Bericht Cybersicherheit für das Jahr 2023

Bericht Cybersicherheit für das Jahr 2023

Wien, 2024

Bundeskanzleramt

Bundesministerium
Inneres

Bundesministerium
Landesverteidigung

Bundesministerium
Europäische und internationale
Angelegenheiten

Impressum

Medieninhaber, Verleger und Herausgeber:
Bundeskanzleramt
Ballhausplatz 2, 1010 Wien
bundeskanzleramt.gv.at
Fotonachweis: iStock
Layout: BKA Design & Grafik
Druck: Druckwerkstatt Handels GmbH
Wien, Dezember 2024

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. Dadurch wird auch § 4 Abs. 1 Z. 1 Netz- und Informationssystemsicherheits-gesetz entsprochen. Der letzte Bericht wurde im Dezember 2023 vorgelegt.

Der aktuelle Bericht Cybersicherheit für das Jahr 2023 baut auf den Inhalten des letzt-jährigen Berichtes auf und ergänzt diesen um aktuelle Entwicklungen mit Schwerpunkten in den Bereichen internationale und operationelle Entwicklungen. Beobachtungszeitraum ist das Jahr 2023, einzelne aktuelle Entwicklungen im Jahr 2024 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

Bei den im Berichtsjahr 2023 relevanten Phänomenen handelte es sich um eine Fortführung und Weiterentwicklung mehrerer nachfolgend beschriebener und bereits bestehender Bedrohungserscheinungen der letzten Jahre. „Ransomware-Gruppierungen“ und „Private-Sector-Offensive-Actors“ (PSOA) stellen Österreich vor anhaltende und dynamische Herausforderungen und bedrohen die Cybersicherheit. Zusätzlich spielen auch geopolitische Konflikte sowie nachrichtendienstliche Aktivitäten eine große Rolle in der Cyberdomäne.

1.1 Lage Cybersicherheit – operative Ebene

1.1.1 Ransomware

Ransomware gilt weiterhin als größte Cyberbedrohung. Aufgrund der Popularität des Ransomware-Marktes konnte in den letzten Jahren eine Professionalisierung des Phänomens beobachtet werden, wodurch Ransomware-Gruppierungen gewisse Ähnlichkeiten mit Klein- und Mittelunternehmen entwickelt haben. Mehrere interne Hierarchieebenen dienen der Umsetzung und Koordination von Entwicklung, Zahlungsabwicklung und Support, um dadurch den Partnerinnen und Partnern (sogenannte *Affiliates*) die zur Verfügung gestellten Services möglichst professionell bereitzustellen. Dabei ist zu beobachten, dass Cyberkriminelle oft nicht an ausländische Strafverfolgungsbehörden ausgeliefert werden und dadurch selbst nach Veröffentlichung ihrer Identitäten gegenüber ausländischen Ermittlungsbehörden– solange sie den entsprechenden Staat nicht verlassen – unangreifbar bleiben.

Österreich verstärkt Ziel von Ransomware-Angriffen

Daher ist eine Bekämpfung von Ransomware-Gruppierungen mit Hilfe von ermittlungstechnischen Ansätzen oftmals nur durch gezielte Entfernung (eng. *Takedowns*) der *Ransomware as a Service*-Infrastruktur möglich. Diese *Takedowns* zielen auf das international koordinierte Abschalten der für den Betrieb der Ransomware verwendeten Systeme ab. Der erwünschte Effekt ist die partielle oder vollständige Destabilisierung der Funktionalität der kriminellen Software. Aufgrund der bisherigen Erfolge internationaler Ermittlungsbehörden haben auch die Betreiberinnen und Betreiber der Ransomware-Infrastruktur dazugelernt, um die Auswirkungen von gezielten *Takedowns* möglichst gering zu halten. Auch die Direktion Staatsschutz und Nachrichtendienst (DSN) wirkte an internationalen Aktionen zum Ziel Ransomware-Gruppierungen einzuschränken, mit.

Bei Ransomware handelt es sich um Erpressungssoftware, die ein IT-System sperren kann. Anschließend wird ein Lösegeld für die Freigabe gefordert. ‚Ransom' ist der englische Begriff für ‚Lösegeld'.

Den Grad an Professionalität, der bei Cyberangriffen zum Einsatz kommt, zeigt auch nachfolgendes Beispiel: Die „MOVEit"-Sicherheitslücke, welche im Mai 2023 entdeckt wurde, betraf die Datenübertragungssoftware „MOVEit Transfer" eines Herstellers. Die Folgen dieser Schwachstelle waren beträchtlich, da diese weltweit verbreitet ist und dementsprechend eine hohe Zahl an Betroffenen vorhanden war. Die Sicherheitslücke wurde von der für Ransomware-Angriffe bekannten Ransomware-Gruppierung „Cl0p" ausgenutzt, um Daten zu stehlen und die betroffenen Unternehmen und Organisationen mit der Veröffentlichung zu erpressen.

Die Gruppe zielte dabei unter anderem auf große Finanzinstitute ab, wobei sie sensible Kundeninformationen wie Namen und Bankdaten erbeutete. Diese Aktionen demonstrieren die Fähigkeit der Gruppe, sowohl technisch fortgeschrittene Angriffe durchzuführen als auch erhebliche Schäden finanzieller und datenschutzrechtlicher Natur anzurichten, die oftmals auch Reputationsschäden der Opfer nach sich ziehen.

Österreich ist seit 2021 Mitglied der von den USA ins Leben gerufenen *Counter Ransomware Initiative* zur internationalen Zusammenarbeit im Kampf gegen Ransomware-Bedrohungen (siehe auch 2.8).

1.1.2 Private-Sector-Offensive-Actors (PSOA)

Bereits seit einigen Jahren sind es die als „Private-Sector-Offensive-Actors“ titulierten Unternehmen und Entitäten mit oder ohne staatlichem Hintergrund, die aufgrund ihrer Ausrichtung nach wie vor ein nicht kalkulierbares Risiko für die österreichische gesamtstaatliche Cybersicherheit darstellen. Grund dafür ist auch die bestehende und teilweise unterschiedliche Rechtsordnung im europäischen Raum.

> „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.

Ein Beispiel, das durch wiederholte mediale Berichterstattung bereits eine breite Bekanntheit erlangt hat, ist das Unternehmen NSO Group mit seinem Produkt „Pegasus“. „Pegasus“ kann neben der Verwendung gegen terroristische Organisationen und deren Mitglieder auch zur Überwachung von (Oppositions-)Politikerinnen und -Politikern, Journalistinnen und Journalisten sowie Menschenrechtsorganisationen verwendet werden. Im Jahr 2023 kam es darüber hinaus zu Angriffsversuchen eines weiteren, funktional ähnlichen Produktes namens „Predator“ gegen EU-Politikerinnen und -Politiker sowie gegen Diplomatinnen und Diplomaten. Aufgrund dieser und bereits vergangener Vorkommnisse in der Europäischen Union beschäftigte sich das Europäische Parlament in einem Untersuchungsausschuss mit der Thematik der kommerziellen Spionagesoftware und PSOA. Österreich unterstützt auf internationaler Ebene Bemühungen zur Bekämpfung der Verbreitung und des Missbrauchs kommerzieller Spionageprogramme und hat sich

der von den USA initiierten gemeinsamen Erklärung vom März 2023[1] zu diesem Thema angeschlossen.

Für die Entwicklung und den Vertrieb von kommerzieller Spionagesoftware werden oftmals als Firmensitz Länder mit weniger strikten Exportregularien gewählt, wodurch auch der Verkauf an Staaten mit geringer ausgeprägten rechtlichen Schutzmechanismen ermöglicht wird. In der Praxis ist zu beobachten, dass sich der nicht legitime Einsatz nur sehr schwer reglementieren und kontrollieren lässt. Die Beweismittelsicherung wird mitunter erschwert, da Strafverfolgungsbehörden oft erst mit dem Bekanntwerden eines Vorfalles durch Medienberichte ihre Ermittlungstätigkeit aufnehmen.

Unbenommen davon sind auch Sicherheitsbehörden bei ihrer Aufgabenerfüllung von Produkten und Lösungen mit ähnlichem oder gleichem Funktionsumfang abhängig – immer vorausgesetzt, es existieren rechtliche Rahmenbedingungen und Voraussetzungen. Insbesondere im Bereich der Strafverfolgung im Zusammenhang mit Extremismus- und Terrorismusbekämpfung sowie Spionage ist eine ausreichende Ressourcenausstattung und der rechtskonforme Einsatz von derartigen Technologien wesentlich für die Ermittlungserfolge. Gleichzeitig muss auch bei den Anbietenden derartiger Technologien Vorsorge getragen werden, um einer missbräuchlichen Anwendung entgegenzutreten.

---

1 Joint Statement on Efforts to Counter the Proliferation & Misuse of Commercial Spyware

1.1.3 Geopolitische Konflikte, nachrichtendienstliche und hacktivistische Aktionen

In den letzten Jahren, insbesondere seit dem Beginn des russischen Angriffskrieges gegen die Ukraine, hat sich die Cyberkomponente zu einem ständigen Begleiter in militärisch-kriegerischen Konflikten entwickelt. Österreich ist von solchen internationalen Konflikten mit Cyberaktivitäten durch einen „Spill-Over-Effekt" betroffen. Durch den „Spill-Over-Effekt" betreffen Cyberangriffe potenziell einen größeren Kreis an Opfern als die ursprünglich anvisierten Ziele.

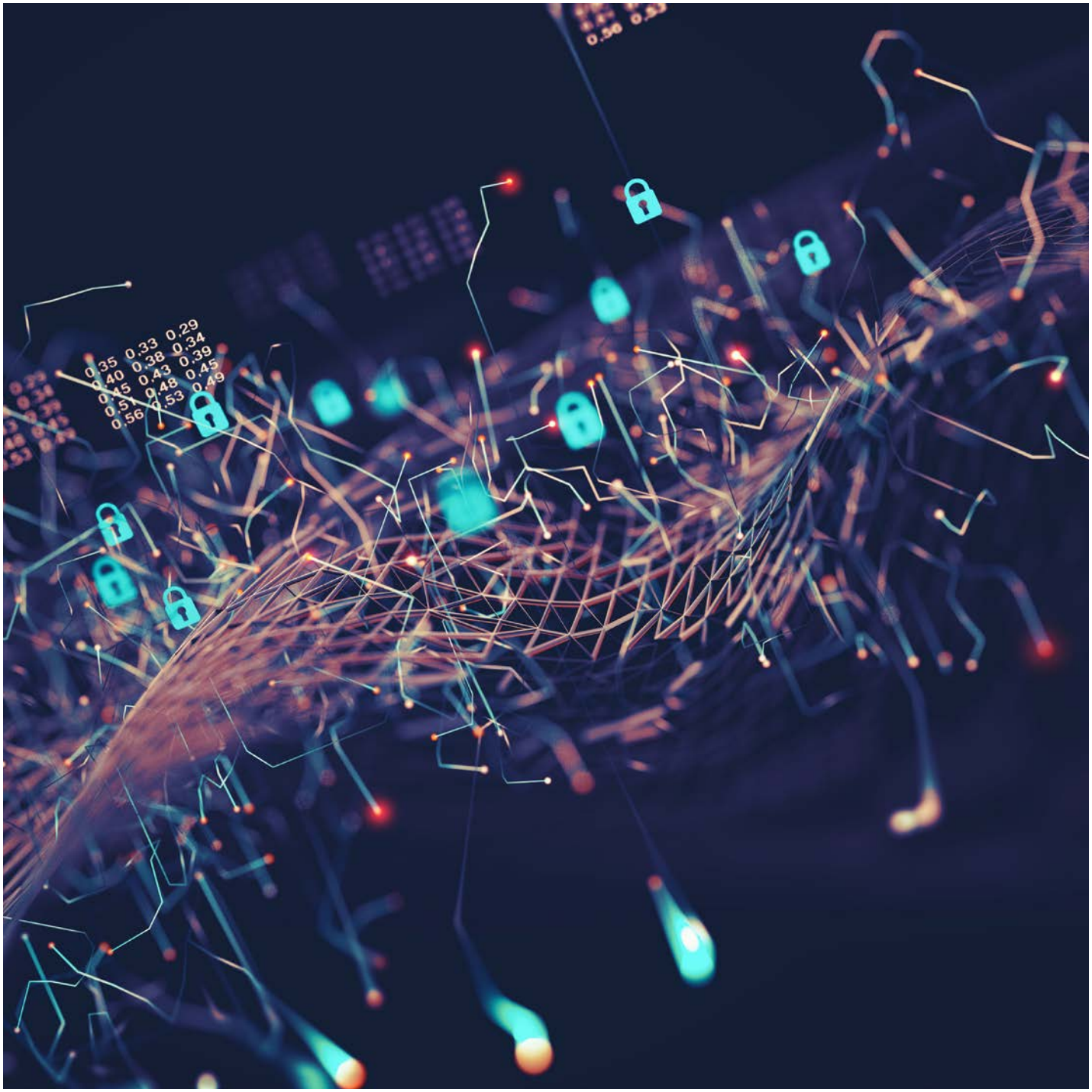
> Der Begriff „Spill-Over-Effekt" bezieht sich auf unerwünschte Auswirkungen oder Übertragungen eines begrenzten Bereiches oder Kontextes auf andere Bereiche oder Kontexte. Dies kann negative oder positive Auswirkungen haben, je nachdem, wie sich der Effekt auf die umliegenden Bereiche ausbreitet.

Zwar verwirklichte sich das oftmals prognostizierte sogenannte „Cyber-Pearl-Harbor-Szenario"[2] bisher nicht, jedoch können auch kontinuierliche und gezielte Cyberangriffe massive Auswirkungen, etwa durch mediale Berichterstattung und die damit einhergehende Formung oder Bestätigung eines gewünschten Narratives verursachen. Besonders in der Anfangsphase des russischen Angriffskrieges gegen die Ukraine wurde auch Schadsoftware, sogenannte „Wiper", eingesetzt, die dazu dienen sollte, digitale Infrastruktur zu stören oder zu beschädigen. So wurde unter anderem auch die Steuerung von Windrädern in der Europäischen Union (EU) beeinträchtigt, da die Schadsoftware Modems unbrauchbar machte, die der Satellitenkommunikation dienten und bei tausenden Windrädern zum Einsatz kamen.

---

2 Als „Cyber-Pearl-Harbor-Szenario" wird ein überfallsartiger Cyberangriff mit verheerenden Auswirkungen auf Computernetzwerke und die damit verbundenen nicht-digitalen Auswirkungen verstanden.

Cyberangriffe gehen aber nicht nur von staatlichen oder staatlich-gestützten Akteuren aus, sondern vermehrt auch von vermeintlich zivilgesellschaftlichen Gruppierungen. Diese wollen durch ihren Aktionismus, der ein Spektrum von einfachen bis intensiven Überlastungsangriffen, sogenannte DDoS-Attacken *(Distributed Denial of Service)*, der Verunstaltung von Webseiten *(Defacements)*, Hacking und der Veröffentlichung von erbeuteten Daten bis hin zur Verwendung von Ransomware, umfasst. Schäden unterschiedlichster Natur und Intensität bewirken. In diesem Zusammenhang wurde 2023 der Fall „Vulkan Files“ durch Leaks bekannt. Der russische IT-Dienstleister NTC Vulkan arbeitete demnach direkt mit den russischen Nachrichtendiensten zusammen und stellte Infrastruktur für Cyberangriffe zur Verfügung.


0.35 0.33 0.29
0.40 0.38 0.34
0.45 0.43 0.39
0.51 0.48 0.45
0.56 0.53 0.49

1.2 Lage Cybersicherheit – Unternehmen und Sicherheitsdienstleister

Zur Erstellung des vorliegenden Berichtes wurden auch in diesem Berichtsjahr wieder Unternehmen der kritischen Infrastruktur und 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 soll ein weitgehend vollständiges Bild der Cyberlage in Österreich möglich werden. Dabei liegt das Augenmerk nicht auf konkreten Vorfällen, sondern auf Trends und Entwicklungen im Sinne einer Überblicksdarstellung.

1.2.1 Unternehmen der kritischen Infrastruktur und verfassungsmäßige Einrichtungen

Kooperation mit kritischen Infrastrukturen für umfassende Cyberlagebilder

Im Berichtsjahr 2023 wurden erneut bei der Mehrheit der befragten österreichischen Unternehmen der kritischen Infrastruktur Investitionen im Bereich der Cybersicherheit getätigt. Keines der Unternehmen verminderte das Budget für 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.

Abbildung 1: Wurden in Ihrer Firma 2023 neue IT-Security-Maßnahmen implementiert, welche die Erkennbarkeit von IT-Sicherheitsvorfällen erhöhen können?

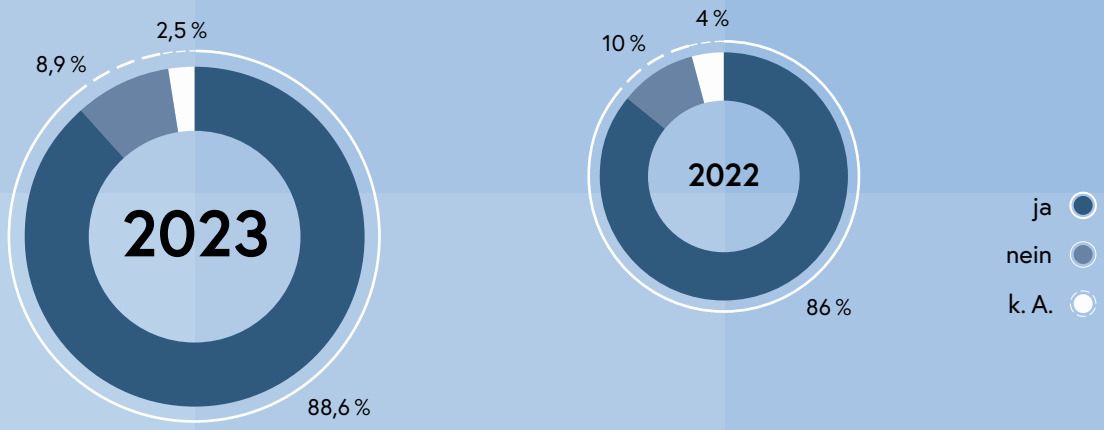
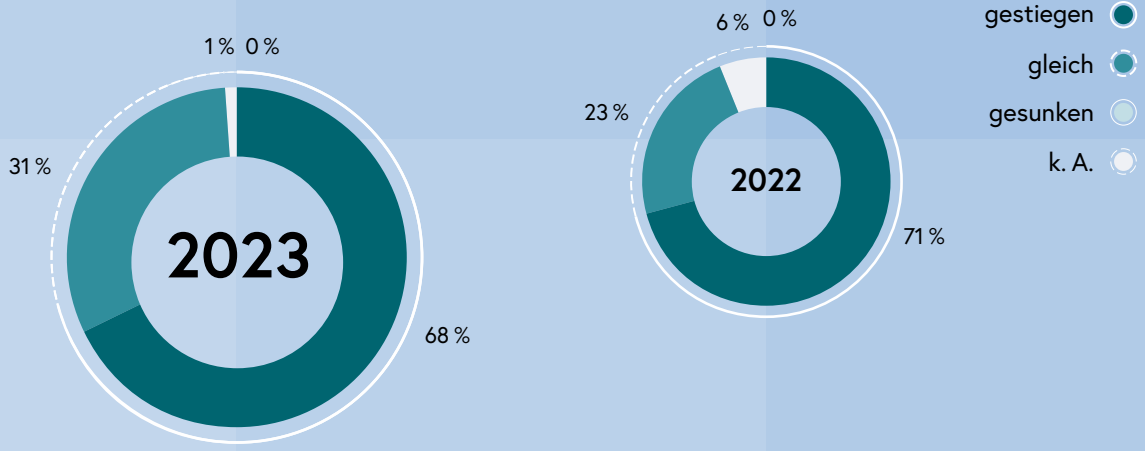


Abbildung 2: Wie hat sich in Ihrer Firma im Jahr 2023 das für IT-Security zur Verfügung stehende Budget gegenüber dem Jahr 2022 verändert?



Neu eingeführte Sicherheitsmaßnahmen umfassten im Beobachtungszeitraum die Einführung von Maßnahmen, um eine bessere Sichtbarkeit in die eigene Infrastruktur zu erhalten, wie insbesondere

- Security Information and Event Management (SIEM)-,
- Security Operations Center (SOC)-,
- Network Detection and Response (NDR)-,
- Endpoint Detection and Response (DER)- oder
- Information Security Management System (ISMS)-Lösungen.

Für einen eine umfassendere Sicherheitsstrategie (*Defense in Depth*) wurde innerhalb der Windows-Domäne auf mehreren Ebenen von Administrationsberechtigungen, beziehungsweise rollenbasierte Berechtigungen, und PAM (*Privileged Access Management*) zurückgegriffen. Um mit Hilfe von Erkenntnissen externer Bedrohungen die eigene Infrastruktur besser absichern zu können, werden *Cyber Threat Intelligence*[3] oder Services zum Durchsuchen des Darknets, dem absichtlich isolierten, verborgenen Teil des Internets, zugekauft.

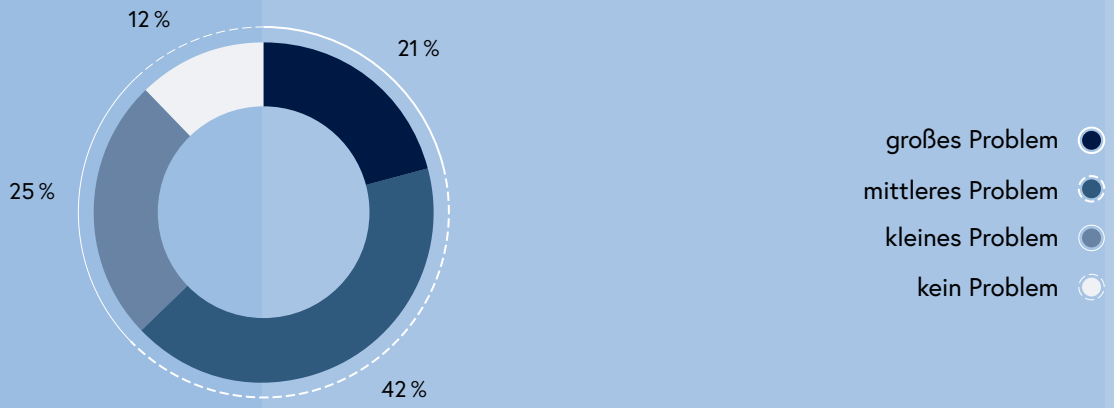
Zusätzlich mussten auch Sicherheitslösungen für die eigene Cloudinfrastruktur und Operational Technology (OT)-Systeme berücksichtigt werden. Organisatorisch wurden Awareness-Kampagnen, Übungen und die Anbindung eines 24/7–Computer Security Incident Response Teams (CSIRT) umgesetzt. Nachdem IT-Sicherheit über die technischen

3 Cyber Threat Intelligence (CTI) bezeichnet Informationen über aktuelle oder potenzielle Cyberbedrohungen, die durch eine umfassende Analyse von Datenquellen gewonnen werden.

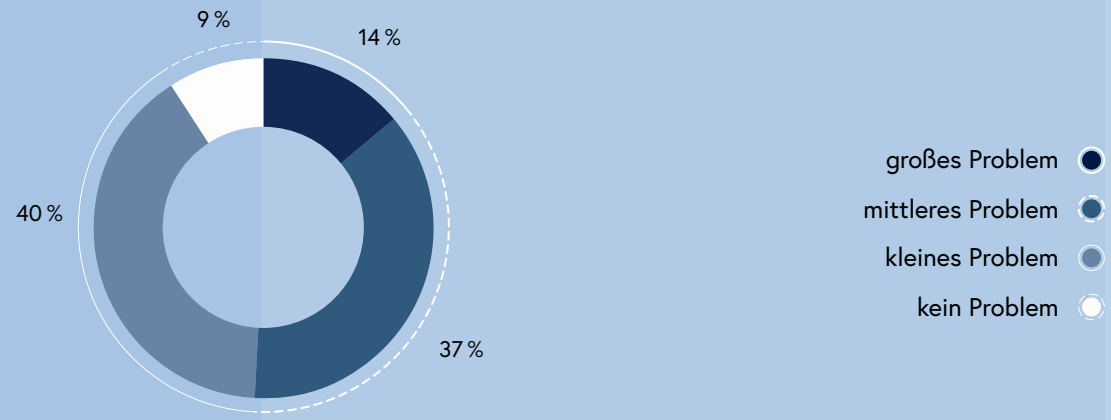
Maßnahmen hinausgedacht werden muss, wurden mehrjährige Roadmaps, Human-Risk-Management und sowohl physische als auch organisatorische Konzepte entwickelt. Zur Gewährleistung der Sicherheit wurden Vertraulichkeitsstufen für interne Dokumente entwickelt.

Die Einschätzung der Vorfallsursachen zeigt auch für 2023 das Bild, dass primär Täterinnen und Täter von außen das größte Problem für Unternehmen waren. Gefolgt von technischen Gebrechen, die auch den Betrieb hemmen können. Die derzeitige Auffassung zeigt, dass Innentäterinnen und -täter großteils entweder als kein oder als ein kleines Problem für Organisationen angesehen werden.

Abbildung 3: Wie beurteilen Sie die „Vorfallsursache“ für Außentäterinnen und -täter für das Jahr 2023?



Wie beurteilen Sie die „Vorfallsursache“ für Innentäterinnen und -täter für das Jahr 2023?



Wie beurteilen Sie die „Vorfallsursache“ für technisches Gebrechen für das Jahr 2023?

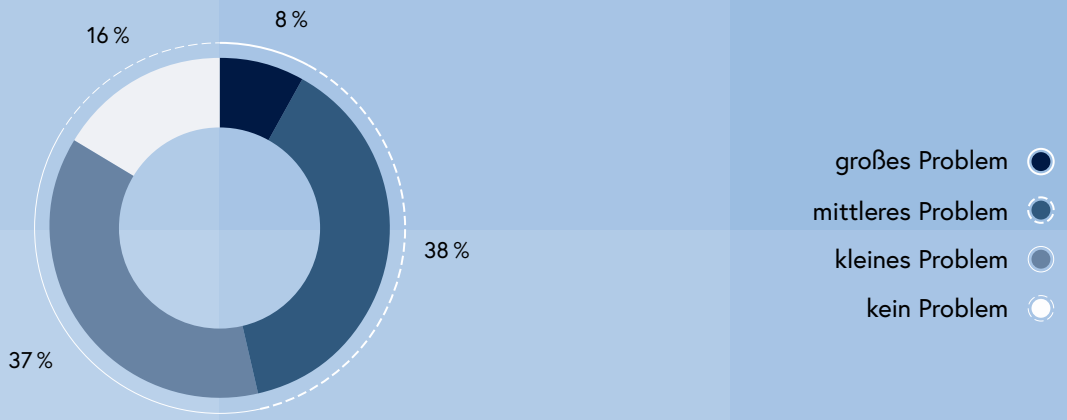
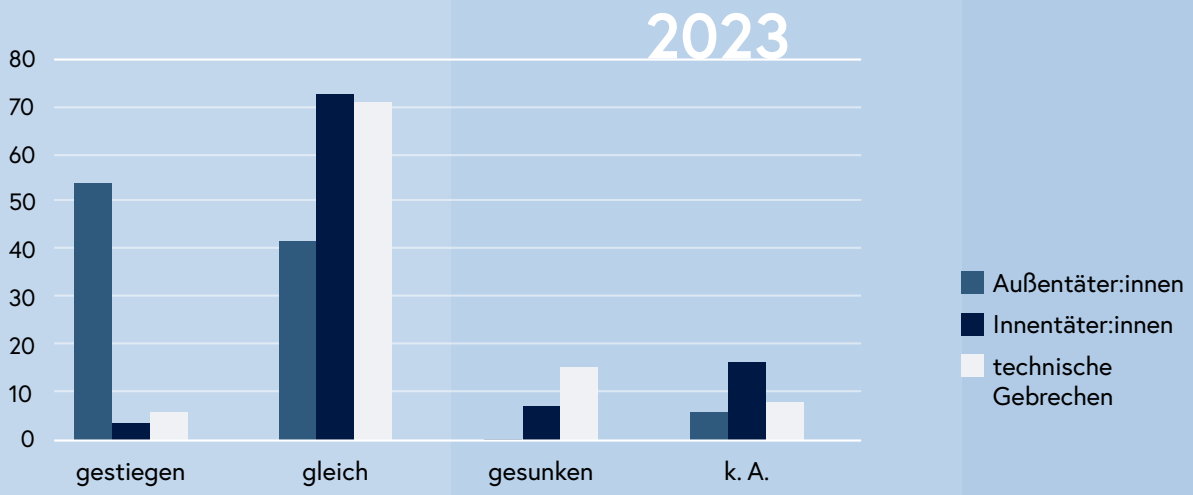


Abbildung 4: Und welche Trends konnten Sie 2023 diesbezüglich gegenüber 2022 beobachten?



Die Erkenntnisse der befragten Firmen zeigten, dass einer der wichtigsten Faktoren bei der eigenen IT-Sicherheit die Schulungsmaßnahmen der Benutzerinnen und Benutzer sind. Angreifende wissen, dass Userinnen und User das schwächste Glied in der Kette darstellen und versuchen dementsprechend, Organisationen anzugreifen. Abgesehen davon sollte IT-Sicherheit mehrstufig aufgebaut sein, um Schwachstellen in einzelnen Schichten kompensieren zu können. Die Fähigkeiten der Angreifenden verbessern sich laufend, daher sind ein risikoorientiertes Vorgehen, interne Planspiele sowie auch Cyber-Resilienz-Tests unerlässlich. Klare Rollendefinitionen und Prozesse sind sowohl für den täglichen Dienstbetrieb als auch im Fall von Sicherheitsvorfällen wichtig.

Sofern Firmen ein Teil multinationaler Konzernen sind, sollte auch darauf geachtet werden, dass Risikoeinschätzungen und Maßnahmen regional gedacht werden. Regulatorisch und rechtlich sollte zusätzlich eine Einbindung externer Dienstleistender sicherheitstechnisch durchdacht und konzipiert werden, um die eigene IT-Sicherheit nicht durch diese zu beeinträchtigen.

Das eigene Fachpersonal ist ein Schlüsselfaktor bei IT-Sicherheitsprozessen und ein Personalabgang kann Projekte zeitlich verzögern. Daher ist die längerfristige Bindung von Mitarbeitenden mit Hilfe geförderter Schulungsmaßnahmen ein wichtiger Bestandteil, damit diese in der eigenen Organisation wachsen, aber gleichzeitig auch erhalten bleiben können.

Zukünftige Trends verdeutlichen die drohende Gefahr durch Künstliche Intelligenz (KI), eine zunehmende Komplexität in der Kern-IT sowie mögliche IT-Sicherheitsbedenken bei einem Übergang zur Cloudinfrastruktur. KI kann gleichzeitig auch in Zusammenhang mit anderen IT-Sicherheitsmaßnahmen eine große Unterstützung zur Überwachung und für die Maßnahmen-Priorisierung sein. Die Compliance-Anforderungen steigen, während der Fachkräftemangel weiterhin anhält. Während die Anzahl privater Dienstleistende für unterschiedliche Unternehmensgrößen zunimmt, wächst auch die Anzahl an Dienstleistenden, deren Leistung nicht den erwarteten professionellen Standards entspricht.

1.2.2 Führende private Unternehmen aus der Cybersicherheitsbranche

Aus den eingegangenen Beantwortungen der Befragung von führenden privaten Unternehmen aus dem Bereich der Sicherheitsdienstleistenden für das Jahr 2023 lassen sich nachfolgend angeführte Trends und gewonnene Erkenntnisse ableiten. Die Rücklaufquote der Beantwortung für das Jahr 2023 ist im Vergleich zum Vorjahr leicht gestiegen.

Trends

+ gestiegen, = gleichbleibend, – fallend, k.A. keine Angabe, * anonymisierter Name

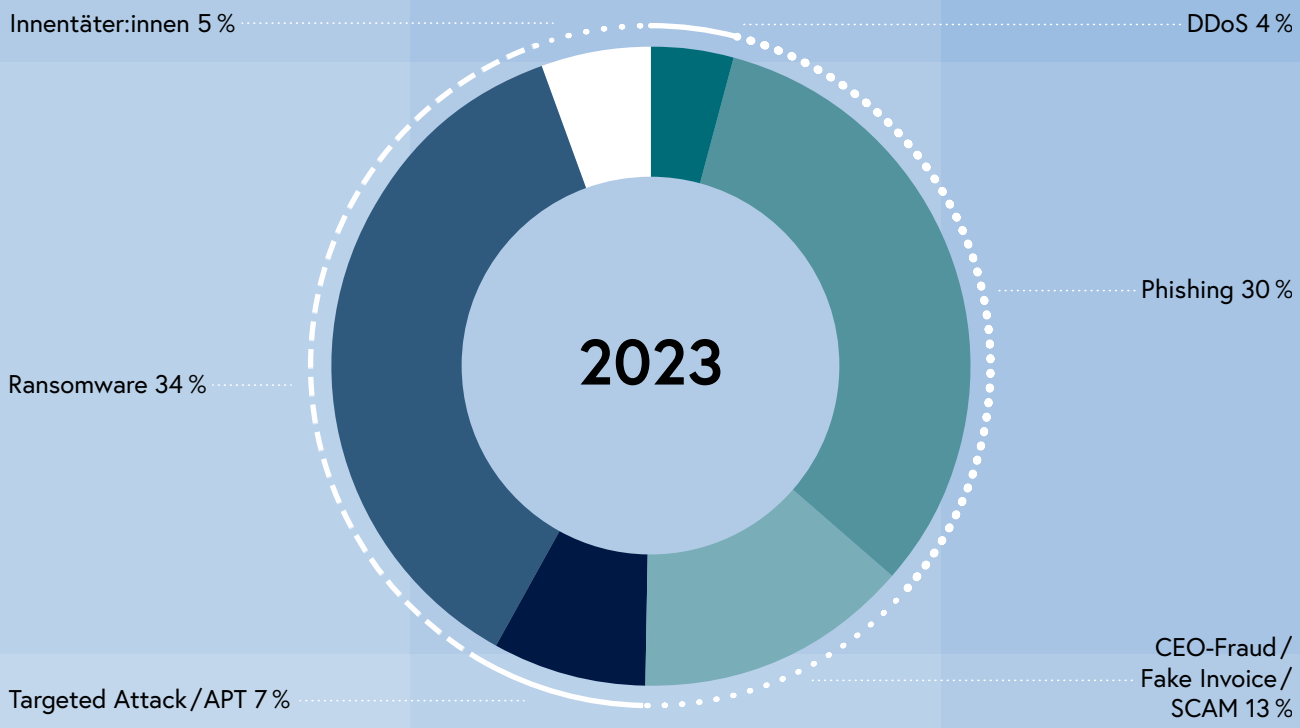
	SecConsult	SEC 01*	PWC	SEC 02*	SEC 03*	Ikarus	Secutec
Phishing	=	=	=	=	=	+	+
Ransomware	+	=	=	–	=	+	+
CEO-Fraud/Fake Invoice/SCAM	=	=	–	=	+	+	+
Targeted Attack/APT	+	=	k.A.	=	+	k.A.	=
DDoS	=	=	–	=	–	+	=
Innentäter:innen	+	=	k.A.	+	=	k.A.	k.A.

Gemeldete Vorfälle

* anonymisierter Name

	SecConsult	SEC 01*	PWC	SEC 02*	SEC 03*	Ikarus	Secutec
Infektion von Smartphones	0	0	0	0	0	0	0
Anzahl der involvierten Vorfälle	45	4	20	32	25	~25	13

Abbildung 5: Vorfallsarten im Berichtszeitraum



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

Phishing: Die Resilienz der Unternehmen gegenüber Phishing wird nach wie vor als unzureichend bewertet. 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. Insbesondere gezielte E-Mails, die spezifisch auf das Unternehmen zugeschnitten sind, haben weiterhin eine hohe Erfolgsquote. Awareness-Trainings können diesen Angriffsvektor nicht vollständig eliminieren, stellen jedoch ein geeignetes Mittel zur Reduzierung dieses Risikos dar.

Ransomware: Ransomware stellt weiterhin die größte Cybersicherheitsbedrohung dar und wird auch in den kommenden Jahren ein konstanter Begleiter sein. Im Berichtszeitraum wurden häufig Angriffe von Gruppen beobachtet, die *Ransomware-as-a-Service* anbieten. Initiale Angriffsvektoren umfassten unter anderem gestohlene beziehungsweise gekaufte Zugangsdaten, Phishing sowie die Ausnutzung von Schwachstellen in nicht aktualisierten externen Services.

Awareness-Trainings können Gefahrenpotenzial reduzieren

Eine gründlichere Vorbereitung auf das Management von Sicherheitsvorfällen, eine umfassendere Sicherheitsstrategie (*Defense in Depth*)-Strategie, ein verbessertes Backupkonzept sowie ein effektives *Attack Surface Management* können derartigen Angriffen vorbeugen. Darüber hinaus könnten besser gestaltete interne Awareness-Maßnahmen oder technische reaktive Maßnahmen helfen, um gegen diese Bedrohungsart besser aufgestellt zu sein.

CEO-Fraud/Fake Invoice/SCAM: Diese Bedrohung, die durch Betrugshandlungen durch die Verwendung falscher Identitäten oder Rechnungen entsteht, erfolgt oftmals auch in Kombination mit anderen Angriffen. Mittlerweile sind viele sensibilisiert für diese Art von Täuschung. Schulungen in diesem Bereich sollen helfen, nicht Opfer dieses Phänomens zu werden.

Innentäterinnen und -täter: Durch Maßnahmen zur Überwachung interner Zugriffe auf Datenbanken bzw. die wertvollsten, sensibelsten Daten oder Vermögenswerte eines Unternehmens kann das Risiko durch Täterinnen und Täter innerhalb der eigenen Organisation eingeschränkt werden. Es ist wichtig, das Bewusstsein für dieses Risiko auf Managementebene zu schärfen und im Falle eines Vorfalls frühzeitig den Betriebsrat und die interne Rechtsabteilung einzubinden.

Ständige Herausforderung durch Datendiebstähle

Targeted Attack/Advanced Persistent Threat (APT)
Die Anzahl registrierter gezielter Angriffe bei den befragten Unternehmen ist im Gesamtvolumen als gering anzusehen. Ähnlich wie bei Ransomware-Angriffen sind grundlegende IT-Sicherheitsmaßnahmen, einschließlich eines Verbots der Verwendung privater Geräte im Firmensystem, förderlich, um eigene Systeme gegen diese Angriffe zu schützen.

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 oder diese zumindest regional eindämmen.

1.3 Lage Cybercrime

Die Betrachtung der polizeilichen Kriminalstatistik lässt mit 65.864 angezeigten Delikten im Jahr 2023 eine Steigerung von 9,4 Prozent gegenüber dem Jahr 2022 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 stieg 2023 erneut an

Der Begriff Cybercrime umfasst:

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

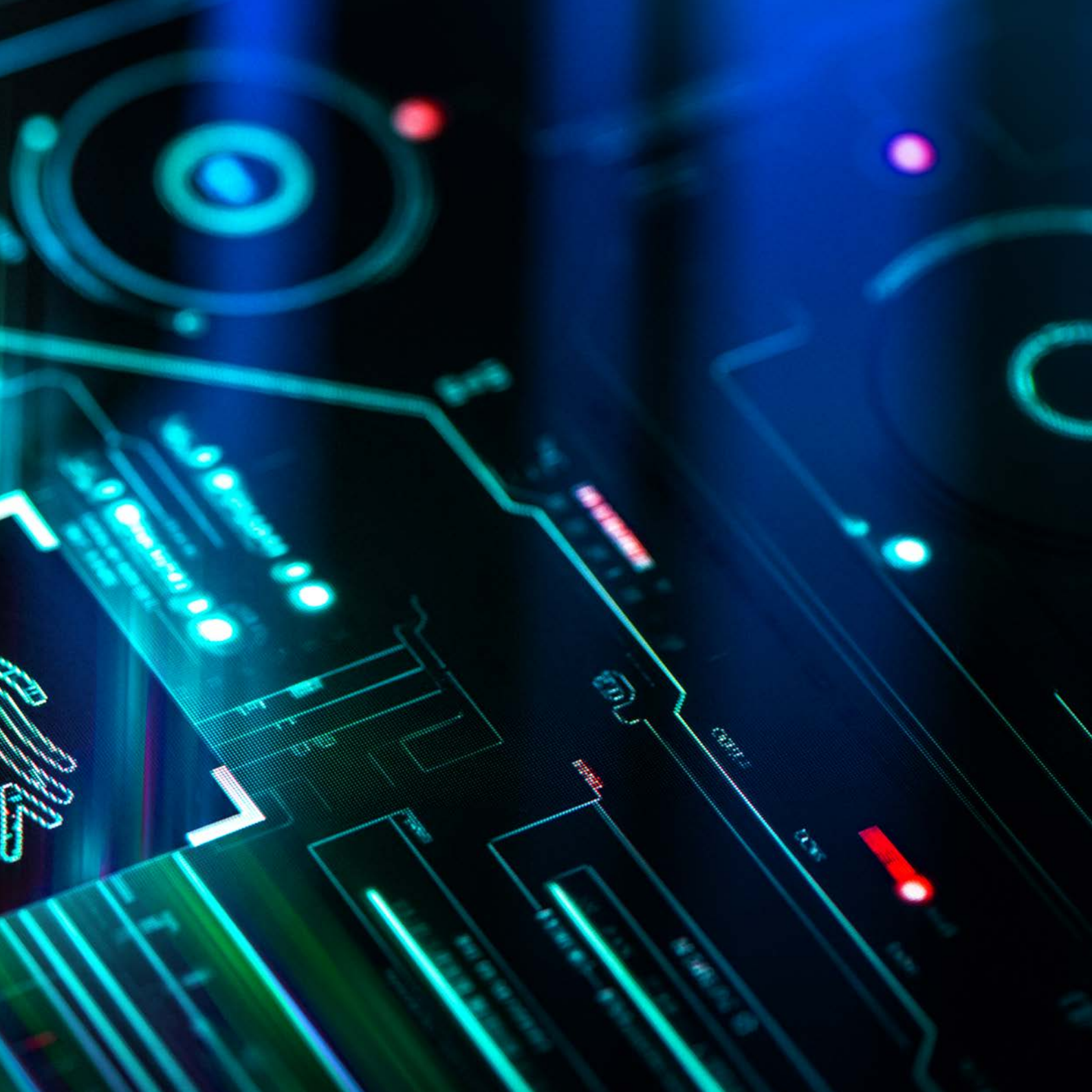
1.3.1 Cybercrime im engeren Sinn

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, die Datenbeschädigung oder der betrügerische Datenverarbeitungsmissbrauch.

Die Zahl der Fälle von Cybercrime im engeren Sinne ist 2023 im Vergleich zu 2022 um 6,4 Prozent auf 20.951 Anzeigen gesunken. Dies ist hauptsächlich auf eine geänderte statistische Erfassung der Anzeigen bei der Behebung von Geld mit gestohlenen Bankomatkarten zurückzuführen. Der Oberste Gerichtshof (OGH) hat im Jahr 2023 festgestellt, dass eine erfolgte Behebung nicht den Tatbestand des § 148a StGB erfüllt, wodurch es zu einer geänderten Erfassung kommt und diese nicht mehr als Cybercrime-Tatbestand in der Statistik erfasst wird. Die Aufklärungsquote bei Cybercrime im engeren Sinn ist um 0,5 Prozent auf 20,6 Prozent gesunken.

Im Bereich der Ransomware-Anzeigen ist zu beobachten, dass sowohl die Angriffsqualität zunimmt, insbesondere durch Ausnützung aktueller Sicherheitslücken, als auch die jeweiligen Schadenshöhen in den einzelnen Fällen ansteigen. Im Cybercrime Competence Center (C4) des Bundeskriminalamtes werden die angezeigten Ransomware-Fälle zentral erfasst und auf Gemeinsamkeiten analysiert. Ausgenommen sind jene Fälle, die aufgrund der Geschäftseinteilung in den Zuständigkeitsbereich anderer Behörden und Dienststellen fallen (wie z. B. der Direktion Staatsschutz und Nachrichtendienst [DSN]).

So wurden im Bundesgebiet im Jahr 2023 insgesamt 148 Fälle von Ransomware-Angriffen zur Anzeige gebracht. Die Angriffe richteten sich sowohl gegen Privatpersonen, EPUs (Ein-Personen-Unternehmen), KMUs (kleine und mittlere Unternehmen), Konzerne, Bildungseinrichtungen, das Gesundheitswesen, Gemeinden und Städte. Dabei wurden die Angriffe von 35 unterschiedlichen Tätergruppierungen durchgeführt. Es konnte keine spezifische Konzentration der Angriffe auf bestimmte Sektoren festgestellt werden. Bei größeren Unternehmen steigt die Gefahr, dass neben der Verschlüsselung auch die Veröffentlichung von Unternehmensdaten angedroht wird. Nach einem Schadensfall ist bei größeren Unternehmen damit zu rechnen, dass es trotz vorhandener Backups zu Produktionsausfällen von drei bis sieben Tagen kommen kann. Aufgrund zunehmender Arbeitsteilung *(Crime-as-a-Service)* und Vernetzung der Tätergruppen wird die Strafverfolgung zunehmend erschwert.



1.3.2 Internetbetrug

Internetbetrug ist größter Faktor im Bereich Cybersicherheit

Der Internetbetrug stellt zahlenmäßig den größten Faktor im Bereich der Cyberkriminalität dar und ist auch maßgeblich für den letztjährigen Gesamtanstieg der Delikte mitverantwortlich. Mehr als die Hälfte der erfassten Anzeigen im Bereich Internetkriminalität fallen auf Betrugsdelikte: 2023 wurden 34.069 Fälle von Internetbetrug angezeigt, ein Plus von 23,3 Prozent. Die Aufklärungsquote betrug 30,7 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 potenzielle Opfer angesprochen werden. Der Bestellbetrug – vonseiten der Kaufenden als auch der Verkaufenden – gehört hierbei zu den größten Bereichen, gefolgt von unbefugten Abbuchungen von Bankkonten der Opfer. Auch Anrufbetrug (Stichwort „falsche Polizistin und falscher Polizist"), international agierende Callcenter sowie digitaler Investmentbetrug trieben die Statistik in die Höhe.

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, Internetbetrug, pornographische Darstellungen Minderjähriger (§ 207a StGB) und die Anbahnung von Sexualkontakten zu Unmündigen (§ 208a StGB).

Im Bereich der sonstigen Kriminalität im Internet wurde im Jahr 2023 ein leichter Anstieg der Delikte verzeichnet. Der Grund 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-Tools oder Erpressungssoftware bzw. Ransomware. Ebenso wurde ein vermehrter Vertrieb von Falschgeld, Kinderpornografie und Kreditkartendaten wahrgenommen. § 207a StGB (Pornographische Darstellungen Minderjähriger) verzeichnete einen Zuwachs von 8,9 % im Jahresvergleich (2.245 angezeigte Fälle 2023).

Durch die im Darknet angebotenen Dienste stiegen vor allem Erpressungen mit Ransomware und Massenerpressungsmails stark an, meist begleitet von Geldforderungen in Kryptowährungen. 2023 wurden 3.891 Erpressungen im Internet angezeigt, eine Steigerung von 13,6 Prozent gegenüber dem Vorjahr (3.424 angezeigte Fälle).

Zunahmen wurden beispielsweise bei § 106 StGB (Schwere Nötigung) mit 307 Anzeigen sowie § 107 StGB (Gefährliche Drohung) mit 1.209 Anzeigen und § 107a StGB (Beharrliche Verfolgung) mit 470 Anzeigen verzeichnet. Die Anzeigen nach § 223 StGB (Urkundenfälschung) und dem Verbotsgesetz (Wiederbetätigung) nahmen ab, halten sich jedoch nach wie vor auf hohem Niveau (bspw. 729 Anzeigen nach § 3g VerbotsG).

Auffällig ist die hohe Anzahl von Angriffen, bei denen Distributed Denial of Services (DDoS) mit Erpressung kombiniert wird. Angreifende überlasten hierbei zunächst eine Anwendung des Opfers. Anschließend folgt eine Zahlungsaufforderung. Wird dieser nicht nachgekommen, folgen weitere DDoS-Attacken.

Auch konnte festgestellt werden, dass Hackerinnen und Hacker Künstliche Intelligenz (KI) für die Programmierung von Malware (Schadsoftware) nutzen. Da es sich bei der KI um ein lernendes System handelt, ist anzunehmen, dass in Zukunft stets komplexere Schadsoftware damit erstellt wird. Neben Malware könnte die Software beim Erstellen von Darknet-Marktplätzen oder Phishing zum Einsatz kommen.

1.4 Cyberlage Landesverteidigung

Cyber hat sich zu einem kritischen Bereich für nationale Sicherheitsinteressen entwickelt, und die Herausforderungen in diesem Bereich sind im vergangenen Jahr weiter gewachsen. Das sich entwickelnde Sicherheitsumfeld bringt – besonders im Licht des Kriegs in der Ukraine – eine zunehmende Komplexität und Dynamik mit sich. Cyberbedrohungen sind in ihrer Intensität und Vielfalt auch im Jahr 2023 weiter gestiegen. Verschiedene Akteure, darunter Cyberkriminelle und staatliche Einheiten, setzen innovative Methoden zur Infiltration von kritischen Infrastrukturen und Institutionen, sowie öffentlichkeitswirksame Distributed Denial of Services (DDoS)-Angriffe ein.

Schutz der österreichischen Souveränität im Cyberraum

Die Bedeutung der militärischen Dimension in Bezug auf Cyberaktivitäten wird weiter zunehmen. Fast alle Konflikte der letzten Jahre haben mit Cyberaktivitäten begonnen. Als Vorarbeit zu konventionellen Kampfhandlungen haben Hackerangriffe auf kritische Infrastrukturen (Strom-, Wasser-, Gas- Versorgungseinrichtungen, Telekommunikationseinrichtungen) stattgefunden. Sowohl in subkonventionellen, hybriden als auch terroristischen Szenarien wurde und werden Cyberaktivitäten genutzt, um für die eigene Seite in allen Phasen Vorteile zu erkämpfen. Es ist daher für die Sicherheit eines Landes und seinen Verteidigungsanstrengungen entscheidend, über Mittel zu verfügen, die einen Angriff früh genug erkennen lassen und entsprechende Gegenmaßnahmen ermöglichen. Zukünftige militärische Einsätze erfordern daher zwangsläufig Cyber- und Informationskräfte, und die Cyber- und Informationskomponente wird in hybriden Konfliktszenarien noch wichtiger. Dazu sind weitere militärische Kapazitäten mit entsprechender Durchhaltefähigkeit aufzubauen.

Der starke Anstieg der Bedrohungen durch vermehrte, gezielte Cyberangriffe war auch im Jahr 2023 nicht zu übersehen. Die zunehmende Digitalisierung und Vernetzung von Systemen in verschiedenen Sektoren wie Industrie, Gesundheitswesen und Militär birgt gleichermaßen Potentiale als auch Herausforderungen.

Durch diesen rasanten technologischen Wandel und die damit verbundene Digitalisierung werden Gesellschaft und Militär zunehmend mit der virtuellen Welt verwoben, wodurch die Zivilgesellschaft vermehrt zum Ziel hybrider Kriegsführung wird. Dies zeigt sich nicht zuletzt durch das Auftreten von Desinformationskampagnen, Fake News und Deep Fakes, die auch 2023 weiter zunahmen. Insbesondere Künstliche Intelligenz (KI) spielt in diesem Zusammenhang eine zentrale Rolle. Hybride Konflikte nutzen verstärkt Cyberaktivitäten sowie das elektromagnetische Spektrum. Die Beeinträchtigung oder Funktionsunfähigkeit von Teilsystemen wird durch den Einsatz von Cyber- und Informationskräften in militärischen oder hybriden Kriegsführungsstrategien angestrebt.

Ein wichtiges Ziel ist daher die digitale Souveränität Europas weiter zu fördern und eigene Akzente im Bereich Hard- und Software zu setzen, um die Abhängigkeit von asiatischen und amerikanischen Märkten zu verringern. Neben Bestrebungen für eine eigene Chip-Produktion wird auch die Entwicklung eines europäischen Betriebssystem mit hohen Sicherheitsstandards als wichtig erachtet, um die Abhängigkeit von Monopolisten zu reduzieren und die Einhaltung europäischer Rechtsnormen in Bezug auf Datensicherheit zu gewährleisten. Der Austausch von Informationen und Know-how innerhalb der europäischen Partnerschaft wird als entscheidend betrachtet.

Im Bereich Cybersicherheit nimmt die Bedeutung der Aufrechterhaltung kritischer Infrastrukturen und des Schutzes digitaler Dienste vor dem Hintergrund zunehmender Eintrittswahrscheinlichkeiten und Vulnerabilitäten stark zu. Daher ist es unbedingt notwendig, militärische Kapazitäten wie Einsatztruppen (sogenannte *Rapid Response Teams*) aufzubauen.

Das Österreichische Bundesheer (ÖBH) ist laufend in Kontakt mit den Sicherheitsgremien auf nationaler, europäischer und internationaler Ebene, um die Cyberverteidigung Österreichs zu gewährleisten. Um staatliche Souveränität und Resilienz für Österreich im Bereich Cyber sicherzustellen, ist eine umfassende Zusammenarbeit der zuständigen Stellen für Cybersicherheit, Cyberintelligence, Cyberkriminalität, Cyberdiplomatie und Cyberverteidigung und den Schutz kritischer Infrastrukturen auf staatlicher Ebene unerlässlich. Insbesondere angesichts hybrider Kriegsführung und der damit verbundenen Kaskadeneffekte ist eine gesamtstaatliche Zusammenarbeit relevanter denn je.

2
Internationale Entwicklungen

2.1 Europäische Union (EU)

Die zunehmende Bedeutung der Cybersicherheit zeigte sich auch im Jahr 2023. Dieses Thema wird in immer mehr internationalen Organisationen oder multilateralen Foren aufgegriffen.

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

Die Cyberdiplomatie und Cyber-Außenpolitik auf internationaler und EU-Ebene fällt in die Zuständigkeit des Bundesministeriums für europäische und internationale Angelegenheiten (BMEIA). Dem Bundeskanzleramt (BKA) obliegt die Koordination der Cybersicherheit im Zusammenhang mit der EU.

Im Allgemeinen setzt sich Österreich auf internationaler Ebene für ein freies, offenes und sicheres Internet ein, wobei die Einhaltung der Menschenrechte auch im virtuellen Raum gewährleistet sein 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 Horizontal Working Party on Cyber Issues

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 Cyberangelegenheiten, insbesondere für die Cyberpolitik und gesetzgeberische 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), der EU-Cybersicherheitsagentur (ENISA) und dem Europäischen Kompetenzzentrum für Cybersicherheit (ECCC) zusammen.

Insgesamt gab es 64 Sitzungen der HWP Cyber im Jahr 2023, nahezu ident mit dem Rekordjahr 2022 mit 67 Sitzungen. Dies zeugt von der kontinuierlich hohen Arbeitsintensität zur Weiterentwicklung der europäischen Cybersicherheitspolitik. Im Bereich der Verhandlung von Rechtsakten stand vor allem die Umsetzung der Ende 2022 veröffentlichten NIS-2-Richtlinie[4], die Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der gesamten Union vorgibt, im Vordergrund, welche primär im Zuge der NIS-Kooperationsgruppe bzw. deren Work-Streams erfolgten (siehe 2.1.2).

2023 wurden die finalen Lesungen und Bearbeitungen der am 15. September 2022 vorgestellten Verordnung, dem Cyber Resilience Act (CRA), über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen vorgenommen. Der CRA soll für Hardware- und Softwareprodukte verbindliche Cybersicherheitsanforderungen

4 Richtlinie (EU) 2022/2555

einführen 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. Mit dem vierten Ausschuss der Ständigen Vertreter (AStV)-Trilog am 30. November 2023 wurde eine vorläufige Einigung erzielt.

Schutz durch einheitliche Standards für Cybersicherheit in der EU

Auch die am 18. April 2023 im Zuge des „Cybersecurity Packages 2023" vorgestellte Verordnung über Maßnahmen zur Stärkung der Solidarität und der Kapazitäten in der Union zur Aufdeckung von, Vorbereitung auf und Reaktion auf Bedrohungen der Cybersicherheit und entsprechende Vorfälle (Cyber Solidarity Act oder CSoA) wurde dieses Jahr in zahlreichen Sitzungen bearbeitet und modifiziert – eine vorläufige Einigung diesbezüglich wurde Anfang 2024 erzielt. Der Cyber Solidarity Act sieht ein europäisches Cybersicherheits-Warnsystem, einen Cybernotfallsmechanismus und einen Überprüfungsmechanismus für Cybersicherheitsvorfälle vor. Das Cybersicherheits-Warnsystem soll durch eine europaweite Infrastruktur nationaler und grenzübergreifender sogenannter „Cyber Hubs" realisiert werden. Diese Cyber Hubs sollen Erkenntnisse über Cyberbedrohungen sammeln und analysieren. Aufgrund dieses Cybersicherheit-Warnsystems sollen sie in der Lage sein, zeitnah grenzüberschreitende Warnungen auszugeben.

Der Cybernotfallmechanismus soll

- Die Vorsorge stärken, indem Einrichtungen in besonders kritischen Sektoren (Gesundheitsversorgung, Verkehr, Energie usw.) auf potenzielle Schwachstellen getestet werden,
- eine EU-Cybersicherheitsreserve mit Sicherheitsvorfall-Notdiensten vertrauenswürdiger Anbieter aufbauen, die bei schwerwiegenden Cybersicherheitsvorfällen oder Cybersicherheitsvorfällen großen Ausmaßes auf Ersuchen eines Mitgliedstaats sofort eingreifen können,
- und finanzielle Förderung der gegenseitigen Amtshilfe zwischen nationalen Behörden der Mitgliedstaaten ermöglichen.

Der Mechanismus zur Überprüfung von Cybersicherheitsvorfällen soll Überprüfungen und Bewertungen schwerwiegender Cybersicherheitsvorfälle ermöglichen. Zudem soll die EU-Cybersicherheitsagentur (ENISA) auf Ersuchen der Kommission, des EU-CyCLONe-Netzes (Europäisches Netzwerk der Verbindungsorganisationen für Cyberkrisen) oder des CSIRTs-Netzes ENISA Cybersicherheitsvorfälle und die Reaktion darauf überprüfen können. Anschließend soll ENISA einen Bericht mit gewonnenen Erkenntnissen und Empfehlungen vorlegen.

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

2.1.2 NIS-Kooperationsgruppe

Die Kooperationsgruppe für Netz- und Informationssicherheit (NIS-Kooperationsgruppe) wurde durch die NIS-1-Richtlinie[5] 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 Agentur der Europäischen Union für Cybersicherheit (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 mittlerweile als wichtiges Forum und Bezugspunkt für die Diskussion zur Umsetzung der Cybersicherheitspolitiken innerhalb der EU etabliert.

Das neue Arbeitsprogramm für den Zeitraum 2022 bis 2024 sieht die Umsetzung der NIS-2-Richtlinie[6] als oberste Priorität an und betont gleichzeitig auch die Wichtigkeit von strategischen Diskussionen über wichtige Aspekte der Cybersicherheit in der EU, wie zum Beispiel die fünfte Generation des Mobilfunknetzes (5G), Künstliche Intelligenz oder das Internet der Dinge sowie die damit verbundene Zusammenarbeit sowohl innerhalb als auch außerhalb der EU.

Die NIS-Kooperationsgruppe traf sich im Jahr 2023 zu fünf Plenarsitzungen und zu 30 Sitzungen im Rahmen ihrer Arbeitsbereiche *(Workstream-Meetings)*. Neben den Entwicklungen, die in diesen verschiedenen Workstreams im Hinblick auf die Umsetzung der

5 Richtlinie (EU) 2016/1148
6 Richtlinie (EU) 2022/2555

NIS-2-Richtlinie[7] erreicht wurden, konnten vor allem auch Guidelines für die koordinierte Offenlegung von Schwachstellen (*Coordinated Vulnerability Disclosure* [CVD]) fertiggestellt werden. Außerdem wurde ein Referenzdokument über Risikomanagementmaßnahmen erstellt, das die Cybersicherheitsbehörde durch technische Richtlinien zu den Sicherheitsmaßnahmen unterstützt.

2.1.3 Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats

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. Cyber zählt zu den 13 Domänen hybrider Bedrohungen und stellt häufig ein Schlüsselelement hybrider Einflussnahme dar. Die Arbeitsgruppe dient der Koordinierung innerhalb des Rates und der Zusammenarbeit mit den anderen Organen, Diensten und Agenturen der EU.

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 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 unter anderem ein gemeinsames Lagebild, einen gemeinsamen Entscheidungsfindungsprozess sowie mögliche Antworten in Bezug auf hybride Bedrohungsakteure vor. Für den Fall, dass Cyberangriffe Teil einer hybriden Kampagne sind, ist ein koordiniertes Vorgehen zusammen mit der HWP Cyber Issues vorgesehen (siehe 2.1.1).

---

7 Richtlinie (EU) 2022/2555

Um die Reaktionsfähigkeiten der EU auf hybride Bedrohungen zu verbessern, haben sich die EU Mitgliedstaaten im Rahmen des Strategischen Kompasses zudem auf die Schaffung von EU-Schnelleinsatzteams für hybride Bedrohungen (*Hybrid Rapid Response Teams* [HRRT]) geeinigt. Diese sollen sich auf einschlägige nationale und EU-interne zivile und militärische Fachkenntnisse, z. B. im Cybersicherheitsbereich, stützen, um EU-Mitgliedstaaten und Partnerländer bei der Bekämpfung hybrider Bedrohungen zu unterstützen.

2.1.4 EU-Zertifizierungsrahmen (Cybersecurity Act)

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

Der europäische Rechtsakt zur Cybersicherheit (Cybersecurity Act), der bereits im Jahr 2019 in Kraft getreten ist, etabliert 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 darin festgelegten Sicherheitsanforderungen genügen. Anbieter und Hersteller von IKT-Produkten, -Diensten und -Prozessen 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 anderer relevanter nationaler Behörden zusammen. Österreich wird in der ECCG durch das Bundesministe-

rium für Finanzen (BMF) und das strategische NIS-Büro des Bundeskanzleramtes (BKA) vertreten. Die ECCG traf sich im Jahr 2023 zu fünf 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 EU-Cybersicherheitsagentur (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"[8] sowie auf relevante Common Criteria-Schutzprofile für *embedded Universal Integrated Circuit Card* (eUICC)[9] beziehen. Zu den umfangreichen Arbeiten im Bereich der Cybersicherheitszertifizierung von 5G-Netzen siehe 2.1.5.

---

8 Das „GSMA Network Equipment Security Assurance Scheme" (NESAS) ist eine Initiative der GSMA (Global System for Mobile Communications Association). Sie zielt darauf ab, einen Sicherheitsrahmen und eine Evaluierungsmethodik für die Beurteilung der Sicherheit von Netzwerkausrüstung in Telekommunikationsnetzen zu etablieren, insbesondere im Bereich der mobilen Netzwerke.

9 Die „embedded Universal Integrated Circuit Card" (eUICC) ist eine fest eingebaute universelle integrierte Schaltungskarte.

2023 befanden sich alle drei Schemata noch in Ausarbeitung. Anfang 2024 hat die Europäische Kommission das erste europäische Schema für die Cybersicherheitszertifizierung („European Union Common Criteria Scheme“ [EUCC]) im Einklang mit dem EU-Rechtsakt zur Cybersicherheit angenommen. Das EUCC-Schema ermöglicht die freiwillige Zertifizierung von IKT-Produkten, -Diensten und -Prozessen, um sie für Nutzerinnen und Nutzer vertrauenswürdiger zu machen. Die Durchführungsverordnung dazu wird am 27. Februar 2025 in Geltung treten. Mit dem bereits erwähnten Cybersecurity Package 2023 wurde der Cybersecurity Act noch um ein zusätzliches, für Anbieter verwalteter Sicherheitsdienste relevantes Zertifizierungsschema erweitert und befindet sich momentan in Ausarbeitung. Eine vorläufige Einigung konnte mit Anfang 2024 erzielt werden.

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* (5G-Toolbox) vollends umzusetzen. Hier unterschied die 5G-Toolbox zwischen technischen und strategischen Maßnahmen. Der erste Teil der in der 5G-Toolbox vorgeschlagenen technischen Maßnahmen wurde, wie im Bericht des Jahres 2022 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 5G-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, 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 der Bundesminister für Finanzen (BMF) aus Gründen der nationalen Sicherheit nach Befassung eines eigens eingerichteten Expertengremiums (des Beirats für die Sicherheit von elektronischen Netzen). Dieser hat 2023 dem zuständigen Bundesminister einen ersten Wahrnehmungsbericht vorgelegt.

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

Der Work Stream der NIS-Kooperationsgruppe zur Cybersicherheit von 5G-Netzen (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-Herstellenden und bessere Unabhängigkeit von den bisherigen Herstellenden erreicht (Stichwort Vendor-Lock-In) und somit die in der 5G-Toolbox geforderte Anbieterdiversität umgesetzt werden. Am 15.06.2023 wurde dahingehend ein zweiter Fortschrittsbericht der Umsetzung der 5G-Toolbox adaptiert und zusätzlich weiter an dem Nevers Call Risk Assessment gearbeitet.

Der NIS CG 5G Work Stream dient weiterhin als Schnittstelle zum Informationsaustausch zwischen den einzelnen Gruppen und unterstützt auch die Entwicklung eines 5G-Zertifizierungsschema durch die EU-Cybersicherheitsagentur (ENISA).

2.1.6 Cyberdiplomatie

EU-Vision für das globale und offene Internet

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 durch Cyberaktivitäten reagiert werden kann. Die *Cyber Diplomacy Toolbox* umfasst neben präventiven, kooperativen und stabilisierenden auch restriktive Maßnahmen. Letztere wurden 2020 erstmals im Rahmen des Cybersanktionen-Regimes gegen Personen und Entitäten verhängt und sehen Einreiseverbote und das Einfrieren von Vermögenswerten vor.

In Umsetzung des Strategischen Kompasses für Sicherheit und Verteidigung vom März 2022 wurden 2023 die Umsetzungsrichtlinien der *Cyber Diplomacy Toolbox* überarbeitet, um ihre Wirksamkeit und Effizienz zu erhöhen und die EU-Cyberdiplomatie auszubauen. Basis sind die fünf Säulen der EU-Cyberposition: 1. Resilienz stärken, 2. Solidarität und umfassendes Krisenmanagement ausbauen, 3. die EU-Vision für Cyberaktivitäten voranbringen, 4. Zusammenarbeit mit Partnerländern und internationalen Organisation verstärken und 5. Cyberangriffe verhindern und auf sie antworten. Im Jahr 2023 wurden die Werkzeuge der *Cyber Diplomacy Toolbox* insbesondere für einen besseren Informationsaustausch zu Cybervorfällen und ein gemeinsames Lagebild genutzt. Darüber hinaus gab es ein gemeinsames Statement zum Schutz demokratischer Prozesse vor bösartigen Cyberangriffen.

Ein wichtiger Teil der Cyberdiplomatie auf EU-Ebene ist die Erarbeitung gemeinsamer Positionen und Strategien zu Cyberthemen auf internationaler Ebene, allen voran im Rahmen der Vereinten Nationen (siehe 2.2). Standard- und Normensetzung für neue Technologien und Cyberaktivitäten sind längst geopolitische Konfliktzonen und die Zunahme an Cyberangriffen durch staatlich gelenkte Akteure ist Teil der geopolitischen 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

Bundesministerium für europäische und internationale Angelegenheiten (BMEIA) 2021 eingesetzte Sonderbeauftragte für Cyber-Außenpolitik und Cybersicherheit konnte 2023 mit der Delegationsleitung in multilateralen Verhandlungen, der Durchführung bilateraler Cyber-Dialoge und der Mitwirkung am EU-Netzwerk der Cyberbotschafterinnen und -botschafter das Engagement Österreichs in der internationalen Cyberdiplomatie weiter stärken.

2.1.7 Netz nationaler Koordinierungszentren und Europäisches Kompetenzzentrum

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 2023 weiterhin auf organisatorische Aufbauaktivitäten sowie inhaltliche Arbeiten, um seinen Auftrag gemäß der Verordnung (EU) 2021/887 des Europäischen Parlaments und des Rates vom 20. Mai 2021 zu erfüllen. Diese Verordnung sieht die Einrichtung des ECCC und des Netzwerks nationaler Koordinierungszentren (*National Coordination Centres* [NCC]) vor, um den Kompetenzaufbau sowie die Steigerung der Resilienz, digitaler Souveränität und Wettbewerbsfähigkeit der EU im Bereich Cybersicherheit zu erfüllen.

Das ECCC verabschiedete im März 2023 eine Strategische Agenda, die über Förderschwerpunkte im Bereich Cybersicherheit informieren soll und durch die Arbeiten an einem sogenannten Action Plan 2023 weiter operationalisiert wurde. Der Verwaltungsrat (*Governing Board*) des ECCC fand sich im Jahr 2023 unter Teilnahme des Bundeskanzleramts drei Mal zusammen. Im Herbst 2023 wurde der Italiener Luca Tagliaretti als Exekutivdirektor des ECCC für vier Jahre gewählt.

Zukünftig wird das ECCC eine tragende Rolle bei der Umsetzung des EU-Finanzierungsprogramms „Digitales Europa (DEP)“[10] 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:

Aufbau einer europäischen Cybersicherheits-kompetenz-gemeinschaft

- 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 gängiger Hard- und Software;
- der Steigerung der globalen Wettbewerbsfähigkeit und der hohen Standards der Cybersicherheitsbranche der EU sowie der Verwandlung der Cybersicherheit in einen Wettbewerbsvorteil für andere Wirtschaftszweige der EU.

Ein konkretes Beispiel sind zwei Projekte zum Aufbau von grenzüberschreitender Security Operation Center (SOC)-Infrastruktur zwischen Mitgliedstaaten, wodurch zukünftig (Bedrohungs-)Informationen zu Cyberaktivitäten ausgetauscht werden können. Die an den Projekten teilnehmenden Mitgliedstaaten werden gemeinsam mit dem ECCC mit DEP-Mitteln Infrastruktur einkaufen und betreiben. Nach konzeptuellen Vorarbeiten in einer eigens dafür eingerichteten Arbeitsgruppe des ECCC-Verwaltungsrates wurde im Jahr 2023 der gemeinsame Ankauf von Infrastruktur weiter vorbereitet. Diese Projekte sollen in weiterer Folge bei der Durchführung des Cyber Solidarity Acts (siehe 2.1.1) unterstützen.

---

10 Verordnung (EU) 2021/694

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 sowie die nationale Cybersicherheits-Community europäisch vernetzen. In Österreich wird das Nationale Koordinierungszentrum (NCC) vom BKA in Kooperation mit der Österreichischen Forschungsförderungsgesellschaft (FFG) betrieben (siehe 3.9).

Das NCC nahm darüber hinaus an Sitzungen des NCC-Netzwerkes und von ECCC-Arbeitsgruppen aktiv teil. Diese umfassten insbesondere die ECCC-Arbeitsgruppen zu Cybersecurity Skills und zur Einrichtung der Europäischen Kompetenzgemeinschaft.

2.1.8 Cybersecurity Skills

Die Europäische Kommission hat am 18.04.2023 eine Gemeinsame Mitteilung mit dem Titel *„Closing the cybersecurity talent gap to boost the EU's competitiveness, growth and Resilience"* veröffentlicht, welche Vorschläge zu einer koordinierteren Vorgehensweise zwischen Mitgliedstaaten, EU-Institutionen und privaten Akteuren unterbreitet. Diese politische Willensbekundung wurde in den Ratsschlussfolgerungen zur Cyberabwehrpolitik im Mai 2023 durch die Mitgliedsstaaten begrüßt. In der gemeinsamen Mitteilung wird die Gründung eines sogenannten EDICs (Europäisches Digitales Infrastrukturkonsortium) durch interessierte Mitgliedsstaaten vorgeschlagen, um die Initiative zu implementieren und einen Beitrag zum Schließen der Fachkräftelücke im Bereich der Cybersicherheit zu leisten.

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 Cybersicherheit 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 von Informations- und Kommunikationstechnologie 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 Cyberaktivitäten 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 Berichte der Open-Ended Working Group (OEWG) zu Cybersicherheit sowie der Regierungsexpertinnen- und -expertengruppe (GGE) mit ihrem normativen „Rahmen für verantwortungsvolles staatliche Verhalten im Cyberraum“ die Grundlage für die Arbeiten der auf Betreiben von Russland und China lancierten neuen OEWG zu Cybersicherheit 2021–2025. Diese hielt 2023 drei substantielle sowie eine informelle Sitzung ab und einigte sich im Juli 2023 im Konsens auf den Zweiten Jährlichen Fortschrittsbericht. Letzterer bildet gleichzeitig einen Fahrplan für die weitere Arbeit der Gruppe im Jahr 2024, unter anderem zum Vorschlag einer „Checkliste“ zur Umsetzung der Normen für verantwortungsvolles Verhalten von Staaten und der Einrichtung eines globalen Netzwerkes von nationalen Kontaktpersonen für Cybersicherheit nach Vorbild der OSZE. Österreich brachte sich insbesondere in den Beratungen über die verschiedenen Aspekte der Anwendung des Völkerrechts auf Cyberoperationen ein.

Wie 2022 wurden von der VN-GV 2023 drei Resolutionen zum Thema Cybersicherheit angenommen: Zwei bezogen sich auf die Arbeit der OEWG 2021–2025 und eine auf das 2021 beschlossene Aktionsprogramm der Vereinten Nationen zur Cybersicherheit. Eine von Singapur als Vorsitz der OEWG eingebrachte Entscheidung zur Annahme des zweiten Fortschrittsberichts der OEWG wurde im Konsens angenommen. Aufbauend auf den Resolutionen der Vorjahre brachte Frankreich gemeinsam mit einer überregionalen Gruppe von Staaten, darunter Österreich und die gesamte EU, wiederum eine Resolution zur Ausarbeitung eines Aktionsprogramms der Vereinten Nationen zu Cybersicherheit ein, die mit überwältigender Mehrheit angenommen wurde. Russland brachte erneut eine eigene, inhaltlich dem Sachstand der OEWG nicht entsprechende, Resolution ein, die gegen die Stimmen westlicher und gleichgesinnter Staaten angenommen wurde. Das „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. Zur Frage, wie das Aktionsprogramm ausgestaltet sein soll, übermittelte der Generalsekretär der Vereinten Nationen (VN-GS), aufbauend auf den Stellungnahmen der Mitgliedsstaaten, im April 2023 einen eigenständigen Bericht.

In seinem Vorschlag für eine „Neue Agenda für den Frieden" in Vorbereitung des VN-Zukunftsgipfels im Herbst 2024 hebt der VN-GS hervor, dass geopolitische Spannungen und Konflikte durch bösartige Cyberoperationen von staatlichen und nichtstaatlichen Akteuren weiter verstärkt werden. In einem eigenen Aktionspunkt schlägt er deshalb Maßnahmen für die Prävention bösartiger Cyberoperationen und den Schutz kritischer Infrastruktur vor. Zentral ist die Aufforderung an alle Staaten, die Normen für verantwortungsvolles Verhalten von Staaten einzuhalten.

Die Beratungen zu Cybersicherheit werden durch das Büro der VN für Abrüstungsfragen (*United Nations Office for Disarmament Affairs* – [UNODA]) unterstützt. Das Institut der VN für Abrüstungsforschung (*United Nations Institute for Disarmament Research* – [UNIDIR]) trägt mit der Veröffentlichung wissenschaftlicher Publikationen sowie der

Veranstaltung thematischer Konferenzen zu den internationalen Cybersicherheitsdiskussionen bei. Die alljährliche UNIDIR „Cyber Stability Conference“ tagte im März 2023.

In Vorbereitung auf den VN-Zukunftsgipfel 2024 wurden 2023 intensive Konsultationen mit Mitgliedstaaten und Stakeholdern über die mögliche Ausgestaltung des künftigen VN-Paktes zu Fragen der digitalen Kooperation („Global Digtal Compact“) durchgeführt, der auch Bestimmungen zu Cybersicherheit enthält. Der VN-GS setzte im Herbst ein *High Level Advisory Board on Artificial Intelligence* (HLAB AI) ein, das vor dem Zukunftsgipfel seine Empfehlungen über die Ausgestaltung globaler Standards und Governance von Künstlicher Intelligenz vorlegen soll. Ein Zwischenbericht wurde Ende Dezember 2023 vorgelegt, ein Schlussbericht soll Mitte September 2024 präsentiert werden.

Bei der Weltfunkkonferenz der Internationalen Fernmeldeunion (ITU) der Regierungsbevollmächtigten in Bukarest (26. September bis 14. Oktober 2022) nahmen die Mitgliedstaaten eine neue Strategie für die Organisation an. Diese Strategie, die auf Druck der Entwicklungsländer und aufbauend auf der bei der Weltkonferenz zur Entwicklung der Telekommunikation in Kigali angenommenen „Kigali Declaration“ entstand, gibt der ITU zum ersten Mal ein explizites Mandat zum Kapazitätenaufbau im Bereich Cybersicherheit. Auf dieser Basis verstärkte die ITU ihre Arbeit in diesem Bereich im Jahr 2023. Die Internationale Weltfunkkonferenz (WRC-23) im November/Dezember 2023 in Dubai behandelte wichtige Fragen mit indirekten Auswirkungen auf die Cybersicherheit, wie den Einsatz von satellitengetragenen Radarsystemen (*space-borne radar sounders*) und Höhenplattformen (HAPS) sowie die internationale Kooperation zur Vermeidung schädlicher Interferenzen.

Für Fragen der Internet Governance ist neben den VN-Spezialorganisationen und dem WSIS-Forum das Internet Governance Forum (IGF) die bedeutendste globale Multistakeholder-Plattform für Diskussionen und Austausch unter den vielen Akteuren, einschließlich Regierungen, Zivilgesellschaft, Privatsektor, Wissenschaft und technischen Gemeinschaften. Das IGF befasst sich 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 nachhaltig stärken.

Dem 15-köpfigen Gremium, das von Vint Cerf, dem „Vater des Internets", geleitet wird, gehört auch Bundesministerin für EU und Verfassung Karoline Edtstadler als einzige westliche Regierungsvertreterin an. Sie lud die Miglieder des IGF Leadership Panel im März 2023 zu einer Strategiebesprechung nach Wien ein, in deren Rahmen es unter anderem Treffen mit der IGF „Multistakeholder Advisory Group" (MAG) und mit der Führung von UNODC gab. Das IGF Leadership Panel arbeitete 2023 an verschiedenen Positionspapieren. Dazu gehörten ein Beitrag zum *Global Digital Compact* und ein inhaltlicher Rahmen für das Internet Governance Forum unter dem Titel „The Internet We Want", der auch ein Kapitel zum Thema Sicherheit enthält. Zudem erarbeitete das Panel Vorschläge zur Einbindung der Multistakeholder bei den Verhandlungen zum Global Digital Compact.

Cyberkriminalität hat sich rasch zu einer globalen und äußerst profitablen Verbrechenssparte entwickelt. Das VN-Büro für Drogen- und Verbrechensbekämpfung (UNODC) in Wien ist weiterhin ein unverzichtbarer Bestandteil in der effektiven weltweiten Bekämpfung von Cyberkriminalität. 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 wurde quer durch alle Gremien thematisiert, einschließlich der Kommission für Verbrechensverhütung und Strafrechtspflege (CCPCJ).

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 fanden an den VN-Standorten Wien und New York unter Vorsitz von Botschafterin Mebarki, Ständige Vertreterin Algeriens in Wien bzw. Genf, statt und wurden schließlich am 9. August 2024 erfolgreich abgeschlossen. 2023 fanden drei Verhandlungsrunden – zwei davon in Wien – sowie weitere informelle Sitzungen unter breiter Teilnahme von Expertinnen und Experten der VN-Mitgliedstaaten statt. 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 Nichtregierungsorganisationen, Think Tanks, der Privatsektor und andere wichtige Stakeholder an diesem Prozess mitwirken. UNODC fungiert als Sekretariat für den Verhandlungsprozess, womit dem Amtssitz Wien eine wichtige Rolle zukommt. Österreich hat sich in den Verhandlungen zusammen mit seinen internationalen Partnern aktiv dafür eingesetzt, dass die zukünftige VN-Konvention starke menschenrechtliche Bestimmungen enthält, um zu verhindern, dass sie von Staaten zur Legitimierung repressiver Maßnahmen missbraucht werden kann.

Im Rahmen der 53. Tagung des VN-Menschenrechtsrats brachte Österreich gemeinsam mit Südkorea, Brasilien, Dänemark, Marokko und Singapur die dritte Resolution zu „Neuen Technologien und Menschenrechten“ ein. Im Rahmen der 78. VN-GV unterstützte Österreich die Resolution zu „Förderung und Schutz der Menschenrechte im Kontext digitaler Technologien“. Dabei handelte es sich um die erste Resolution der VN-GV zu den Auswirkungen Künstlicher Intelligenz auf die Menschenrechte. Die Resolution konnte im Konsens verabschiedet werden.

Die ebenfalls von Österreich 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 Organisation des Nordatlantikvertrags (NATO)

Cyberaktivitäten als eine militärische Domäne für die NATO und ihre Alliierten – neben Land, See, Luft und Weltraum – finden in den drei Kernaufgaben der NATO Niederschlag: Abschreckung und Verteidigung, Krisenmanagement und kooperativen Sicherheit.

Als Reaktion auf die sich entwickelnde Cyber-Bedrohungslandschaft hat die NATO die Cyber Defence in ihren strategischen Rahmen integriert. Das Bündnis hat Mechanismen zur Erkennung, Prävention und Reaktion auf Cyber-Bedrohungen etabliert, wobei der Schutz kritischer Infrastrukturen und der Austausch von Informationen und Best Practices unter den Alliierten im Vordergrund steht. Die Annahme des *Cyber Defence Pledge* im Jahr 2016 und dessen anschließende Verbesserung im Jahr 2023 unterstreichen das kollektive Engagement zur Stärkung der nationalen Cyber Defence-Fähigkeiten.

Die Cyber-Defence-Strategie der NATO umfasst Governance, Evolution und Zusammenarbeit mit internationalen Partnern und dem privaten Sektor. Die Governance Struktur des Bündnisses erleichtert die politische, militärische und technische Koordination, wobei das *Cyber Defence Committee* und die *NATO Communications and Information Agency* (NCIA) eine Schlüsselrolle bei der Implementierung der Strategie und der operativen Unterstützung spielen.

Die Zusammenarbeit mit Partnerländern, internationalen Organisationen und dem privaten Sektor ist integraler Bestandteil der Cyber-Defence-Bemühungen der NATO. Kooperative Initiativen mit der EU, den Vereinte Nationen (VN) und der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) sowie das Engagement mit Industrie und Wissenschaft verbessern die Kapazität des Bündnisses, Cyber-Bedrohungen effektiv zu adressieren. Das Engagement der NATO für einen freies, offenes und sicheres Umfeld für Cyberaktivitäten, ausgerichtet an internationalem Recht und Normen, untermauert ihren Ansatz zur Förderung von Stabilität und zur Verringerung des Risikos von Konflikten im digitalen Raum.

Österreich kooperiert als Partnerland eng mit der NATO und beteiligt sich auf technischer Ebene an Sitzungen des Digital-Policy-Kommittees 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) außerdem einen Offizier im „NATO Cooperative Cyber Defence Center of Excellence" (CCDCoE) in Tallinn. Ziel der Zusammenarbeit ist die Steigerung der Fähigkeiten zur nationalen Cyberverteidigung.

Der umfassende Ansatz der NATO zur Cyber Defence, der Prävention, Resilienz und Reaktion ausbalanciert, gewährleistet die Bereitschaft des Bündnisses, Cyber-Bedrohungen zu bekämpfen und abzumildern. Durch kontinuierliche Anpassung, Zusammenarbeit und Investitionen in Cyber-Fähigkeiten zielt die NATO darauf ab, die Sicherheit und demokratischen Werte ihrer Alliierten in einer zunehmend digitalen Welt zu schützen.

2.4 Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE)

OSCE Organization for Security and Co-operation in Europe

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 Vereinten Nationen (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) in Hinblick auf Cyberaktivitäten eine Vorreiterrolle. Die Annahme der 16 vertrauensbildenden Maßnahmen stellt global gesehen den ambitioniertesten Versuch zur Stärkung der internationalen Kooperation im Feld der Cybersicherheit außerhalb der VN dar.

Ziel ist es zwischenstaatliche Spannungen, die aus der Nutzung von Informations- und Kommunikationstechnologien entstehen, unter den teilnehmenden Staaten der OSZE zu minimieren. Dazu wird der Austausch von Informationen, die Etablierung von Kommunikationskanälen und den Aufbau von Kapazitäten angeregt. Die OSZE-Arbeit konzentriert sich darüber hinaus auf die Wahrung und Stärkung der Menschenrechte im Cyberkontext sowie die Bekämpfung von Desinformation und Hassrede, insbesondere gegen Frauen und Mädchen.

Für die Weiterentwicklung und Implementierung der VBM ist die Informelle Arbeitsgruppe zu Cyber (Cyber-IWG) vorrangig zuständig. 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 und Cyberattacken in diesem Zusammenhang weiter ein besonderer Schwerpunkt waren. 2023 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 VBM 14 zu Public-Private-Partnerships voran.

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 2023 fand diese Konferenz mit den Schwerpunktthemen Cyber/ICT Sicherheit und insbesondere Bewusstseinschaffung gegenüber verstärkten Cyberangriffen in Skopje im Rahmen des nordmazedonischen 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 der Sicherheit digitaler Produkte und Dienstleistungen. Dabei wird auf die Expertise aus OECD- und Partnerländern, Wirtschaft, Zivilgesellschaft und der technischen Internet-Community gesetzt.

In Österreich nimmt das Bundeskanzleramt (BKA) die inhaltliche Koordination für diese Arbeitsgruppe wahr. Auch im vergangenen Jahr wurden Berichte (Reports) zu beispielsweise den Themenbereichen „enhancing the security of communication infrastructure“ oder „regulatory sandboxes in artificial intelligence“ finalisiert oder deren Erarbeitung begonnen.

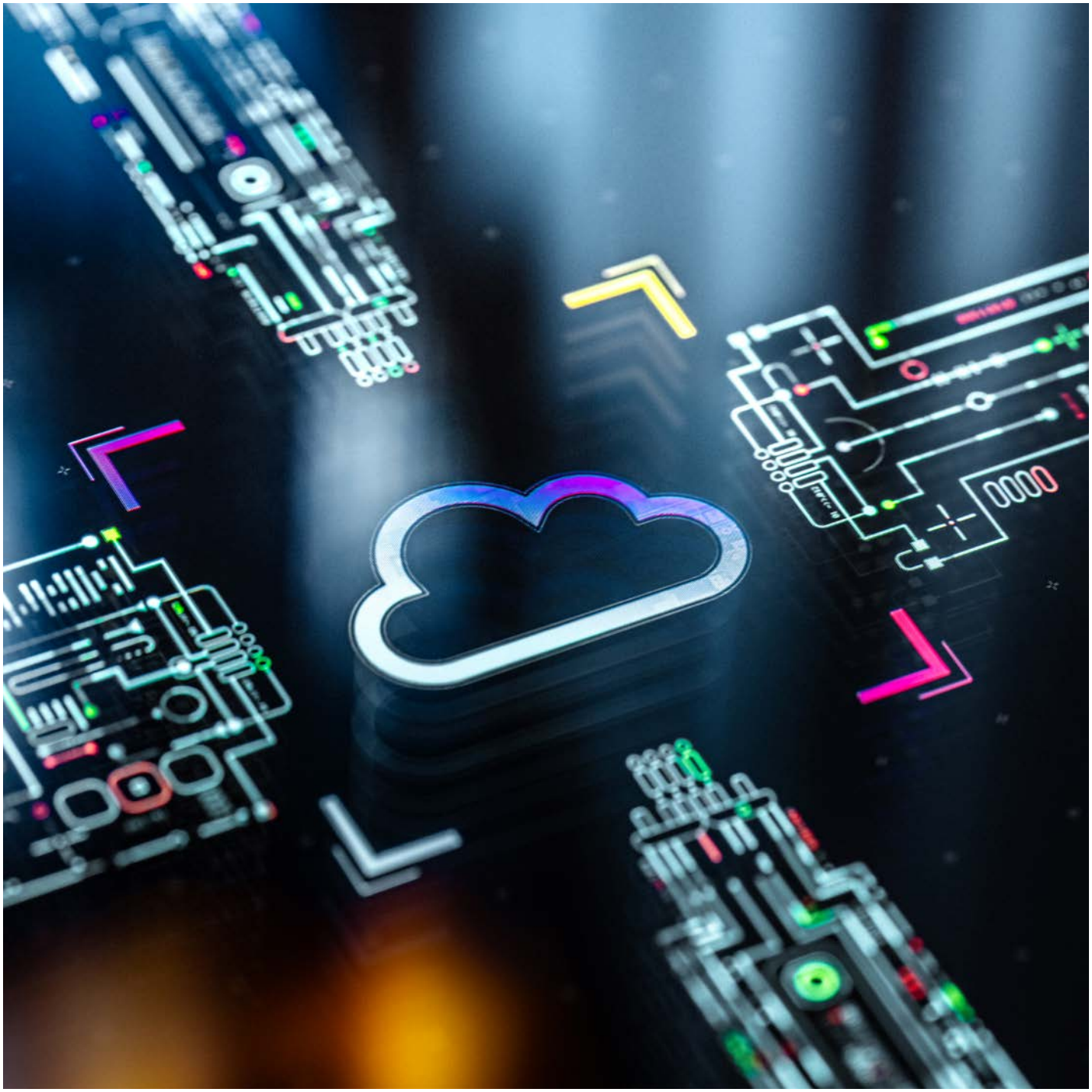
2.6 Europarat

Den Kern der Aktivitäten des Europarates im Bereich Cybersicherheit bildet die „Budapest-Konvention“ aus 2001, die mit aktuell 69 Ratifikationen (2023 Kamerun) 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 Beweis-

mitteln befasst. In zwei Unterzeichnungskonferenzen wurde das Zweite Zusatzprotokoll bislang von 41 Staaten, darunter Österreich, unterzeichnet. Im Jahr 2023 wurde es von den ersten beiden Staaten ratifiziert (Serbien und Japan). 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 Staatsanwältinnen und Staatsanwälten. Darüber hinaus wurden 2023 die gemeinsamen Europarats- und EU-Projekte „iProceeds-2“ in Südosteuropa und der Türkei, die sich auf Erträge aus Cyberkriminalität und die Sicherstellung elektronischer Beweismittel konzentrieren, sowie die Projekte „Cyber South“ und „Cyber East“ unterstützt. Diese beiden Projekte, in Kooperation mit dem Europäischen Nachbarschaftsinstrument, zielen darauf ab, die Strukturen in der südlichen und östlichen Nachbarschaft Europas zu verbessern. Zudem wurde das weltweit agierende Projekt „GLACY+“, das in Zusammenarbeit mit Interpol durchgeführt wird, gefördert. Ende 2023 wurde, aufbauend auf „GLACY+“ außerdem das Projekt „GLACY-e“ mit Fokus auf Länder in Afrika, Asien/Pazifik und Lateinamerika gestartet.

Das „Octopus Project“ fördert außerdem die Umsetzung der Budapest-Konvention und damit zusammenhängende 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 Ende 2023 in Bukarest statt und behandelte das Thema der Sicherung und des Teilens elektronischer Beweismittel. Anlässlich des 10-jährigen Bestehens des C-PROC wurde zudem die bisherige kapazitätsbildende Arbeit evaluiert und ein Ausblick auf zukünftige Projekte gegeben.



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 Juni 2023 veröffentlicht wurde, behandelt die Frage des Umfangs des Geltungsbereichs verfahrensrechtlicher Bestimmungen und der Maßnahmen zur internationalen Zusammenarbeit.

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.

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

Das Computer Security Incident Response Teams-Netzwerk (CSIRTs-Netzwerk oder CNW) wurde durch die die EU-Richtlinie 2016/1148 (NIS-1-Richtlinie) geschaffen, welche dessen Tätigkeitsbereich festgelegt. Das CSIRTs-Netzwerk setzt sich aus Vertreterinnen und Vertretern der CSIRTs der Mitgliedstaaten und des Computer Emergency Response Team (CERT)-EU zusammen. Die Europäische Kommission (EK) nimmt als Beobachterin am CSIRTs-Netzwerk teil. Die EU-Cybersicherheitsagentur (ENISA) führt die Sekretariatsgeschäfte und unterstützt aktiv die Zusammenarbeit zwischen den CSIRTs. Österreich ist im CSIRTs-Netzwerk durch das GovCERT Austria, CERT.at und das Austrian Energy CERT (AEC) vertreten.

Das Netzwerk arbeitet primär online. 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 sowie die Förderung einer schnellen und effektiven operativen Zusammenarbeit. Dies dient der Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der EU.

Das Netzwerk trifft sich in der Regel dreimal pro Jahr. 2023 fanden diese Treffen im März in Lissabon, im Juni in Stockholm und im September in León statt. Im November 2023 wurde die vertiefte Zusammenarbeit, sowohl im Tagesgeschäft als auch bei größeren Vorfällen, mit der CyberSOPEx geprobt – einer kompakten Übung zur Eskalation und Kooperation im CSIRTs Network. Um die übergeordneten Ziele des CSIRTs-Netzwerkes zu erreichen, werden unter anderem einheitliche technische Lösungen angestrebt und Versuche unternommen, eine gemeinsame Taxonomie zu etablieren.

2.8 Andere Gremien und Foren

Freedom Online Coalition

Die „Freedom Online Coalition“ ist eine informelle Vereinigung von Staaten, die sich für die effektive Online-Umsetzung weltweiter Menschenrechte einsetzt. Auch Österreich gehört dieser Initiative an, die im Dezember 2011 von den Niederlanden gegründet wurde und mittlerweile 38 Mitgliedstaaten umfasst.

International Counter Ransomware Initiative (CRI)

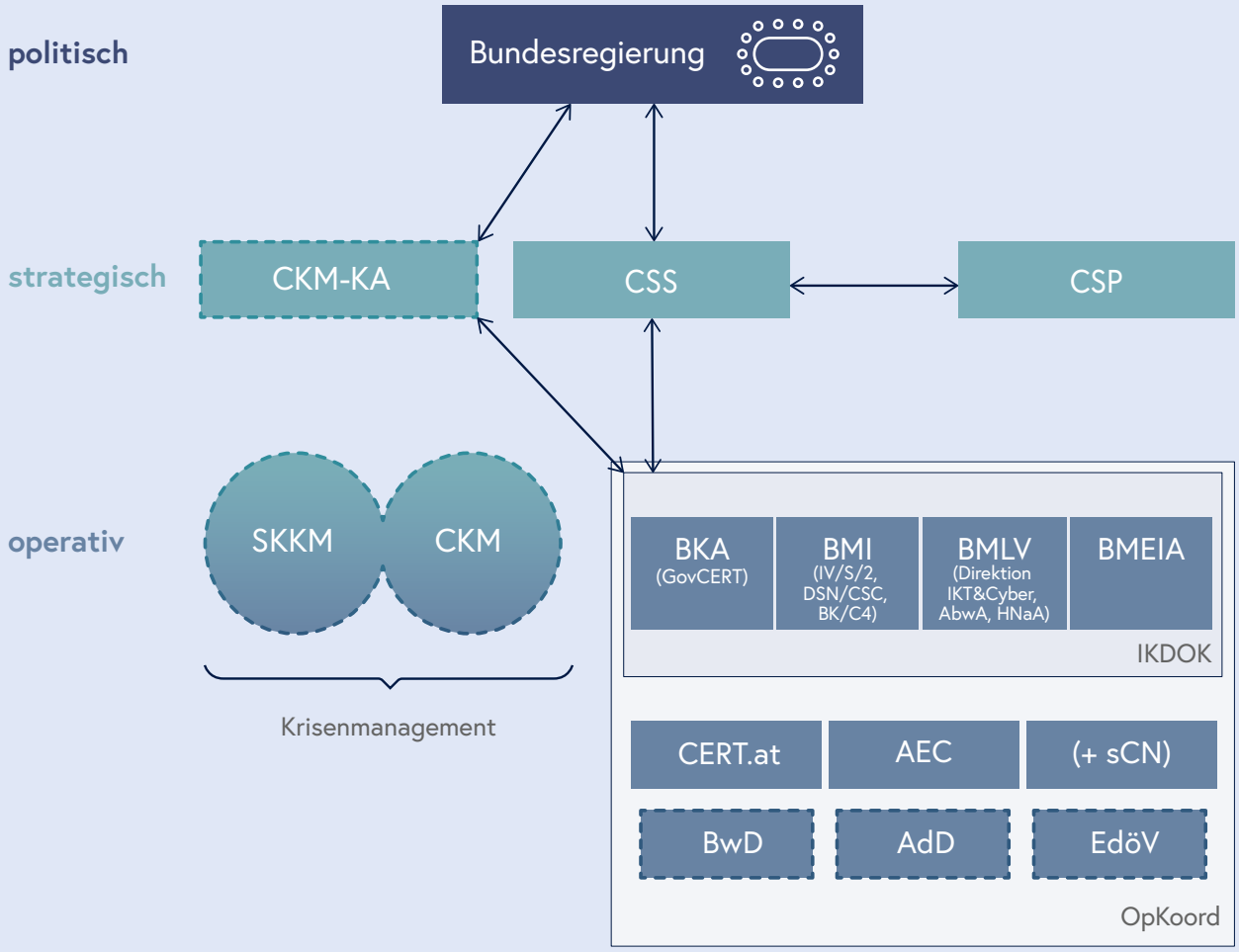
Die International Counter Ransomware Initiative (CRI) wurde 2021 von den USA ins Leben gerufen, um die internationale Zusammenarbeit bei der Bekämpfung von Ransomware-Kriminalität zu stärken. Zu den mehr als 60 Mitgliedern zählen vor allem gleichgesinnte Staaten, aber auch Organisationen wie Interpol und die Europäische Union (EU). Österreich trat bereits kurz nach der Gründung der Initiative bei und hat sich von Anfang an engagiert beteiligt, auch mit hochrangiger Vertretung bei den bisherigen drei Gipfeltreffen der Initiative in Washington, zuletzt zwischen 31. Oktober und 1. November

2023 unter Leitung des Direktors des Bundeskriminalamts, General Andreas Holzer. Das Bundesministerium für Inneres (BMI), das Bundesministerium für Finanzen (BMF) und das Bundesministerium für europäische und internationale Angelegenheiten (BMEIA) bringen sich in jedem der drei Arbeitsfelder der CRI, International Counter Ransomware Task Force/ICRTF, Policy Pillar, Diplomacy and Capacity Building Pillar, ein.

3
Nationale Akteure

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

3.1 Verfassungsschutzrelevante Cybersicherheit

Die Direktion 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. Hierfür bedient sich die DSN 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 die Taxonomie und Beschäftigung mit neuen Phänomenen im Cyber-Bereich und der Reaktion auf aktuelle Trends. Um einen Erfahrungs- und Wissensaustausch zu ermöglichen und zu fördern, setzt die DSN auf die Zusammenarbeit der Strafverfolgungsbehörden und der Cybersicherheits-Community, zu der Stakeholder aus Wirtschaft und Forschung zählen. Ziel ist, gemeinsam die Resilienz und die Kommunikation in diesem Bereich zu fördern. Ebenso findet der Austausch mit ausländischen Sicherheitsbehörden statt, um die eigenen Erkenntnisse zu teilen und eine globale Sicht auf Bedrohungen zu gewährleisten.

Bei den im Berichtsjahr 2023 relevanten verfassungsschutzrelevanten Phänomenen handelte es sich um eine Fortführung und Weiterentwicklung mehrerer nachfolgend beschriebener und bereits bestehender Bedrohungserscheinungen der letzten Jahre. „Advanced Persistent Threats“ (APT), „Private-Sector-Offensive-Actors“ (PSOA) und Ransomware-Gruppierungen stellen die Sicherheitsbehörden, insbesondere die nachrichtendienstliche Bearbeitung des Aufgabenspektrums Cybersicherheit, vor anhaltende und dynamische Herausforderungen. Zusätzlich spielen auch geopolitische Konflikte eine große Rolle in der Cyberdomäne (siehe 1.1).

3.2 Cyber Crime Competence Center (C4)

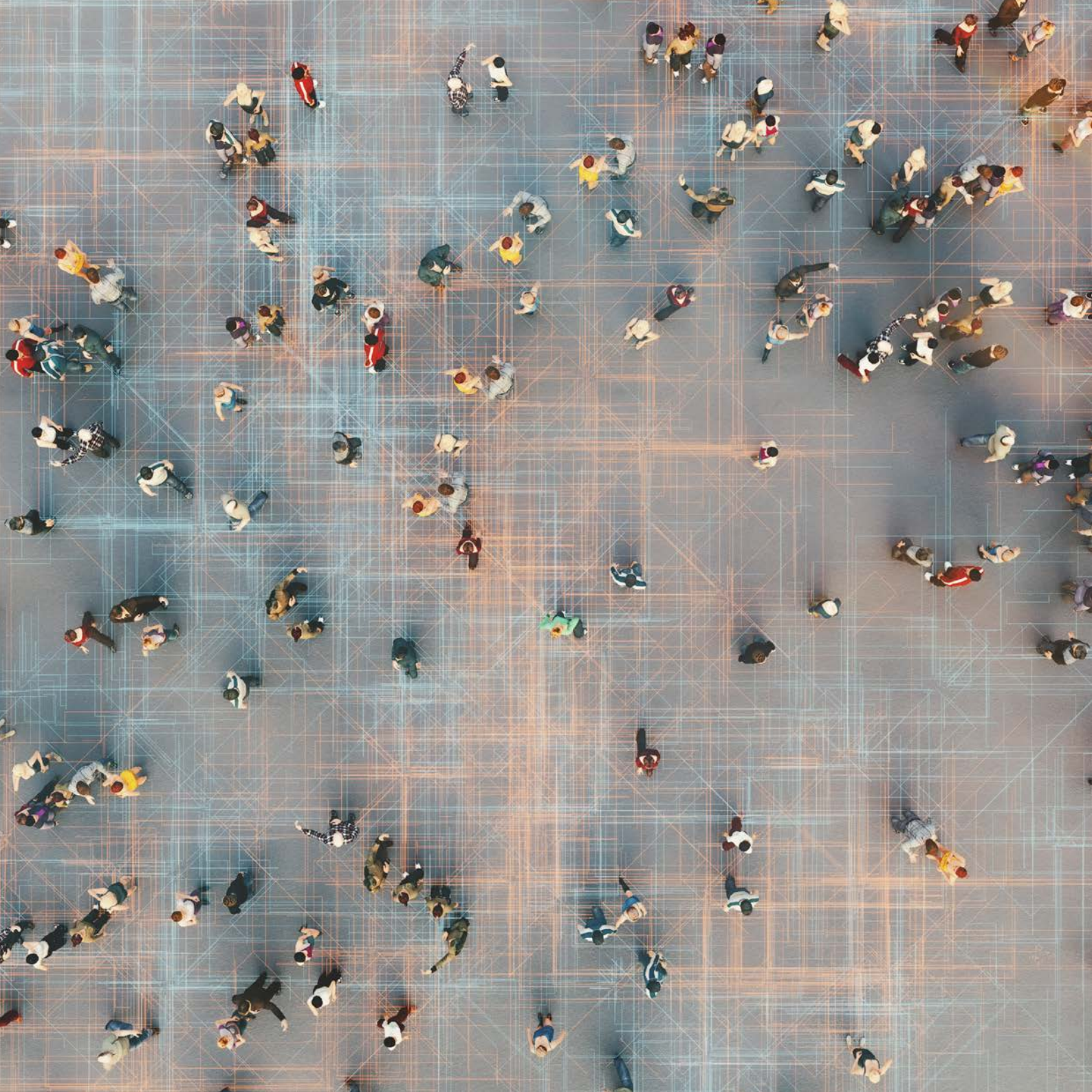
Das Cybercrime Competence Center (C4) ist die nationale und internationale Koordinierungs- und Meldestelle zur Bekämpfung von Cybercrime. Das Zentrum setzt sich aus technisch und fachlich hochspezialisierten Expertinnen und Experten aus den Bereichen Ermittlung, Forensik und Technik zusammen.

Die sowohl für Cybercrime 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.

Die Umstrukturierungsphase des C4 ist noch nicht abgeschlossen. Aufbauend auf das bestehende Organisationsgefüge werden die Ressourcen des C4 erweitert und gliedern sich künftig in folgende Bereiche:

3.2.1 Zentrale Aufgaben

Hierbei handelt es sich um die zentrale Koordinationsstelle bei der Bekämpfung von Cyberkriminalität. Die Zuständigkeit umfasst die zentrale Administration und Organisation von Projekten und Förderprogrammen, internationalen Kooperationen, die Entwicklung und Organisation nationaler und internationaler Ausbildungsprogramme, das Beschaffungswesen für IKT-Hardware und Software und die Koordinierung sämtlicher fachbereichsübergreifender Angelegenheiten.



3.2.2 IT-Beweissicherung

Die Fachexpertise zur Sicherung und Auswertung von elektronischen Beweismitteln bildet das Kernstück des C4. Neben der IT-Forensik und Mobilen Forensik haben sich weitere Fachbereiche entwickelt, die zunehmend an Bedeutung gewinnen. Dazu gehören die Multimedia-Forensik, die Elektronik- und IoT[11]-Forensik sowie der KFZ-Forensik.

3.2.3 IT-Ermittlungen

Zur adäquaten Bekämpfung von High-Tech-Crime werden operative Unterstützungsteams die bestehenden Ermittlungsbereiche erweitern und auch mobil zur Verfügung stehen. Spezialisierte Ermittlungseinheiten für die Fachrichtungen Darknet sowie Kryptowährungen und Blockchain (einschließlich der Sicherstellung und Verwertung von Kryptowährungen) sind notwendig, um die erforderliche Expertise bei Ermittlungen bereitzustellen. Auch der Bereich „Complex Cybercrime“, der sich mit Cybercrime-Delikten und Massenphänomenen befasst, deren Ermittlungsansätze überwiegend im digitalen Bereich liegen, wird künftig abgedeckt. Dieser Bereich umfasst Delikte mit hohem Schadenspotential und internationalen Zusammenhängen. Zu den IT-Ermittlungen zählen zudem die Meldestelle für Internetkriminalität sowie die Zentrale Anfragestelle Social Media & Online Service Provider (ZASP). Die ZASP führt zentrale Abfragen bei Social-Media-Plattformen und Internetdienstanbietern durch. Die Meldestelle gegen Cybercrime unter against-cybercrime@bmi.gv.at ist die Ansprechstelle für Bürgerinnen und Bürger sowie für nationale Strafverfolgungsbehörden im Zusammenhang mit IT-Delikten.

3.2.4 Entwicklung & Innovation

Aufgabe ist die Unterstützung von digitaler Forensik und digitalen Ermittlungen mit wissenschaftlicher Expertise sowie die bedarfsorientierte Entwicklung von Tools und Skripten, welche international auch für andere Strafverfolgungsbehörden zur Verfügung

11 Internet der Dinge

gestellt werden. Ein wesentlicher Teil ist darüber hinaus die internationale Zusammenarbeit mit Forschungsinstituten und -institutionen.

3.2.5 Digitales Beweismittelmanagement

Das digitale Beweismittelmanagement fasst jene Kompetenzen zusammen, die für eine zeitgemäße kriminalpolizeiliche Bearbeitung komplexer Fälle mit großen Datenmengen notwendig sind. Dies umfasst die technische Aufbereitung sichergestellter digitaler Beweismittel zur systematischen Indizierung und nachfolgenden Bereitstellung für die Ermittlungsbereiche im Bundeskriminalamt und, bei Bedarf, in den Landeskriminalämtern. Ebenso gehört das Fallmanagement dazu, das als Schnittstelle zwischen Forensikerinnen und Forensikern, Ermittlerinnen und Ermittlern, Technikerinnen und Technikern sowie gegebenenfalls der Justiz fungiert.

3.3 Direktion IKT & Cyber

Die Notwendigkeit einer robusten Verteidigung vor Cyber-Bedrohungen steht im Mittelpunkt der Bemühungen der Direktion IKT & Cyber im Bundesministerium für Landesverteidigung (BMLV). Primäres Ziel der Direktion ist es, die Integrität, Vertraulichkeit und Verfügbarkeit der IKT des Österreichischen Bundesheer (ÖBH) zu gewährleisten und somit die Souveränität sowie Sicherheit Österreichs zu schützen. In der Direktion IKT & Cyber werden alle Elemente der Cyberkräfte des ÖBH zusammengeführt. Die Cyberkräfte umfassen die IKT-Truppe, die Cyber-Truppe und die Elektronischer Kampf (EloKa)-Truppe. Sie sind jene Elemente im ÖBH, die die anderen Teilstreitkräfte (Land, Luft) sowie alle Führungsebenen miteinander verbinden und damit die Kommunikations- und Führungsfähigkeit herstellen. Sie beobachten und bewerten die Lage der Cyberaktivitäten, 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 ÖBH in eigenen Netzwerken reibungslos stattfinden kann. Sie sorgen permanent für die Informationshoheit und

Kontrolle über die eigenen Systeme. Gerade im Einsatz ist es überlebenswichtig, dass sichere Verbindungen bestehen und Informationen schnell und sicher zur richtigen Zeit am richtigen Ort verfügbar sind.

Organisatorisch besteht die Direktion IKT & Cyber aus folgenden drei Abteilungen

- IKT & Cyber Planung (IKTCyPl),
- IKT & Cyber Einsatz (IKTCyE) und der
- Führungsabteilung (FüAbt).

Die Abteilung IKTCyPl ist die Planungskomponente der Direktion und unter anderem zuständig für die Planung und Grundlagenerstellung der Führungsunterstützung inklusive Cybersicherheit.

Die Abteilung IKTCyE ist die Einsatzkomponente der Direktion. Sie ist für die Führungsunterstützung, die elektronische Kampfführung und für die Cyber-Kampfführung bei allen Einsätzen des Bundesheeres verantwortlich.

Neben den angeführten Abteilungen sind fünf Fachbereiche im IKT & Cybersicherheitszentrum zusammengefasst, die sich primär mit der Umsetzung der planerischen Vorgaben und der Implementierung beschaffter Systeme beschäftigen. Die Mitarbeiterinnen und Mitarbeiter des IKT & Cybersicherheitszentrum schaffen die Voraussetzungen für die Verlegbarkeit, Mobilität, Autarkie, Resilienz und internationale Interoperabilität sowie die Basis für die Informationsüberlegenheit auf dem modernen, digitalen und hybriden Gefechtsfeld.

Das Leistungsspektrum erstreckt sich somit von der strategischen Planung über die operative Umsetzung bis hin zur taktischen Durchführung sämtlicher Belange der IKT- und geoinformationsbezogenen Aufgaben des ÖBH.

3.4 Abwehramt (AbwA)

Unter dem Begriff der Cyberverteidigung werden alle Anstrengungen des Österreichischen Bundesheers (ÖBH) im Zusammenhang mit Cyberaktivitäten 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 zur Cyber-Bedrohungslandschaft zusammenführt, analysiert und als Grundlage der Beurteilung von Gegenmaßnahmen dient. Durch diese und weitere Maßnahmen soll kontinuierlich ein hohes Maß an Sicherheit der militärischen IKT-Infrastruktur gewährleistet werden.

3.5 Heeresnachrichtenamt (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 von Cyberaktivitäten 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 IKDOK (Innerer Kreis der Operativen Koordinierungsstruktur). Es ist mit seinem strategischen Anteil im Bundeskanzleramt angesiedelt. Die Erbringung operativer und operationeller Leistungen erfolgt im Rahmen einer Public-Private-Partnership mit CERT.at. Das GovCERT Austria stellt den Kontaktpunkt des Computer Emergency Response Team (CERT) für Österreich in Bezug auf die Netze der öffentlichen Verwaltung dar und steht mit internationalen Organisationen und Kontakten 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 NIS-Gesetz 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 Cybersicherheits-Organisationen sowie eigens dafür entwickelte Software[12] und ist an zahlreichen nationalen und europäischen Forschungsprojekten[13] beteiligt Darüber hinaus informiert CERT.at über Social Media und Mailinglisten über aktuelle Bedrohungen und Schutzmaßnahmen.

Das Austrian Energy CERT (AEC) ist ein akkreditiertes, brancheneigenes Computer Emergency Response Team bzw. Computersicherheits-Ereignis- und Reaktionsteam (CERT) 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 Sicherheitsvorfalls-

12 https://github.com/certat
13 https://cert.at/de/ueber-uns/projekte

Management die Bearbeitung täglich eingehender Anfragen und Sicherheitsmeldungen, die Durchführung von Schulungstätigkeiten, die Teilnahme an internationalen Cybersicherheitsübungen sowie die Mitarbeit bei der Erstellung technischer Sicherheitskonzepte für die Elektrizitäts- und Erdgaswirtschaft. Darüber hinaus erfüllt das AEC die Rolle des primären Ansprechpartners bei nationalen und internationalen Security Incidents im Energiesektor. Damit wird neben schneller und effizienter 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-Cybersicherheitsagentur (ENISA) zur Erhöhung der IT-Sicherheit bei kritischen Infrastrukturen. Sie stellen auch die österreichischen Mitglieder des Computer Security Incident Response Team (CSIRT)-Netzwerk der EU (siehe 2.7). Die genannten drei CERTs werden in erster Linie bei Sicherheitsbedrohungen und -ereignissen aktiv. Dies geschieht durch Verständigung der 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.

Das NISG sieht 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 herausgeben, erste allgemeine technische Unterstützung bei der Reaktion auf Sicherheitsvorfälle 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, ein Health-CERT ist mit 2023 in Vorbereitung), 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.

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 2023 erfolgreich fort. In 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 Aktivitäten gesetzt (siehe 2.1). Ein Schwerpunkt bildete dabei die Koordinierung und Vertretung der österreichischen Position in den Verhandlungen zum Cyber Resilience Act.

3.8 Operative Netz- und Informationssystemsicherheit

Mit 1. Juli 2022 wurde nach einer vorübergehenden organisatorischen Zwischenlösung die heutige Abteilung IV/S/2 – Netz- und Informationssystemsicherheit (NIS) im Bun-

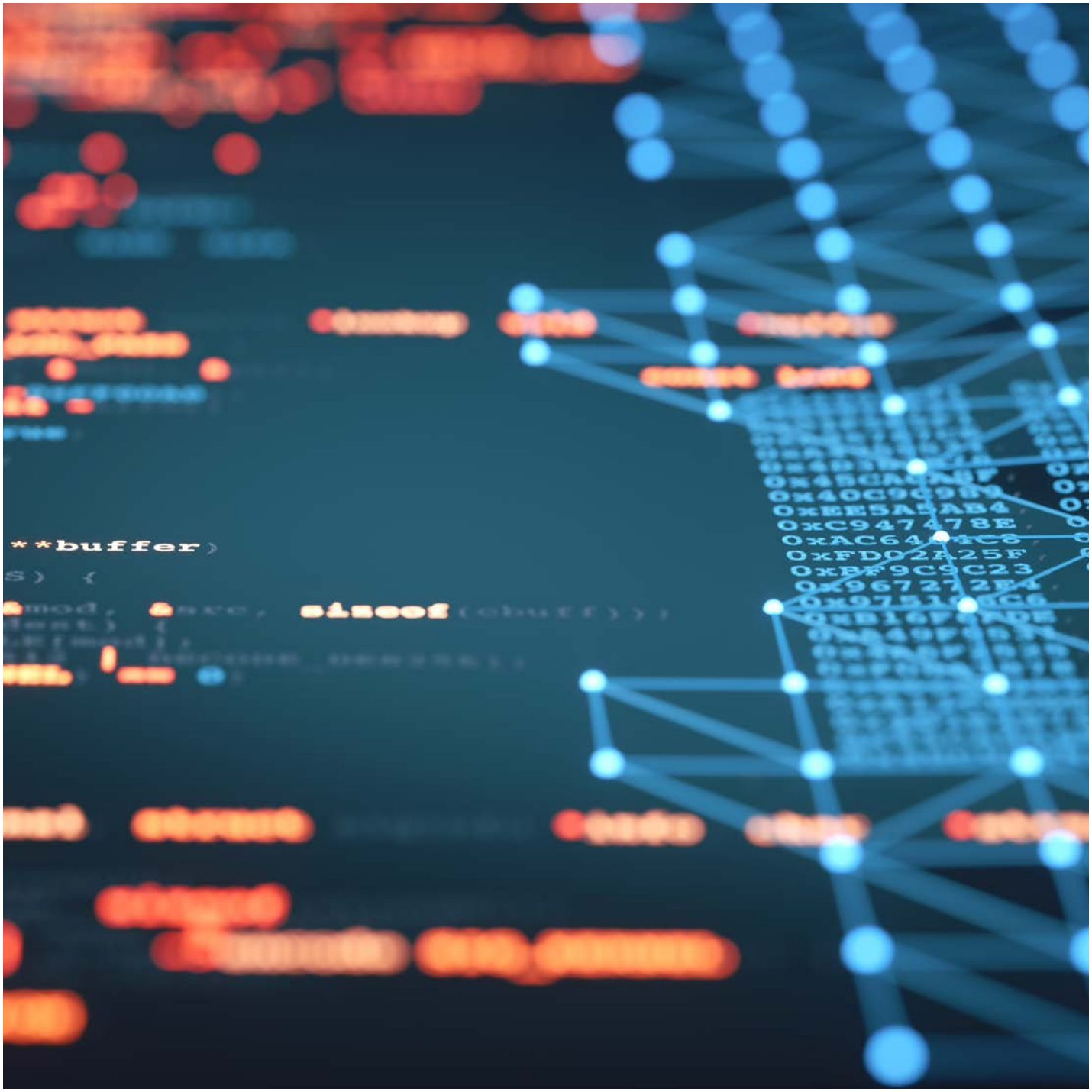
desministerium für Inneres (BMI) eingerichtet. Wie im Bericht Cybersicherheit für das Jahr 2022 ausgeführt, erfüllt die Abteilung BMI IV/S/2 und die ihr nachgeordneten Referate die Funktion der operativen Behörde für Netz- und Informationssystemsicherheit (NIS-Behörde) für Österreich. Diese Tätigkeit beinhaltet ein breites Spektrum an Aufgabenstellungen, deren wesentliche Zielsetzung die Sicherstellung von Cybersicherheit und die Erhöhung der gesamtstaatlichen Resilienz in Österreich ist. Im Zentrum der Aktivitäten 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. Zusätzlich nimmt die Abteilung eine koordinierende Rolle innerhalb der gesamtstaatlichen Operativen Koordinierungsstruktur (OpKoord) und ihres Inneren Kreises (IKDOK) wahr. Darüber hinaus unterstützt sie dem NISG unterworfene Entitäten mittels Sensibilisierungsvorträgen und Publikationen im Bereich der Cyber-Prävention.

Organisatorische Weiterentwicklungen

Ungeachtet aller Erfolge, die mit der Umsetzung der NIS-Richtlinie erzielt werden konnte, führte die uneinheitliche Umsetzung in den Mitgliedsstaaten zu einer mangelhaften Harmonisierung, die damit ein wirksames Vorgehen gegen aktuelle und neue Herausforderungen im Bereich Cybersicherheit verhindert hat.

Die NIS-2-Richtlinie[14] trat am 16. Januar 2023 in Kraft und muss bis 17. Oktober 2024 in nationales Recht umgesetzt werden. Die neue Richtlinie versucht, den bestehenden Rechtsrahmen zu modernisieren und eine Harmonisierung der zum Teil unterschiedlichen Implementierungen der Mitgliedsstaaten zu erwirken. Durch die Ausweitung des Anwendungsbereichs auf neue Sektoren sollen Resilienz- und Reaktionskapazitäten öffentlicher und privater Stellen, der zuständigen Behörden und der Europäischen Union insgesamt verbessert werden. Im Rahmen eines umfassenden Programms wurde im Beobachtungs-

14 Richtlinie (EU) 2022/2555


**buffer
sizeof

zeitraum in Einzelprojekten an einer Konsolidierung verschiedener neuer und bisheriger Aufgaben der strategischen und operativen Cybersicherheit in ein neu zu schaffendes nationales Cybersicherheitszentrum (NCSZ) im Bundesministerium für Inneres gearbeitet.

3.8.1 Recht und Audit

Im Beobachtungszeitraum ist der organisatorische Aufbau der NIS-Behörde unverändert geblieben. Nach wie vor ist die Kernaufgabe des Referats IV/S/2/a (Recht und Audit) die regelmäßige Überprüfung der Einhaltung der verpflichtenden Sicherheitsvorkehrungen bei den dem NISG unterworfenen Unternehmen und Organisationen sowie die diesbezügliche Verfahrensführung im Rahmen des NISG. Dies beinhaltet im Bedarfsfall das Aussprechen von Empfehlungen oder bescheidmäßiger Anordnungen zur Umsetzung oder Anpassung von Sicherheitsvorkehrungen an Normunterworfene.

3.8.2 Cyberlagezentrum, Prävention, Kommunikation

Mitarbeitende des Referats IV/S/2/b (Cyberlagezentrum, Prävention, Kommunikation) verfolgen laufend aktuelle Entwicklungen im Bereich der Cybersicherheit, um damit ein permanentes Lagebild fortzuschreiben. Das durch die verfolgten Entwicklungen in Zusammenhang mit Sicherheitsvorfällen, Angriffsmustern und Warnungen erstellte Lagebild wird Bedarfsträgern innerhalb und außerhalb des Ressorts zur Verfügung gestellt. Darüber hinaus sind hier auch die nationale Meldesammelstelle, der „Single Point of Contact“, welcher als Anlaufstelle für NIS-Behörden anderer Mitgliedsstaaten der EU dient, und das IKDOK-Office angesiedelt. Der Fachbereich Prävention ist für die Konzeption und Durchführung von Präventionsveranstaltungen sowie für die Erstellung von diesbezüglichen Unterlagen und Publikationen verantwortlich. Mitarbeitende des Referats IV/S/2/b arbeiten auch an der 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.

3.8.3 NIS Technische Einrichtungen

Das Referat IV/S/2/c (NIS Technische Einrichtungen) ist als technischer Dienstleister der operativen NIS-Behörde für die Konzeption, den Aufbau und den fachlichen Betrieb der für die Erfüllung der Aufgaben der Abteilung erforderlichen Informations- und Kommunikationssysteme verantwortlich. 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 in einem Team gebündelt, das mit dem Einsatz modernster Mittel und Methoden diese Leistung erbringt.

3.9 Nationales Koordinierungszentrum für Cybersicherheit (NCC-AT)

NCC-AT
Nationales Koordinierungszentrum Cybersicherheit

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 Europäischen Union 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 rechtlichen 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.

2023 fokussierten die Bemühungen auf den organisatorischen und personellen Aufbau des NCC-AT sowie auf die Anwerbung von EU-Fördermittel in diesem Zusammenhang. Im zweiten Halbjahr 2023 konnte auf dieser Grundlage das EU-geförderte Projekt NCC-AT gestartet werden, welches die Basis für folgende Aktivitäten war:

- Angebot von Informations- und Serviceangeboten zu (EU-)Fördermöglichkeiten insbesondere aus dem EU-Förderprogramm „Digitales Europa“ (Webseite ncc.gv.at, Newsletter, individuelle Beratung durch die FFG);
- Erste Ausschreibungsrunde der FFG-Förderschiene „Cyber Security Scheck“ in Höhe von zwei Millionen Euro zur Unterstützung von kleinen und mittleren Unternehmen (KMU) im Anwendungsbereich der NIS-2-Richtlinie[15] bei der Umsetzung von technischen Cybersicherheitslösungen;
- Kick-off Veranstaltung mit 170 Teilnehmenden in Wien;
- Vernetzungstätigkeiten auf europäischer und nationaler Ebene;
- Mitwirkung an strategischen Arbeiten im NCC-Netzwerk und in ECCC-Arbeitsgruppen.

Hierzu sei auf das Kapitel 2.1.7 verwiesen.

15 Richtlinie (EU) 2022/2555

4
Nationale Strukturen

4.1 Innerer Kreis der Operativen Koordinierungsstrukturen (IKDOK)

Um eine gesamtstaatliche Resilienz gegen Cyberbedrohungen zu gewährleisten, ist eine gut gefestigte Struktur und Zusammenarbeit zwischen den mit Cybersicherheit beauftragten Organisationseinheiten essenziell. 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 Operativen Koordinierungsstruktur (OpKoord) und besonders dem Inneren Kreis der Operativen Koordinierungsstrukturen (IKDOK) eine dauerhafte Struktur zur Koordination auf der operativen Ebene.

Der IKDOK setzt sich aus Vertreterinnen und Vertretern des Bundesministerium für Inneres (BMI, insb. IV/S/2, DSN, BK/C4), des Bundeskanzleramt (BKA) inklusive des GovCERT, des Bundesministerium für europäische und internationale Angelegenheiten (BMEIA) sowie des Bundesministerium für Landesverteidigung (BMLV) inklusive Abwehramt (AbwA), Direktion IKT & Cyber und Heeres-Nachrichtenamt (HNaA) zusammen.

Das BMI (IV/S/2) übernimmt dabei administrative und koordinierende Aufgaben des Gremiums und leitet die Sitzungen. Die regelmäßig erstellten Lagebilder sowie weitere Informationen der einzelnen Organisationseinheiten des IKDOK und der OpKoord werden den jeweiligen Zielgruppen zur Verfügung gestellt.

Die Hauptaufgaben des IKDOK liegen bei der Erfassung und Bewertung eines monatlichen Lagebildes über Risiken, Vorfälle und Sicherheitsvorfälle, die Erstellung von situativen Lagebildern, des regelmäßigen Austauschs 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).

4.2 CERT-Verbund Austria

Der Computer Emergency Response Team bzw. Computersicherheits-Ereignis- und Reaktionsteam (CERT)-Verbund Austria wurde 2011 als Kooperation aller damals existierenden österreichischen 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. Alle 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 klassischen IT-Sicherheitsteam und einem CERT ist, dass die Kommunikations- und Zusammenarbeitsbereitschaft mit Dritten ein Teil des Kernauftrages ist. Ein CERT soll 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 Task Force (TF) (dt. Einsatzkommando)-CSIRT und dem EU-Computer Security Incident Response Teams (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.

Die aktuell 17 mitwirkenden Teams haben sich 2023 in sechs Treffen, die jeweils von einem der Teilnehmenden ausgerichtet werden, ausgetauscht. Dabei steht jeder Termin unter einem Hauptthema, zu dem alle CERTs ihre Erfahrungen beitragen. Sie kommunizieren aber auch außerhalb der regelmäßigen Treffen über sichere Kommunikationskanäle und im persönlichen Kontakt, wenn es die Situation erfordert. So können über Organisations- und Unternehmensgrenzen hinweg sehr rasch Lagebilder erstellt und Maßnahmen abgestimmt werden.

Cyber Sicherheit Plattform

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. Die CSP ist in der Österreichischen Strategie für Cybersicherheit (ÖSCS) als Plattform für öffentlich-private Zusammenarbeit vorgesehen. Das Bundeskanzleramt unterstützt als Sekretariat. 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 Strategie für Cybersicherheit und der Ausgestaltung des legistischen Rahmens zur Cybersicherheit in Österreich (Stichwort NIS2).

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 (nationales Computersicherheits-Ereignis- und Reaktionsteam) und mit Unterstützung des Bundeskanzleramts (BKA) gegründet und später durch das GovCERT erweitert. Zielgruppe sind alle Sektoren der strategischen Infrastruktur sowie die öffentliche Verwaltung in Österreich. Der ATC bietet 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, die 2023 in Loipersdorf stattfand.

Im Jahr 2023 lag der Schwerpunkt der behandelten Themen bei den Vorbereitungen zur NIS-2-Richtlinie[16]. Der Trust Circle wurde genutzt, um die aus der NIS-2-Richtlinie erwarteten Vorgaben mit den Praxiserfahrungen der Teilnehmenden zu vergleichen. Im Finanzbereich waren wiederum DORA[17] und die daraus entstehenden Aufgaben für Unternehmen prioritäres Thema.

Der Trust Circle wurde auch 2023 um weitere Teilnehmende erweitert, insbesondere im Bereich der Industrie. Die Teilnehmenden werden dabei in den meisten Fällen durch bereits aktive Organisationen angesprochen und eingeladen; ein Nachweis für den Nutzen des Trust Circles in der täglichen Praxis. Aufgrund des Wachstums des ATC und

16 Netz- und Informationssicherheit Richtlinie (EU) 2022/2555
17 Digital Operational Resilience Act (DORA), Verordnung (EU) 2022/2554

um auch den Teilnehmenden aus den Bundesländern einen regelmäßigen Austausch zu ermöglichen, wurde mit Ende 2023 beschlossen, dass die Circle-Treffen ab 2024 hybrid (online und vor Ort bei CERT.at in Wien) stattfinden werden.

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 zu fördern und nachhaltig zu stärken. Dies geschieht durch die Bereitstellung zielgruppenspezifischer Handlungsempfehlungen.

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.

2023 umfassten die Aktivitäten im Zusammenhang mit dem IKT-Sicherheitsportal insgesamt die Erstellung von 142 Newsartikeln, 14 Publikationseinträgen, 13 Videos und 2 Podcast-Folgen. Zusätzlich wurde jeden Monat ein Schwerpunktthema zu aktuellen Trends festgelegt, zu dem themenspezifische Videos und Fachbeiträge veröffentlicht wurden. Die Videos entstehen gemeinsam mit Expertinnen und Experten der jeweiligen fachlichen Disziplinen. Themenschwerpunkte waren beispielsweise zu Jahresbeginn „Digitale Neujahrsvorsätze", im Frühjahr/Sommer „Digitale Freizeit und Sport" und „IT-Security unterwegs" sowie im Herbst „Digitales Lernen". Ein jährlich wiederkehrender

Schwerpunkt im Oktober ist der „European Cyber Security Month“ (ECSM) rund um österreichischen Aktivitäten, die im Zuge dessen veranstaltet wurden.

Durch ein internes monatliches Trendmonitoring wurde der Blickwinkel auf aktuelle Sicherheitsthemen, Akteure und technische Trends ergänzt und konnte in die Contenterstellung miteinfließen. Einzelne Artikel wurden inhaltlich aktualisiert und teilweise mit Informationsgrafiken ergänzt, wodurch eine noch verständlichere Aufbereitung der Inhalte erreicht wurde.

Im Zuge der Digitalen Kompetenzoffensive für Österreich (DKO) wurde die erste Folge des Cybersicherheitspodcasts „Web of Trust“ veröffentlicht. Mithilfe von Reportagen, Selbstversuchen und spannenden Gästen werden die wichtigsten Fragen rund um mehr Sicherheit in der digitalen Welt beantwortet. Weitere Folgen wurden bereits produziert und werden laufend online gestellt. Innerhalb der jeweiligen Podcast-Beschreibung werden inhaltlich passende Artikel zu onlinesicherheit.gv.at verlinkt.

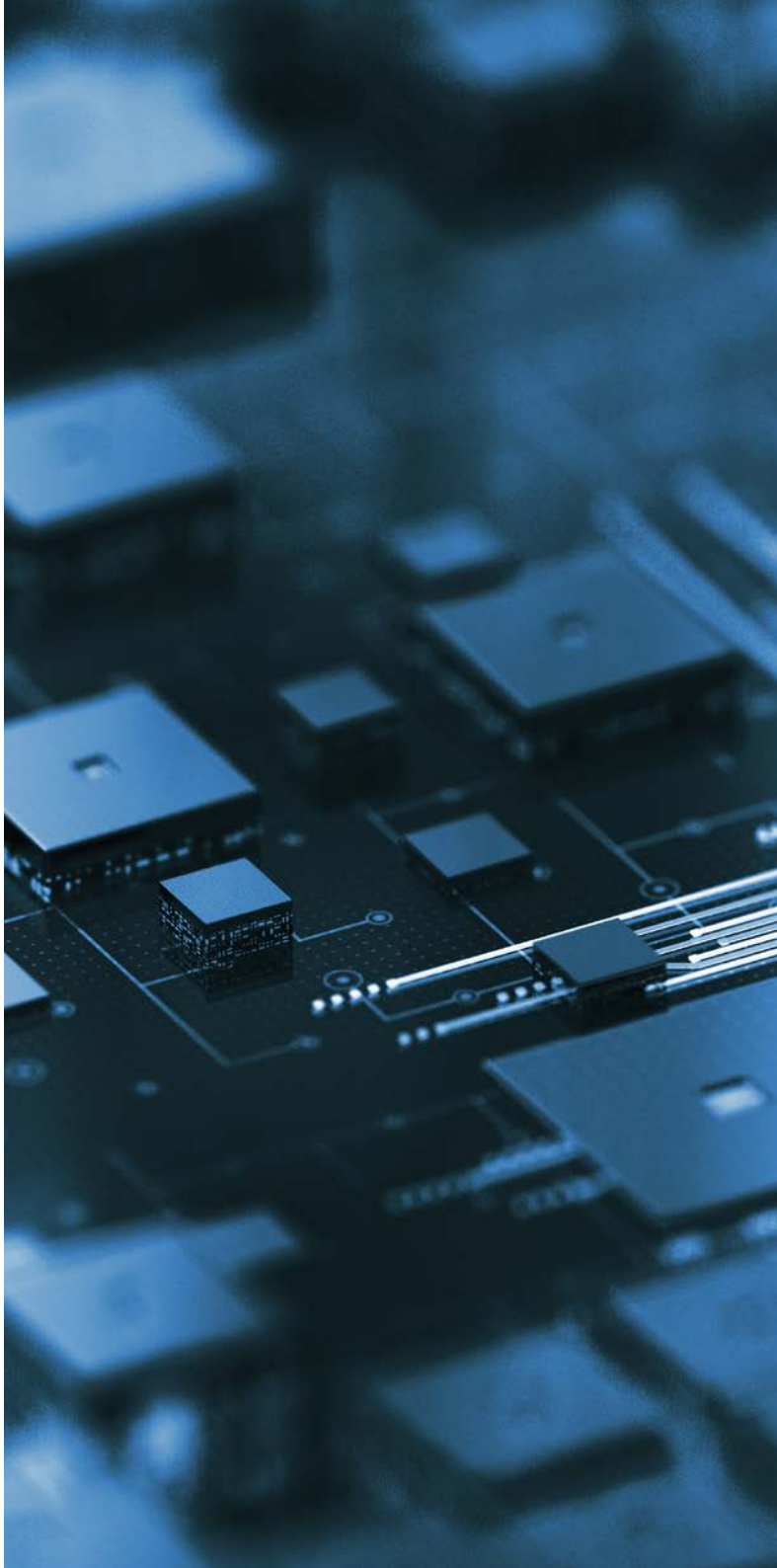
Das Ziel, einer höheren Reichweite durch multimedialen Content mittels Veröffentlichung unterschiedlicher Formate (Artikel, Interview, Video, Podcast) und einer gezielten Suchmaschinenoptimierung zu erreichen, zeichnete sich 2023 bereits ab. Die Anzahl der Besucherinnen und Besucher erhöhte sich auf 976.114, dies entsprach einem Anstieg um 124,3 % gegenüber 2022.

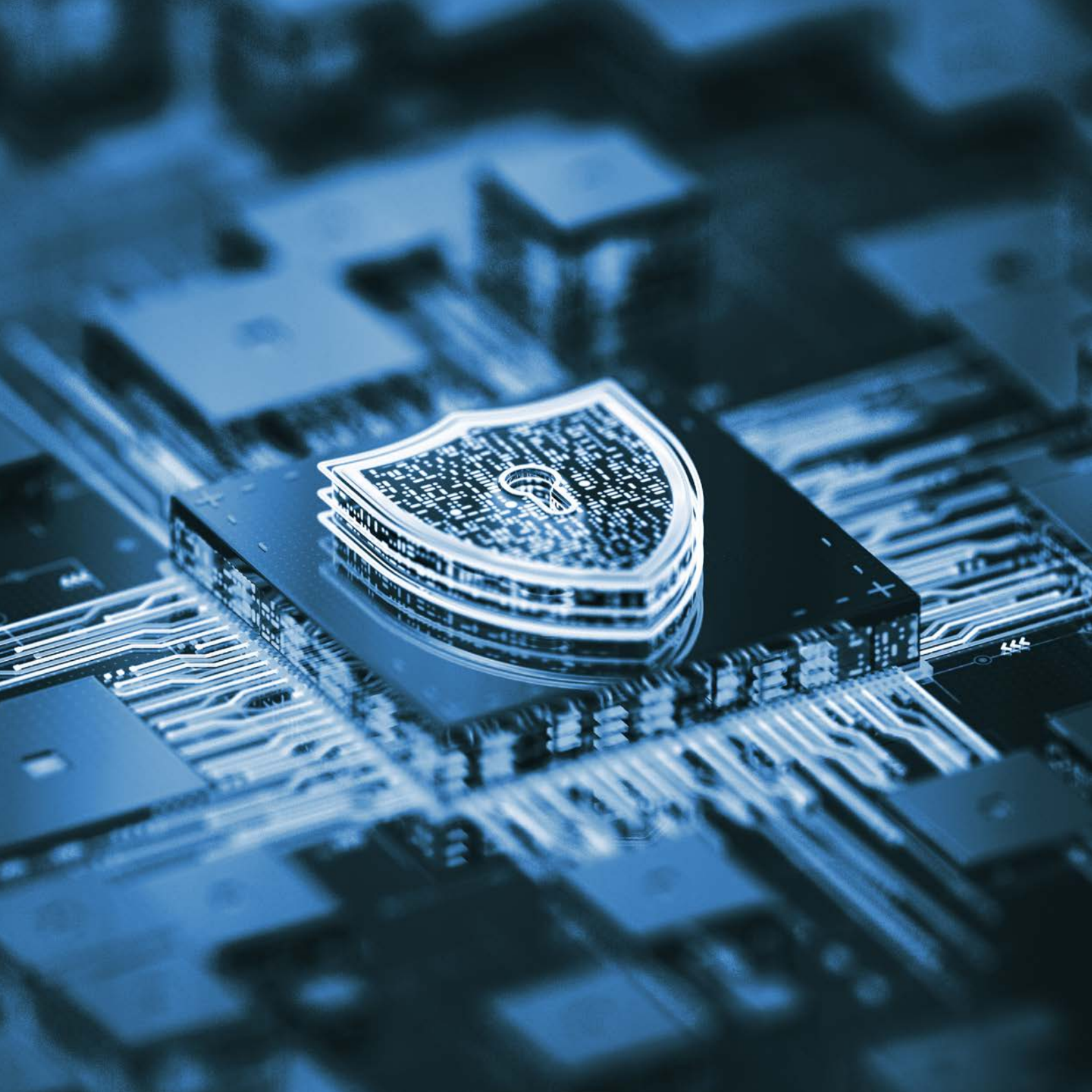
4.6 Nationales Cybersicherheitsforschungsprogramm K-PASS

Das im Jahr 2023 ins Leben gerufene nationale Cybersicherheitsforschungsprogramm Kybernet-Pass (K-PASS) ist die erstmalige Etablierung eines vollständig auf Cybersicherheit ausgelegten Forschungsförderungsinstrumentes in Österreich. K-Pass steht unter Verantwortung des Bundesministeriums für Finanzen (BMF). Es unterstützt primär österreichische Unternehmen und Forschungseinrichtungen bei der Entwicklung neuer Technologien sowie bei der Gewinnung erforderlichen Wissens, um die digitale Sicherheit Österreichs zu erhöhen und Wertschöpfung zu generieren. Ziel ist die Schaffung marktnaher Forschungsergebnisse zu digitaler Sicherheit für sämtliche Sicherheitsanwendende bzw. Bedarfstragende (etwa Polizei oder Feuerwehr, aber auch sicherheitsrelevante Unternehmen wie Verbund oder Flughafen Wien).

K-Pass in Kürze

Budget	€ 5 Mio. für jährliche Ausschreibungen
Rechtliche Grundlage	Verwaltungsübereinkommen zwischen BKA und BMF
Programmeigentümer	BMF
Programmabwicklung	Forschungsförderungsgesellschaft (FFG)
Programmstart / 1. Ausschreibung	30. Oktober 2023 – 1. März 2024
Forschungszeitraum	Ø 2 Jahre
TRL & Förderungsintensität	Bis zum Technologiereifegrad (TRL) 6; Finanzierung bis zu 85 % (Ausnahme Instrument F&E-Dienstleistungen: Finanzierung bis zu 100 %)
Adressaten	• Bundesministerien und sonstige Behörden • Betreiber kritischer Infrastrukturen • Unternehmen • Forschungseinrichtungen und Universitäten





5 Cyberübungen

Österreich beteiligt sich aktiv an Übungen zur Reaktion auf Cybersicherheitsvorfälle.

5.1 BlueOlex

BlueOlex ist eine Veranstaltungsserie, die jährlich durch den Ratsvorsitz mit Unterstützung der EU-Cybersicherheitsagentur (ENISA) und der Europäischen Kommission (EK) durchgeführt wird.

Übergeordnetes Ziel der BlueOlex 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 fünfte Ausgabe der BlueOlex wurde am 2. Oktober 2023 in Den Haag in Verbindung mit der niederländischen Cybersicherheitskonferenz ONE veranstaltet.

Der Schwerpunkt der Übung lag, wie auch schon in 2022, auf der Überprüfung und Weiterentwicklung der „Standard Operating Procedures (SOP)" des Europäische Netzwerkes der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe). Darüber hinaus konzentrierte sich die Übung auf die horizontale Interaktion zwischen den Mitgliedstaaten und relevanten Institutionen, Organisationen und Agenturen der EU (EUIBA). An der Konferenz nahmen die EU-CyCLONe-Executives der einzelnen Mitgliedstaaten teil, wobei auch von den meisten Mitgliedstaaten mindestens ein EU-CyCLONe-Officer als Unterstützung beteiligt war. Österreich wurde durch Mitarbeitende des Bundesministerium für Inneres (BMI) (IV/S/2) vertreten.

Die zentrale Aufgabe von EU-CyCLONe ist es, die koordinierte Bewältigung von Cybersicherheitsvorfällen großen Ausmaßes nach der NIS-2-Richtlinie[18] und den regelmäßigen Austausch relevanter Informationen zwischen den Mitgliedern sicherzustellen. EU-CyCLONe arbeitet dabei auf operativer Ebene und fungiert damit als Bindeglied zwischen der

18 Netz- und Informationssicherheit Richtlinie (EU) 2022/2555

technischen und der strategischen/politischen Ebene. Für die Übung wurde ein Szenario ausgewählt, in dem zuerst der europaweite Energiesektor und später weitere Sektoren durch einen Cybersicherheitsvorfall betroffen waren. Dabei wurden die Übungsinhalte theoretisch durchgespielt, wobei das vorrangige Ziel war, darauf aufbauend Diskussionen zu möglichen sowie 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.

5.2 Locked Shields

Die Teilnahme an der größten Live-Fire-Cyber-Defence-Übung der NATO, „Locked Shields", ist besonders hervorzuheben: Seit 2012 stellt das militärische Cyber-Zentrum (MilCyZ) des Bundesministerium für Landesverteidigung (BMLV) – unter Einbindung von Milizexpertinnen und -experten – den größten Anteil der österreichischen Training Audience. Diese übt den Einsatz eines sogenannten „Cyber Rapid Response Teams" zur Bekämpfung eines hybrid agierenden, staatlichen Gegners. 2023 war es für das Österreichische Bundesheer (ÖBH) die bisher größte Einsatzübung: Knapp 150 militärische und zivile Cyberexpertinnen und -experten konnten zwei Wochen lang die kollaborative Cyber-Verteidigung gegen einen gemeinsamen virtuellen Gegner üben und neueste Technologien und Prozesse zur Anwendung bringen. Erstmalig wurden in diese militärische Übung auch Vertretende der nationalen kritischen Infrastruktur eingebunden. Auch 2024 wird sich das MilCyZ wieder in die „Locked Shields" und weiteren EU- und NATO- sowie nationalen Übungen einbringen.

5.3 Crossed Swords (XS)

Das NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE) veranstaltet jährlich zwei Übungen, an denen die Direktion IKT & Cyber des Österreichischen Bundesheers (ÖBH) teilnimmt: Crossed Swords (XS23) und Locked Shields. Dabei handelt es sich um interaktive, realistische Simulationen, die den Expertinnen und Experten für Cybersicherheit der Allianz ermöglichen, ihre Fähigkeiten im Schutz kritischer Infrastrukturen zu verbessern. Crossed Swords baut auf Locked Shields (siehe 5.2) auf und konzentriert sich auf offensive Cyberoperationen. Über 20 Länder, darunter NATO- und Nicht-NATO-Mitglieder, nehmen mit 400 Systemen teil. Die Übung bietet technisches Red-Teaming-Training für Penetrationstesterinnen und -tester, Forensikexpertinnen und -experten und Awareness Spezialistinnen und -spezialistinnen. Die XS23 zielt darauf ab, Cyberexpertinnen und -experten in der Durchführung vollständiger offensiver Cyberoperationen zu schulen. Die Teilnehmenden, darunter Operatoren, Forensikexpertinnen und -experten und Führungskräfte, trainieren in einem fiktiven Konfliktszenario zweier Nationen und simulieren entsprechende Operationen im Cyberbereich. Die Übung integriert akademische und industrielle Partner, um Authentizität und realitätsnahe Herausforderungen zu gewährleisten. Ziel ist die Planung und Durchführung taktischer und technischer Operationen, die Cyberangriffe umfassen und digitale forensische Fähigkeiten integrieren. Die Übung fördert die Zusammenarbeit Verbündeter und Partner und stärkt das Verständnis und die Partnerschaften durch taktische und technische Koordination während einer Cybermission.

5.4 Military Interoperability Conference (MIC)

In den vergangenen Jahren führte die Direktion IKT & Cyber des Österreichischen Bundesheers (ÖBH) im Rahmen eines European Defence Agency (EDA)-Projektes eine Live-Fire-Cyber-Defence-Übung durch, die speziell der Verbesserung der europäischen Zusammenarbeit zwischen den nationalen militärischen Computer-Notfallteams (mil-CERTs) der Mitgliedstaaten diente.

An der Übung nahmen mehr als 200 Expertinnen und Experten aus 15 EDA-Mitgliedstaaten und der Schweiz teil, die remote miteinander verbunden waren. Die Veranstaltung bestand sowohl aus einem technischen Teil, in dem das Vorfallmanagement (hier insbesondere die Erkennung und das Teilen von Informationen mit den anderen Teams) im Vordergrund stand, als auch aus einem operativen Teil, in welchem die internationale Kooperation zwischen der Leitungsebene der milCERTs diskutiert wurde. Österreich erreichte dabei den 4. Platz in der Gesamtwertung, sowie in der Sonderwertung „bester SitRep“ (Bericht über die „Situational Awareness“ in der Übung) zum 3. Mal in Folge den ersten Platz.

Zudem stellte das österreichische milCERT das kleinste Team der gesamten Übung mit letztendlich fünf aktiven Teilnehmenden. Das erfolgreich erreichte Ziel der Übungswoche war es, die Kooperation der militärischen CERTs zu intensivieren und die Dynamik des Vorfallmanagements zu beobachten. Hierbei lag der besondere Schwerpunkt auf dem Informationsaustausch, einem Schlüsselfaktor der modernen Cyberverteidigung.

Während die europäischen Länder bei der Einrichtung von Mechanismen und Verfahren für den Informationsaustausch zwischen zivilen CERTs weit vorangekommen sind, sind solche Kooperations- und Kommunikationskanäle im militärischen Bereich schlechter entwickelt, auch aufgrund der hohen Sensibilität der Informationen. Angesichts dessen haben viele Beteiligte die Notwendigkeit geäußert, die in zivilen Kreisen angewandte Praxis des Informationsaustauschs auch auf milCERTs und deren Operationen auszuweiten. In der

neuen EU-Cybersicherheitsstrategie, die im Dezember 2022 veröffentlicht wurde, wird hervorgehoben, dass diese Initiative dazu beitrage, die Zusammenarbeit zwischen den Mitgliedstaaten erheblich zu verbessern. Daher beteiligt sich die Direktion IKT & Cyber des ÖBH an dem EDA-Cat A Projekt „Military Computer Emergency Response Team Operational Network" (MICNET), welches im November 2023 von 19 EU-Mitgliedstaaten unterschrieben wurde. Weitere Mitgliedstaaten haben bereits ihr Interesse bekundet.

5.5 Waveform Development Olympiad (WDO)

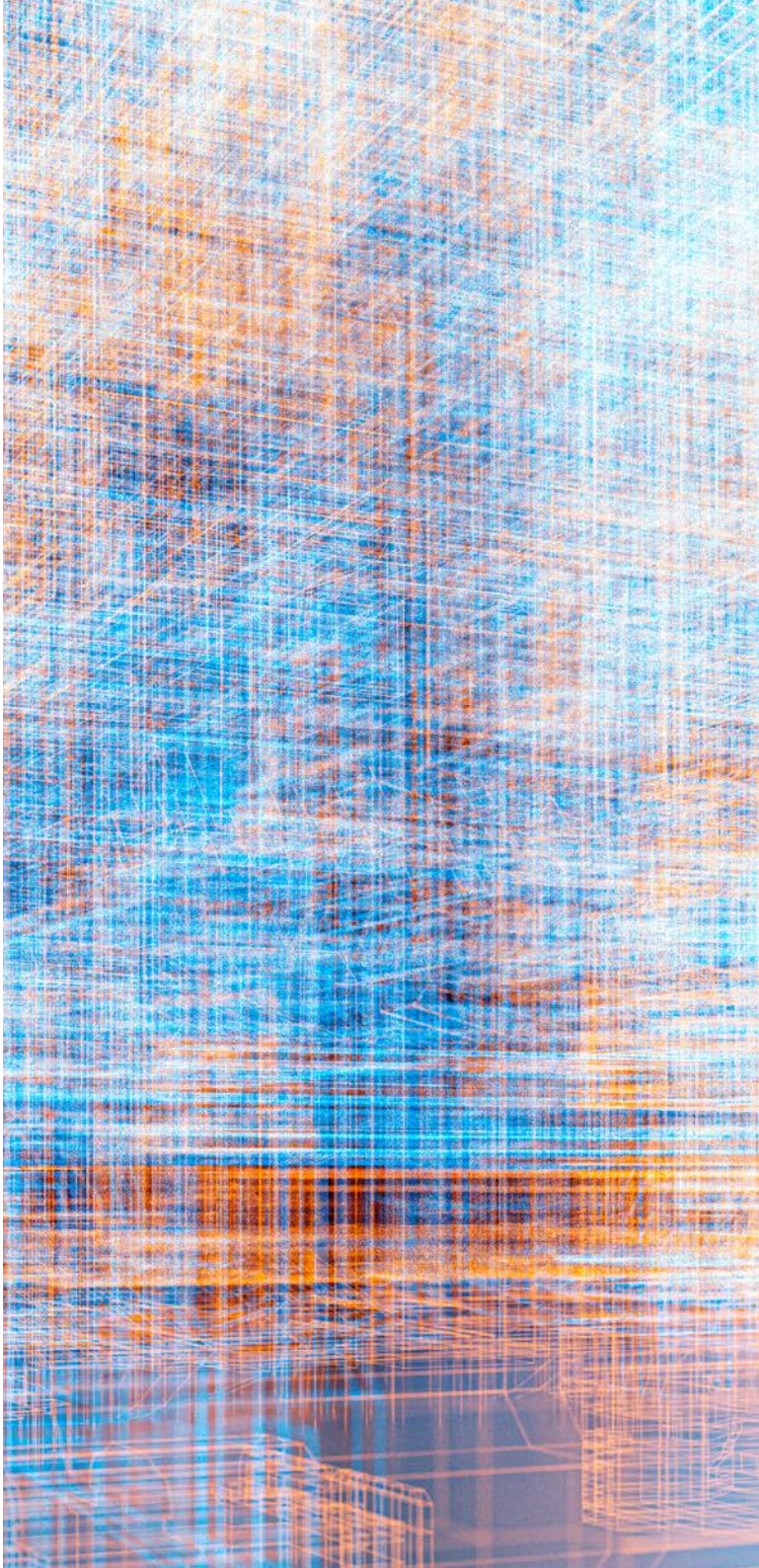
Das Begegnen der Gefahr von Radio Controlled Improvised Explosive Devices (RCIED) für unsere Soldatinnen und Soldaten erfordert stetiges Engagement. Im Bereich der Elektronischen Kampfführung (EloKa) geschieht dies unter anderem durch technische Maßnahmen mit Force Protection-Systemen, beispielsweise mit sogenannten Counter RCIED Electronic Warfare (CREW)-Systemen. Der Umfang dieser technischen Bedrohungen erstreckt sich einerseits von RCIED und andererseits bis zu small Unmanned Areal Vehicles (sUAV) als elektromagnetisch beeinflussbare Systeme im Kontext der RCIEDs.

Neben nationalen Anstrengungen beteiligt sich Österreich auch an internationalen Aktivitäten, um eine bestmögliche Wirksamkeit gegen diese globalen Bedrohungen zu erreichen. Konkret geschieht dies mit einer multinationalen Kooperation im NATO „Team of Experts on Electronic Countermeasures for RCIED". Eine der vielen Aktivitäten ist die regelmäßige Durchführung der sogenannten „Waveform Development Olympiad" (WDO). Bei dieser, bis dato in verschiedenen europäischen Ländern durchgeführten, technischen Veranstaltung liegt der Arbeitsfokus auf dem Wissensaustausch zu neuen Bedrohungen und den erforderlichen Gegenmaßnahmen, des gegenseitigen Kennenlernens der unterschiedlichen CREW-Systeme und Synchronisationsverfahren, der Verbesserung der Mess- und Testverfahren sowie von erforderlichen Testaufbauten und ebenfalls auf der Signalanalyse zur weiteren Bedrohungsanalyse. 2023 nahm zum zweiten Mal eine österreichische Delegation von technischem EloKa-Fachpersonal des Unterstützungs-

zentrums EloKa (UZEloKa) des militärischen Cyber-Zentrums (MilCyZ) der Direktion IKT und Cyber im Österreichischen Bundessheer (ÖBH) an der WDO 2023 in Deutschland teil. Im November 2023 waren insgesamt neun Staaten (Deutschland, Niederlande, Belgien, Frankreich, Dänemark, Norwegen, Schweden, Luxemburg und Österreich) zu Gast in Greding.

5.6 Cyber-Range Exercise (CRX)

In diesem Jahr veranstaltete das militärische Cyber-Zentrum (MilCyZ) der Direktion IKT & Cyber des Österreichischen Bundesheeres (ÖBH) erstmalig eine eigene Cyber-Übung für fortgeschrittene Cyber-Expertinnen und -Experten. Durch Zuhilfenahme einer externen Cyber Range-Infrastruktur und Trainerinnen und Trainern über die Kooperation mit Estland, konnte eine Schulung mit anschließender Blue- und Red-Team-Übung stattfinden. Im Zuge dieser Übung wurden Cyber-Verteidigungs- und Angriffssimulationen unter Ausbildungsbedingungen absolviert. Neben dem Training für österreichische Kräfte, wurden im Zuge der internationalen Zusammenarbeit Cyber-Expertinnen und -Experten der Schweiz eingeladen, um am Training teilzunehmen.



6 Zusammenfassung / Ausblick

Der vorliegende Bericht präsentiert umfangreiche Einschätzungen, Entwicklungen und Aktivitäten im Bereich der Cybersicherheit im Jahr 2023 in Österreich und stellt diese in gewohnter Weise in fünf Kapiteln dar.

Der Bericht und die eingemeldeten Maßnahmen zeigen, dass Cybersicherheit weiterhin ein zentrales Thema für Wirtschaft, Gesellschaft und Verwaltung bleibt. Die fortschreitende Digitalisierung und die zunehmende Vernetzung haben die Angriffsflächen für Cyberbedrohungen erweitert. Die von den Behörden und befragten Unternehmen vorgebrachten Ursachen für Cybersicherheitsvorfälle sind vielseitig. Hervorzuheben ist weiterhin die hohe Anzahl an Ransomware-Gruppierungen, die durch die Verschlüsselung von IT-Systemen mit hohen Lösegeldforderungen das Wirtschafts- und Gesellschaftsleben in Österreich belasten (siehe Kapitel 1). Die nationalen Strukturen (siehe Kapitel 3 und 4) halfen auch 2023 mit diesen Herausforderungen umzugehen: Beispielsweise lag im Bereich Cyberkriminalität trotz erneut stark angestiegener Anzahl von Anzeigen von Delikte im Jahr 2023 die Aufklärungsquote bei Delikten mit Bezug auf Cyberkriminalität im engeren Sinne bei rund einem Fünftel. Auf operativer Ebene hat das nationale Computernotfallteam CERT.at 2023 in vielen Fällen die Rolle übernommen, mit den verfügbaren Informationen Warnungen für weitere potenzielle Opfer zu erstellen, damit sich diese rechtzeitig schützen können und informierte über aktuelle Bedrohungen und Schutzmaßnahmen. 2023 wurde das neue Sicherheitsforschungsprogramm K-PASS auf den Weg gebracht und die erste Ausschreibung gestartet, welches mit zukünftig 5 Millionen Euro pro Jahr die marktnahe Beforschung von Cybersicherheit unterstützen soll. Ein weiterer wichtiger Aspekt des Jahres 2023 war die verstärkte internationale und europäische Zusammenarbeit. Geopolitische Entwicklungen unterstreichen die Bedeutung einer koordinierten Reaktion und Vorbeugung auf Cyberbedrohungen. Österreich hat sich daher aktiv an internationalen Foren und Übungen und Kooperationen beteiligt (siehe Kapitel 2 und Kapitel 5).

Ausblick

Aus dem Bericht lassen sich Lagebild und Entwicklungen des Jahres 2023 rückblickend beobachten. Für das Jahr 2024 zeichnen sich mehrere Trends und Herausforderungen ab: Eine der bedeutendsten Bedrohungen wird durch die zunehmende Komplexität der IT-Landschaft und den Übergang zur Cloud-Infrastruktur erwartet. Hierbei spielen auch Sicherheitsbedenken eine zentrale Rolle. Künstliche Intelligenz (KI) wird sowohl als potenzielle Bedrohung als auch als Unterstützung für die IT-Sicherheitsüberwachung und Priorisierung von Maßnahmen gesehen. Einen Ausblick der wichtigsten längerfristigen Risiken im Bereich der Cybersicherheit präsentiert die EU-Cybersicherheitsagentur (ENISA) in einer regelmäßig angepassten Analyse „Foresight Cybersecurity Threats For 2030". Darin werden für Anfang 2024 folgenden Bedrohungsszenarien angeführt:

Cybersicherheit als gesamtstaatliche Aufgabe

1. Kompromittierte Lieferketten aufgrund von Softwareabhängigkeiten
2. Skills und Fachkräfte-Knappheit
3. Menschliches Versagen und das Ausnutzen von alten IT-Systemen in cyber-physischen Ökosystemen
4. Ausnutzen von nicht gepatchten und überholten Systemen
5. Anstieg autoritärer, digitaler Überwachungssysteme und Verlust von Privatsphäre
6. Grenzüberschreitende IKT-Dienstanbieter als einzelne Fehlerstelle
7. Hochentwickelte Desinformationskampagnen
8. Anstieg von hochentwickelten hybriden Bedrohungen
9. Missbrauch von Künstlicher Intelligenz
10. Physische Auswirkungen von natürlichen oder umweltbasierten Störungen von kritischer digitaler Infrastruktur

Diese Aufzählung zeigt, wie wichtig Maßnahmen auf allen Ebenen – operativ, technisch, strategisch, rechtlich, ethisch – sind. Die 2021 angenommene Österreichische Strategie für Cybersicherheit mit ihren zwölf Zielen versucht einen Rahmen zu bieten, um auf die Herausforderungen zu reagieren. 2023 umfasste der halbjährlich aktualisierte Maßnahmenkatalog 136 Maßnahmen des öffentlichen und privaten Sektors. 60 Maßnahmen alleine wurden von

Unternehmen und Regulatoren eingemeldet. Die Strategie und der Maßnahmenkatalog sind auf der Webseite des Bundeskanzleramts bundeskanzleramt.gv.at veröffentlicht.

Die im Jahr 2023 begonnen Arbeiten zur nationalen Umsetzung der NIS2-Richtlinie (RL EU 2022/2555) sind darüber hinaus hervorzuheben. Mit diesem Rechtsakt haben sich die Mitgliedstaaten der EU und das Europäische Parlament auf eine Modernisierung des Rechtsrahmens zu Cybersicherheitsanforderungen und der dazugehörigen Governance für kritische Infrastruktur geeinigt, die nun bis 17. Oktober 2024 in nationales Recht gegossen werden muss. Die neue Richtlinie versucht, den bestehenden Rechtsrahmen zu modernisieren und eine Harmonisierung der zum Teil unterschiedlichen Implementierungen der Mitgliedsstaaten zu erwirken. Durch die Ausweitung des Anwendungsbereichs auf neue Sektoren sollen die Resilienz- und Reaktionskapazitäten öffentlicher und privater Stellen, der zuständigen Behörden und der Europäischen Union insgesamt verbessert werden. Dabei ist die Einbindung vielseitiger Akteure notwendig. 2024 wird daher der Ansatz – Cybersicherheit als gesamtstaatliche Aufgabe – im Sinne der Österreichischen Strategie für Cybersicherheit (ÖSCS 2021) fortgeführt werden.

Tabellenanhang

Tabelle zu Abbildung 1: Wurden in Ihrer Firma 2023 neue IT-Security-Maßnahmen implementiert, welche die Erkennbarkeit von IT-Sicherheitsvorfällen erhöhen können?

Antwortmöglichkeit	Anzahl	Verhältnis
Ja	70	88,6 %
Nein	7	8,9 %
keine Angabe	2	2,5 %

Tabelle zu Abbildung 2: Wie hat sich in Ihrer Firma im Jahr 2023 das für IT-Security zur Verfügung stehende Budget gegenüber dem Jahr 2022 verändert?

Antwortmöglichkeit	Anzahl	Verhältnis
Gestiegen	48	68 %
Gleich geblieben	21	31 %
Gesunken	0	0 %
keine Angabe	1	1 %

Tabelle zu Abbildung 3: Wie beurteilen Sie die „Vorfallsursache“ für das Jahr 2023?

Beurteilung	Außentäterinnen und -täter	Verhältnis	Innentäterinnen und -täter	Verhältnis	technisches Gebrechen	Verhältnis
Großes Problem	15	21 %	7	9 %	6	8 %
Mittleres Problem	31	42 %	10	14 %	28	38 %
Kleines Problem	18	25 %	27	37 %	27	37 %
Kein Problem	9	12 %	29	40 %	12	17 %

Tabelle zu Abbildung 4: Und welche Trends konnten Sie 2023 diesbezüglich gegenüber 2022 beobachten?

Beurteilung	Außentäterinnen und -täter	Verhältnis	Innentäterinnen und -täter	Verhältnis	technisches Gebrechen	Verhältnis
Gestiegen	39	53 %	39	53 %	4	6 %
Gleich geblieben	30	41 %	30	41 %	52	71 %
Gesunken	0	0 %	0	0 %	11	15 %
keine Angabe	4	6 %	4	6 %	6	8 %
Summe	73		73		73	

Tabelle zu Abbildung 5: Vorfallsarten im Berichtszeitraum

Vorfallsart	Prozentsatz (%)
DDoS (Distributed Denial of Services)	4
Innentäter:innen	5
Ransomware	34
Phishing	30
Targeted Attack / APT	7
CEO-Fraud / Fake Invoice / SCAM	13