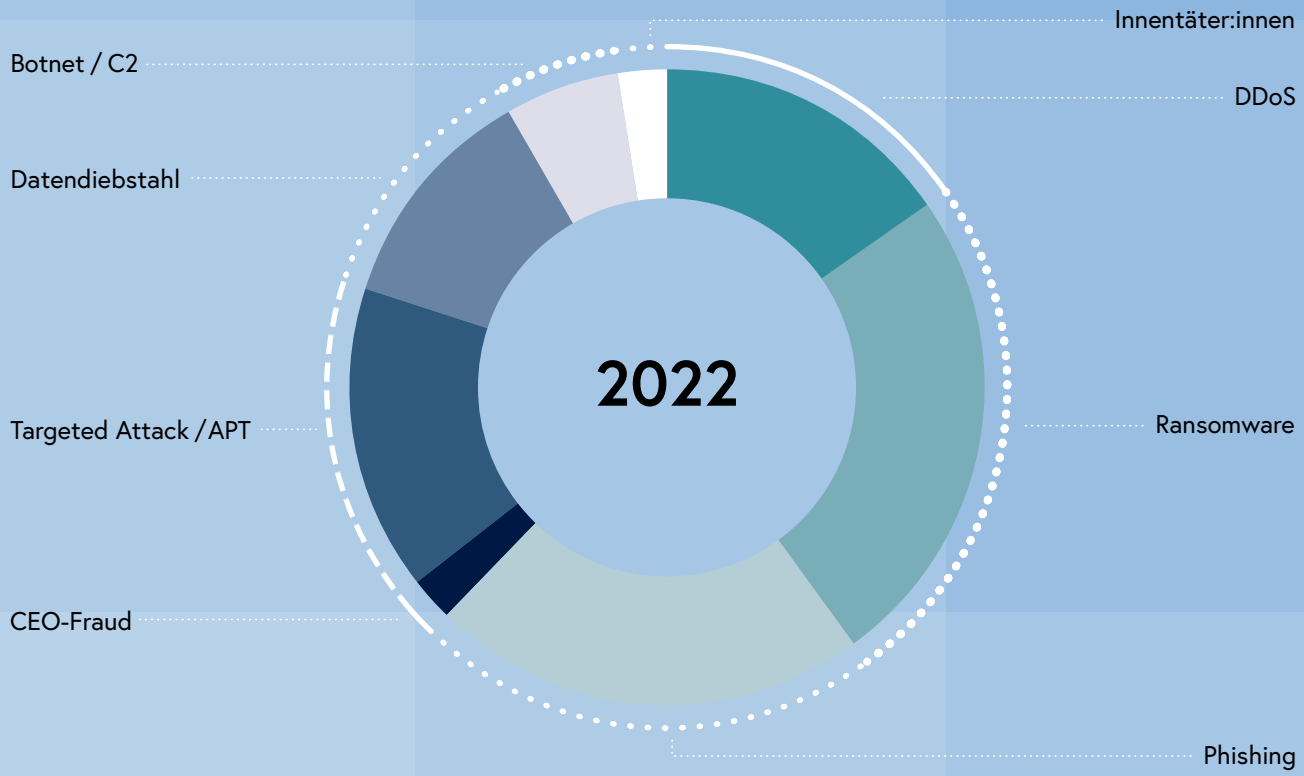
Es sei wichtig, die Lieferkettensicherheit weiter durch Vorgaben von Mindeststandards für Dienstleistende und Lieferantinnen und Lieferanten zu verbessern und Strukturen auf- und auszubauen, um mit Hilfe von Analysen rasch auf Vorfälle reagieren zu können. Beim Vorfallsmanagement sei darüber hinaus eine gute interne und externe Zusammenarbeit wesentlich. Absicherungsmaßnahmen – wie etwa die Einführung von Multi-Faktor-Authentifizierung – werden Unternehmen in den nächsten Jahren etwa bei der Frage der privaten und beruflichen Nutzung von Geräten begleiten.

1.2.2 Lageeinschätzung führender privater Unternehmen aus der Cybersicherheitsbranche

Aus den eingegangenen Beantwortungen der Befragung von führenden privaten Unternehmen aus dem Bereich der Sicherheitsdienstleistenden für das Jahr 2022 lassen sich nachfolgend angeführte Trends und *Lessons Identified* ableiten. Die Rücklaufquote der Beantwortung für das Jahr 2022 ist im Vergleich zum Vorjahr geringer ausgefallen.



Folgende Vorfallsarten waren im Berichtszeitraum bei den rückmeldenden privaten Unternehmen aus dem Bereich der Sicherheitsdienstleister sichtbar:



Folgende Vorfallsarten waren im Berichtszeitraum bei den rückmeldenden privaten Unternehmen aus dem Bereich der Sicherheitsdienstleister sichtbar:

Phishing: Die Resilienz der Unternehmen in Bezug auf Phishing wird noch immer nicht als ausreichend beurteilt. Die Sensibilisierung der Mitarbeitenden, um gefälschte E-Mails und Webseiten zu erkennen, die darauf abzielen, beispielsweise an persönliche Daten zu gelangen, ist oft nicht ausreichend und entsprechendes Bewusstsein in Hinsicht auf Gefahren und Auswirkungen nicht ausreichend vorhanden. Gerade gezielte, auf das Unternehmen und deren Spezifika angepasste E-Mails haben immer noch eine hohe Durchschlagsquote. Auch wenn Awareness-Trainings diesen Angriffsvektor nicht vollständig eliminieren können, sind sie ein probates Mittel, um dieses Gefahrenpotential entsprechend zu reduzieren.

„Detection & Visibility is key" – also das zeitnahe Erkennen und Sichtbarmachen von Cybersicherheitsvorfällen im eigenen Netzwerk – wird als Schlüsselfähigkeit gesehen. Nicht nur um Phishing-Angriffe zu erkennen, sondern auch, um im Zuge der Auswirkungsanalyse auskunftsfähig zu werden.

Awareness-Trainings können Gefahrenpotential reduzieren

Ransomware: Ransomware als die größte Cybersicherheitsbedrohung des Beobachtungszeitraums wird auch in den kommenden Jahren ein konstanter Begleiter sein. Aus technischer Sicht beugt eine Netzwerksegmentierung vor, dass sich Angreifende im IT-Netzwerk ausbreiten und Lösegeldforderungen für die dadurch verschlüsselten Daten stellen können. Das Sicherheitsniveau innerhalb der „Außenverteidigung" ist oftmals weiterhin eine ungelöste Herausforderung. Zusätzlich hat nicht jedes Unternehmen eine Backup-Strategie, die bei Ransomware-Vorfällen verlorene Daten ersetzt.

CEO-Fraud / Business Email Compromise / Fake Invoice / SCAM

Business Email Compromise (BEC), das auf Betrugshandlungen durch die Verwendung falscher Identitäten abzielt, wird oft mit anderen Angriffen kombiniert. Die Sensibilisierung für diese Bedrohung steigt. Mittlerweile haben viele eine gesunde Skepsis gegenüber

dieser Art von *Beeinflussung*. Schulungen in diesem Bereich sollen helfen, nicht Opfer dieses Phänomens zu werden.

Botnet / Command-and-Control-Server (C2): Ohne laufender Sicherheitsüberwachung bleiben mit Schadsoftware infizierte Systeme aktiv, um auf Befehle der Botnetzadministrierenden zu warten. Dadurch wird die eigene Infrastruktur für die Aufgaben Fremder zweckentfremdet und kann für das Opfer auch rechtliche Probleme nach sich ziehen. Veraltete Betriebssysteme (*Legacy Systeme*) sind weiterhin im Einsatz und ein willkommenes Einfallstor für diese Bots und deren Betreibende.

Datendiebstähle sind eine permanente Herausforderung

Datendiebstahl: Datendiebstähle erfolgten im Berichtszeitraum häufig in Kombination mit Ransomware-Angriffen und sind eine permanente Herausforderung. Es wird angenommen, dass die Dunkelziffer von unerkanntem oder nicht gemeldetem Datendiebstahl noch viel höher ausfällt.

Targeted Attack / Advanced Persistent Threat (APT)
Die Anzahl registrierter gezielter Angriffe bei den befragten Unternehmen steigt, ist aber im Gesamtvolumen immer noch als gering anzusehen. Jedoch sind APT-Angriffe immer mit überproportional hohem Schadensausmaß verbunden.

Denial of Service (DDos): Die Abwehr von DDoS-Angriffen erfolgt am effizientesten auf Ebene der Telekomprovider. Dort sollten DDoS-Schutzmechanismen implementiert werden. Wo es vom Inhalt des Webservices her möglich ist, können *Content Delivery Networks (CDNs)* vor DDos-Angriffen schützen bzw. diese zumindest regional eindämmen.

1.3 Lage Cybercrime

Die Betrachtung der polizeilichen Kriminalstatistik lässt mit 60.195 angezeigten Delikten im Jahr 2022 eine Steigerung von 30,4 Prozent gegenüber dem Jahr 2021 erkennen. Die genauen Deliktszahlen werden jährlich im Frühjahr mit der kriminalpolizeilichen Kriminalstatistik veröffentlicht. Eine tiefergehende Analyse und Beschreibung der kriminalpolizeilichen Phänomene erfolgt mit dem jährlichen Cybercrime Report des Bundeskriminalamtes.

Cyberkriminalität ist 2022 wieder gestiegen

Der Begriff Cybercrime umfasst:

- Cybercrime im engeren Sinn,
- Internetbetrug und
- sonstige Kriminalität im Internet.

1.3.1 Cybercrime im engeren Sinn

Im Bereich Cybercrime im engeren Sinn sind die Anzeigen im Jahr 2022 gegenüber dem Jahr 2021 um 44,5 Prozent auf insgesamt 22.376 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. Angriffe durch Schadsoftware, DDoS-Angriffe und widerrechtliche Zugriffe auf Computernetzwerke und -systeme lassen auch 2022 die Anzahl der Anzeigen hierzu enorm steigen. Die Aufklärungsquote ist im Vergleich zum Vorjahr um 2,4 Prozentpunkte auf 21,1 Prozent gestiegen. Erkenntnisse aus dem Bereich DDoS-Protection lassen den Schluss zu, dass Angriffe auf Netzwerkebene zugenommen haben. Ebenso musste festgestellt werden, dass sich die Dauer und Heftigkeit der Angriffe verstärkt haben.

Bei den Anzeigen im Bereich der Ransomware kann beobachtet werden, dass sowohl die Angriffs-Qualität steigt – vermehrt durch Ausnützung aktueller Sicherheitslücken – als auch die jeweiligen Schadenshöhen in den einzelnen Fällen. So wurden im Bundesgebiet

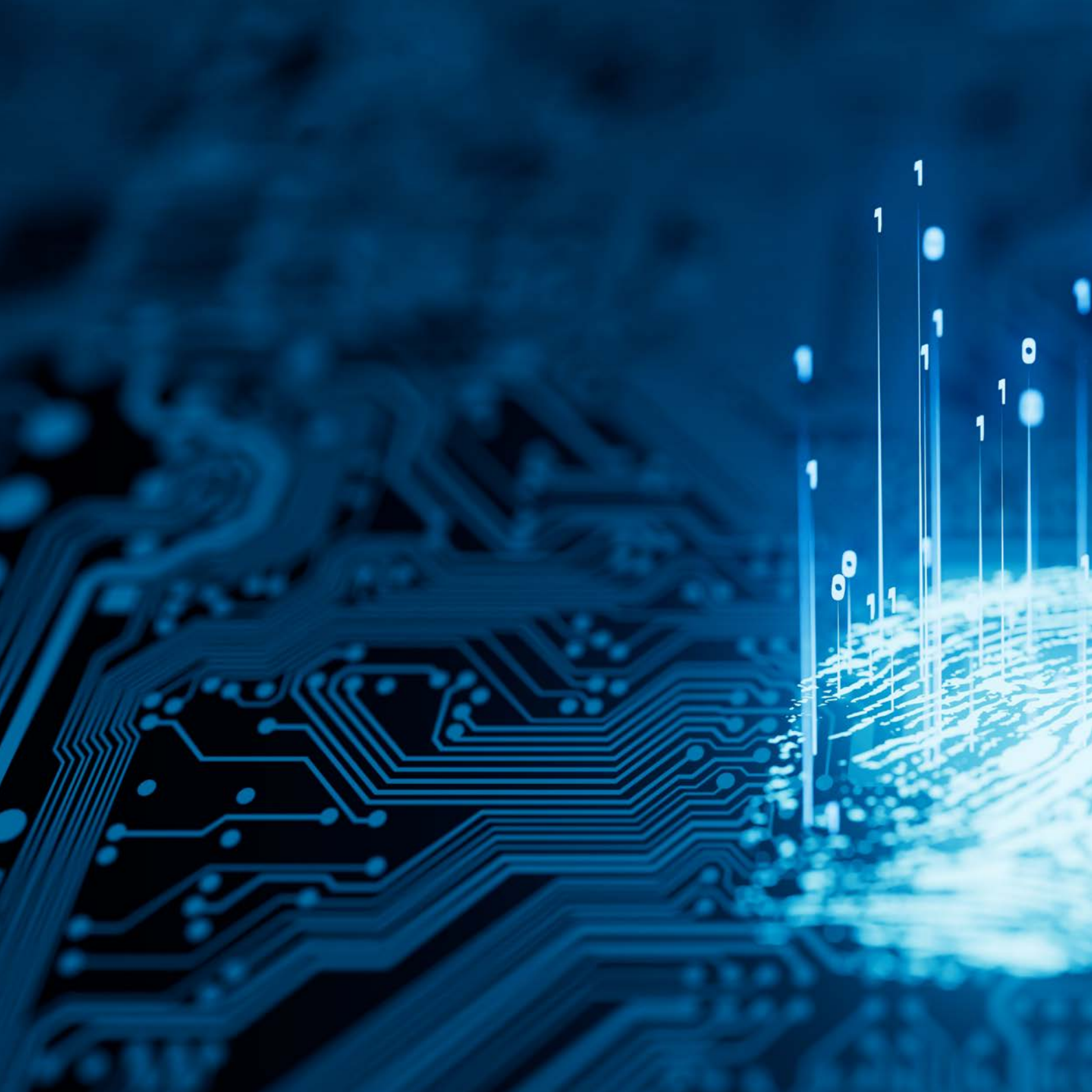
im Jahr 2022 insgesamt 181 Fälle von Ransomware zur Anzeige gebracht. Die Angriffe erfolgten sowohl auf Privatpersonen, Ein-Personen-Unternehmen (EPU) wie auch auf kleine und mittlere Unternehmen (KMUs), Konzerne, Bildungseinrichtungen, das Gesundheitswesen, Gemeinden und Städten. Rund 30 unterschiedliche Tätergruppierungen führten die Angriffe durch. Dass sich diese auf bestimmte Bereiche konzentrieren, konnte nicht festgestellt werden. Bei größeren Unternehmen steigt die Gefahr, dass zusätzlich zur Verschlüsselung auch noch mit der Veröffentlichung von Unternehmensdaten gedroht wird. Nach einem Schadensfall ist gerade bei größeren Unternehmen damit zu rechnen, dass es trotz vorhandener Backups für mindestens drei bis sieben Tage zu Produktionsausfällen kommen kann. Aufgrund zunehmender Arbeitsteilung („*Crime-as-a-Service*“) und Vernetzung der Tätergruppen wird eine erfolgreiche Strafverfolgung zunehmend erschwert.

Ebenso werden immer häufiger Cybermobbing-Vorfälle zur Anzeige gebracht.

1.3.2 Internetbetrug

Cybermobbing-Vorfälle werden häufiger angezeigt

Der Internetbetrug stellt zahlenmäßig den größten Faktor im Bereich der Cyberkriminalität dar und ist auch maßgeblich für den letztjährigen Gesamtanstieg der Delikte mitverantwortlich. Fast die Hälfte der Internetdelikte fallen auf Betrugsdelikte: 2022 wurden 27.629 Fälle von Internetbetrug angezeigt. Das ist ein Plus von 23,1 Prozent. Mit der fortschreitenden Digitalisierung verlagern sich Betrugsdelikte immer mehr ins Netz. Für die Täterinnen und Täter ist es ein Leichtes, aufgrund technischer Anonymisierung sowie Verschleierung der Finanzflüsse Betrugshandlungen unerkannt und damit „sicher“ durchzuführen. Zusätzlich können durch den weltweiten Online-Zugang immer mehr Menschen als potentielle Opfer angesprochen werden. Der Bestellbetrug – sowohl käufer- als auch verkäuferseitig – gehört hierbei zu den größten Bereichen, gefolgt von unbefugten Abbuchungen von Bankkonten der Opfer. Auch der Anrufbetrug (Stichwort „falscher Polizist“) und international agierende Call Center trieben die Statistik in die Höhe, ebenso wie der digitale Investmentbetrug.



1.3.3 Sonstige Kriminalität im Internet

Unter sonstiger Kriminalität im Internet versteht man Straftaten, die ihren Tatort im Internet haben. Ausgenommen sind Cybercrime im engeren Sinn, der Internetbetrug, pornografische Darstellungen Minderjähriger (§ 207a StGB) und die Anbahnung von Sexualkontakten zu Unmündigen (§ 208a StGB). Auch hier wurde im Jahr 2022 ein Anstieg der Delikte verzeichnet. Der Grund hierfür 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 Hacking-Werkzeuge oder Erpressungstrojaner. Ebenso wurde ein vermehrter Vertrieb von Falschgeld, Kinderpornografie, Kreditkartendaten und gefälschten Urkunden wahrgenommen. § 207a StGB (Pornographische Darstellungen Minderjähriger) verzeichnete einen Zuwachs von 7,3 Prozent im Jahresvergleich (2.061 angezeigte Fälle 2022). Durch die im Darknet angebotenen Dienste stiegen vor allem Erpressungen mit Ransomware und Massenerpressungsmails sehr stark an, meist begleitet von Geldforderungen in Bitcoins.

Deutliche Zunahmen wurden auch bei § 105 StGB (Nötigung) mit 450 Anzeigen und § 106 StGB (Schwere Nötigung) mit 270 Anzeigen verzeichnet. Ebenso stiegen Anzeigen nach § 223 StGB (Urkundenfälschung) und § 3g Verbotsgesetz (Wiederbetätigung).

Auffällig ist die Zunahme von Angriffen, bei denen DDoS-Angriffe mit Erpressung kombiniert wird. Angreifende überlasten hierbei zunächst eine Anwendung des Opfers. Anschließend folgt eine Zahlungsaufforderung. Wird dieser nicht nachgekommen, folgen weitere DDoS-Angriffe. Auch konnte festgestellt werden, dass Hackerinnen und Hacker Künstliche Intelligenz (KI) für die Programmierung von Malware nutzen, wobei dies erste Tests zu sein scheinen. Da es sich bei der KI um ein lernendes System handelt, ist anzunehmen, dass in Zukunft auch komplexe Schadsoftware damit erstellt werden könnte. Neben Malware könnte die Software beim Erstellen von Darknet-Marktplätzen oder Phishing zum Einsatz kommen.

Ebenso konnte beobachtet werden, dass Anschlussdelikte nach einem Diebstahl oder Verlust von Bankomatkarten mit NFC-Funktion steigen. Derzeit können mit diesen Karten fünf Bezahlvorgänge bis 50 Euro ohne Eingabe eines PINs durchgeführt werden.

1.4 Cyberlage Landesverteidigung

Das Jahr 2022 wurde im Cyberraum vor allem durch die Folgen des russischen Angriffskriegs gegen die Ukraine sowie auch noch von der COVID-19-Pandemie geprägt.

Desinformationskampagnen werden als Teil der Cyberdomäne betrachtet

Der langjährige, hybrid ausgetragene Konflikt zwischen Russland und Ukraine eskalierte im Februar 2022 unter intensiver Nutzung der Cyberdomäne im unmittelbaren Vorfeld des militärischen Angriffes. Die derzeitige Erkenntnis ist, dass Cyberoperationen im Rahmen der hybriden Kriegsführung eine steigende Bedeutung im Informationsraum, zur unmittelbaren Unterstützung von Luft- und Bodenoperationen und bei Angriffen und Sabotageattacken gegen zivile und militärische kritische Infrastruktur zukommen. Wenn auch eine direkte Eskalation im Cyberraum gegen die Unterstützerländer der Ukraine bzw. jener Länder, welche Sanktionen gegenüber Russland mittragen, bisher ausgeblieben ist, kann dies zukünftig nicht ausgeschlossen werden.

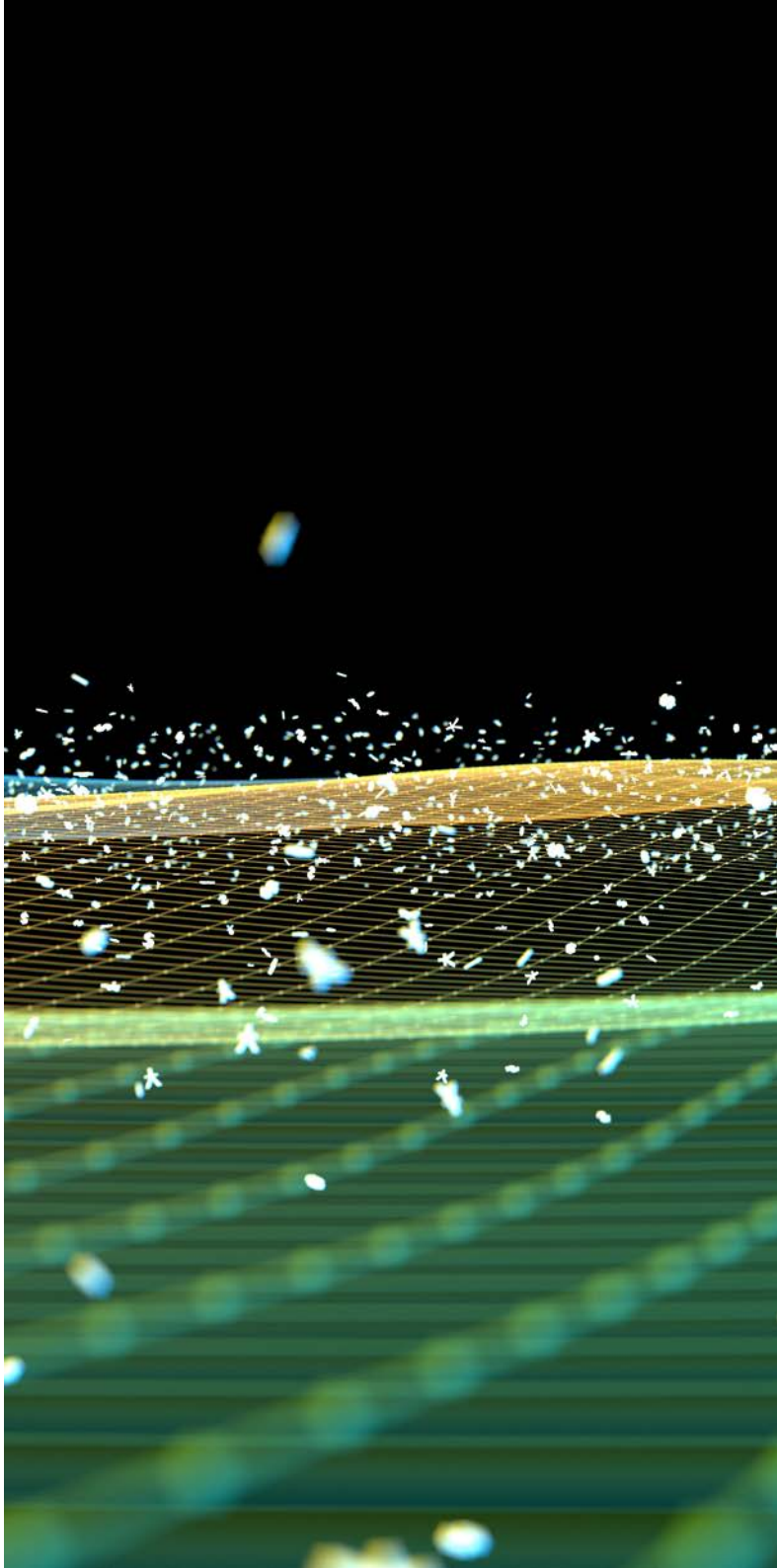
Tendenziell ist 2022 eine Zunahme an Cyberbedrohungen für die kritische Infrastruktur, die öffentliche Verwaltung, Forschung, Industrie sowie politische Institutionen und internationale Organisationen in Österreich und Europa festzustellen. Neben klassischen Cyberbedrohungen, wie Ransomware oder DDos-Angriffe, werden auch Bedrohungen des Informationsraums als Teil der Cyberdomäne betrachtet. Der Informationsraum wird unter anderem durch Desinformationskampagnen und/oder Manipulation in Sozialen Medien durch seine meinungsbeeinflussende Wirkung in der Gesellschaft – im Krieg um Narrative – zu einer wesentlichen Komponente auch im Kampf mit konventionellen militärischen Kräften. Das Ziel solcher Desinformationskampagnen richtet sich vor allem darauf aus, den gesellschaftlichen Zusammenhalt zu schwächen, zur allgemeinen Verunsicherung beizutragen, eine Spaltung der EU oder von Verbündeten zu bewirken, Regierungen oder demokratische Systeme zu untergraben sowie den Wehrwillen einer Gesellschaft und in den Streitkräften zu schwächen.

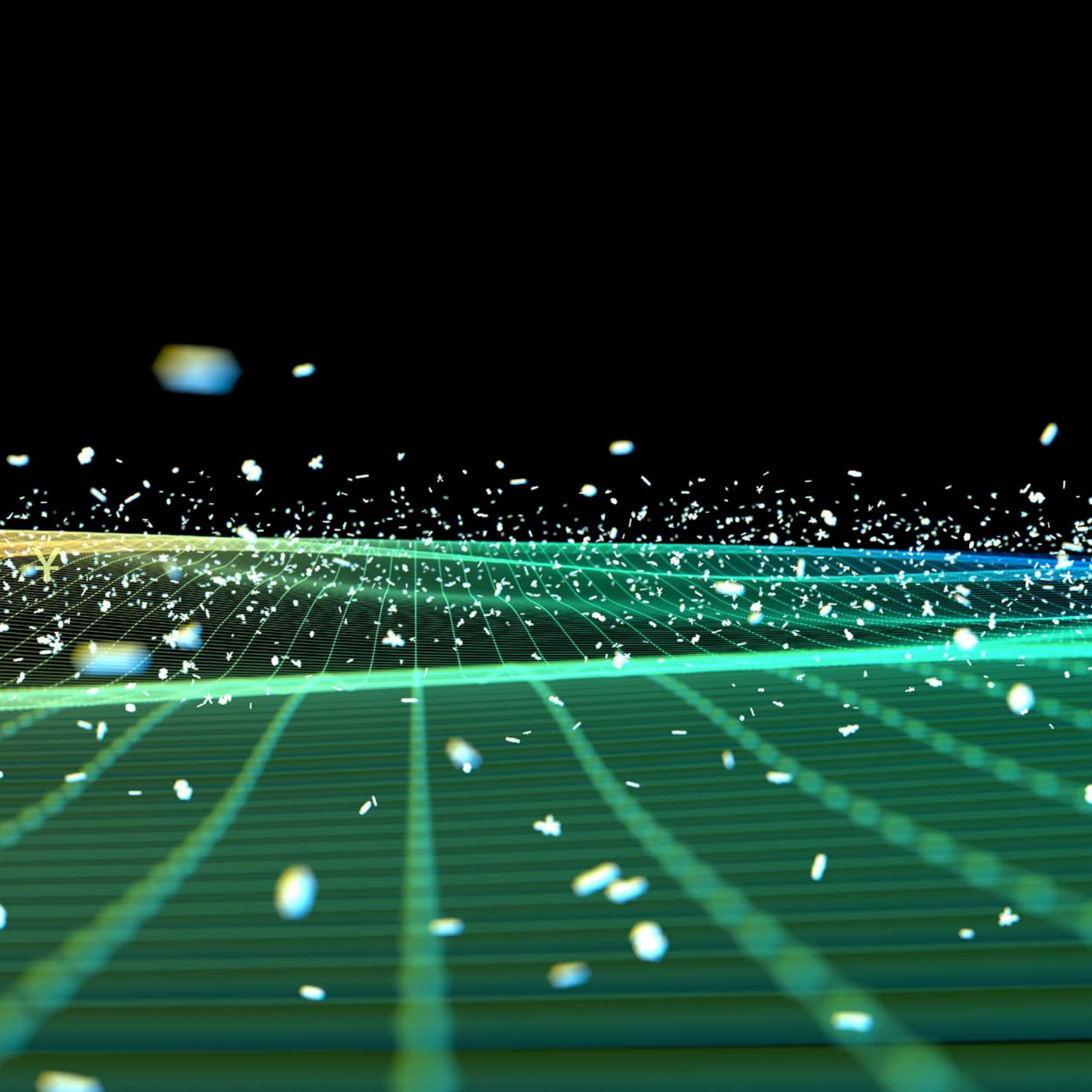
Im Bereich Cyberverteidigung wird die Bedeutung des Einsatzes in der militärischen Domäne weiter steigen. Kein militärischer Einsatz wird ohne Cyber- und Informationskräfte durchführbar sein. Der Cyber- und Informationsraum und das elektromagnetische Spektrum, aber auch der Weltraum sowie die steigenden Möglichkeiten im Zusammenhang mit Künstlicher Intelligenz, werden im Rahmen hybrider Konfliktaustragung künftig noch mehr an Bedeutung gewinnen. Ein zusätzliches Eskalationspotential sind die anhaltenden und bereits auf einem hohen Niveau stattfindenden Cyberangriffe von nichtstaatlichen Cyberakteuren, welche das bisherige Kriegsbild verzerren. Um diesen Herausforderungen begegnen zu können, empfiehlt es sich, umfangreiche militärische und zivile Kapazitäten mit entsprechender Durchhaltefähigkeit aufzubauen.

Das Bundesministerium für Landesverteidigung (BMLV) und das Österreichische Bundesheer (ÖBH) verfügen über umfangreiche Fähigkeiten zum Eigenschutz sowie zum Schutz der österreichischen Souveränität im Cyberraum. Die erforderlichen Qualitäten sind größtenteils vorhanden bzw. im weiteren Aufbau, sollten jedoch gleichzeitig konsequent weiter ausgebaut werden, um den durch die Digitalisierung der Streitkräfte steigenden Schutzbedarf zu bewältigen.

Schutz der österreichischen Souveränität im Cyberraum

Das ÖBH ist laufend in Kontakt mit den Sicherheitsgremien auf nationaler, europäischer und internationaler Ebene, um die Cyberverteidigung Österreichs zu gewährleisten. Die Cyberverteidigung umfasst sowohl alle Maßnahmen der Informations- und Kommunikationstechnologiesicherheit als auch Maßnahmen zur Abwehr von souveränitätsgefährdenden Cyberangriffen auf die Republik Österreich. Um in und für Österreich staatliche Souveränität und Resilienz im Cyberraum sicherstellen zu können, müssen die für die Bereiche Cybersicherheit, Cyberintelligence, Cyberkriminalität, Cyberdiplomatie und Cyberverteidigung sowie Schutz kritischer Infrastrukturen zuständigen Stellen gesamtstaatlich zusammenarbeiten und ihr Wissen laufend an die fortschreitenden Herausforderungen anpassen.





2
Internationale Entwicklungen

Die Europäische Union und ihre Mitgliedstaaten setzen sich nachdrücklich für einen offenen, freien, stabilen und sicheren Cyberraum ein, in dem die Menschenrechte, die Grundfreiheiten und die Rechtsstaatlichkeit uneingeschränkt geachtet werden.

Damit sollen soziale Stabilität, Wirtschaftswachstum, Wohlstand und die Integrität freier und demokratischer Gesellschaften gewährleistet werden

2.1 Europäische Union (EU)

Die zunehmende Bedeutung der Cybersicherheit zeigte sich auch im Jahr 2022. Dieses Thema wird in immer mehr internationalen Organisationen oder multilateralen Foren aufgegriffen.

Cybersicherheit wird dabei nicht nur in den direkt darauf Bezug nehmenden Rechtsakten[1] adressiert, sondern erlangt auch in anderen Themenbereichen zunehmend Bedeutung (etwa im Bereich der Künstlichen Intelligenz).[2]

Außen- und sicherheitspolitische Maßnahmen werden vom Bundesministerium für europäische und internationale Angelegenheiten (BMEIA) koordiniert, dem Bundeskanzleramt (BKA) obliegt die Koordination der Cybersicherheit im Zusammenhang mit der Europäischen Union (EU).

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.

2.1.1 Horizontale Gruppe „Fragen des Cyberraums“ (HWPCI)

Die Horizontale Arbeitsgruppe für Cyberangelegenheiten (*Horizontal Working Party on Cyber Issues* [HWP Cyber]) wurde im Jahr 2016 eingerichtet und ist für die Koordinierung der Arbeit des Rates der EU zu Angelegenheiten im Cyberrraum, insbesondere für die

1 Etwa die bereits geltenden NIS2-Richtlinie (RL EU 2022/2555) und die DORA-Verordnung (VO EU 2022/2554) sowie den derzeit verhandelten Rechtsakten,

2 siehe etwa den Vorschlag einer KI-Verordnung (COM/2021/206 final).

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 Arbeitsplattform, die eine Harmonisierung und ein einheitliches Vorgehen in Fragen der Cyberpolitik ermöglicht.

Die Ratsarbeitsgruppe arbeitet eng mit anderen verwandten Arbeitsgruppen sowie 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 European Union Agency for Cybersecurity (ENISA) zusammen.

NIS-2-Richtlinie trat im Jänner 2023 in Kraft

Ingesamt gab es mit 67 Sitzungen der HWP Cyber im Jahr 2022 sogar um sieben Sitzungen mehr als im Rekordjahr 2021, was abermals von der hohen Arbeitsintensität zur Weiterentwicklung der europäischen Cybersicherheitspolitik zeugt. Im Bereich der Verhandlung von Rechtsakten stand dabei zu Beginn des Jahres der Abschluss und die Trilogverhandlungen der am 14. Dezember 2020 von der Europäischen Kommision vorgestellten NIS-2-Richtlinie[3], die Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der gesamten Union vorgibt, im Vordergrund. Unter der französischen Ratspräsidentschaft gelang am 12. Mai 2022 eine politische Einigung zwischen Rat und Europäischen Parlament. Unter tschechischer Ratspräsidentschaft nahm das Europäische Parlament den Rechtstext in erster Lesung am 10. November 2022, bei der Tagung des Rates der EU am 28. November 2022 an. Die NIS-2-Richtlinie wurde am 27. Dezember 2022 veröffentlicht und trat am 16. Jänner 2023 in Kraft.

Hier wurden auch die ersten Lesungen und Bearbeitungen der am 15. September 2022 vorgestellten Verordnung über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen (*Cyber Resilience Act oder CRA*) vorgenommen. Der CRA soll für Hardware- und Softwareprodukte verbindliche Cybersicherheitsanforderungen einführen

3 Richtlinie (EU) 2022/2555

und so Verbraucherinnen und Verbraucher sowie Unternehmen vor digitalen Produkten mit unzureichenden Sicherheitsmerkmalen schützen und unionsweit digitale Standards harmonisieren. Unter anderem soll sichergestellt werden, dass Produkte mit digitalen Elementen weniger Schwachstellen aufweisen, dass die Herstellenden für die Cybersicherheit verantwortlich sind und dass Kundinnen und Kunden ausreichend über mögliche Cyberrisiken informiert werden. In der Praxis soll dies mittels eines Konformitätsbewertungsverfahrens, einer entsprechenden Kennzeichnung und der Überprüfung durch Überwachungsbehörden umgesetzt werden. Die inhaltliche Bearbeitung startete allerdings erst richtig unter der Schwedischen Präsidentschaft ab dem ersten Halbjahr 2023.

In der HWP Cyber wurden die „Schlussfolgerungen des Rates zur Cyberhaltung (*EU cyber posture*)“, die am 23. Mai 2022 vom Rat beschlossen wurden, in Umsetzung des Strategischen Kompasses für Sicherheit und Verteidigung, vorbereitet, welche die Entschlossenheit der EU bei der Bewältigung von Cyberangriffen untermauern sollen.

Schlussfolgerungen des Rates zur Sicherheit von IKT-Lieferketten angenommen

Des Weiteren nahm der Rat die Schlussfolgerungen zur Sicherheit der IKT-Lieferketten an, welche ebenfalls von der HWP Cyber vorbereitet und am 17. Oktober 2022 vom Rat angenommen wurden. Diese Ratsschlussfolgerungen betonen die zunehmende Bedeutung der Geopolitik für die Cybersicherheit insbesondere der Cybersicherheit der IKT-Lieferketten. Zudem versuchen sie nun, diese Risiken und Abhängigkeiten aufzuzeigen und betonen die Notwendigkeit, Maßnahmen zu treffen.

Zu den umfangreichen Arbeiten der HWP Cyber im Bereich der Cyberdiplomatie siehe Kapitel 2.1.6.

2.1.2 NIS-Kooperationsgruppe

Die NIS-Kooperationsgruppe wurde durch die ehemalige NIS1-Richtlinie[4] eingesetzt und dient der Unterstützung und Erleichterung der strategischen Zusammenarbeit sowie des Informationsaustausches zwischen den Mitgliedstaaten. Sie setzt sich aus Vertreterinnen und Vertretern der Mitgliedstaaten, der Europäischen Kommission und der ENISA zusammen. Der Vorsitz wird von der jeweiligen Ratspräsidentschaft gehalten.

Die NIS-Kooperationsgruppe nimmt ihre Aktivitäten auf der Grundlage von zweijährigen Arbeitsprogrammen wahr. Während das erste Arbeitsprogramm für den Zeitraum 2018 bis 2020 ein erster Schritt war, um die Arbeitsmethoden der NIS-Kooperationsgruppe zu gestalten, Vertrauen zwischen den Mitgliedsstaaten aufzubauen und die dringendsten Ergebnisse im Zusammenhang mit der Umsetzung der NIS-Richtlinie zu erarbeiten, hat sich die NIS-Kooperationsgruppe in der Zwischenzeit als wichtiges Forum und Bezugspunkt für die Diskussion über Cybersicherheitspolitiken innerhalb der EU etabliert. Das neue Arbeitsprogramm für den Zeitraum 2020 bis 2022 beauftragt eine Bestandsaufnahme der bisher erbrachten Leistungen, eine Bewertung, deren Auswirkungen und die Identifikation von Verbesserungspotentialen. Ziel ist es, die Umsetzung der NIS-Richtlinie weiterhin zu erleichtern, den Informationsaustausch weiter zu operationalisieren sowie eine strategische Diskussion über wichtige politische Dokumente für die Cybersicherheit in der EU, wie zum Beispiel in Bezug auf 5G, Künstliche Intelligenz oder das Internet der Dinge, zu ermöglichen.

Die NIS-Kooperationsgruppe traf sich im Jahr 2022 zu vier Plenarsitzungen und zu mehr als 20 Sitzungen im Rahmen ihrer Arbeitsbereiche („*Work Stream Meetings*“). Auch im Jahr 2022 wurden neue Referenzdokumente von der NIS-Kooperationsgruppe erarbeitet und veröffentlicht. Einen Schwerpunkt bildete die Arbeit am Thema der Cybersicherheit

4 Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union.

von 5G-Netzen. Bei den veröffentlichten Referenzdokumenten handelt es sich konkret um technische Richtlinien zu Sicherheitsmaßnahmen für Top-Level-Domain Name Registries vom März 2022 und eine Bericht zur Cybersicherheit von Open-RAN vom Mai 2022.

2.1.3 Horizontale Arbeitsgruppe zur Stärkung der Resilienz und zur Abwehr hybrider Bedrohungen (HWP ERCHT)

Die Horizontale Arbeitsgruppe zur Stärkung der Resilienz und zur Abwehr hybrider Bedrohungen (HWP ERCHT) wurde im Jahr 2019 eingerichtet. Der Fokus der Arbeit liegt auf der Verbesserung der Resilienz der EU und ihrer Mitgliedstaaten, dem gemeinsamen Vorgehen bei der Abwehr von hybriden Bedrohungen sowie der Bekämpfung von Desinformation. Die Arbeitsgruppe dient der Koordinierung innerhalb des Rates und der Zusammenarbeit mit den anderen Organen, Diensten und Agenturen der EU. Böswillige Cyberaktivitäten stellen häufig Schlüsselelemente hybrider Bedrohungen dar und werden in diesem Kontext von den Arbeiten der HWP ERCHT umfasst.

In Umsetzung des Strategischen Kompasses für Sicherheit und Verteidigung wurde 2022 ein EU-Instrumentarium für eine koordinierte Reaktion der EU auf gegen sie und ihre Partnerinnen und Partner gerichtete hybride Bedrohungen und Kampagnen („*EU Hybrid Toolbox*“) entwickelt. Dazu wurden vom Rat im Juni 2022 Ratsschlussfolgerungen angenommen und im Dezember Durchführungsleitlinien gebilligt. Diese sehen u.a. die Erstellung eines gemeinsamen Lagebildes, die Festlegung eines Entscheidungsfindungsprozesses sowie die Schaffung eines Rahmens für mögliche Antworten in Bezug auf hybride Bedrohungsakteure vor. Für den Fall, dass Cyberangriffe Teil einer hybriden Kampagne sind, sieht die hybride Toolbox eine Koordinierung mit der EU Cyber Diplomacy Toolbox vor. Außerdem soll die hybride Toolbox auch genutzt werden, um gegen Informationsmanipulation und Einmischung aus dem Ausland (*Foreign Information Manipulation and Interference, FIMI*) vorzugehen. Dazu soll im Laufe des Jahres 2023 ebenfalls ein Instrumentarium entwickelt werden, um Bedrohungen besser zu erkennen, zu analysieren und auf sie zu reagieren.

Darüber hinaus enthalten die 2022 angenommene Richtlinie für ein hohes gemeinsames Maß an Cybersicherheit in der gesamten Union (NIS 2) und die Richtlinie über die Resilienz kritischer Einrichtungen (CER) Maßnahmen, die für die Resilienz der EU gegenüber hybriden Bedrohungen relevant sind.

2.1.4 EU-Zertifizierungsrahmen (Cybersecurity Act)

Durch Zertifizierung Vertrauen in IKT-Produkte, -Dienste und -Prozesse stärken

Der bereits im Jahr 2019 in Kraft getretene Cybersecurity Act schafft unter anderem einen europäischen Zertifizierungsrahmen für Cybersicherheit. Dieser legt einen Mechanismus fest, mit dem europäische Schemata für die Cybersicherheitszertifizierung geschaffen werden. In weiterer Folge soll der europäische Zertifizierungsrahmen für Cybersicherheit bescheinigen, dass IKT-Produkte, -Dienste und -Prozesse, die nach einem solchen Schema bewertet wurden, den festgelegten Sicherheitsanforderungen genügen. Anbietende und Herstellende können sich zukünftig freiwillig zu einer Cybersicherheitszertifizierung von IKT-Produkten, -Diensten und -Prozessen entscheiden. Ein Cybersicherheitszertifikat wird EU-weit anerkannt. Durch den Nachweis, dass ein Produkt die angegebenen Sicherheitsfunktionen erfüllt oder bestimmte Sicherheitsanforderungen einhält, kann Cybersicherheitszertifizierung wesentlich dazu beitragen, das Vertrauen in IKT-Produkte, -Dienste und -Prozesse zu stärken und damit das ordnungsgemäße Funktionieren des digitalen Binnenmarktes gewährleisten.

Die „Europäische Gruppe für die Cybersicherheitszertifizierung“ (*European Cybersecurity Certification Group* [ECCG]) wurde durch den Cybersecurity Act eingesetzt und nahm ihre Arbeit im Jahr 2019 auf. Die ECCG setzt sich aus Vertreterinnen und Vertretern der nationalen Behörden für die Cybersicherheitszertifizierung oder Vertreterinnen und Vertretern anderer einschlägiger nationaler Behörden zusammen. Österreich wird in der ECCG durch das Bundesministerium für Digitalisierung und Wirtschaftsstandort (BMDW) und das strategische NIS-Büro des Bundeskanzleramtes (BKA) vertreten. Die ECCG traf sich im Jahr 2022 zu zwei Plenarsitzungen.

Des Weiteren führt die im Jahr 2020 eingerichtete Gruppe der Interessenträger für die Cybersicherheitszertifizierung (*Stakeholders Cybersecurity Certification Group* [SCCG]) unter dem gemeinsamen Vorsitz der Europäischen Komimission (EK) und der ENISA ihre Arbeit fort. Die SCCG setzt sich aus Vertreterinnen und Vertretern aus akademischen Einrichtungen, Verbraucherschutzorganisationen, Konformitätsbewertungsstellen, Organisationen, die Normen entwickeln, Unternehmen, Handelsverbände und anderen zusammen und soll in strategischen Fragen der Cybersicherheitszertifizierung beraten.

Neben den bereits im Jahr 2019 von der EK bei ENISA zur Ausarbeitung beauftragten möglichen Schemata für die Cybersicherheitszertifizierung (das ist einerseits das *„European Union Common Criteria Scheme"* [EUCC] sowie andererseits das „European Union Cybersecurity Certification Scheme on Cloud Services" [EUCS]) wurde im Jahr 2021 im Jänner ein drittes Schema für die Cybersicherheitszertifizierung beauftragt. Dieses läuft unter dem Namen EU5G und hat die Cybersicherheit von 5G-Netzwerken zum Gegenstand. Das Schema soll sich beim Anwendungsbereich auf das GSMA *Network Equipment Security Assurance Scheme* sowie auf relevante *Common Criteria*-Schutzprofile für *embedded Universal Integrated Circuit Card* (eUICC) beziehen. Zu den umfangreichen Arbeiten im Bereich der Cybersicherheitszertifizierung von 5G-Netzen siehe Kapitel 2.1.5.

Alle drei Schemata befinden sich momentan noch in Ausarbeitung.

2.1.5 Cybersicherheit von 5G-Netzen

Die Sicherheit der als fünfte Generation des Mobilfunknetzes (5G) betitelten Technologie stand wie auch in den Vorjahren im Fokus der Aufmerksamkeit von Cybersicherheitsbehörden.

Bereits 2021 war es möglich, die am 29. Jänner 2020 vorgestellte „Cybersecurity of 5G networks EU Toolbox of risk mitigating measures", im Folgenden „Toolbox", vollends umzusetzen. Hier unterschied die Toolbox zwischen technischen und strategischen Maßnahmen.

Der erste Teil der in der Toolbox vorgeschlagenen technischen Maßnahmen wurde, wie im Bericht des Vorjahres angeführt, mit der am 4. Juli 2020 in Kraft getretenen Verordnung der RTR („Telekom-Netzsicherheitsverordnung 2020 – TK-NSiV 2020“) umgesetzt.

Mit dem am 1. November 2021 in Kraft getretenen Telekommunikationsgesetz 2021 (TKG 2021) wurde der zweite Teil der aus der Toolbox stammenden Maßnahmen, die sogenannten strategischen Maßnahmen, umgesetzt. Das TKG beinhaltet in § 45 eine eigene Definition für einen Hochrisikolieferant, welcher demnach jemand ist, bei *„dem davon auszugehen ist, dass er mit hoher Wahrscheinlichkeit die für ihn in der EU geltenden einschlägigen Normen, insbesondere im Bereich der Informationssicherheit und des Datenschutzes, nicht oder nicht ständig einzuhalten in der Lage ist“*. Hierbei wird auch die Möglichkeit geschaffen, einen Hersteller von der Lieferung sicherheitsrelevanter Komponenten oder Netzbestandteile ganz oder teilweise – etwa eingeschränkt auf bestimmte sicherheitsrelevante Geschäftsbereiche, Waren- oder Dienstleistungsgruppen oder einzelne Hard- und Softwarekomponenten sowie auf einen bestimmten Zeitraum oder ein bestimmtes geografisches Gebiet – auszuschließen. Darüber entscheidet die Bundesministerin für Landwirtschaft, Regionen und Tourismus (BMLRT) aus Gründen der nationalen Sicherheit nach Befassung eines eigens eingerichteten Expertengremiums. Am 21. November 2022 fand das erste Treffen des Expertengremiums (Fachbeirat-Netzsicherheit) in den Räumlichkeiten der RTR statt.

Mit dem TKG 2021 wird auch der European Electronic Communications Code (EECC, Richtlinie (EU) 2018/1972) nationalstaatlich umgesetzt.

Der Work Stream der NIS-Kooperationsgruppe *„on the cybersecurity of 5G networks“* (NIS CG 5G Work Stream) beschäftigte sich im letzten Jahr vor allem mit der Einsetzbarkeit von Open RAN für die europäischen Telekommunikationsnetze. Bei Open-RAN (RAN steht für „Radio Access Network“) handelt es sich um eine Initiative, die zum Ziel hat, die Interoperabilität im Zugangsnetz (RAN) der Mobilfunknetze zu verbessern bzw. zu fördern. Dabei soll durch die Definition von zusätzlichen Standards und Schnittstellen

eine Diversifizierung der RAN-Hersteller und bessere Unabhängigkeit von den bisherigen Herstellern erreicht (Stichwort Vendor-Lock-In) und somit die in der 5G Toolbox geforderte Anbieterdiversität umgesetzt werden.

Für die Definition und Ersichtlichmachung relevanter Standards und Organisationen spielt der 2020 gegründete Sub-Work-Stream *„SubGroup on 5G standardisation and certification"* eine große Rolle. 2022 konzentrierte er sich vor allem auf die Zusammenarbeit mit Stakeholdern im Bereich Zertifizierung und Standardisierung zur Unterstützung derer Fähigkeiten, sowie auf die Umsetzung des EU-5G-Scheme. Auch die Entwicklung eines 5G Zertifizierungsschema durch ENISA wird durch den Sub-Work-Stream unterstützt.

Der NIS CG 5G Work Stream dient weiterhin als Schnittstelle zum Informationsaustausch zwischen den einzelnen Gruppen.

2.1.6 Cyberdiplomatie

Die Cyber Diplomacy Toolbox der EU aus 2017 sieht diplomatische und politische Maßnahmen vor, wie im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik der EU (GASP) koordiniert auf Völkerrechtsverletzungen im Cyberraum reagiert werden kann. Die Toolbox umfasst neben präventiven, kooperativen und stabilisierenden auch restriktive Maßnahmen. Letztere wurden erstmals 2020 gegen Personen und Entitäten im Rahmen des Cybersanktionenregimes verhängt und sehen Einreiseverbote und das Einfrieren von Vermögenswerten vor. Allein im Kontext des russischen Angriffkrieges gegen die Ukraine kam die Cyber Diplomacy Toolbox 2022 drei Mal zum Einsatz. So wurde ein staatlicher Akteur hinter dem Cyberangriff gegen das Satellitennetzwerk KA-SAT von Viasat öffentlich benannt.

In Umsetzung des Strategischen Kompasses für Sicherheit und Verteidigung vom März 2022 und der Ratsschlussfolgerungen zur EU-Cyberabwehr vom Mai 2022 wird daran gearbeitet, die Wirksamkeit und Effizienz der Cyber Diplomacy Toolbox der EU zu erhöhen und die EU-Cyberabwehrpolitik auszubauen. Demnach beruht die EU-Cyberabwehr auf

den fünf Säulen Cyberresilienz, solidarisches Krisenmanagement, Förderung der EU-Vision für den Cyberraum, internationale Zusammenarbeit sowie Vorbeugung von, Verteidigung gegen und Reaktion auf Cyberangriffe.

EU-Vision für das globale und offene Internet

Ein wichtiger Teil der Cyberdiplomatie auf EU-Ebene ist die Erarbeitung gemeinsamer Positionen und Strategien zu Cyberthemen auf internationaler Ebene, allen voran in Zusammenarbeit mit den Vereinten Nationen (siehe Kapitel 2.2). Denn Standard- und Normensetzung für neue Technologien und den Cyberraum sind längst geopolitische Konfliktzonen und die Zunahme an Cyberangriffen durch staatlich gelenkte Akteure verstärkt die geopolitische Polarisierung. Mit dem Anspruch einer EU-Führungsrolle auf internationaler und regionaler Ebene soll die EU-Vision für das globale und offene Internet verankert und dabei sichergestellt werden, dass neue Technologien auf Menschen und den Schutz ihrer Privatsphäre fokussieren und ihr Einsatz rechtmäßig und ethisch erfolgt. Der vom BMEIA 2021 eingesetzte Sonderbeauftragte für Cyber-Außenpolitik und Cyber-Sicherheit konnte 2022 mit der Delegationsleitung in multilateralen Verhandlungen, der Durchführung bilateraler Cyber-Dialoge und der Mitwirkung am EU-Netzwerk der Cyberbotschafter die Sichtbarkeit Österreichs in der internationalen Cyberdiplomatie weiter stärken.

2.1.7 Europäisches Kompetenzzentrum für Industrie, Technologie und Forschung im Bereich der Cybersicherheit und Netzwerk nationaler Koordinierungszentren

Das Europäische Kompetenzzentrum für Industrie, Technologie und Forschung im Bereich der Cybersicherheit (*European Cybersecurity Industrial, Technology and Research Competence Centre* [ECCC]) fokussierte seine Arbeit im Jahr 2022 weiterhin auf organisatorische Aufbauaktivitäten sowie erste inhaltliche Arbeiten, um seinen Auftrag gemäß der Verordnung (EU) 2021/887 des Europäischen Parlaments und des Rates vom 20. Mai 2021 zur Einrichtung des ECCC und des Netzwerks nationaler Koordinierungszentren (National Coordination Centres [NCC]), im Bereich Kompetenzaufbau und der Steigerung von Resilienz, digitaler Souveränität und Wettbewerbsfähigkeit der Europäischen Union

zu erfüllen. Der Verwaltungsrat des ECCC richtete dazu insgesamt sieben Arbeitsgruppen ein, die unter anderem die erste gemeinsame Maßnahme zur Errichtung von grenzüberschreitenden Sicherheitoperationszentren (*Security Operations Centres*, SOC) vorbereiteten. Ziel war es, die Grundlagen für eine für 2023 geplante erste gemeinsame Beschaffung des ECCC und interessierten Mitgliedstaaten von SOC-Infrastruktur zu erarbeiten. Durch die Bündelung von nationalen und EU-Mitteln sollen für die Anschaffung und die Inbetriebnahme von grenzüberschreitender Infrastruktur zur Erkennung von Bedrohungsdaten im Jahr 2023 über 30 Millionen Euro zu Verfügung gestellt werden. Darüber hinaus fokussierten die Arbeitsgruppen auf die Themen Aufbau der Europäischen Kompetenzgemeinschaft und des Netzwerkes nationaler Koordinierungszentren, Cybersicherheit Skills, die Zusammenarbeit mit der Ukraine sowie die inhaltliche Erarbeitung einer Strategischen Agenda, die zukünftig Förderschwerpunkte des ECCC informieren soll. Für 2023 ist die Eröffnung des Sitzes des ECCC in Bukarest geplant.

Der Verwaltungsrat (*Governing Board*) des ECCC fand sich im Jahr 2022 unter Teilnahme des Bundeskanzleramts (BKA) vier Mal zusammen. Im Vordergrund standen in erster Linie die Annahme administrativer Entscheidungen, die nötig sind, um das ECCC in Betrieb nehmen zu können, aber auch erste inhaltlichen Abstimmungen zu strategischen Förderprioritäten und das Vorhaben, gemeinsam in grenzüberschreitende SOC-Infrastruktur zu investieren.

Zukünftig wird das ECCC eine tragende Rolle bei der Umsetzung des EU-Finanzierungsprogramms „Digitales Europa“ (Verordnung (EU) 2021/694) einnehmen und zur Umsetzung des EU-Forschungsförderungsprogrammes Horizont Europa beitragen. Es erstellt des Weiteren einen Rahmen für die Steigerung und Koordinierung von Investitionen in die Cybersicherheit zwischen der EU, den Mitgliedstaaten und, indirekt, der Industrie. In diesem Zusammenhang ist es der Auftrag des ECCC und des Netzwerks, die EU zu unterstützen bei:

- der Stärkung ihrer Führungsrolle im Bereich der Cybersicherheit, um das Vertrauen und die Sicherheit, einschließlich der Vertraulichkeit, Integrität und Zugänglichkeit von Daten, zu steigern;
- der Förderung der Abwehrfähigkeit und Zuverlässigkeit der Netz- und Informationssysteme, darunter der kritischen Infrastruktur und der gängigen Hard- und Software;
- der Steigerung der globalen Wettbewerbsfähigkeit und hoher Standards der Cybersicherheitsbranche der EU und der Verwandlung der Cybersicherheit in einen Wettbewerbsvorteil für andere Wirtschaftszweige der EU.

Einrichtung einer Europäischen Kompetenzgemeinschaft

Das ebenfalls mit der Verordnung eingerichtete Netzwerk nationaler Koordinierungszentren unterstützt das ECCC bei seinen Aufgaben und soll sich auf nationaler Ebene für die Entwicklung neuer Cybersicherheitskapazitäten und den weiteren Kompetenzausbau einsetzen und soll die nationale Cybersicherheits-Community europäisch vernetzen. In Österreich wird das Nationale Koordinierungszentrum (NCC) vom BKA in Kooperation mit der Österreichischen Forschungsförderungsgesellschaft (FFG) betrieben. 2022 fokussierten die Bemühungen insbesondere auf die Vorbereitungen eines Antrages für EU-Mittel für den Aufbau des NCC, inklusive einer ersten eigenen Förderung, sowie auf die Bewerbung des Programms Digitales Europa (Verordnung (EU) 2021/694) im Bereich Cybersicherheit in Österreich durch unter anderem Informationsveranstaltungen, Veranstaltungsteilnahmen und Einzelberatungen. Darüber hinaus nahm das NCC an Sitzungen des NCC-Netzwerkes und von ECCC-Arbeitsgruppen aktiv teil. Diese umfassten insbesondere die ECCC-Arbeitsgruppen zu SOC und zur Einrichtung der Europäischen Kompetenzgemeinschaft.

2.2 Vereinte Nationen (VN)

Seit der erstmaligen Befassung des 1. Komitees (Abrüstung und internationale Sicherheit) der Generalversammlung der Vereinten Nationen (VN-GV) mit dem Thema Cybersicher-

heit im Jahr 1998 beschäftigt sich die VN-GV mit zunehmender Intensität mit dieser Thematik. Die Staaten verfolgen in diesem Rahmen das Ziel, die aus der Nutzung des Cyberraumes entstehenden Risiken für die internationale Sicherheit und 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 besonders wichtig sind:

- Völkerrecht,
- nicht-bindende Normen für verantwortungsvolles Staatenverhalten,
- vertrauensbildende Maßnahmen (VBM) und
- Aufbau von Kapazitäten.

Für Österreich, die EU und gleichgesinnte Staaten bilden die 2021 im Konsens angenommenen Empfehlungen der Open-Ended Working Group (OEWG) zu Cybersicherheit und der Regierungsexpertengruppe (GGE) die Grundlage für die Arbeiten der auf Betreiben von Russland und China lancierten neuen OEWG zu Cybersicherheit 2021 – 2025. Sie setzte 2022 ihre Arbeit mit der Annahme von Verfahrensregeln im Frühjahr sowie der Einigung auf einen Fortschrittsbericht im Juli fort. Letzterer bildet gleichzeitig einen Fahrplan für die weitere Arbeit der Gruppe im Jahr 2023, unter anderem zum Vorschlag der Einrichtung eines VN-weiten Netzwerks nationaler Kontaktpunkte für Cybersicherheit.

Nachdem es 2021 noch möglich gewesen war, das Thema Cybersicherheit in einer Resolution der VN-GV im 1. Komitee im Konsens abzuhandeln, gab es 2022 gleich drei Texte zu dem Thema. Neben einer von Singapur eingebrachten Entscheidung zum Fortschrittsbericht der OEWG, brachte Russland eine eigene, inhaltlich dem Sachstand der OEWG nicht entsprechende, Resolution ein. Diese Resolution wurde von Österreich und den meisten westlichen Staaten abgelehnt. Zudem brachte Frankreich, unter anderem mit Unterstützung Österreichs und der EU, eine Resolution zur Ausarbeitung eines Aktionsplans zu Cybersicherheit ein. Das sogenannte „UN Programme of Action“ zielt auf die Etablierung eines aktionsorientierten Mechanismus zur Überprüfung und Förderung der

praktischen Umsetzung des VN-Rahmens für verantwortungsvolles Staatenverhalten im Cyberraum ab. Dazu war 2022 ein Bericht des Generalsekretärs der VN (VN-GS) unter Einholung der Positionen der VN-Mitgliedstaaten zu den Fragen, wie die Ausarbeitung eines Aktionsplans erfolgen und wie sich dieser Plan zur OEWG verhalten soll, in Vorbereitung.

Der Bereich der internationalen Cybersicherheit findet sich ebenso in der 2018 lancierten Abrüstungsagenda des VN-GS wieder. Im dazugehörigen Implementierungsplan sind der Cybersicherheit zwei Aktionsbereiche gewidmet. Einer bezieht sich auf die friedliche Konfliktbeilegung, der andere auf die Stärkung sich entwickelnden Normen im Cyberraum. 2022 wurden die dahingehenden Implementierungsmaßnahmen durch die Staaten fortgesetzt.

Unterstützt wird die Umsetzung der Abrüstungsagenda 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.

Das von VN-GS Guterres 2018 einberufene High-level Panel on Digital Cooperation (HLPDC) legte im Jahr 2019 konkrete 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 vor. Darauf aufbauend erarbeitete VN-GS Guterres im Jahr 2020 einen Bericht („Road Map for Digital Cooperation"), der unter dem Titel „Connect, respect, protect" unter anderem die Einsetzung eines „Tech-Envoys" des VN-GS vorsah. Die Stelle im Rang eines Under-Secretary General wurde im Sommer mit dem indischen Diplomaten Amandeep Singh Gill besetzt. Aufgabe des „Tech Envoy" ist neben der Digitalisierung des VN-Systems, die Koordination und Vorbereitung der Ausarbeitung eines künftigen VN-Pakts zu globalen Fragen der digitalen Transformation „UN Global

Digital Compact“. Der Global Digital Compact soll beim VN-Zukunftsgipfel im Herbst 2024 angenommen werden.

Die Internationale Fernmeldeunion (ITU) mit Sitz in Genf wurde durch den „Weltgipfel für die Informationsgesellschaft“ (WSIS) mit dem „Aufbau von Vertrauen und Sicherheit bei der Nutzung von Informations- und Kommunikationstechnologie (IKT)“ beauftragt. 2007 legte die Organisation die umstrittene Globale Agenda für Cybersicherheit (GCA) als Rahmen für die internationale Zusammenarbeit in diesem Bereich vor. Bei der ITU-Konferenz der Regierungsbevollmächtigten in Bukarest (26. September bis 14. Oktober 2022) nahmen die Mitgliedstaaten eine neue Strategie für die Organisation an, die – auf Druck der Entwicklungsländer und aufbauend auf der bei der Weltkonferenz zur Entwicklung der Telekommunikation in Kigali angenommenen „Kigali Declaration“ – der Organisation zum ersten Mal ein explizites Mandat zum Kapazitätenaufbau im Bereich Cybersicherheit gibt.

Für Fragen der Internet Governance ist das Internet Governance Forum (IGF) mit Sitz in Genf die bedeutendste globale Plattform für Diskussionen und Austausch unter den vielen Akteuren, einschließlich Regierungen, Zivilgesellschaft, Privatsektor, Wissenschaft und Fachöffentlichkeit. Neben den technischen Fragen der Internet Governance im engeren Sinn befasst sich das IGF auch mit aktuellen Herausforderungen der Internetpolitik und der digitalen Transformation, wie Künstliche Intelligenz, Plattformregulierung, Datenwirtschaft, Cybersicherheit sowie nachhaltige Digitalisierung. Das im Sommer 2022 durch den VN-GS eingerichtete „IGF Leadership Panel“ soll die Rolle des IGF im VN-System nachhaltig stärken. Das 15-köpfige Gremium, das von Vint Cerf, dem „Vater des Internets“, geleitet wird, umfasst auch Bundesministerin für EU und Verfassung Karoline Edtstadler als einzige westliche Regierungsvertreterin. Das „IGF Leadership Panel“ soll auch einen Beitrag zum Global Digital Compact leisten.

Anlässlich der 11. WTO-Ministerkonferenz (MC11) 2017 in Buenos Aires wurde eine gemeinsame Initiative zu e-Commerce ins Leben gerufen. Die Arbeiten bei der von 71 WTO

Mitgliedern unterstützten, gemeinsamen Initiative über Regeln beim elektronischen Geschäftsverkehr schreiten voran. Bei Cybersecurity sowie e-Unterschrift, e-Authentifizierung, e-Verträgen, Konsumentenschutz einschließlich Spam, papierlosem Handel, Transparenz und Open Government Data gelang eine Einigung. Schwierig gestalten sich die Gespräche bei den sensiblen Themen Quellcode, Datenflüsse und Datenschutz. Zum Jahresende 2022 wurde ein konsolidierter Text vorgelegt, auf dessen Basis die Arbeiten bis zur 13. WTO-Ministerkonferenz (MC13) in Abu Dhabi 2024 abgeschlossen werden sollen.

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. Durch das „Global Programme on Cybercrime" unterstützt UNODC Mitgliedstaaten mit dem Aufbau von Kapazitäten, der Prävention und Bewusstseinsschaffung in der Bekämpfung von Cyberkriminalität. Österreich beteiligt sich seit 2020 mit freiwilligen Beiträgen an der Umsetzung von Initiativen in diesem Bereich.

Der Anstieg von Cyberkriminalität als Folge der Covid-Pandemie wurde quer durch alle Gremien thematisiert, einschließlich der Kommission für Verbrechensverhütung und Strafrechtspflege (CCPCJ) und der Suchtstoffkommission (CND).

Im Jahr 2019 wurde das Ad hoc-Komitee (AHC) zur Ausarbeitung eines umfassenden internationalen Übereinkommens über die Bekämpfung der Nutzung von Informations- und Kommunikationstechnologien zu kriminellen Zwecken (VN-Cybercrimekonvention) geschaffen. Nach der Einigung auf die Modalitäten des Prozesses im Jahr 2021 haben die inhaltlichen Verhandlungen für eine solche VN-Cybercrimekonvention im Februar 2022 begonnen. Die Verhandlungen finden zur Hälfte am VN-Standort in Wien und zur Hälfte in New York unter Vorsitz der Ständigen Vertreterin Algeriens in Wien statt und sollen 2024 abgeschlossen werden. 2022 wurden in drei Verhandlungsrunden unter breiter Teilnahme von Expertinnen und Experten der VN-Mitgliedstaaten die Schwerpunkte für

die zukünftige Konvention erarbeitet und eine erste Lesung von Textelementen für die verschiedenen Kapitel durchgeführt. Dabei betonten zahlreiche Staaten das Anliegen, dass eine VN-Cybercrimekonvention im Konsens angenommen werden soll, um als globale Grundlage für eine verstärkte Zusammenarbeit unter den Staaten im Kampf gegen Cyberkriminalität zu dienen. Neben VN-Mitgliedstaaten können NGOs, Think Tanks, der Privatsektor und andere wichtige Stakeholder an diesem Prozess mitwirken. UNODC fungiert als Sekretariat für den Verhandlungsprozess, womit dem Amtsitz Wien eine wichtige Rolle zukommt.

Im Rahmen der 51. Tagung des VN-Menschenrechtsrats (VN-MRR) im September 2022 brachte Österreich gemeinsam mit Panama eine Resolution unter dem Titel „Human rights implications of new and emerging technologies in the military domain" ein, die nach intensiven Verhandlungen im Konsens angenommen wurde. Die Resolution beauftragt einen entsprechenden Bericht, der dem VN-MRR 2025 vorgelegt wird und verschränkt Österreichs Engagement im Abrüstungs-, Menschenrechts- und digitalen Bereich.

Die ebenfalls von AT eingebrachte Resolution zu Sicherheit von Journalistinnen und Journalisten thematisiert mehrfach die besonderen Gefahren für Journalistinnen und Journalisten im digitalen Raum und diesbezügliche Schutz- und Abwehrmaßnahmen. Weiters verurteilt sie Maßnahmen, die vorsätzlich den digitalen Informationsfluss verhindern oder behindern.

2.3 NATO

Als militärisch-politische Allianz mit einem starken Fokus auf Sicherheit und gemeinsame Verteidigung befasst sich die North Atlantic Treaty Organization (NATO) seit über zehn Jahren, aber vor allem seit der Anerkennung des Cyberraums als operative Domäne, die auch Artikel 5 (Bündnisfall) auslösen kann, vermehrt mit den Verteidigungsaspekten von Cybersicherheit. Im seit Juni 2022 geltenden Strategischen Konzept der NATO wird be-

tont, dass die Wahrung der sicheren Nutzung des Weltraums und des Cyberraums und des ungehinderten Zugangs dazu für eine wirksame Abschreckung und Verteidigung von entscheidender Bedeutung ist. Die NATO will hierbei ihre Fähigkeit verbessern, im Weltraum und Cyberraum wirksam zu operieren, um unter Zuhilfenahme aller verfügbaren Instrumente dem gesamten Spektrum an Bedrohungen vorzubeugen, diese zu erkennen, abzuwehren und auf diese zu reagieren.

Im Zuge der aktuellen Beschäftigung mit den Chancen und Gefahren durch aufkommende und bahnbrechende Technologien wurde der NATO die Bedeutung von gesicherten Daten (dabei besonders in Zusammenhang mit Big Data, Künstlicher Intelligenz, Autonomie, Quantentechnologie und Weltraum) und somit erforderlicher Schutzmaßnahmen verstärkt bewusst. Als Reaktion auf die geänderte Bedrohungslandschaft und zwischenzeitlich erfolgten Maßnahmen im Bereich der Widerstandsfähigkeit verabschiedete die Allianz 2022 die „NATO's Digital Transformation", die bis spätestens 2030 vollständig implementiert werden soll.

Österreich kooperiert hier als Partnerland unverändert 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, die auf die Interoperabilität für gemeinsame Operationen und Missionen abzielen.

Seit 2013 stellt das Bundesministerium für Landesverteidigung (BMLV) einen Offizier im „NATO Cooperative Cyber Defence Center of Excellence" (CCDCoE) 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 entsendet Österreich auch einen Mitarbeiter des BMLV in das „European Centre of Excellence for Countering Hybrid Threats" in Helsinki, an dem sich auch die NATO-Mitgliedstaaten beteiligen.

2.4 Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE)

Als größte zwischenstaatliche 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, vor allem das Sekretariat in Wien und das weite Netz an Feldmissionen). Andererseits übernahm die OSZE bei der Ausarbeitung vertrauensbildender Maßnahmen (VBM) im Cyberraum eine Vorreiterrolle. Die Annahme der 16 VBM stellt global gesehen den ambitioniertesten Versuch zur Stärkung der internationalen Kooperation im Feld der Cybersicherheit außerhalb der VN dar. Ziel ist es, durch 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. Die OSZE-Arbeit konzentriert sich darüber hinaus auf die Wahrung und Stärkung der Menschenrechte im Cyberraum sowie die Bekämpfung von Desinformation und Hassrede.

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, wobei der russische Angriffskrieg gegen die Ukraine 2022 naturgemäß ein besonderer Schwerpunkt war. 2022 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 Vorbereitung einer effektiven Zusammenarbeit im Falle einer Cyberkrise. Österreich treibt gemeinsam mit Belgien, Estland, Finnland, Italien und Schweden die Umsetzung der CBM 14 zu Public-

Private-Partnerships voran und stellte im Juni 2022 die Bemühungen des Vereins „Cyber Security Austria“ im Bereich der Cyberausbildung und Talentsuche vor.

Neben der institutionalisierten Behandlung der Thematik durch die Cyber-IWG setzen seit einigen Jahren die jeweiligen Vorsitzstaaten der OSZE die Cybersicherheit auf ihre Vorsitzagenda und halten regelmäßig Cybersicherheitskonferenzen ab. Im Jahr 2022 fand diese Konferenz mit den Schwerpunktthemen Schaffung von gesellschaftlicher Resilienz durch Stärkung der öffentlichen Aufmerksamkeit für Cyberbedrohungen, der Rolle der Privatwirtschaft und der Cyber-Bildung in Lodz im Rahmen des polnischen OSZE-Vorsitzes statt.

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 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. Die WPSDE organisiert Workshops und Konferenzen, ein virtuelles Treffen aller Teilnehmenden fand im April 2022 statt.

In Österreich nimmt das BKA die inhaltliche Koordination für diese Arbeitsgruppe wahr.

Wie im Cybersicherheits-Bericht der Vorjahre bereits angeführt, wurde die Überarbeitung der OECD Recommendation on Digital Security Risk Management for Economic

and Social Prosperity aus dem Jahr 2015 weitergeführt. Dabei wurde der ursprüngliche Bericht in eigene Unterkapitel getrennt, die separat als Empfehlungen (Recommendation) erschienen sind: Eine Recommendation on digital security risk management, eine Recommendation on national digital security strategies, eine Recommendation on the digital security of products und eine Recommendation on vulnerability treatment. Diese Dokumente wurden vom OECD-Rat am 26. September 2022 auf Vorschlag des Ausschusses für die Politik der digitalen Wirtschaft (CDEP) angenommen und auf der CDEP-Ministertagung am 14. Dezember 2022 vorgestellt.

Auch zusätzliche Berichte (Reports) mit sehr interessanten Themenbereichen konnten dieses Jahr finalisiert werden, wie zum Beispiel: „Enhancing the security of communication networks at the infrastructure and protocol levels“, „Security of the DNS: An introduction for policy makers“ und „Security of Routing“.

2.6 Europarat

Den Kern der Aktivitäten des Europarates im Bereich Cybersicherheit bildet die „Budapest-Konvention“ aus 2001, die mit aktuell 68 Ratifikationen (2022 Brasilien und Nigeria) 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. Seit 12. Mai 2022 liegt das Zweite Zusatzprotokoll zur Budapest-Konvention zur Unterzeichnung auf, das sich mit internationaler Rechtshilfe und dem damit verbundenen grenzüberschreitenden Zugang zu elektronischen Beweismitteln befasst. In zwei Unterzeichnungskonferenzen wurde es bislang von 31 Staaten, darunter Österreich, unterzeichnet. Es tritt in Kraft, sobald es in fünf Staaten ratifiziert wurde.

Die Umsetzung der Konvention wird vom Komitee der Konvention zu Cyberkriminalität (T-CY) überwacht. Staaten werden außerdem über kapazitätsbildende Projekte unterstützt, die durch ein Cybercrime-Programmbüro des Europarates in Bukarest (C-PROC) koordiniert werden. Hierzu gehören auch die Beratung bei einschlägigen Legislativmaßnahmen und Hilfe bei der Ausbildung von Richterinnen und Richtern sowie und Staatsanwältinnen und Staatsanwälten. Darüber hinaus werden die Projekte „iProceeds-2“ in Südosteuropa mit Fokus auf Erträgen aus Cyberkriminalität, „Cyber South“ und „Cyber East“ (Projekte in Kooperation mit dem Europäischen Nachbarschaftsinstrument, die auf die Verbesserung der Strukturen in der südlichen und östlichen Nachbarschaft Europas abzielen) sowie das weltweit agierende und in Zusammenarbeit mit Interpol durchgeführte „GLACY+“ unterstützt.

Das „Octopus Project“ fördert außerdem die Umsetzung der Budapest-Konvention und damit zusammenhängender Standards. Die sogenannten „Oktopus-Konferenzen“, die alle zwölf bis 18 Monate stattfinden, dienen Expertinnen und Experten sowie Organisationen als wichtige Plattform im Bereich Cyberkriminalität. Die letzte Konferenz fand 2021 statt und befasste sich anlässlich des 20-jährigen Bestehens der Budapest-Konvention mit

dem Thema Zusammenarbeit im Rahmen bestehender Instrumente sowie mit Herausforderungen der COVID-19-Pandemie.

Seit 2012 werden zudem Leitfäden („Guidance Notes“) zur Budapest-Konvention erarbeitet und veröffentlicht. Diese sollen den Vertragsstaaten die effektive Anwendung und Umsetzung erleichtern. Der bislang letzte derartige Leitfaden, der im November 2022 veröffentlicht wurde, behandelt das Thema Cybererpressung.

Zu den weiteren Instrumenten des Europarats zählt die 2018 modernisierte Datenschutzkonvention des Europarates (ETS 108). Österreich hat das entsprechende Änderungsprotokoll 2022 ratifiziert. Die Lanzarote-Konvention zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch leistet einen wesentlichen Beitrag zum Online-Schutz von Kindern. Ebenso im Bereich Cybersicherheit wirken wird das in Verhandlung befindliche verbindliche Menschenrechtsinstrument zu Künstlicher Intelligenz.

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

Im Sommer 2016 wurde durch das Europäische Parlament (EP) und den Rat der EU die EU-Richtlinie 2016 / 1148 (NIS-Richtlinie) erlassen, durch selbige das CSIRTs-Netzwerk (CNW) geschaffen und dessen Tätigkeitsbereich festgelegt. Das CSIRTs-Netzwerk setzt sich aus Vertreterinnen und Vertretern der CSIRTs der Mitgliedstaaten (gemäß Artikel 9 NIS Richtlinie) und des CERT EU zusammen. Die Europäische Kommission (EK) nimmt als Beobachterin am CSIRTs-Netzwerk teil. Die EU Agentur ENISA führt die Sekretariatsgeschäfte und unterstützt aktiv die Zusammenarbeit zwischen den CSIRTs. Die österreichischen Teilnehmenden im CSIRTs-Netzwerk sind das GovCERT Austria, CERT.at und das Austrian Energy CERT (AEC).

Das Netzwerk arbeitet primär online, die Kommunikation erfolgt über ein Webportal, Mailinglisten und ein Instant Messaging System. Die Treffen des CNW dienen dem Informationsaustausch bezüglich der Dienste, Tätigkeiten und Kooperationsfähigkeiten der CSIRTs. Ebenso werden auf freiwilliger Basis Informationen zu relevanten Sicherheitsvorfällen ausgetauscht und aus Übungen gewonnene Erkenntnisse zur Sicherheit von Netz- und Informationssystemen 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.

Die Treffen des CNW im Jahr 2022 waren natürlich stark von den möglichen Auswirkungen des Ukraine-Krieges auf die Cybersicherheit-Landschaft Europas geprägt. Aber auch die Nachwirkungen von Log4J waren zu Beginn des Jahres noch ein Thema, zu dem sich die CSIRTs beraten haben. Zusätzlich zu aktuellen Bedrohungsthemen tauscht sich das CSIRTs-Netzwerk auch zu Forschungs- und Entwicklungsinitiativen (z.B. MeliCERTes 2) oder internationalen Übungen aus, wie z.B. zu der im Juni durchgeführten Cyber Europe 2022. Die Treffen im Jahr 2022 fanden online und vor Ort (Paris und Brünn) statt.

2.8 Andere Gremien und Foren

Freedom Online Coalition

Die „Freedom Online Coalition“ ist eine informelle Vereinigung von Staaten, die sich für die effektive Umsetzung weltweiter Online-Menschenrechte einsetzt. Auch Österreich gehört dieser Initiative an, die im Dezember 2011 von den Niederlanden gegründet wurde und mittlerweile 35 Mitgliedstaaten umfasst.

3
Nationale Akteure

3.1 Cyber Security Center (CSC)

Das Cyber Security Center in der Direktion für Staatsschutz und Nachrichtendienst (DSN) fungiert als operative Koordinierungsstelle für Meldungen und Anfragen zu Angriffen auf die Systeme und Infrastruktur von verfassungsmäßigen Einrichtungen sowie solchen, die der kritischen Infrastruktur zuzuordnen sind. Dabei liegt der Fokus verstärkt auf zielgerichteten Angriffen sowie deren technischer Vorfallsbearbeitung. Dafür bedient sich das CSC eines breiten Spektrums an Fähigkeiten und Techniken wie beispielsweise Cyber Threat Intelligence, Incident Response, Malware Analysis und Reverse Engineering. Im Zuge der Tätigkeit ergibt sich zwangsläufig auch die Taxonomie und Beschäftigung mit neuen Phänomen im Cyberbereich und der Reaktion auf aktuelle Trends. Um einen Erfahrungs- und Wissensaustausch zu ermöglichen und zu fördern setzt das CSC auch auf die Schwarmintelligenz der Cybersecurity Community, zu der auch Stakeholder aus der Wirtschaft sowie der Forschung zählen. Ziel ist, gemeinsam die Resilienz und die Kommunikation in diesem Bereich zu fördern. Ebenso findet der Austausch mit Partnerdiensten statt, um die eigenen Erkenntnisse zu teilen und eine globale Sicht auf die Materie zu erhalten.

3.2 Cybercrime Competence Center (C4)

Das Cybercrime Competence Center (C4) ist die nationale und internationale Koordinierungs- und Meldestelle zur Bekämpfung von Cyberkriminalität. Das Zentrum setzt sich aus technisch und fachlich hochspezialisierten Expertinnen und Experten aus den Bereichen Ermittlung, Forensik und Technik zusammen.

Die sowohl für Cyberkriminalität im engeren Sinn 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 im Bundeskriminalamt 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 Polizeibedienstete (Bezirks-IT-Ermittlerinnen und -Ermittler), die den ersteinschreitenden Beamtinnen und Beamten (First Responder) die notwendige Unterstützung bieten können.

Derzeit befindet sich das C4 in der Umstrukturierungsphase. Aufbauend auf das bestehende Organisationsgefüge werden Ressourcen des C4 erweitert und gliedern sich künftig in folgende Bereiche:

3.2.1 Zentrale Aufgaben

Zentrale Administration und Organisation für Projekte und Förderprogramme, Internationale Kooperationen, Entwicklung und Organisation nationaler und internationaler Ausbildungsprogramme, Beschaffungswesen IKT Hard- und Software.

3.2.2 IT-Beweissicherung

Die Fachexpertise zur Sicherung und Auswertung von elektronischen Beweismitteln gehört zum Kernstück des C4. Dazu zählen neben der IT-Forensik und Mobilen Forensik auch die Fachbereiche der Multimedia Forensik, Elektronik und IOT-Forensik sowie KFZ-Forensik.

3.2.3 IT-Ermittlungen

Zur adäquaten Bekämpfung von *High-Tech*-Kriminalität erweitern operative Unterstützungsteams die bestehenden Ermittlungsbereiche und sollen auch in mobiler Form zur Verfügung stehen. Spezialisierte Ermittlungseinheiten für die Fachrichtungen Darknet wie auch Kryptowährungen/Blockchain (mitunter zuständig für die Sicherstellung und Verwertung von Kryptowährungen) sind für die Bereitstellung der notwendigen Expertise bei Ermittlungen notwendig. Es ist geplant auch den Bereich „Complex Cybercrime" abzudecken. Dabei wird auf Delikte der Cyberkriminalität und auf Massenphänomene eingegangen, deren Ermittlungsansätze zum überwiegenden Teil im digitalen Bereich liegen, ein hohes Schadenspotential und internationale Zusammenhänge aufweisen.

3.2.4 Entwicklung & Innovation

Unterstützung von digitaler Forensik und digitalen Ermittlungen mit wissenschaftlicher Expertise sowie bedarfsorientierte Entwicklung von Tools und Skripten, welche international auch für andere Strafverfolgungsbehörden zur Verfügung gestellt werden. Internationale Zusammenarbeit mit Forschungsinstituten und Institutionen.

3.2.5 Digitales Beweismittelmanagement

Das digitale Beweismittelmanagement fasst die Kompetenzen zusammen, die für eine zeitgemäße kriminalpolizeiliche Bearbeitung komplexer Fälle mit großen Datenmengen notwendig sind. Das umfasst die technische Aufbereitung sichergestellter digitaler Beweismittel für eine systematische Indizierung und nachfolgende Bereitstellung für die Ermittlungsbereiche im Bundeskriminalamt und bei Bedarf der Landeskriminalämter, sowie das Fallmanagement als Schnittstelle zwischen Forensikerinnen und Forensikern, Ermittelnden, Technikerinnen und Technikern und gegebenenfalls der Justiz.

3.2.6 Meldestelle & Zentrale Anfragestelle Social Media und Online Service Provider

Die Meldestelle ist Ansprechstelle für Bürgerinnen und Bürger (against-cybercrime@bmi.gv.at) und Strafverfolgende (national und international) im Zusammenhang mit IT-Delikten. Sie ist zuständig für die Durchführung von Amtshilfeersuchen, Vorabdatensicherungen, Erkennung von neuen Phänomenen der Cyberkriminalität sowie neuer Modi Operandi. Die Zentrale Anfragestelle Social Media & Online Service Provider (ZASP) wurde eingerichtet, um die Abfragen und den dahinterliegenden Abwicklungsprozess bei Social Media Plattformen und Online Service Providern für Sachbearbeiterinnen und Sachbearbeiter zu vereinheitlichen und zu erleichtern.

3.3 Direktion IKT & Cyber

In der Direktion IKT & Cyber im Bundesministerium für Landesverteidigung (BMLV) werden alle Elemente der Cyberkräfte des Österreichischen Bundesheeres (ÖBH) zusammengeführt. Die Cyberkräfte sind jene Elemente im ÖBH, welche die anderen Teilstreitkräfte (Land, Luft) aber auch alle Führungsebenen (vom Ministerium bis zur Gruppenkommandantin / zum Gruppenkommandanten) miteinander verbinden und damit die Kommunikations- und Führungsfähigkeit herstellen. Sie beobachten und bewerten die Lage im Cyberraum, ergreifen alle erforderlichen Maßnahmen zum Schutz der militärischen Netze und stehen auf Anforderung gesamtstaatlich bereit. Die Cyberkräfte sind dafür verantwortlich, dass jede Art der Kommunikation und Datenübertragung im Österreichischen Bundesheer in eigenen Netzwerken reibungslos stattfinden kann. Sie sorgen permanent für die Informationshoheit und Kontrolle über die eigenen Systeme.

Die Cyberkräfte im Österreichischen Bundesheer umfassen die IKT-Truppe, die Cyber-Truppe und die Elektronischer Kampf (EloKa)-Truppe.

3.4 Abwehramt (AbwA)

Unter dem Begriff der Cyberverteidigung werden alle Anstrengungen des Österreichischen Bundesheeres (ÖBH) im Cyberraum als Gesamtes verstanden. Das Abwehramt (AbwA) wirkt mit seinen Kompetenzen und nachrichtendienstlichen Zugängen an dieser mit, es stellt hierzu sein Lagebild zur Verfügung, welches gesamtstaatliche und auch nachrichtendienstliche Informationen aus und über den Cyberraum zusammenführt, analysiert und als Grundlage der Beurteilung von Gegenmaßnahmen dient. Durch diese und weitere Maßnahmen soll permanent ein hohes Maß an Sicherheit der militärischen IKT-Infrastruktur gewährleistet werden.

3.5 Heeres-Nachrichtenamt (HNaA)

Das Heeresnachrichtenamt (HNaA) ist der strategische Auslandsnachrichtendienst Österreichs. Als solcher beschafft er Informationen über das Ausland, wertet sie aus und stellt die Ergebnisse der obersten politischen und militärischen Führung zur Verfügung. Dazu gehört auch die Beobachtung nachrichtendienstlich relevanter Entwicklungen und Vorgänge im und um den Cyberraum als Aspekt des gesamtheitlichen nachrichtendienstlichen Lagebildes. Durch das Erkennen von Cyberbedrohungen leistet es einen wesentlichen Beitrag zur Entscheidungsfindung bezüglich einzuleitender gesamtstaatlicher Gegenmaßnahmen und einer möglichen Attribuierung.

3.6 GovCERT, CERT.at und Austrian Energy CERT

Das GovCERT Austria ist gemäß Netz- und Informationssystemsicherheitsgesetz (NISG) das Computer-Notfallteam der öffentlichen Verwaltung und Mitglied des Inneren Kreises der Operativen Koordinierungsstruktur (IKDOK). Es ist mit seinem strategischen Anteil im Bundeskanzleramt (BKA) angesiedelt, die Erbringung operativer und operationeller Leistungen erfolgt im Rahmen einer Public-Private-Partnership mit CERT.at. Das GovCERT Austria stellt den CERT Point of Contact für Österreich in Bezug auf die Netze der öffentlichen Verwaltung dar und steht mit internationalen Organisationen und Ansprechpartnern wie der European Government CERTs (EGC) Group oder der Central European Cyber Security Plattform (CECSP) im engen Austausch.

Bereits seit März 2019 nimmt CERT.at die Rolle des nationalen 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. Dazu nutzt CERT.at sein Kontaktnetzwerk zu internationalen CERTs und anderen Cybersicherheit-Organisationen sowie eigens dafür entwickelte Software[5] und ist an zahlreichen nationalen und europäischen Forschungsprojekten[6] beteiligt. Auch 2022 war das Ziel von CERT.at und seinen internationalen Partnern, ihrer Constituency einen Informationsvorsprung gegenüber Angreifenden zu geben. Die Bereitschaft, während eines Angriffes Informationen mit externen Organisationen zu teilen, ist aktuell nicht sehr ausgeprägt – oft aus Sorge vor rechtlichen oder medialen Konsequenzen. CERT.at hat 2022 in vielen Fällen die Rolle übernommen, mit den verfügbaren Informationen Warnungen für weitere potentielle Opfer zu erstellen, damit diese sich rechtzeitig schützen können. Darüber hinaus informiert CERT.at über Social Media und Mailinglisten über aktuelle Bedrohungen und Schutzmaßnahmen.

---

5 https://github.com/certat

6 https://cert.at/de/ueber-uns/projekte

Das Austrian Energy CERT (AEC) ist ein akkreditiertes, brancheneigenes Computer Emergency Response Team für die österreichische Energieindustrie. Das Ziel des AEC ist die Stärkung der IT-Sicherheitskompetenz des Energiesektors und die Erhöhung der Resilienz des Sektors gegenüber Cyberangriffen. Zu den Aufgaben gehört neben dem Security Incident Management 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 primären Ansprechpartners (Single Point of Contact) bei nationalen und internationalen Security Incidents im Energiesektor. Damit 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 NISG und decken damit die Vorgaben der europäischen Richtlinie für Netz- und Informationssicherheit sowie die Empfehlungen der EU-Agentur ENISA für die Erhöhung der IT-Sicherheit bei kritischen Infrastrukturen ab. Sie stellen auch die österreichischen Mitglieder des CSIRTs-Netzwerk der EU. Alle drei werden in erster Linie bei Sicherheitsbedrohungen und -ereignissen aktiv. Dies geschieht durch Verständigung von betroffenen Stellen oder auf Basis eigener Recherchen. Darüber hinaus führen alle drei Computer-Notfallteams auch vorbeugende Maßnahmen wie Früherkennung, Öffentlichkeitsarbeit, Beratung und Unterstützung im Anlassfall sowie auf Anfrage durch. Die Aufgabenbereiche der CERTs sind im NISG 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 Bundesministerium für Inneres (BMI) weitergeleitet. Auf freiwillige Meldungen trifft dies ebenfalls zu, allerdings können diese Meldungen vor

der Weiterleitung an das BMI von den Sektor-CERTs anonymisiert werden. Für die Einrichtungen der öffentlichen Verwaltung – mit Ausnahme jener im IKDOK vertretenen – nimmt GovCERT Austria die Entgegennahme und Weiterleitung solcher Meldungen vor. Zusätzlich kann GovCERT Austria auch Frühwarnungen, Alarmmeldungen, Handlungsempfehlungen und Bekanntmachungen vornehmen, erste allgemeine technische Unterstützung bei der Reaktion auf einen Sicherheitsvorfall leisten, Risiken, Vorfälle und Sicherheitsvorfälle beobachten und analysieren sowie die Lage beurteilen. Das NISG sieht zur Wahrnehmung dieser Meldestellenfunktion die Etablierung eigener Branchen- oder Sektoren CERTs in jedem Sektor vor. Wurde in einem Bereich noch kein eigenes CERT etabliert (aktuell existieren nur das GovCERT und das AEC als Sektoren-CERTs), werden die Aufgaben des Computer-Notfallteams und die der Meldestelle durch CERT.at wahrgenommen. CERT.at hat dafür eine Meldeplattform unter https://nis.cert.at eingerichtet. Dort können auch von jeder Organisation freiwillige Meldungen eingetragen werden, die helfen, ein besseres Cyberlagebild zu schaffen.

2022 stieg die Anzahl der freiwilligen Meldungen gegenüber den Vorjahren an, es sind aber weiterhin noch nicht ausreichend Meldungen vorhanden, um daraus alleine ein Lagebild zu erzeugen. Das Ziel aller drei CERTs ist daher, die Anzahl der freiwilligen Meldungen weiter zu erhöhen, was durch Aufklärung und aktive Bewerbung des Nutzens erreicht werden soll.

3.7 Büro für strategische Netz- und Informationssystemsicherheit

Das im BKA angesiedelte Büro für strategische Netz- und Informationssystemsicherheit („strategisches NIS-Büro“) führte seine Arbeit im Jahr 2022 erfolgreich fort. Im Hinblick auf die Vertretung Österreichs in der NIS-Kooperationsgruppe sowie in anderen EU-weiten und internationalen Gremien für die Sicherheit von Netz- und Informationssystemen, denen strategische Aufgaben zugewiesen sind, wurden umfangreiche Aktivi-

täten gesetzt. Hierzu sei auf das Kapitel 2.1 verwiesen. Ein Schwerpunkt bildete dabei die Koordinierung und Vertretung der österreichischen Position in den Verhandlungen zum Cyber Resilience Act.

3.8 Operative Netz- und Informationssystemsicherheit

Wie bereits im Bericht Cybersicherheit für das Jahr 2021 dargestellt, wurde das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) am 30. November 2021 im Zuge einer umfassenden Reform aufgelöst und als Direktion für Staatsschutz und Nachrichtendienst (DSN) neu gegründet. Die Aufgaben, die bis zu diesem Zeitpunkt von der Abteilung II/BVT/5 wahrgenommen worden waren, wurden in der Folge zwischen der DSN und der Sektion IV des Bundesministeriums für Inneres (BMI) aufgeteilt.

Mit 1. Juli 2022 wurde nach einer vorübergehenden organisatorischen Zwischenlösung die heutige Abteilung IV/S/2 – Netz- und Informationssystemsicherheit (NIS) im BMI eingerichtet. Die Abteilung und die ihr nachgeordneten Referate erfüllen die Funktion der operativen NIS-Behörde für Österreich. Diese Tätigkeit umfasst ein breites Spektrum an Aufgabenstellungen, deren wesentliche Zielsetzung die Sicherstellung von Cybersicherheit und die Erhöhung der gesamtstaatlichen Resilienz in Österreich ist.

Im Zentrum dieser Tätigkeiten steht die behördliche Aufsicht über die Umsetzung der Vorgaben des Netz- und Informationssystemsicherheitsgesetzes (NISG) durch Betreiber wesentlicher Dienste, Anbieter digitaler Dienste sowie Einrichtungen der öffentlichen Verwaltung. Weiters nimmt die Abteilung eine koordinierende Rolle innerhalb der gesamtstaatlichen Operativen Koordinierungsstruktur (OpKoord) und ihres Inneren Kreises (IKDOK) wahr und unterstützt darüber hinaus die dem NISG unterworfenen Entitäten im Bereich der Cyber-Prävention.

3.8.1 Recht und Audit

Das Referat IV/S/2/a (Recht und Audit) erfüllt einen wesentlichen Teil der Aufgabenstellungen der operativen NIS-Behörde. Eine Kernaufgabe der Mitarbeitenden dieses Bereiches ist die regelmäßige Überprüfung der Einhaltung der verpflichtenden Sicherheitsvorkehrungen bei den dem NISG unterworfenen Unternehmen und Organisationen. Dem Referat obliegt dabei unter anderem die diesbezügliche Verfahrensführung im Rahmen des NISG, die Feststellung der mit der Durchführung der Überprüfungen beauftragten qualifizierten Stellen sowie die aktive Teilnahme an diesbezüglichen Arbeitsgruppen nationaler und internationaler Gremien. Als Behörde gehört es auch zu den Aufgaben dieses Referats, Empfehlungen und im Bedarfsfall bescheidmäßige Anordnungen zur Umsetzung oder Anpassung von Sicherheitsvorkehrungen auszusprechen.

3.8.2 Cyberlagezentrum, Prävention, Kommunikation

Im Referat IV/S/2/b (Cyberlagezentrum, Prävention, Kommunikation) ist ein breites Feld an zentralen Tätigkeiten innerhalb der operativen NIS-Behörde zusammengefasst. Mitarbeitende des Referats verfolgen die aktuellen Entwicklungen im Bereich der Cybersicherheit, wie beispielsweise Sicherheitsvorfälle, Angriffsmuster und Warnungen, um daraus ein permanentes Lagebild zu erstellen, das Bedarfsträgern innerhalb und außerhalb des Ressorts zur Verfügung gestellt wird. Gleichfalls betreuen Mitarbeiterinnen und Mitarbeiter des Referats die Meldesammelstelle sowie den „Single Point of Contact“ als Anlaufstelle für NIS-Behörden anderer Mitgliedsstaaten der EU. Teil dieser Tätigkeit ist auch die Analyse und Weiterverarbeitung der einlangenden Meldungen. Darüber hinaus koordinieren Mitarbeitende des Referats die Treffen der „Operativen Koordinierungsstruktur“ (OpKoord) und ihres „Inneren Kreises“ (IKDOK) und tragen in internationalen Gremien zur Kooperation der EU-Mitgliedstaaten im Bereich der Cybersicherheit bei. Der Fachbereich Prävention ist schließlich für die Planung, Koordination und Durchführung von Präventionsveranstaltungen und Workshops sowie für die Konzeption und Erstellung von diesbezüglichen Unterlagen und Publikationen verantwortlich.

3.8.3 NIS Technische Einrichtungen

Das Referat IV/S/2/c (NIS Technische Einrichtungen) ist einer der wesentlichen technischen Dienstleister der operativen NIS-Behörde. Die zentrale Aufgabe der Mitarbeitenden dieses Bereiches ist die Konzeption, der Aufbau und der kontinuierliche fachliche Betrieb der für die Erfüllung der Aufgaben der Abteilung erforderlichen spezialisierten Informations- und Kommunikationssysteme nach dem NISG. Darüber hinaus erstellt das Referat technische Analysen eingehender Vorfallsmeldungen und unterstützt die Aufgabenerfüllung des Präventionsbereichs durch fundierte und aktuelle technische Informationen zur Vorbeugung von Sicherheitsvorfällen. Die für die Erfüllung der genannten Aufgaben erforderliche technische Kompetenz und Expertise ist hier in einem jungen, innovativen Team gebündelt, das seine Leistungen mit dem Einsatz modernster Mittel und Methoden erbringt.

NCC-AT
Nationales Koordinierungszentrum Cybersicherheit

3.9 Nationales Koordinierungszentrum für Cybersicherheit (NCC-AT)

Das Nationale Koordinierungszentrum für Cybersicherheit (NCC-AT) bildet als Teil des EU-weiten Netzwerks nationaler Koordinierungszentren zusammen mit dem Europäischen Kompetenzzentrum für Industrie, Technologie und Forschung im Bereich der Cybersicherheit (ECCC) den europäischen Rahmen zur Unterstützung der Innovations- und Industriepolitik im Bereich der Cybersicherheit. Ziel ist es, durch Community Building und Koordinierung der Bemühungen im Bereich Kompetenzaufbau die Kapazitäten im Bereich Cybersicherheit in Österreich und der EU zu stärken, Resilienz auszubauen und so die Gesellschaft und Wirtschaft gegenüber Cyberbedrohungen zu schützen. Zudem soll die Exzellenz in der Forschung gesichert und die Wettbewerbsfähigkeit der europäischen Industrie ermöglicht werden.

In Österreich setzt das Bundeskanzleramt (BKA) in Kooperation mit der Österreichischen Forschungsförderungsgesellschaft (FFG) das NCC-AT um und erfüllt damit den recht-

lichen Auftrag der 2021 in Kraft getretenen Verordnung (EU) 2021/887 zur Einrichtung des Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit und des Netzwerks nationaler Koordinierungszentren.

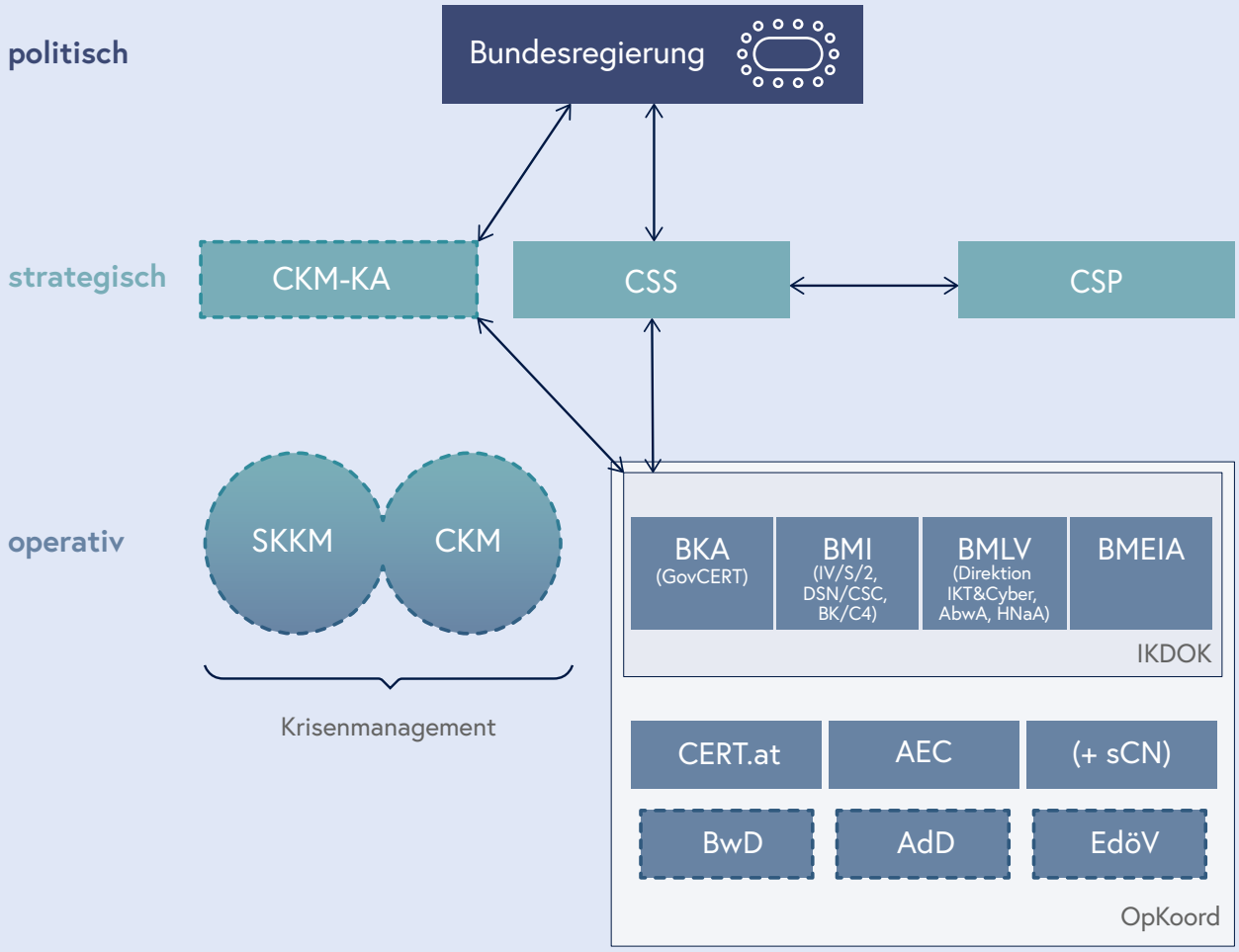
2022 fokussierten die Bemühungen auf den Aufbau des NCC-AT. Im Mittelpunkt standen die Vorbereitungen eines Antrages für EU-Mittel für den Aufbau des NCC-AT, inklusive einer ersten eigenen Förderung, sowie auf die Bewerbung des Programms Digitales Europa (Verordnung (EU) 2021/694) im Bereich Cybersicherheit in Österreich durch unter anderem Informationsveranstaltungen, Veranstaltungsteilnahmen und Einzelberatungen. Darüber hinaus nahm das NCC-AT an Sitzungen des NCC-Netzwerkes und von ECCC-Arbeitsgruppen aktiv teil. Hierzu sei auf das Kapitel 2.1 verwiesen.


0.0011

4
Nationale Strukturen

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
BMI IV/S/2. Abteilung Netz- und Informationssicherheit
BMLV..... Bundesministerium für Landesverteidigung
BwD ..... Betreiber wesentlicher Dienste
C4 ..... Cybercrime 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
DSN ..... Direktion für Staatsschutz und Nachrichtendienst
EdöV..... Einrichtungen der öffentlichen Verwaltung
GovCERT.. Government Computer Emergency Response Team Austria
HNaA..... Heeresnachrichtenamt
IKDOK..... Innerer Kreis der Operativen Koordinierungsstruktur
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
(IV/S/2,
DSN/CSC,
BK/C4)
BMLV
(Direktion
IKT&Cyber,
AbwA, HNaA)
BMEIA
IKDOK
CERT.at
AEC
(+ sCN)
BwD
AdD
EdöV
OpKoord

4.1 Innerer Kreis der Operativen Koordinierungsstruktur (IKDOK)

Erhöhung der Cyber-Resilienz durch Zusammenarbeit

Der Schlüssel für nachhaltigen Erfolg bei der Erhöhung der Resilienz gegenüber Gefahren aus dem Cyberraum liegt in der Zusammenarbeit. Das Netz- und Informationssicherheitsgesetz (NISG) stellt in diesem Zusammenhang die wichtigste Grundlage zur interministeriellen Zusammenarbeit im Bereich der Sicherheit von Netz- und Informationssystemen in Österreich dar und etabliert mit der „Operative Koordinierungsstruktur" (OpKoord) eine dauerhafte Struktur zur Koordination auf der operativen Ebene. Teil davon ist der IKDOK, eine interministerielle Struktur zur Koordination auf operativer Ebene. Während die OpKoord vorrangig die Erörterung eines gesamtheitlichen Lagebildes vornimmt, das auch freiwillige Meldungen einbezieht, liegen die Hauptaufgaben des IKDOK bei der Erfassung und Bewertung des Lagebildes über Risiken, Vorfälle und Sicherheitsvorfälle sowie in der Unterstützung des Koordinationsausschusses im Cyberkrisenmanagement (CKM).

Dem IKDOK, unterstützt durch die OpKoord, kommt dabei im Krisenfall die Funktion einer direkten Schnittstelle zum gesamtstaatlichen Cyber-Krisenmanagement zu. Dabei orientiert sich das CKM hinsichtlich anzuwendender Mechanismen und Prozesse stark an den bereits bewährten und erprobten Abläufen des staatlichen Krisen- und Katastrophenschutzmanagements (SKKM). Der IKDOK setzt sich aus Vertreterinnen und Vertretern des BMI (IV/S/2, DSN, BK/C4), des BKA (GovCERT), des BMEIA sowie des BMLV (AbwA, IKT&Cyber, HNaA) zusammen. Das BMI (IV/S/2) koordiniert dabei die Arbeiten im Gremium und leitet die Sitzungen. Die regelmäßig erstellten Lagebilder der IKDOK und der OpKoord werden den jeweiligen Zielgruppen zu Verfügung gestellt.

4.2 CERT-Verbund Austria

Der CERT-Verbund Austria wurde 2011 als Kooperation aller damals existierenden österreichischen Computer-Notdienste (Computer Emergency Response Teams; CERTs) des öffentlichen Bereichs und jener der privaten Sektoren gegründet. Intention war die Bündelung der verfügbaren Kräfte zur optimalen Nutzung des gemeinsamen Know-hows der CERTs. Die Teilnahme am CERT-Verbund Austria ist freiwillig. Die Teilnehmenden verpflichten 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 Verbundes.

Einer der Unterschiede zwischen einem klassischem IT-Sicherheitsteam und einem CERT ist, dass die Kommunikations- und Zusammenarbeitsbereitschaft mit Dritten ein Teil des Kernauftrages ist. Ein CERT muss Schnittstellen nach außen bieten, sich vernetzen und mit anderen Teams zusammenarbeiten. International sind die CERTs global in FIRST (Forum of Incident Response and Security Teams) sowie in Europa im TF-CSIRT und dem EU CSIRTs Netzwerk organisiert.

Ein flächendeckendes Netz an CERTs ist eines der wirksamsten Mittel zur Absicherung der vernetzten Informations- und Kommunikationssysteme. Die stetig wachsende Anzahl an CERTs, CSIRTs, Security Operations Centers (SOC) und Cyber Defence Teams in den österreichischen Unternehmen sowie deren gelebte enge Partnerschaft bestätigen dies.

Seit der Gründung des CERT-Verbundes Austria haben sich die aktuell 17 mitwirkenden Teams in 56 Sitzungen getroffen und sind auch außerhalb der regelmäßigen Treffen über sichere Kommunikationskanäle in ständigem Austausch miteinander. So können über Organisations- und Unternehmensgrenzen hinweg sehr rasch Lagebilder erstellt und Maßnahmen abgestimmt werden.

4.3 Cyber Sicherheit Plattform (CSP)

Als fixer Bestandteil des österreichischen Cyber-Ökosystems fungiert die Cyber Sicherheit Plattform (CSP) seit einigen Jahren als bisher zentrale strategische Austausch- und Kooperationsplattform zwischen Wirtschaft, Wissenschaft und öffentlicher Verwaltung. Sie genießt das Vertrauen aller relevanter Stakeholder und dient dem Erfahrungs- und Informationsaustausch im Bereich Cybersicherheit mit besonderem Fokus auf kritische Infrastrukturen. Die CSP leistet wichtige Beiträge bei der Weiterentwicklung der österreichischen Cybersicherheitsstrategie und der Ausgestaltung des legistischen Rahmens zur Cybersicherheit in Österreich (Stichwort NIS2). Beteiligungen der CSP durch ihre Mitglieder an internationalen Arbeitsgruppen wie der ENISA oder der UNODC Cyber Crime Convention runden das Gesamtbild ab. Auch 2023 wird die CSP ihren Beitrag zur Gestaltung der Cybersicherheit in Österreich leisten.

AUSTRIAN TRUST CIRCLE

4.4 Austrian Trust Circle (ATC)

Der Austrian Trust Circle (ATC) ist eine nationale Initiative für den fachlichen Informationsaustausch zu Cybersicherheit und damit in Zusammenhang stehender Vorfälle. Der ATC wurde im Jahr 2011 durch CERT.at und mit Unterstützung des BKA gegründet und später durch das GovCERT erweitert. Zielgruppe sind alle Sektoren der strategischen Infrastruktur sowie die öffentliche Verwaltung in Österreich. Der ATC bietet den Teilnehmenden einen formellen Rahmen für praxisnahen Informationsaustausch und gemeinsame Projekte im Sicherheitsbereich. Um das Vertrauen herzustellen, das einen „Trust Circle“ auszeichnet, verpflichten sich alle Teilnehmenden zur Einhaltung eines Code of Conduct und des Traffic Light Protokolls (TLP) nach der Definition des Forum of Incident Response and Security Teams (FIRST).

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;
  - zu Expertinnen und Experten für das BKA im Krisenfall.

Neben regelmäßigen Treffen innerhalb der einzelnen Sektoren-Circles wird der Austausch zwischen den Sektoren inklusive der öffentlichen Verwaltung einmal im Jahr im Rahmen einer zweitägigen Veranstaltung gefördert.

Im Jahr 2022 lag der Schwerpunkt der behandelten Themen bei dem starken Anstieg von Ransomwarefällen in Österreich (mit dem medialen Höhepunkt in Form des Angriffes auf das Land Kärnten) und den damit verbundenen Rahmenbedingungen. Der Trust Circle bietet für den gegenseitigen Erfahrungsaustausch zu den Details der erfolgten Angriffe den notwendigen vertraulichen Rahmen. In Verbindung damit wurde auch über Best Practices zu Tools für den Informationsaustausch, „Blue vs. Red Team"-Übungen, Cybersicherheit im Automotive-Bereich und aktuelle Forschungsergebnisse zu Kryptografie diskutiert. Einen weiteren Schwerpunkt stellten die Auswirkungen des Ukraine-Krieges auf die Cybersicherheit-Aktivitäten österreichischer Behörden und Unternehmen dar. Und auch der regulative Bereich wurde neuerlich intensiv diskutiert, im Speziellen in Form der voraussichtlichen Auswirkungen von NIS 2 und DORA auf die davon betroffenen Organisationen.

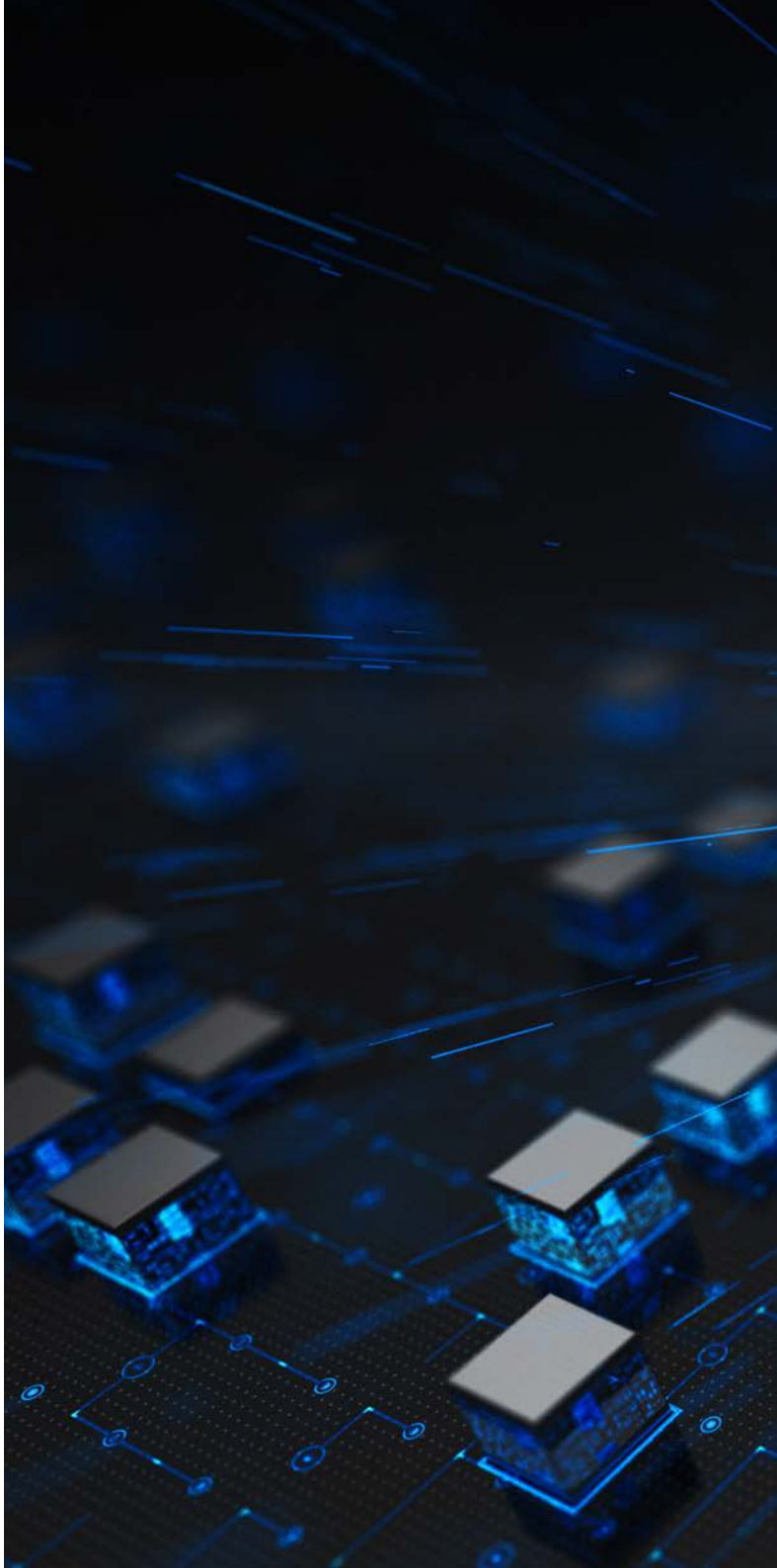
4.5 IKT-Sicherheitsportal

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 (ÖSCS) 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 40 Kooperationspartnerinnen und -partnern (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.

2022 umfassten die Aktivitäten auf dem IKT-Sicherheitsportal insgesamt die Erstellung von 131 Newsartikeln, 35 Publikationseinträgen und 44 Veranstaltungseinträgen. Jedes Monat wurde ein Schwerpunktthema zu aktuellen Trends festgelegt, wozu jeweils ein Video und insgesamt 131 Fachbeiträge veröffentlicht wurden. Dies waren beispielsweise im Jänner mobile Zahlungssysteme, im Mai „Bring Your Own Identity“ sowie im Oktober ein wiederkehrender Schwerpunkt zum „European Cyber Security Month“ (ECSM) und den österreichischen Aktivitäten, die im Zuge dessen veranstaltet wurden. Die Videos entstehen gemeinsam mit Expertinnen und Experten der jeweiligen fachlichen Disziplinen. Regelmäßig werden Inhalte zu IT-Sicherheitsthemen des Alltags wie etwa auf Reisen oder zum Online-Shopping kurz vor Weihnachten behandelt. Unter den Themenschwerpunkten wird auch der Bezug von Cybersicherheit zu aktuellen Trends wie Künstliche Intelligenz (KI) bereits frühzeitig behandelt. Des Weiteren wurde der Cybermonitor, eine

statistische Aufbereitung der zwölf wesentlichsten Gefährdungen im Bereich der IKT- und Cybersicherheit, laufend aktualisiert und modernisiert. Der Cybermonitor bietet zu den jeweiligen Kategorien eine grafische Darstellung zur Entwicklung der Gefährdungslage und zeigt dadurch aktuelle Trends auf und visualisiert die Entwicklungen in ausgewählten Themenfeldern der IT-Sicherheit aus den vergangenen Jahren.



5 Cyberübungen

5.1 EU milCERT Interoperabilitätskonferenz 2022 (MIC22)

Von 17. bis 19. Februar 2022 fand die zweite milCERT Interoperabilitätskonferenz (MIC) der EU im technischen Bereich statt. Veranstaltet wurde diese von der Europäischen Verteidigungsagentur (EDA). Ziel dieser Übungsserie ist es, die Kommunikation und Zusammenarbeit und somit das Vertrauen unter den europäischen militärischen Computer Emergency Readiness Teams (milCERTs) zu stärken. Dieses Jahr nahmen 200 Expertinnen und Experten aus 19 Mitgliedstaaten teil, darunter zehn Personen des österreichischen milCERTs.

Bei Planspielen kann der Krisenfall erprobt werden

Wichtiger Teil der Konferenz war eine technische Cyber-Defence-Übung, bei welcher Angriffe auf ein virtuelles Netzwerk simuliert wurden. Dieser Angriffe mussten vom jeweiligen milCERT im eigenen Zuständigkeitsbereich zunächst erkannt und analysiert werden und flossen in ein „nationales" Lagebild, den sogenannten „Situational Report" (kurz: SITREP), ein. SITREPs sind im militärischen Umfeld notwendig, um die Führung über aktuelle Situationen im Rahmen einer aktuelle Lageübersicht zu informieren und notwendigenfalls steuernd eingreifen zu können. Darüber hinaus mussten bei der Übung aus den Detailanalysen Angriffsindikatoren (Spuren, welche die Angreifenden im System hinterlassen haben) erkannt, aufbereitet und mit den anderen Teams geteilt werden. Dieser standardisierte Informationsaustausch stand im Fokus der Übungsserie. Die Übungsleitung bewertete die neben dem SITREP insbesondere die Qualität der mit den anderen Teilnehmenden geteilten Daten und Informationen über die zentrale „Malware Information Sharing Platform" (MISP).

Das österreichische Team erlangte 2022 zum zweiten Mal in Folge den Sieg in der Spezialwertung „Best SITREP" und konnte hinter Finnland den zweiten Platz in der Gesamtwertung erreichen.

5.2 Locked Shields 2022 (LS22)

Seit beinahe zehn Jahren nimmt Österreich an der internationalen Cyberübung „Locked Shields“, die von der NATO-Schulungseinrichtung „NATO Cooperative Cyber Defense Center of Excellence (CCDCOE)“ organisiert wird, teil. Bei der größten Live-Fire Cyber-Defence-Übung der Welt simulierten 2022 über 2000 Cyber-Expertinnen und Experten aus 32 verschiedenen Staaten die Abwehr von Cyberangriffen in einer simulierten hochkomplexen Netzwerkumgebung.

Das Österreichische Bundesheer (ÖBH) beteiligte sich durch das Militärische Cyberzentrum (MilCyZ) in einem gemeinsamen Blue Team mit Deutschland und konnte sich erfolgreich in den Top 10 platzieren.

Die Übung involvierte rund 5500 virtualisierte Systeme, die gegen mehr als 8000 Cyberangriffen verteidigt werden mussten. Der Fokus der Übung lag in diesem Jahr auf der Abwehr von koordinierten Cyberangriffen, die neben militärischen und kritischen Infrastrukturen, zum ersten Mal auch die Simulation des Reservemanagements und der Finanznachrichtensysteme einer Zentralbank umfassten. Das Besondere an der Übungsserie ist, dass die Soldatinnen und Soldaten mit „Live Fire“ konfrontiert wurden. Das bedeutet, dass die Teilnehmenden in Echtzeit und unter hohem Druck Cyberangriffe erkennen und abwehren mussten.

5.3 Common Roof 2022 (CR22)

Von 3. bis 21. Oktober 2022 fand in Österreich, Deutschland und der Schweiz die internationale Übung Common Roof 22 (CR22) statt. Diese Übung zielte auf die Interoperabilität innerhalb der Deutschland-Austria-Schweiz (D-A-CH) Community ab und der Fokus lag in der Bereitstellung eines trilateralen Führungsnetzes für Einsätze im Rahmen der grenzüberschreitenden Katastrophenhilfe und der gemeinsamen Abwehr von

Bedrohungen im Cyberraum. Dabei wurden die jeweiligen nationalen Einsatznetzwerke in ein gemeinsames Netzwerk zusammengeführt und festgelegte betriebliche Abläufe und Prozesse anhand einem Szenario und einem Ablaufplan geübt und gleichzeitig evaluiert.

Die Verantwortlichkeit der Übungsdurchführung, die nationale Übungsleitung und die Netzwerküberwachung des österreichischen Anteiles im multinationalen Netzwerk lag beim Führungsunterstützungs-Bataillon 1 in Villach. Die Soldatinnen und Soldaten führten die beabsichtigten Erprobungen gemeinsam mit Deutschland und der Schweiz durch und überprüften alle interoperablen Fähigkeiten in den Bereichen Betriebsführung, Netzsteuerung und Netzwerküberwachung eines nationalen Einsatznetzes in einem multinationalen Verbund.

5.4 Cyber Europe und Cyber Europe Austria 2022

Alle zwei Jahre organisiert die Agentur ENISA die größte pan-europäische IT Notfall und Krisenübung „Cyber Europe“. Aufgrund der Corona Situation konnte die Übung nicht wie ursprünglich geplant im Jahr 2020 abgehalten, sondern fand im Jahr 2022 zum sechsten Mal statt. Das Cyber Bedrohungsszenario konzentrierte sich dabei rund um den europäischen Gesundheitssektor.

Österreich beteiligt sich unter Federführung des Bundeskanzleramtes (BKA) seit 2010 an der Cyber Europe. Seit 2012 erfolgt dies in Form einer parallel abgehaltenen nationalen Übung, der „Cyber Europe Austria“.

Das vorrangige Ziel der internationalen Cyber Europe ist die Verbesserung der Kooperation auf europäischer Ebene. Im Zuge dessen bot sich 2022 die Möglichkeit, Prozess und Kooperationsmechanismen, welche sich aus der europäischen NIS Richtlinie ergeben, unter den teilnehmenden Staaten im Rahmen eines Szenarios zu beüben. Das Szenario

bestand aus einem internationalen, groß angelegten Cyberangriff auf die Infrastrukturen des europäischen Gesundheitssektors.

Auf nationaler Ebene konnten relevante Akteure aus dem staatlichen wie dem privaten Sektor im Rahmen der Cyber Europe Austria ihre koordinierte Reaktion auf den Cyber Ernstfall bei einem groß angelegten Angriff auf den österreichischen Gesundheitssektor testen. Die Cyber Europe Austria ermöglicht es, nationale Strukturen, Kooperations- und Kommunikationsprozesse auf ihre Effektivität und Effizienz zu testen, um so Stärken und mögliche Defizite aufzuzeigen. Die beteiligten Akteure können auf diese Weise die Vorbereitung auf einen Cyber Ernstfall optimieren und damit die Resilienz Österreichs erhöhen.

Neben der Ausarbeitung von Handlungsempfehlungen aus den Resultaten von Cyber Übungen wie der Cyber Europe Austria, spielen die Kontinuität und das regelmäßige Überprüfen von Strukturen und Prozessen eine große Rolle, um mit den Entwicklungen von Cyber Bedrohungen Schritt halten zu können und so eine nachhaltige Widerstandsfähigkeit dagegen zu erreichen.

5.5 Blue OLEx 2022

Blue OLEx ist eine Veranstaltungsserie, die jährlich mit Unterstützung der ENISA und der Europäischen Kommission (EK) durchgeführt wird. Übergeordnetes Ziel von Blue OLEx ist es, die Zusammenarbeit zwischen den nationalen Behörden für Cybersicherheit, der EK und der ENISA zu stärken, sowie die Bereitschaft und Resilienz der Mitgliedsstaaten im Falle von grenzüberschreitenden Cybervorfällen und -krisen zu evaluieren und kontinuierlich zu verbessern.

Die vierte Ausgabe der Blue OLEx (Blue OLEx 2022) wurde vom litauischen Verteidigungsministerium (MoND) mit Unterstützung der tschechischen EU-Ratspräsidentschaft organisiert und fand am 7. November 2022 in der litauischen Hauptstadt Vilnius statt. Der Schwerpunkt lag diesmal auf der Überprüfung und Weiterentwicklung der Standard Operating Procedures von CyCLONe. Darüber hinaus konzentrierte sich die Übung auf die horizontale Interaktion zwischen den Mitgliedstaaten und relevanten Institutionen, Organisationen und Agenturen der EU (EUIBA).

> Das Cyber Crisis Liaison Organisation Network (CyCLONe) wurde 2021 im Rahmen der zweiten BlueOLEx ins Leben gerufen und durch die NIS2-Richtlinie formell eingerichtet. Die zentrale Aufgabe von CyCLONe ist es, die koordinierte Bewältigung von grenzüberschreitenden Cybervorfällen und -krisen auf EU-Ebene zu unterstützen und den regelmäßigen Austausch relevanter Informationen zwischen den Mitgliedern sicherzustellen. CyCLONe arbeitet dabei auf der operativen Ebene und fungiert damit als Bindeglied zwischen der technischen und der strategischen/politischen Ebene.

Während der Übung wurde ein Szenario durchgespielt, im Rahmen dessen Cybersicherheitsvorfälle im Finanzsektor sowie in der öffentlichen Verwaltung in verschiedenen

EU-Mitgliedsstaaten simuliert wurden. Da die Übung als Tabletop-Exercise angelegt war, wurden die Übungsinhalte nur theoretisch durchgespielt, wobei das vorrangige Ziel war, darauf aufbauend Diskussionen zu möglichen Maßnahmen und Vorgehensweisen anzuregen. Die Ergebnisse dieser Diskussionen sollen dazu beitragen, mögliche Lücken in den bestehenden Standard Operating Procedures zu schließen und gewonnene Erkenntnisse in das Regelwerk einfließen zu lassen.

An der Übung nahmen neben ENISA und EK vor allem hochrangige Führungskräfte der für Cyberkrisenmanagement bzw. Cyberpolitik zuständigen nationalen Behörden aus den Mitgliedstaaten der EU teil. Österreich wurde durch Mitarbeitende des BMI (IV/S/2) vertreten.

6 Zusammenfassung / Ausblick

Der Berichtszeitraum 2022 zeigte erneut, dass mit der fortschreitenden Digitalisierung Cybersicherheit immer mehr an Bedeutung gewinnt. Cybersicherheit ist eine Querschnittsmaterie, die an verschiedensten Stellen ihren Niederschlag findet: Neben Kriminalitätsbekämpfung und Krisenmanagement im Fall von konkreten Cyberangriffen wird mit Hilfe von Strategien und Gesetzen auf europäischer und internationaler Ebene versucht, Rahmen zu schaffen, die Cyberangriffe vorbeugen, die Wirtschaft und Gesellschaft absichern und ein effektives Krisenmanagement sicherstellen. Technologische Entwicklungen führen zu Chancen für die Gesellschaft, im schlimmsten Fall kann ein Missbrauch von neuen Technologien aber auch zum Schaden für Unternehmen und Bürgerinnen und Bürger werden: Beispiele sind das Ausspähen von Betriebsgeheimnissen, die Überwachung von Journalistinnen und Journalisten oder Cybermobbing an Frauen durch technologie-gestützte Werkzeuge. Kurzfristig schaffen versierte Expertinnen und Experten Abhilfe, längerfristig werden Fachkräfte ausgebildet und Forschung und Entwicklung finanziert, um eine cybersichere Zukunft zu garantieren.

Die Österreichische Strategie für Cybersicherheit 2021 mit ihren zwölf Zielen versucht in Österreich einen Rahmen zu bieten, auf die Herausforderungen zu reagieren. Teil der Strategie ist ein halbjährlich aktualisierter Maßnahmenkatalog, der 2022 94 Maßnahmen des öffentlichen und privaten Sektors umfasste.

Die von Cyberangriffen betroffenen österreichischen Akteure fielen 2022 häufig Ransomwareangriffen zum Opfer (siehe Kapitel 1). Der Angriff der Gruppierung „BlackCat“ auf die IT-Systeme der Landesregierung Kärnten führte zum temporären Ausfall von Dienstleistungen für Bürgerinnen und Bürger und verdeutlichte zu welchem Schaden ein derartiger Vorfall führen kann. Zeitnah konnte von den zuständigen Stellen die Funktionstüchtigkeit wiederhergestellt werden.

Die nationalen Strukturen (siehe Kapitel 3 und 4) halfen auch 2022 mit diesen Herausforderungen umzugehen: Beispielsweise sind im Bereich Cyberkriminalität zwar die Anzeigen im Jahr 2022 gegenüber dem Vorjahr stark gestiegen, gleichzeitig aber auch

die Aufklärungsquote bei Delikten mit Bezug auf Cyberkriminalität im engeren Sinne. Auf operativer Ebene hat das nationale Computernotfallteam CERT.at 2022 in vielen Fällen die Rolle übernommen, mit den verfügbaren Informationen Warnungen für weitere potentielle Opfer zu erstellen, damit diese sich rechtzeitig schützen können und informierte über aktuelle Bedrohungen und Schutzmaßnahmen.

Das maßgebliche Gremium für die interministerielle Zusammenarbeit – IKDOK – beobachtete von Anfang an im Rahmen von Sonderlagebildern die zu erwartenden Auswirkungen des russischen Angriffskrieg auf die Ukraine.

Österreich bringt sich aktiv auf EU-Ebene und international ein

So international die Bedrohungslage ist, so international ist auch die Zusammenarbeit, um diesen Herausforderungen zu begegnen (siehe Kapitel 2). Neben den Vorbereitungen auf den Ernstfall, der durch die Teilnahme an internationalen Cyberübungen verfolgt wurde (siehe Kapitel 5), brachte sich Österreich im Rahmen der EU aktiv in die Verhandlungen zukünftiger Rechtsakte ein. Hervorzuheben ist hier die NIS2-Richtlinie (RL EU 2022/2555), die 2022 in Kraft trat, und in Folge in Österreich bis Herbst 2024 umgesetzt werden muss. Ziel ist es, das Cybersicherheitsniveau auch in Österreich weiter anzuheben. Das soll durch ein einheitliches Sicherheitsniveau für Netzwerke und Informationssysteme kritischer Infrastrukturen geschaffen werden, die in geregelten Fällen Cybervorfälle auch an Behörden melden müssen. So sollen die Mitgliedstaaten besser auf Cyberbedrohungen reagieren und vorbeugende Maßnahmen setzen können.

Wien war 2022 darüber hinaus Verhandlungsort für ein neues Abkommen der Vereinten Nationen im Bereich Cyberkriminalität. Ziel ist es, ein weltweites Verständnis zu erreichen, welche internationalen Mindeststandards bei der Verfolgung von Cyberkriminalität gelten sollen. 2024 sollen die Verhandlungen abgeschlossen sein. Am Rande waren auch Nicht-Regierungsorganisationen eingebunden, um die Expertise und Praxiserfahrung mitzuberücksichtigen. Aus Österreich nahm mit Vertreterinnen und Vertretern der Cyber Sicherheit Plattform (CSP) auch die bisherige zentrale Public-Private-Partnership Plattform zu Cybersicherheit teil.

Letzteres zeigt, wie wichtig der gesamtstaatliche Ansatz bei Cybersicherheit ist, um alle Blickwinkel – operativ, technisch, strategisch, rechtlich, ethisch – auf einen Tisch zu bekommen. 2023 wird dieser Ansatz – Cybersicherheit als gesamtstaatliche Aufgabe – im Sinne der Österreichischen Strategie für Cybersicherheit (ÖSCS 2021) fortgeführt werden.

01000100 01100001 01110011 00100000 01010100 01100101 01100001 01101101 00100000 01100100 01100101 01110011 00100000 01000010 01110101 01101110 01100100 01100101 01110011 01101011 01100001 01101110 01111010 01101100 01100101 01110010 01100001 01101101 01110100 01110011 00100000 01100010 01100101 01100100 01100001 01101110 01101011 01110100 00100000 01110011 01101001 01100011 01101000 00100000 01100010 01100101 01101001 00100000 01100001 01101100 01101100 01100101 01101110 00100000 01001101 01101001 01110100 01110011 01110100 01110010 01100101 01101001 01110100 01100101 01110010 01101110 00100000 01100110 01110101 01100101 01110010 00100000 01001001 01101000 01110010 01100101 00100000 01010101 01101110 01110100 01100101 01110010 01110011 01110100 01110101 01100101 01110100 01111010 01110101 01101110 01100111 00101110