Bundesministerium
Inneres

Bericht Cybersicherheit für das Jahr 2024

Bericht Cybersicherheit für das Jahr 2024

Wien, 2025

Bundeskanzleramt

Bundesministerium
Inneres

Bundesministerium
Landesverteidigung

Bundesministerium
Europäische und internationale
Angelegenheiten

Bundesministerium
Finanzen

Impressum

Medieninhaber, Verleger und Herausgeber:
Bundesministerium für Inneres
Herrengasse 7, 1010 Wien

Grafische Gestaltung: Bundesministerium für Inneres
Druck: Digitalprintcenter des BMI

Wien, 2025

Der Bericht Cybersicherheit

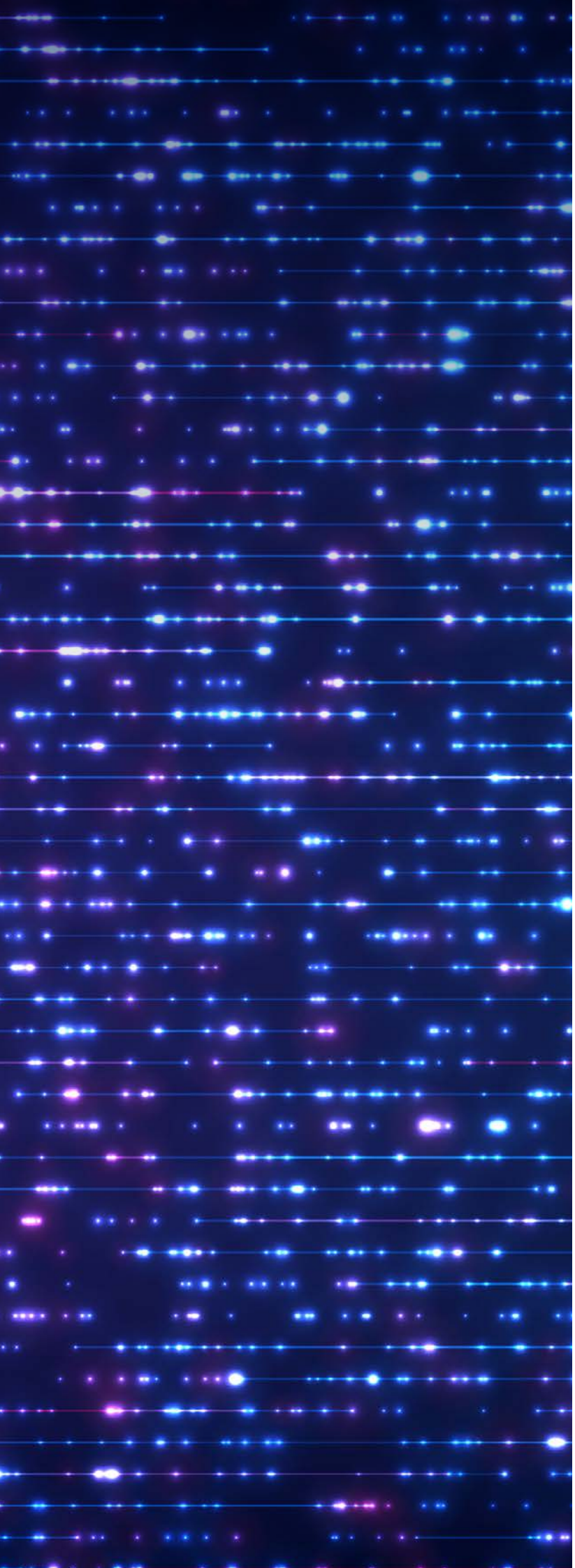
Die Österreichische Strategie für Cybersicherheit (ÖSCS) legt fest, dass durch die Cyber Sicherheit Steuerungsgruppe (CSS) ein jährlicher Bericht zur Cybersicherheit in Österreich erstellt wird. Der letzte Bericht wurde im Dezember 2024 vorgelegt.

Der aktuelle Bericht Cybersicherheit für das Jahr 2024 (Beobachtungszeitraum 1. Jänner 2024 bis 31. Dezember 2024) baut auf den Inhalten des letztjährigen Berichts auf und ergänzt diesen um aktuelle Entwicklungen mit Schwerpunkten in den Bereichen internationale und operationelle Entwicklungen. Beobachtungszeitraum ist das Jahr 2024, einzelne aktuelle Entwicklungen im Jahr 2025 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.

Inhalt

1 Cyberlage



1.1 Lage Cybersicherheit – operative Ebene

1.1.1 Ransomware im Jahr 2024

Ransomware blieb auch im Jahr 2024 eine der größten Cyberbedrohungen weltweit. Die Professionalisierung dieser kriminellen Aktivitäten nahm weiter zu, wobei Gruppen wie LockBit und BlackCat trotz internationaler Strafverfolgungsmaßnahmen weiterhin aktiv waren. Im Februar 2024 gelang es internationalen Strafverfolgungsbehörden, die Infrastruktur der LockBit-Ransomware-Gruppe zu übernehmen und deren Aktivitäten vorübergehend zu unterbrechen. Dennoch zeigte sich die Resilienz solcher Gruppen, da LockBit bereits im April 2024 mit neuen Kampagnen zurückkehrte.

Entwicklung der Bedrohungslage

Die Bedrohung durch Ransomware nahm im Jahr 2024 weiter zu, wobei Angreiferinnen und Angreifer zunehmend auf unentdeckte Schwachstellen in Software und Systemen abzielten. Ein Beispiel hierfür ist die Veröffentlichung der Top 25 der gefährlichsten Software-Schwachstellen des Jahres 2024 durch die US-Behörde CISA und Mitre. Diese Liste zeigte auf, wie kritisch ungepatchte Sicherheitslücken für die IT-Sicherheit sind und wie sie von Angreiferinnen und Angreifern ausgenutzt werden können.

Bekannte internationale Ransomware-Vorfälle

Angriff auf Change Healthcare (USA): Im Jahr 2024 wurde Change Healthcare, ein bedeutendes Unternehmen im Gesundheitssektor, Opfer eines Ransomware-Angriffs. Dieser Vorfall führte zu erheblichen Störungen im Gesundheitswesen und unterstrich die Verwundbarkeit kritischer Infrastrukturen gegenüber Cyberbedrohungen.

Attacke auf Evolve Bank & Trust (USA): Im Sommer 2024 wurde Evolve Bank & Trust, ein Partner vieler Finanztechnologieunternehmen, Ziel eines Ransomware-Angriffs. Die Angreifer drohten, sensible Daten zu veröffentlichen, was die Sicherheitsrisiken im Finanzsektor verdeutlichte.

Cyberangriff auf das Alder-Hey-Kinderkrankenhaus (UK): Im November 2024 wurde das Alder-Hey-Kinderkrankenhaus in Liverpool von der Ransomware-Gruppe INC Ransom angegriffen. Die Hacker behaupteten, Patientinnen- und Patientendaten gestohlen zu haben, was die besonderen Risiken für den Gesundheitssektor aufzeigte.

Auswirkungen auf Unternehmen

Unternehmen standen vor der Herausforderung, ihre IT-Infrastrukturen kontinuierlich zu überwachen und zu sichern, um sich vor Ransomware-Angriffen zu schützen. Die steigende Anzahl von Angriffen führte dazu, dass immer mehr Unternehmen in präventive

Maßnahmen investierten und Notfallpläne entwickelten, um im Falle eines Angriffs schnell reagieren zu können. Dennoch blieben viele Organisationen anfällig, insbesondere, wenn Sicherheitsupdates nicht zeitnah eingespielt oder Sicherheitslücken übersehen wurden.

Wirtschaftliche Auswirkungen

Die durchschnittlichen Kosten für österreichische Unternehmen nach einem Ransomware-Angriff beliefen sich auf etwa 4,7 Mio. Euro, was einen deutlichen Anstieg gegenüber den 2,85 Mio. Euro im Vorjahr darstellt.

1.1.2 Der CrowdStrike-IT-Ausfall im Juli 2024 und seine Auswirkungen

Am Morgen des 19. Juli 2024 kam es weltweit zu massiven IT-Ausfällen, verursacht durch ein fehlerhaftes Update der Sicherheitssoftware „Falcon Sensor" des US-amerikanischen IT-Sicherheitsunternehmens CrowdStrike. Das Update führte zu Systemabstürzen auf Windows-Rechnern, was weitreichende Störungen in verschiedenen Sektoren verursachte.

Internationale Auswirkungen

Besonders betroffen war der Luftverkehr: Flughäfen in Berlin, Köln und Amsterdam meldeten erhebliche Beeinträchtigungen, während in den USA die Luftfahrtaufsicht FAA Flüge von Airlines wie United, American und Delta stoppte. Insgesamt wurden weltweit über 1.000 Flüge gestrichen. In Großbritannien hatten Apotheken Schwierigkeiten, auf Rezepte zuzugreifen und das Buchungssystem des nationalen Gesundheitsdienstes NHS war außer Betrieb. Auch die Londoner Börse und der Fernsehsender Sky News waren von dem Vorfall betroffen. In Australien wurden Geschäfte und Apotheken geschlossen, kritische Infrastrukturen blieben jedoch weitgehend unbeeinträchtigt. In den USA war in mehreren Bundesstaaten die Notrufnummer 911 zeitweise nicht erreichbar. In Deutschland mussten Krankenhäuser Operationen absagen und Teile der öffentlichen Verwaltung waren nur eingeschränkt arbeitsfähig.

Situation in Österreich

In Österreich waren vor allem Fluglinien, Teilbereiche des Gesundheitswesens und die öffentliche Verwaltung betroffen. Dennoch konnten die meisten Unternehmen und Institutionen ihre Systeme relativ rasch wiederherstellen, sodass keine dauerhaften Probleme entstanden.

Sicherheitsimplikationen

Der Vorfall verdeutlichte die Abhängigkeit kritischer Infrastrukturen von Cybersicherheitslösungen und zeigte, wie fehlerhafte Updates weltweit erhebliche Auswirkungen haben

können. Zudem bot der Vorfall potenziellen Angreiferinnen und Angreifern wertvolle Informationen darüber, welche Organisationen CrowdStrike Falcon in ihren Netzwerken einsetzen, was langfristig das Risiko gezielter Cyberangriffe erhöhen könnte.

1.1.3 Geopolitische Konflikte, nachrichtendienstliche und hacktivistische Aktionen

Im Jahr 2024 hat sich die Rolle von Cyberangriffen in geopolitischen Konflikten weiter intensiviert, wobei besonders der fortwährende Krieg in der Ukraine als treibende Kraft hinter der Zunahme von Cyberaktivitäten bleibt. Der NotPetya-Angriff, ursprünglich gegen die Ukraine gerichtet, verursachte weltweit enorme wirtschaftliche Schäden, indem er sich unkontrolliert auf Unternehmen wie Maersk, Merck und DHL ausbreitete. Beim Viasat-Hack 2022, der während des russischen Einmarschs in die Ukraine stattfand, wurden durch die Sabotage von Satellitenmodems auch in Deutschland Windkraftanlagen der Firma Enercon zeitweise vom Fernzugriff abgeschnitten.

Der „Spill-Over-Effekt" beschreibt, wie sich Konflikte und Cyberaktivitäten über nationale Grenzen hinweg ausbreiten und unbeteiligte Dritte in Mitleidenschaft ziehen können. Dieser Effekt bleibt eine zentrale Herausforderung, da Cyberangriffe immer weniger lokalisiert sind und in einem globalisierten digitalen Umfeld weite Kreise ziehen. Ein markanter Trend im Jahr 2024 war die Zunahme von Hybridangriffen, bei denen Cyberoperationen mit traditionellen militärischen Maßnahmen kombiniert wurden, was die Schwelle für die Identifikation und Reaktion auf solche Angriffe weiter erschwert.

Obwohl das im Vorjahr oft prognostizierte „Cyber-Pearl-Harbor-Szenario" auch 2024 nicht realisiert wurde, bleibt die Möglichkeit eines umfassenden, plötzlich ausbrechenden Cyberangriffs bestehen. Anstelle eines einzelnen, großflächigen Angriffs gab es jedoch international eine Zunahme an gezielten, kleineren Angriffen, die jeweils erhebliche, aber lokal begrenzte Auswirkungen hatten. Besonders auffällig war der zunehmende Einsatz von „Wiper"-Malware und Datenlöschsoftware, die auf kritische Infrastrukturen wie Kommunikationsnetzwerke, Energieversorgungssysteme und Finanzinstitute abzielten. Diese Angriffe dienten nicht nur der Sabotage, sondern auch der psychologischen Kriegsführung, indem sie panische Reaktionen in der betroffenen Bevölkerung und in den Medien auslösten.

Im Jahr 2024 nahm auch die Zahl der Cyberangriffe durch nicht staatliche Akteurinnen und Akteure sowie Hacktivistinnen und Hacktivisten deutlich zu. Dies zeigte sich vor allem durch eine Verstärkung von DDoS-Attacken und der Veröffentlichung gestohlener Daten. Besonders auffällig war die Veröffentlichung von vertraulichen Dokumenten durch verschiedene Hackergruppen, die damit sowohl politische als auch wirtschaftliche Ziele verfolgten.

Zusätzlich zu staatlich unterstützten und hacktivistischen Angriffen wurden im Jahr 2024 auch immer häufiger Angriffsmethoden von sogenannten „Cyber-Criminal-Groups“ eingesetzt. Diese Gruppierungen, die oftmals mit staatlichen Akteurinnen und Akteuren zusammenarbeiten oder von diesen finanziert werden, fokussieren sich auf finanzielle Erpressung durch Ransomware-Angriffe. Besonders besorgniserregend war die Zunahme von Angriffen auf den Gesundheitssektor, der 2024 mehrere große Ransomware-Attacken erlebte, die nicht nur den Betrieb von Krankenhäusern und Kliniken gefährdeten, sondern auch die Leben von Patientinnen und Patienten direkt bedrohten.

Abschließend lässt sich sagen, dass das Jahr 2024 einen weiteren Anstieg an hochentwickelten, geopolitisch motivierten Cyberangriffen brachte, die sowohl durch staatliche als auch durch nicht staatliche Akteurinnen und Akteure ausgeführt wurden. Der Spill-Over-Effekt bleibt eine der größten Herausforderungen für die Cybersicherheit in Österreich und Europa, da sich Konflikte und deren digitale Komponenten weiter globalisieren und dabei auch unbeteiligte Nationen in den Strudel der Bedrohung mit hineinziehen.

1.2 Lage Cybersicherheit – Unternehmen und Sicherheitsdienstleister

Für den Bericht Cybersicherheit wurden auch 2024 wieder Unternehmen der kritischen Infrastruktur und verfassungsmäßige Einrichtungen sowie führende private Unternehmen der Cybersicherheitsbranche eingeladen, Informationen zum Berichtsjahr zu sammeln und auf Basis eines Fragebogens zu teilen. Mithilfe ihrer Expertise soll die Cybersicherheitslage Österreichs vollständig aufgezeigt werden. Der Fokus liegt nicht auf einzelnen Vorfällen, sondern auf Trends und Entwicklungen im Sinne einer Überblicksdarstellung.

1.2.1 Befragung von Unternehmen der Kritischen Infrastruktur

Im Berichtsjahr 2024 wurden erneut bei der Mehrheit der befragten österreichischen Unternehmen der kritischen Infrastruktur Investitionen im Bereich der Cybersicherheit getätigt. Nur rund drei Prozent der befragten Unternehmen verminderten das Budget für Cybersicherheit im Vergleich zum Vorjahr. Insgesamt bestätigt sich der Trend, die Ausgaben für IT-Sicherheit auf einem hohen Niveau zu halten. Durch die zielgerichteten Investitionen konnten mutmaßlich schwerwiegende IT-Sicherheitsvorfälle verhindert werden.

Die Sicherheitsmaßnahmen, die im beobachteten Zeitraum eingeführt wurden, umfassten eine Vielzahl von technischen und organisatorischen Maßnahmen zur Verbesserung der Informationssicherheit und Infrastrukturtransparenz. Wesentliche Schritte beinhalteten die Implementierung von Security-Information-and-Event-Management (SIEM)-Lösungen, die Etablierung eines Security Operations Centers (SOC) zur kontinuierlichen Über-

wachung sowie die Einführung von Endpoint-Detection-and-Response (EDR)-Systemen und Network-Detection-and-Response (NDR)-Technologien.

Die Sicherheitsstrategie fokussierte sich auf ein umfassendes „Defense in Depth"-Modell, das durch die Implementierung von Privileged Access Management (PAM) zur Verwaltung von Administrationsberechtigungen sowie durch regelmäßige Vulnerability-Scans zur Identifikation und Behebung von Schwachstellen unterstützt wurde. Besonders hervorzuheben ist die Einführung von Cyber Threat Intelligence, um externe Bedrohungen und Darknet-Aktivitäten zu überwachen sowie die Sicherstellung von Cloud-Infrastruktursicherheit und OT-Systemen.

Langfristig wurden Roadmaps zur Verbesserung der IT-Sicherheit und zum Human-Risk-Management entwickelt, um Sicherheitsstrategien über rein technische Maßnahmen hinaus zu implementieren. Zusätzliche organisatorische Konzepte zur physischen und administrativen Sicherheit sowie die Einführung von Vertraulichkeitsstufen für interne Dokumente runden die Gesamtstrategie ab. Die kontinuierliche Verbesserung und Erweiterung von SIEM-, SOC- und ISMS-Lösungen sowie die Einführung von Zero-Trust-Architekturen sind zentrale Bestandteile der laufenden Sicherheitsmaßnahmen.

Auch im Jahr 2024 konnten Trends in der IT-Security-Branche entdeckt werden: Ein entscheidender Trend ist der vermehrte Einsatz von Künstlicher Intelligenz (KI), der den Unternehmen einerseits im Defend-Bereich durch die Optimierung von SEC-Monitorings, Logauswertungen und vorzeitige Bedrohungserkennung zugutekam. Andererseits kam es mithilfe von Künstlicher Intelligenz im vergangenen Jahr auch zu vermehrten Angriffen auf die Sicherheitsbranche. Auch ein erhöhtes Vorkommen von Phishing-Angriffen konnte wahrgenommen werden.

Die Einschätzung der Vorfallsursachen zeigt auch für 2024 das Bild, dass primär Täterinnen bzw. Täter von außen das größte Problem für Unternehmen waren. Gefolgt von externen Abhängigkeiten (Lieferantinnen und Lieferanten, Dienstleisterinnen und Dienstleister etc.), die auch den Betrieb erschweren können. Die derzeitige Auffassung zeigt, dass Innentäterinnen bzw. -täter großteils entweder als kein oder als ein kleines Problem für Organisationen angesehen werden.

Wurden in Ihrem Unternehmen 2024 neue IT-Security-Maßnahmen implementiert, die Erkennbarkeit von IT-Sicherheitsvorfällen erhöhen können?

Ja: 91 (84,26 Prozent); Nein: 13 (12,04 Prozent); k. A.: 4 (3,7 Prozent)

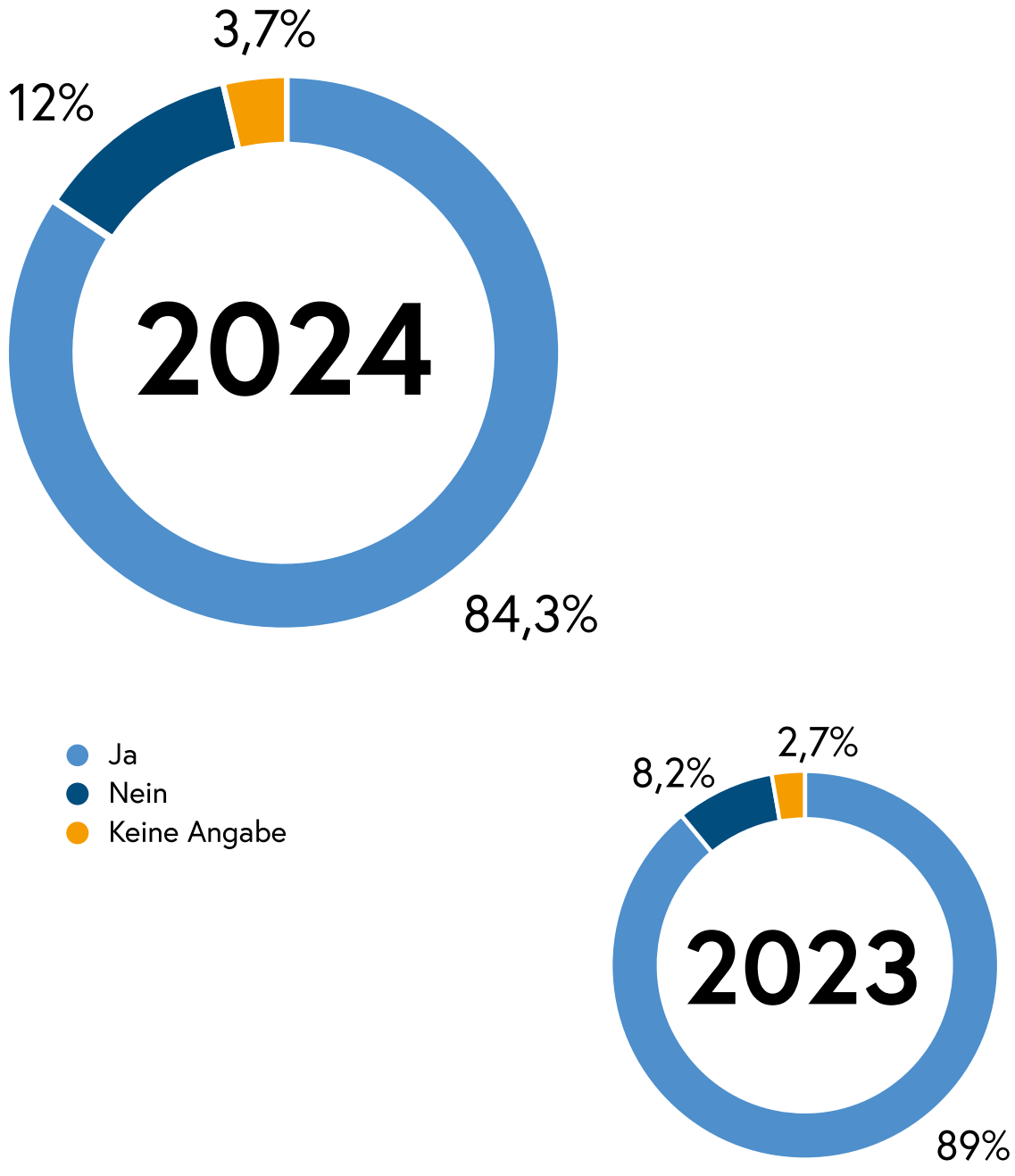


Abbildung 1: Neue IT-Security-Maßnahmen 2024 und Vergleich 2023

Wie hat sich in Ihrem Unternehmen im Jahr 2024 das für IT-Security zur Verfügung stehende Budget gegenüber dem Jahr 2023 verändert?

Gestiegen: 55 (50,93 Prozent); Gleich: 44 (40,74 Prozent); Gesunken: 3 (2,78 Prozent); k. A.: 6 (5,56 Prozent)

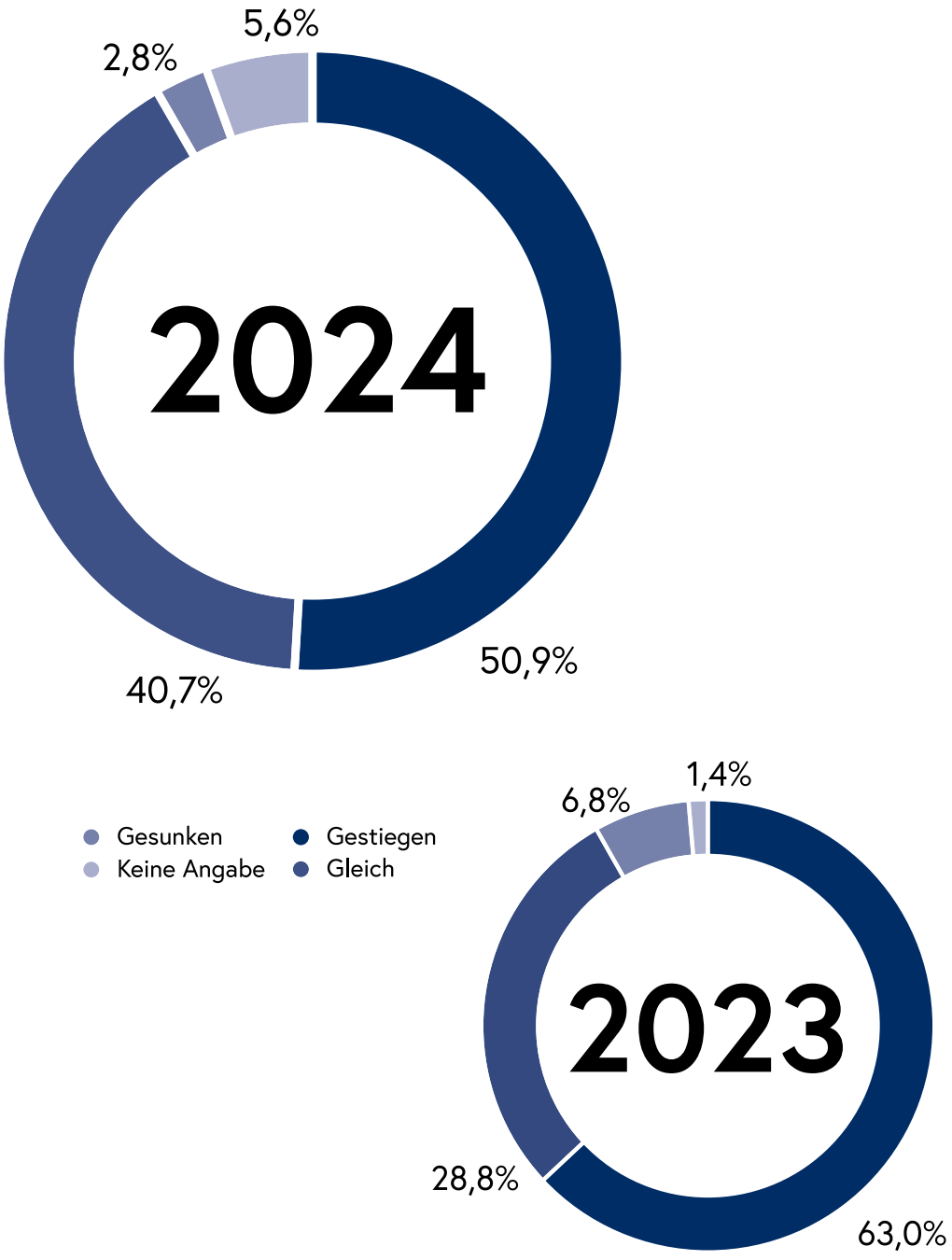


Abbildung 2: IT-Security-Budget 2024 und Vergleich 2023

Außentäterinnen bzw. -täter

Großes Problem: 36 (33,33 Prozent); Mittleres Problem: 37 (34,26 Prozent); Kleines Problem: 24 (22,22 Prozent); Kein Problem: 11 (10,19 Prozent)

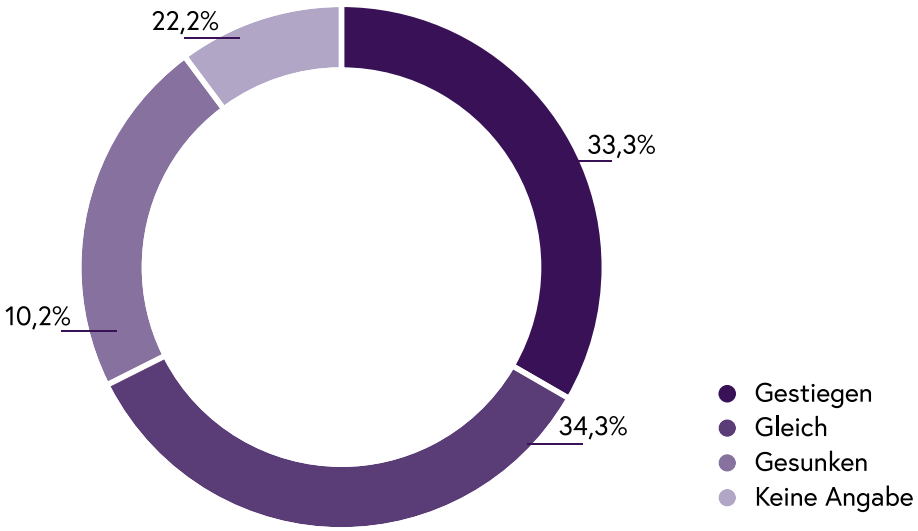


Abbildung 3: Probleme mit Außentäterinnen bzw. -tätern 2024

Innentäterinnen bzw. -täter

Großes Problem: 7 (6,48 Prozent); Mittleres Problem: 15 (13,89 Prozent); Kleines Problem: 59 (54,63 Prozent); Kein Problem: 27 (25 Prozent)

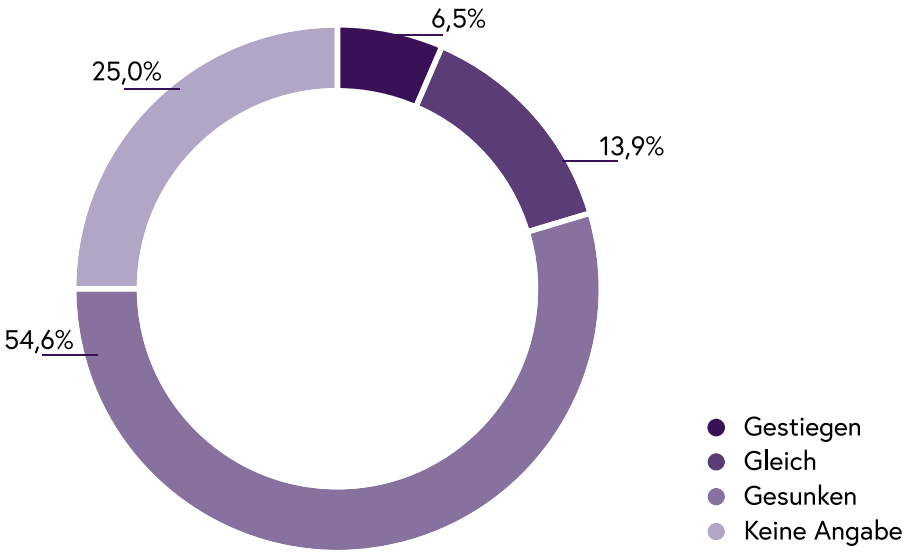


Abbildung 4: Probleme mit Innentäterinnen bzw. -tätern 2024

Technische Gebrechen

Großes Problem: 11 (10,19 Prozent); Mittleres Problem: 45 (41,67 Prozent); Kleines Problem: 44 (40,74 Prozent); Kein Problem: 8 (7,41 Prozent)

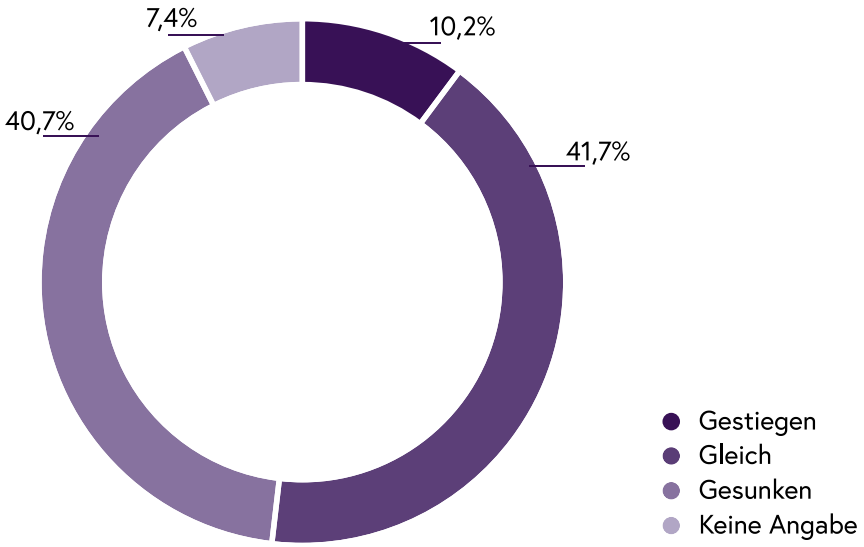


Abbildung 5: Probleme mit technischen Gebrechen 2024

Externe Abhängigkeiten (Lieferantinnen und Lieferanten, Dienstleisterinnen und Dienstleister etc.) – „Supply Chain“

Großes Problem: 25 (23,15 Prozent); Mittleres Problem: 50 (46,30 Prozent); Kleines Problem: 24 (22,22 Prozent); Kein Problem: 9 (8,33 Prozent)

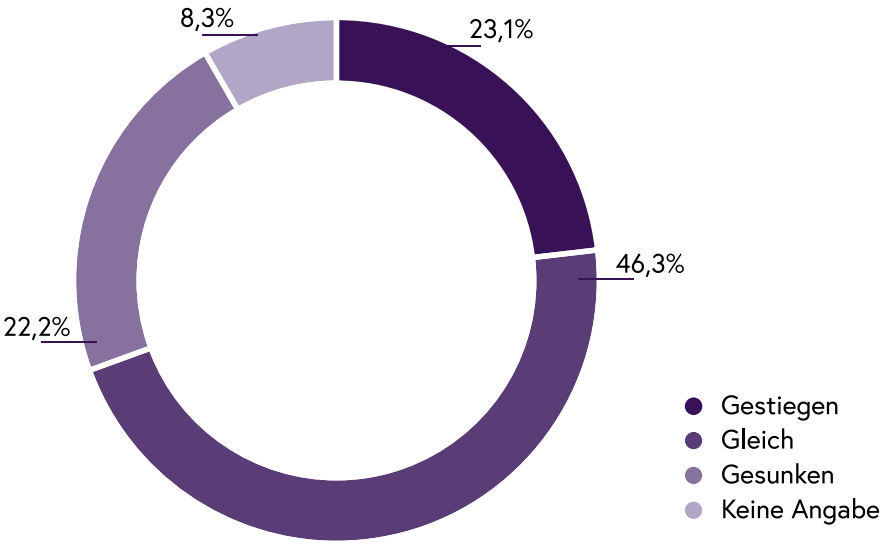


Abbildung 6: Probleme mir externen Abhängigkeiten 2024

Welche Trends konnten Sie 2024 diesbezüglich gegenüber 2023 beobachten?

Außentäterinnen bzw. -täter
Steigend: 62 (57,41 Prozent); Gleichbleibend: 41 (37,96 Prozent); Sinkend: 2 (1,85 Prozent); k. A.: 3 (2,78 Prozent)

Innentäterinnen bzw. -täter
Steigend: 4 (3,70 Prozent); Gleichbleibend: 92 (85,19 Prozent); Sinkend: 3 (2,78 Prozent); k. A.: 9 (8,33 Prozent)

Technische Gebrechen
Steigend: 18 (16,67 Prozent); Gleichbleibend: 76 (70,37 Prozent); Sinkend: 10 (9,26 Prozent); k. A.: 4 (3,70 Prozent)

Externe Abhängigkeiten
Steigend: 47 (43,52 Prozent); Gleichbleibend: 51 (47,22 Prozent); Sinkend: 6 (5,56 Prozent); k. A. 4 (3,70 Prozent)

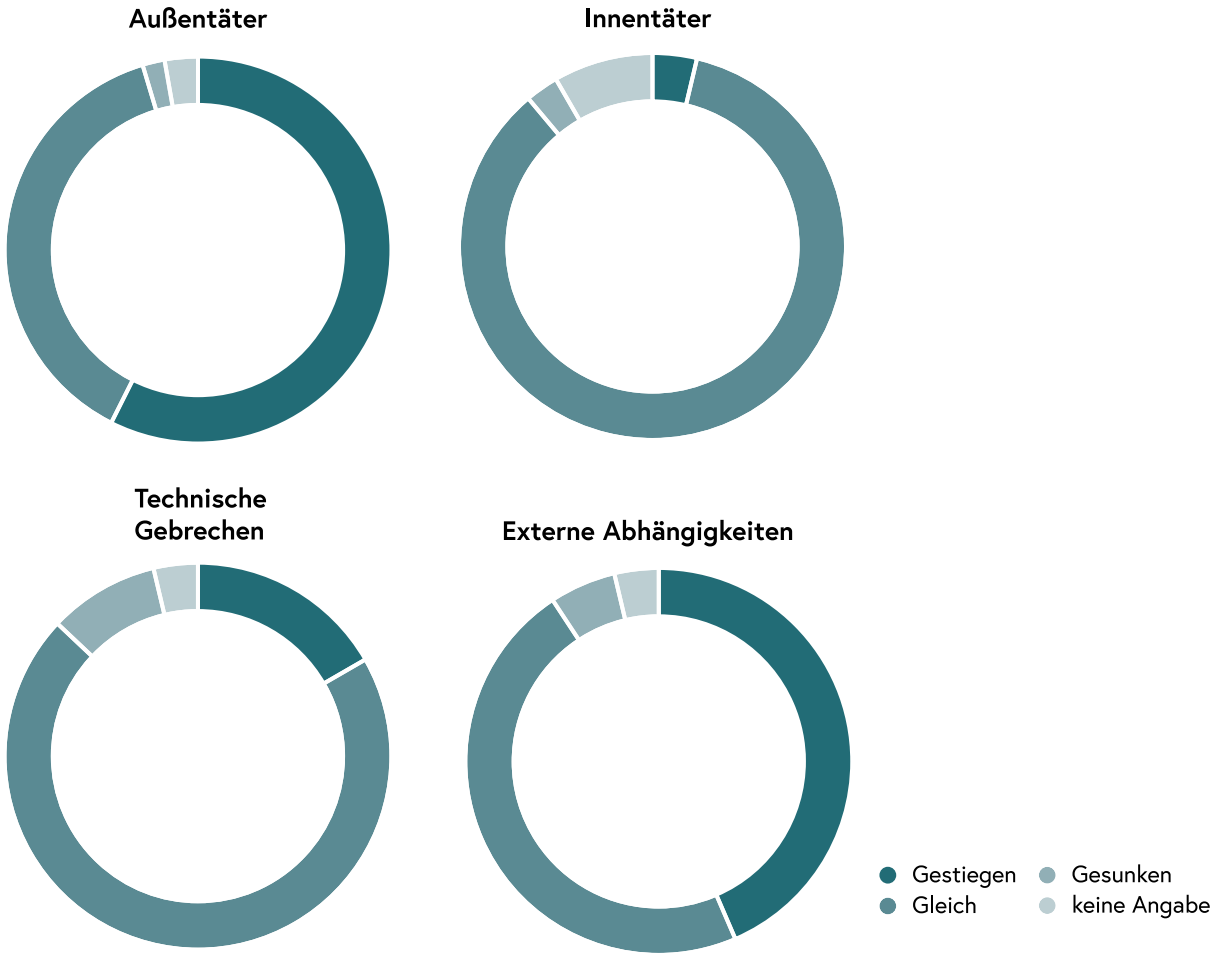


Abbildung 7: Trends 2024

1.2.2 Befragung führender privater Cyber-Sicherheitsdienstleisterinnen und -Sicherheitsdienstleistern

Aus den eingegangenen Antworten der Befragung von führenden privaten Cyber-Sicherheitsdiensterleisterinnen und -Sicherheitsdienstleistern zu den im Jahr 2024 für ihre Kundinnen und Kunden erbrachten Dienstleistungen lassen sich nachfolgend aufgeführte Erkenntnisse ableiten.

Ransomware: 33,9 Prozent; Phishing: 29,7 Prozent; CEO-Fraud/Fake Invoice/Scam: 12,7 Prozent; DDoS: 11,0 Prozent; Targeted Attack/APT: 9,3 Prozent; Innentäterinnen bzw. -täter: 3,4 Prozent

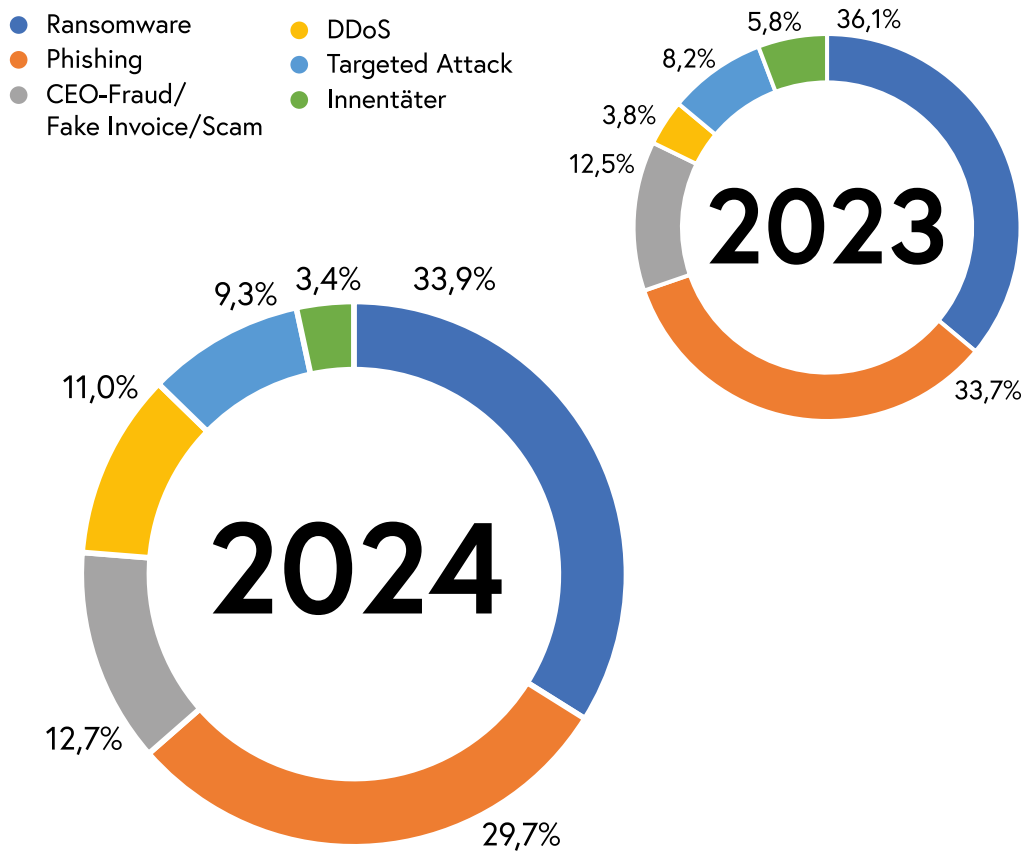


Abbildung 8: Die häufigsten Cyber-Angriffe in Österreich 2024 und Vergleich 2023

In Bezug auf dabei beobachtete Trends zeigt sich dabei folgendes Bild:

	SD 1	SD 2	SD 3	SD 4	SD 5	SD 6	SD 7	SD 8
DDoS	=	=	=	=	k.A.	=	=	+
Ransomware	=	+	=	=	=	-	=	+
Phishing	+	+	+	=	+	+	+	+
CEO-Fraud/Fake Invoice/SCAM	+	=	=	=	+	=	+	+
Targeted Attack/APT	+	+	-	+	=	=	=	+
Innentäterinnen bzw. -täter	=	+	=	k.A.	=	=	+	=

Abbildung 9: Trends zu Cyber-Angriffen in Österreich 2024

Anhand der im Fragebogen ausgewerteten Ergebnisse konnten die verschiedenen Angriffskategorien, die bei den Sicherheitsdienstleisterinnen und -dienstleistern identifiziert wurden, analysiert werden. Dabei werden die relevanten Akteurinnen und Akteure sowie die gewonnenen Erkenntnisse aus den Angriffen dargestellt. Ziel ist, Handlungsempfehlungen für zukünftige Cybersicherheitsmaßnahmen abzuleiten.

DDoS

Im Rahmen der Untersuchung wurde für die Angriffe der Kategorie „DDoS“ (Distributed Denial-of-Service) ausschließlich der Akteur „NoName057“ durch die Unternehmen identifiziert. Aus den Angriffen wurde mitgenommen, dass sich Vorbereitung als entscheidend erweist und reaktive Maßnahmen nur bedingt möglich sind. Von den befragten Sicherheitsdienstleisterinnen und -dienstleistern wird vermehrt eine Empfehlung für Darknet Monitoring ausgesprochen, das Unternehmen helfen soll, potenziellen Angreiferinnen und Angreifern zuvorzukommen.

Ransomware

In der Kategorie Ransomware-Angriffe wurden gehäuft Spear Phishing und Vulnerability Exploitation als zentrale Faktoren für die Angriffe genannt. Die Sicherheitsdienstleisterinnen und -dienstleister machten im Rahmen der Befragung die Akteure Qilin, LockBit und Akira verantwortlich, wobei besonders seit Herbst 2024 häufiger neue Gruppierungen mit deutlich kürzeren Geschäftszyklen bemerkbar wurden.

Ransomware-Angriffe zeigen erneut die entscheidende Bedeutung robuster Sicherheitsmaßnahmen. True Offline Backups sowie regelmäßige Disaster-Recovery- und Restore-Tests sind essenziell, um im Ernstfall handlungsfähig zu bleiben. Die Abdeckung durch XDR-Lösungen ermöglicht eine frühzeitige Identifikation, sofortige Eindämmung und detaillierte Analyse potenzieller Datenexfiltration. Zudem wurde festgestellt, dass in den meisten Fällen öffentlich verfügbare Fernwartungstools für persistente Zugriffe

missbraucht wurden, während RDP in allen analysierten Vorfällen für Lateral Movement genutzt wurde. Daher sind der gezielte Einsatz von XDR-Systemen sowie ein kontinuierliches Darknet-Monitoring essenzielle Maßnahmen zur Erkennung und Abwehr solcher Bedrohungen.

Phishing

Phishing bleibt auch 2024 eine der häufigsten Angriffsmethoden. Da es sich in den meisten Fällen um ein bekanntes Angriffsszenario handelt, kann die Reaktion darauf gut vorbereitet werden, wodurch die Auswirkungen in der Regel gering bleiben. Besonders auffällig ist die Zunahme von O365-Phishing-Angriffen, die häufig als Ausgangspunkt für Man-in-the-Middle-Attacken im Zusammenhang mit gefälschten Rechnungsdokumenten dienen. Daher bleibt eine kontinuierliche Sensibilisierung der Mitarbeiterinnen und Mitarbeiter essenziell, um solche Bedrohungen frühzeitig zu erkennen und abzuwehren.

CEO-Fraud

CEO-Fraud ist weiterhin eine ernstzunehmende Bedrohung, da Social-Engineering-Angriffe immer überzeugender und schwerer zu erkennen sind. Ein internes Kontrollsystem ist daher essenziell und keine bloße Formsache. Zudem zeigt sich, dass öffentlich zugängliche Informationen, insbesondere aus Ausschreibungen, von Angreiferinnen und Angreifern gezielt für Invoice-Scam-Angriffe genutzt werden. Eine gezielte Awareness-Schulung der Mitarbeiterinnen und Mitarbeiter sowie klare Prozesse zur Überprüfung sensibler Zahlungsanweisungen sind daher unverzichtbare Maßnahmen zur Abwehr solcher Betrugsversuche.

APT

Advanced Persistent Threats (APT) nutzen gezielte Angriffsvektoren wie Spear-Phishing, fehlende Multi-Faktor-Authentifizierung (MFA) oder auch „MFA Fatigue“, den Missbrauch gültiger Zugangsdaten, Firewall-Exploits und nutzen ungepatchte Schwachstellen aus. Akteure wie Earth Lusca, Lazarus und Red Scylla sind in diesem Kontext aktiv, wobei die eindeutige Attribution oft schwierig bleibt und für viele Unternehmen nur begrenzten Mehrwert bietet. Um sich gegen diese hochentwickelten Bedrohungen zu schützen, sind konsequente Sicherheitsmaßnahmen wie die Implementierung von MFA, eine strikte Patch-Strategie und umfassende Monitoring-Lösungen unerlässlich.

Eine starke Sicherheitsbasis mit effektivem Vulnerability Management, korrekt konfigurierten XDR-Lösungen und einem DFIR-Retainer ist essenziell. Die Unterscheidung zwischen Ransomware- und APT-Angriffen gestaltet sich schwierig, insbesondere, wenn schwerwiegende Auswirkungen frühzeitig abgewehrt wurden. Während bei Ransomware-Angriffen die Priorität auf einer raschen Wiederherstellung liegt, erfordert die Incident

Response bei APTs ein deutlich höheres Maß an forensischer Analyse und umfassender Sichtbarkeit im Netzwerk.

Innentäterinnen bzw. -täter

Nach dem Austritt von IT-Mitarbeiterinnen und -Mitarbeitern ist ein sofortiger Passwortwechsel essenziell, um unbefugten Zugriff zu verhindern. Zudem ist die frühzeitige Einbindung von Betriebsrätin und Betriebsrat sowie Legal unerlässlich, um rechtliche und organisatorische Aspekte angemessen zu berücksichtigen.

1.3 Lage Cybercrime

Die Betrachtung der polizeilichen Kriminalstatistik lässt mit 62.328 angezeigten Delikten im Jahr 2024 einen leichten Rückgang von 5,4 Prozent gegenüber dem Jahr 2023 erkennen. Die genauen Deliktszahlen werden jährlich im Frühjahr mit der kriminalpolizeilichen Kriminalstatistik veröffentlicht. Eine tiefergehende Analyse und Beschreibung der kriminalpolizeilichen Phänomene erfolgen mit dem jährlichen Cybercrime-Report des Bundeskriminalamts.

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 2024 im Vergleich zu 2023 um 3,4 Prozent auf 20.246 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.

Im Bereich der Ransomware-Anzeigen ist zu beobachten, dass sowohl die Angriffsqualität zunimmt, insbesondere durch Ausnutzung aktueller Sicherheitslücken, als auch die

jeweiligen Schadenshöhen in den einzelnen Fällen ansteigen. Im Cybercrime Competence Center (C4) des Bundeskriminalamts 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 2024 insgesamt 109 Fälle von Ransomware-Angriffen zur Anzeige gebracht. Die Dunkelziffer ist in diesem Bereich sehr hoch. Die Angriffe richteten sich sowohl gegen Privatpersonen, EPUs (Ein-Personen-Unternehmen), KMUs (kleine und mittlere Unternehmen), Konzerne als auch gegen Bildungseinrichtungen, das Gesundheitswesen, Gemeinden und Städte. Dabei wurden die Angriffe von 29 unterschiedlichen Tätergruppierungen durchgeführt. 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

Der Internetbetrug stellt zahlenmäßig den größten Faktor im Bereich der Cyberkriminalität dar. Mehr als die Hälfte der erfassten Anzeigen im Bereich Internetkriminalität fallen auf Betrugsdelikte: 2024 wurden 31.768 Fälle von Internetbetrug angezeigt, ein Rückgang von 6,8 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. Häufige Deliktsformen sind der Bestellbetrug, der digitale Investmentbetrug, der Anrufbetrug (Stichwort: „Falscher Polizist und falsche Polizistin“) sowie alle möglichen Phishingversuche.

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 2024 ein 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.

Durch die im Darknet angebotenen Dienste werden vor allem Erpressungen mit Ransomware begangen bzw. Massenerpressungsmails verschickt, meist begleitet von Geldforderungen in Kryptowährungen. 2024 wurden 2.931 Erpressungen im Internet angezeigt, ein Rückgang von 24,7 Prozent gegenüber dem Vorjahr (3.891 angezeigte Fälle).

Zunahmen wurden beispielsweise bei § 107 StGB (Gefährliche Drohung) mit 1.472 Anzeigen und § 3g Verbotsgesetz (1.222 Anzeigen) verzeichnet.

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

Die militärische Kriegsführung verändert sich durch die zunehmende Nutzung von Informations- und Kommunikationstechnologien kontinuierlich. Eine sich wandelnde Sicherheitslandschaft schafft neue Gefahren, da das Schadenspotenzial an sensiblen Informationen wie z. B. bei der militärischen Kriegsführung enorm groß ist. Statistiken von Cyber-Sicherheitsunternehmen haben aufgezeigt, dass der staatliche und militärische Bereich der zweitmeist attackierte Sektor nach dem Forschungsbereich ist und dass die Angriffe pro Woche im Jahr 2024 im Vergleich zum Vorjahr um 75 Prozent gestiegen sind.

Die Entwicklung der vergangenen Jahre zeigt, dass bei globalen Konflikten unvermeidlich ebenfalls weit verbreitete Cyber-Angriffe durchgeführt werden. Dies ist sowohl beim russischen Angriffskrieg als auch beim anhaltenden Konflikt zwischen Israel und der Hamas der Fall. Dabei kam es in beiden Fällen zu einem sofortigen Anstieg der weltweiten Cyberangriffe sowie zu massiven Desinformationskampagnen.

Einmal mehr wurde durch aktuelle Konflikte die Notwendigkeit unterstrichen, Cyber- und Elektronische Kampfführung (EloKa) sowie Informationsoperationen als integralen Bestandteil der hybriden Kriegsführung zu entwickeln. Dabei wurde deutlich, dass „Cyber-Kriegsführung“ nicht nur offensiv, sondern auch als Mittel zur Informationsgewinnung genutzt wird. Für Österreich ist daher besonders die Stärkung defensiver Cyberfähigkeiten von zentraler Bedeutung. Im Kontext dieser Entwicklungen wird im Österreichischen Bundesheer (ÖBH) die Fähigkeit zur Full Spectrum Cyber Defence angestrebt, um gegen die vielfältigen Bedrohungen im Cyberraum gewappnet zu sein. Der russische Angriffskrieg hat zudem aufgezeigt, wie stark die Cyberdomäne in modernen Konflikten bereits als integraler Bestandteil der Kriegsführung eingesetzt wird, sowohl zur Destabilisierung als auch zur Beeinflussung von strategischer bis taktischer Ebene.

Zusammenfassend lässt sich sagen, dass 2024 ein deutlicher Anstieg der Cyberkriegsaktivitäten zu verzeichnen ist, der durch geopolitische Spannungen, die steigende Raffinesse von Cyberangriffen und die Integration von neuen Technologien in Cyber-Operationen bedingt ist.

Um auf diese Gefahren vorbereitet zu sein, erhöht das ÖBH nicht nur die eigenen Cyber-Verteidigungskapazitäten, sondern trainiert auch im internationalen Umfeld auf höchstem Niveau. Ein herausragendes Highlight war hierbei die erfolgreiche Teilnahme an der Übung Locked Shields 2024. Neben dieser nahm das ÖBH an weiteren EU- und NATO-geführten, groß angelegten Cyber-Übungen, bei denen alle Beteiligten ihre Fähigkeiten unter realistischen Bedingungen testen und festigen konnten, teil.

Das ÖBH hat mit europäischen und internationalen Partnerinnen und Partnern zusammengearbeitet und ist im Rahmen der EU-Verteidigungsinitiative Permanent Structured Cooperation (PESCO) seit Mai 2024 vollwertiges Mitglied des PESCO-CRRT-Projekts (Cyber Rapid Response Team). Im Rahmen dieses Projekts kam es auch zur ÖBH-Beteiligung am Einsatz eines europäischen Cyber Rapid Response Teams im Vorfeld der Präsidentschaftswahlen in Moldau.

Das ÖBH investiert weiterhin in die Kooperationen mit Industrie- und Forschungseinrichtungen, um die neuesten Entwicklungen schnell in die eigenen Strukturen und Fähigkeiten zu integrieren.

Die sichere Integration neuer Waffensysteme sowie moderner Führungs- und Kommunikationsmittel in die IKT-Landschaft und deren „Vollvernetzung“ stellt eine große Herausforderung dar. Das Ziel ist, auf allen Ebenen und in allen militärischen Domänen die Resilienz zu stärken und auch gegen hybride Bedrohungen gewappnet zu sein. Besonderes Augenmerk wird hierbei auf die Auseinandersetzung mit den potenziellen Auswirkungen und Herausforderungen von Technologien wie künstlicher Intelligenz und Quanten-Computing gelegt. Ziel ist, sich sowohl auf die Bedrohungen durch diese Technologien vorzubereiten als auch deren möglichen Einsatz im militärischen Kontext zu untersuchen.

1.5 Verfassungsschutzrelevante Cyberlage

Im Cyberraum stellen sich für den Verfassungsschutz insbesondere Aufgaben bei der Abwehr von Bedrohungen in den Bereichen Cyberspionage, Cybersabotage und Cyber-Enabled Information Operations.[1] In erster Linie handelt es sich hierbei um Bedrohungs-

1 Ein Ziel von Informationsoperationen ist es, die Meinung des Gegenübers zu verändern. In zunehmendem Maße erfolgt dies mit Hilfe von Cyberangriffen. Der Cyberraum dient hier aller-

akteure (Advanced Persistent Threats[2], APTs), die in staatlichem Auftrag handeln. Für Österreich besonders relevant sind in diesem Zusammenhang Russland, China, Iran und Nordkorea. Darüber hinaus treten sogenannte „Hacktivistinnen und Hacktivisten" im Cyberraum in Erscheinung, die mit ihren zumeist harmlosen Angriffen die Aufmerksamkeit der Medien und einer breiten Öffentlichkeit auf ihre Anliegen lenken wollen. Der Verfassungsschutz ist zudem mit dem Schutz kritischer Infrastruktur und verfassungsmäßiger Einrichtungen betraut.

1.5.1 Advanced Persistent Threats

International gesehen liegt der Fokus russischer Nachrichtendienste auf der Unterstützung des russischen Angriffskriegs gegen die Ukraine. Dabei werden drei Achsen verfolgt: Zum einen wird versucht, durch Cyberspionage Unterstützungshandlungen des Westens auszukundschaften. Zum anderen gibt es Bemühungen, durch das gezielte Leaken derart ausgespähter Informationen Wahlergebnisse westlicher Demokratien und deren staatliche Handlungen zu beeinflussen. Der Durchführung von Cybersabotageoperationen in der Ukraine kommt eine abnehmende Bedeutung zu, da diese bisher nicht die erwarteten Wirkungen zeigten. Zu den Zielen russischer Cyberspionage zählen in erster Linie staatliche und politische Institutionen. In Österreich kommt es immer wieder zu Cyberspionageangriffen gegen staatliche und internationale Einrichtungen.

Chinesische Nachrichtendienste verfügen im Cyberraum über weitreichende Fähigkeiten. Kennzeichnend für die Cybereinheiten chinesischer Nachrichtendienste ist ihre Verflechtung mit chinesischen Universitäten und Unternehmen. Daraus resultiert ein umfangreiches Leistungsportfolio, darunter Vorbereitungshandlungen für weitreichende Cybersabotageangriffe gegen andere Staaten. Dabei dringen chinesische Akteurinnen und Akteure in unzureichend gesicherte Anlagen der kritischen Infrastruktur ein. Es ist anzunehmen, dass diese Zugänge hergestellt wurden, um im Konfliktfall rasch signifikante Teile der kritischen Infrastruktur anderer Staaten beeinträchtigen zu können.

Im Cyberraum verfolgen **iranische Nachrichtendienste** in erster Linie strategische Interessen. Um diese zu erreichen, führen sie Spionageoperationen durch. Dabei gewonnene Erkenntnisse werden auch für Desinformationskampagnen (Cyber-Enabled Information Operations) genützt. Ziele sind in erster Linie Unternehmen, die für die iranische Wirt-

---

dings in erster Linie lediglich als Hilfsmittel zur Tatausführung, daher Cyber-Enabled Information Operations. Das Markenzeichen dieser Operationen ist, dass eine Verbindung zur auführenden (staatlichen) Akteurin bzw. zum ausführenden (staatlichen) Akteur möglichst unerkannt bleiben soll. Dazu werden unterschiedliche Methoden verwendet, z. B. Nutzung massenhaft angelegter Social-Media-Konten zur Verbreitung von Desinformation, Erfindung politisch motivierter Hackergruppen zur Verschleierung von staatlichen Aktivitäten wie Hack-and-Leak-Operationen, hinter dem Deckmantel von Anarchismus oder Rebellion.

2 APTs beschreiben nachrichtendienstliche Akteurinnen und Akteure, die mit dem Ziel der klassischen Spionage bzw. auch Wirtschafts- oder Wissenschaftsspionage oder der aktiven Sabotage in IT-Systeme eindringen und diverse Maßnahmen setzen. Dabei wird versucht, möglichst lange unentdeckt zu bleiben, um einen längerfristigen Informationszugriff zu ermöglichen.

schaft relevantes Wissen besitzen. Darüber hinaus werden auch iranische Dissidentinnen und Dissidenten im Westen unter anderem über deren IT-Systeme bzw. -geräte ausspioniert. In der Vergangenheit kam es international, beispielsweise in Albanien und Israel, auch zu Cybersabotageangriffen, die staatlichen iranischen Akteurinnen und Akteuren zugerechnet wurden. Hierbei handelte es sich entweder um kurzfristige Vergeltungsschläge oder um langfristig geplante strategische Operationen militärischen Charakters.

Der Fokus **nordkoreanischer Nachrichtendienste** liegt im Cyberraum auf der Beschaffung von Devisen. Das wirtschaftlich weitgehend isolierte Land benötigt diese dringend, um grundlegende Investitionen tätigen zu können. Dazu setzt Pjöngjang in erster Linie auf Ransomware-Angriffe und „Crypto-Heist" genannte Operationen. Bei diesem Cyberäquivalent eines Bankraubs werden Tauschbörsen von Kryptowährungen gezielt angegriffen und mitunter große Summen erbeutet. Alleine im Jahr 2024 summierten sich diese „Einnahmen" auf über 1,2 Milliarden US-Dollar. Zur Umsetzung greifen nordkoreanische Akteurinnen und Akteure dabei primär Entwicklerinnen und Entwickler von Kryptobörsen und deren Bestandteile an. Dadurch können Kryptovermögen direkt an der Quelle gestohlen werden. Die Ziele nordkoreanischer Ransomware-Angriffe verschieben sich zunehmend in Richtung des Gesundheitssektors. Auf Grund der Gefährdung von Menschenleben wird in diesem Sektor Lösegeldforderungen in der Regel rascher nachgekommen. Teilweise werden die derart lukrierten Gelder wieder in Cyberspionageoperationen investiert. Diese haben in der Regel das Ziel, Informationen und intellektuelles Eigentum mit militärischem oder nuklearem Potenzial aus dem Westen zu beschaffen.

1.5.2 Hacktivismus

Vor dem Hintergrund der aktuellen geopolitischen Konflikte, insbesondere dem russischen Angriffskrieg gegen die Ukraine, tritt das Phänomen des Hacktivismus wieder verstärkt in den Vordergrund. Darunter wird politischer Aktivismus im Cyberraum verstanden, der sich oft in Überlastungsangriffen oder dem gezielten Veröffentlichen entwendeter Informationen manifestiert. Das Ziel hierbei ist die Beeinflussung von gesellschaftlichen Akteurinnen und Akteuren sowie der Bevölkerung. Hacktivistinnen und Hacktivisten können sowohl Einzelpersonen oder Gruppierungen sein, die im Cyberraum aktiv Partei für eine Sache ergreifen oder systematisch Instabilität erzeugen wollen, als auch ausländische Nachrichtendienste, die in beiden Bereichen (Durchführung von Überlastungsangriffen und Veröffentlichung entwendeter Informationen) aktiv sind, um so ihre Ziele zu erreichen. Im Jahr 2024 kam es immer wieder zu hacktivistischen Angriffen auf Steueranlagen von Unternehmen der kritischen Infrastruktur oder auf Webseiten und Internetdienste von öffentlichem Interesse.

Den Hacktivistinnen und Hacktivisten geht es in erster Linie um die Aufmerksamkeit und Stimmung, die sie durch ihre Aktionen und deren mediale Veröffentlichung erzeugen können. Dafür ist es zunächst unerheblich, ob in eine Steueranlage eines Unternehmens tatsächlich aktiv eingegriffen werden konnte oder nur Screenshots der Steueranlage

veröffentlicht werden. Denn durch die geschickte Kombination von authentischen Screenshots mit anderen Darstellungen erwecken diese Akteurinnen und Akteure bereits den Eindruck, sehr tief in das System eines Unternehmens eingedrungen zu sein. Dies allein kann bereits ausreichen, um die angestrebte mediale Aufmerksamkeit zu erreichen.

Im Zuge der Nationalratswahl 2024 kam es zu einer länger andauernden Kampagne gegen österreichische Ziele im Cyberraum. Dabei kamen sogenannte DDoS-Angriffe (Distributed Denial of Service) zum Einsatz. Bei DDoS-Angriffen werden Server und Dienste durch massenhafte Anfragen gezielt überlastet, wodurch auch legitime Anfragen/Zugriffe nicht mehr möglich sind. Die meisten Überlastungsangriffe wurden erfolgreich abgewehrt, sodass diese in der breiten Öffentlichkeit wenig bis gar nicht wahrgenommen werden konnten. Lediglich wenige Seiten waren zeitweise nicht erreichbar, wobei zu keinem Zeitpunkt die Systeme der Wahlbehörden oder die verfassungsmäßige Durchführung der Nationalratswahl beeinträchtigt waren.

2 Internationale Entwicklungen


821439828
struct group_info init_groups = { .usage = ATO
struct group_info *groups_alloc(int gidsetsize
struct group_info *group_info\
int nblocks\
int i\
nblocks = (gidsetsize + NGROUPS_PER_BLOCK - 1
/* Make sure we always allocate at least one
nblocks =

2.1 Europäische Union (EU)

Die zunehmende Bedeutung der Cybersicherheit zeigte sich auch im Jahr 2024. 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 48 Sitzungen der HWP Cyber im Jahr 2024. 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[3], die Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der gesamten Union vorgibt, im Vordergrund,

3 Richtlinie (EU) 2022/2555

die primär im Zuge der NIS-Kooperationsgruppe bzw. deren Work-Streams erfolgten (siehe 2.1.2).

2024 wurden die Trilogverhandlungen sowie die anschließende sprachjuristische Prüfung der am 15. September 2022 vorgestellten Verordnung, des Cyber Resilience Acts (CRA) über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen, abgeschlossen. Der CRA soll für Hardware- und Softwareprodukte verbindliche Cybersicherheitsanforderungen 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. Der Rechtsakt wurde am 23. Oktober 2024 beschlossen, am 20. November 2024 im Amtsblatt der Europäischen Union veröffentlicht und ist seit 10. Dezember 2024 in Kraft, wobei die Vollanwendung der Bestimmungen erst ab 11. Dezember 2027 erfolgt.

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 sowie zur Vorbereitung und Reaktion auf Bedrohungen der Cybersicherheit und entsprechende Vorfälle (Cyber Solidarity Act oder CSoA) wurde dieses Jahr in zahlreichen Sitzungen bearbeitet und adaptiert – eine vorläufige Einigung diesbezüglich wurde Anfang 2024 erzielt. Diese wurde am 24. April 2024 in der ersten Lesung vom EP angenommen, die Annahme durch den Rat der Europäischen Union erfolgte am 2. Dezember 2024. 20 Tage nach der noch ausstehenden Veröffentlichung im Amtsblatt der Europäischen Union wird der Cyber Solidarity Act in Kraft treten. 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 Cybersicherheits-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 Anbieterinnen und 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 und groß angelegter 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[4] eingesetzt und dient der Unterstützung und Erleichterung der strategischen Zusammenarbeit sowie des Informationsaustausches zwischen den Mitgliedstaaten. Sie setzt sich aus Vertreterinnen und Vertretern der Mitgliedstaaten, der Europäischen Kommission und der 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 Mitgliedstaaten aufzubauen und die dringendsten Ergebnisse im Zusammenhang mit der Umsetzung der NIS-Richtlinie zu erarbeiten, hat

4 Richtlinie (EU) 2016/1148

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[5] als oberste Priorität an und betont gleichzeitig auch die Wichtigkeit von strategischen Diskussionen über wichtige Aspekte der Cybersicherheit in der EU, wie beispielsweise 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 2024 zu vier Plenarsitzungen und zu 20 Sitzungen im Rahmen ihrer Arbeitsbereiche (Workstream-Meetings). Neben den Entwicklungen, die in diesen verschiedenen Arbeitsgruppen in Hinblick auf die Umsetzung der NIS-2-Richtlinie[6] erreicht wurden, konnte vor allem auch eine Vielzahl an Hilfsdokumenten fertiggestellt werden, so etwa der Health-Action-Plan, eine einheitliche Methodologie zu Peer-Reviews und zwei Empfehlungen an die Kommission im Zusammenhang mit NIS2 Artikel 21(5) Durchführungsrechtsakt über Risikomanagementmaßnahmen bzw. NIS2 Artikel 23 Durchführungsrechtsakt über Meldepflichten. Außerdem wurde ein Referenzdokument über Risikomanagement-Maßnahmen erstellt, das die Cybersicherheitsbehörde durch technische Richtlinien zu den Sicherheitsmaßnahmen unterstützt.

Mehrere weitere Entwürfe befinden sich derzeit noch in Ausarbeitung, wie etwa eine Roadmap zum Übergang auf Post-Quanten-Kryptografie sowie NIS-Leitfäden für die zuständigen Behörden in den Bereichen „Gemeinsame Zusammenarbeit“ und „Zuständigkeiten“.

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 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 Part-

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

ner gerichtete hybride Bedrohungen und Kampagnen („EU Hybrid Toolbox“) entwickelt. Diesbezügliche Ratsschlussfolgerungen und Durchführungsleitlinien aus dem Jahr 2022 sehen unter anderem ein gemeinsames Lagebild, einen gemeinsamen Entscheidungsfindungsprozess sowie mögliche Antworten in Bezug auf hybride Bedrohungsakteurinnen und -akteure vor. Bei Cyberangriffen als Teil einer hybriden Kampagne wird das Vorgehen mit der HWP Cyber Issues koordiniert (siehe 2.1.1).

Um die Reaktionsfähigkeiten der EU auf hybride Bedrohungen zu verbessern, sieht der Strategische Kompass zudem die Schaffung von EU-Schnelleinsatzteams für hybride Bedrohungen (Hybrid Rapid Response Teams - HRRT) vor. Diese sollen sich auf einschlägige nationale und EU-interne zivile und militärische Fachexpertise, z. B. im Cybersicherheitsbereich, stützen, um EU-Mitgliedstaaten, Partnerländer sowie GSVP-Missionen und Operationen bei der Abwehr hybrider Bedrohungen zu unterstützen. Am 21. Mai 2024 wurde das Rahmenwerk für den Einsatz von HRRTs vom Rat angenommen. Im November 2024 erfolgte die Annahme der operativen Leitlinien sowie der dazugehörigen Profile für die Auswahl geeigneter Expertinnen und Experten.

2.1.4 EU-Zertifizierungsrahmen (Cybersecurity Act)

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. Anbieterinnen und Anbieter sowie Herstellerinnen und Hersteller von IKT-Produkten, -Diensten und -Prozessen können sich zukünftig freiwillig für eine 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 eine Cybersicherheitszertifizierung wesentlich dazu beitragen, das Vertrauen in IKT-Produkte, -Dienste und -Prozesse zu stärken und damit das ordnungsgemäße Funktionieren des digitalen Binnenmarktes zu 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 Bundesministerium für Finanzen (BMF) und das strategische NIS-Büro des Bundeskanzleramtes (BKA) vertreten. Die ECCG traf sich im Jahr 2024 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 unter anderem aus Vertreterinnen und Vertretern aus akademischen Einrichtungen, Verbraucherschutzorganisationen, Konformitätsbewertungsstellen, Organisationen, die Normen entwickeln, Unternehmen und Handelsverbänden zusammen und soll in strategischen Fragen der Cybersicherheitszertifizierung beraten.

Anfang 2024 hat die Europäische Kommission mit dem „European Union Common Criteria Scheme“ (EUCC) das erste europäische Schema für die Cybersicherheitszertifizierung angenommen. Die entsprechende Durchführungsverordnung ist am 27. Februar 2025 in Geltung getreten. Die Arbeiten zum „European Union Cybersecurity Certification Scheme on Cloud Services“ (EUCS), das die Zertifizierung von Clouddiensten zum Gegenstand hat, sowie zum „EU5G“, das die Cybersicherheit von 5G-Netzwerken zum Gegenstand hat, dauern nach wie vor an. Zu den umfangreichen Arbeiten im Bereich der Cybersicherheitszertifizierung von 5G-Netzen siehe Kapitel 2.1.5. Im Berichtszeitraum wurde die ENISA zudem mit der Ausarbeitung eines neuen Zertifizierungsschemas für „EU Digital Identity Wallets“ (EUDI) beauftragt. Mit der Änderung des Cybersecurity Acts wurde darüber hinaus die rechtliche Grundlage für ein „Europäisches Schema für die Cybersicherheitszertifizierung für verwaltete Sicherheitsdienste“ gelegt.

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 technischen Maßnahmen, die in der 5G-Toolbox vorgeschlagen wurden, konnte, 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 werden.

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 „Hochrisikolieferanten“, der 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, Herstellerinnen und 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 bzw. die Bundesministerin für Finanzen (BMF) aus Gründen der nationalen Sicherheit nach Befassung eines eigens eingerichteten Expertengremiums (des Beirats für die Sicherheit von elektronischen Netzen). Dieser legt dem zuständigen Bundesminister bzw. der Bundesministerin einen jährlichen Wahrnehmungsbericht.

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 vergangenen Jahr nach dem Nevers-Call (Treffen der EU-Telekomminister in Never und die anschließende Kommunikations-Note) vor allem mit dem Nevers Call Risk Assessment gearbeitet, in dem die Mitgliedstaaten dazu aufgefordert wurden, Abhängigkeiten von sogenannten „High Risk Vendors“ zu identifizieren und bestmöglich zu mitigieren. Hier zeigt sich, dass immer mehr Mitgliedstaaten schon präventive oder konkrete Maßnahmen, wie etwa besondere Genehmigungsverfahren oder Ausschluss von gewissen Herstellerinnen und Herstellern von Teilen der Netze oder gesamt, treffen.

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

2.1.6 Cyberdiplomatie

Die Cyber Diplomacy Toolbox der EU aus 2017 sieht diplomatische und politische Maßnahmen vor, wie im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik der EU (GASP) koordiniert auf Völkerrechtsverletzungen durch Cyberaktivitäten reagiert werden kann. Sie umfasst neben präventiven, kooperativen und stabilisierenden auch restriktive Maßnahmen. Letztere wurden 2020 erstmals im Rahmen des Cyber-Sanktionenregimes 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. Die Basis dafür bilden 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 2024 wurden die Werkzeuge der Cyber Diplomacy Toolbox insbesondere für einen besseren Informationsaustausch zu Cybervorfällen und gemeinsame Erklärungen („naming and shaming") genutzt: Die EU verurteilte in der Erklärung der EU-27 vom 3. Mai 2024 das fortgesetzte bösartige Verhalten der Russischen Föderation im Cyberraum. Am 29. Jänner 2024 bekundeten die EU-27 ihre Solidarität mit Australien, das von einem massiven Ransomware-Angriff auf den Gesundheitssektor betroffen war. Eine Solidaritätserklärung gab die EU auch am 25. März 2024 in Bezug auf die Reaktion des Vereinigten Königreichs auf Cyberangriffe aus China ab. Das Cyber-Sanktionenregime wird regelmäßig verlängert und erweitert. So wurden am 24. Juni 2024 sechs weitere Personen gelistet, darunter erstmals auch Cyberkriminelle für Ransomware-Angriffe auf essenzielle Dienste wie Gesundheit und Bankenwesen.

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 Akteurinnen und Akteure ist Teil der geopolitischen Polarisierung. Mit dem Anspruch einer EU-Führungsrolle auf internationaler und regionaler Ebene soll die EU-Vision für das globale, sichere, freie und offene Internet verankert und dabei sichergestellt werden, dass sich neue Technologien auf Menschen und den Schutz ihrer Privatsphäre fokussieren und ihr Einsatz rechtmäßig und ethisch korrekt erfolgt. Der vom Bundesministerium für europäische und internationale Angelegenheiten (BMEIA) 2021 eingesetzte Sonderbeauftragte für Cyber-Außenpolitik und Cybersicherheit konnte 2024 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) erlangte im Jahr 2024 nach intensiven Aufbauaktivitäten seine finanzielle Autonomie und bezog mit rund 30 Mitarbeitenden Büroräumlichkeiten in Bukarest in Rumänien. Damit ist es nun in der Lage, seinen Auftrag gemäß der Verordnung (EU) 2021/887 des Europäischen Parlaments und des Rates vom 20. Mai 2021 vollumfänglich 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 verantwortet und implementiert das EU-Finanzierungsprogramm „Digitales Europa (DEP)“[7] im Bereich der Cybersicherheit und wickelt das EU-Forschungsförderungsprogramm Horizont Europa im Bereich Cybersicherheit (Cluster 3) ab. 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. Dies erfolgt durch:

- Stärkung ihrer Führungsrolle im Bereich der Cybersicherheit, um das Vertrauen und die Sicherheit, einschließlich der Vertraulichkeit, Integrität und Zugänglichkeit von Daten, zu steigern;
- Förderung der Abwehrfähigkeit und Zuverlässigkeit der Netz- und Informationssysteme, darunter der kritischen Infrastruktur und gängiger Hard- und Software;
- 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.

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 wurde im Berichtszeitraum das Nationale Koordinierungszentrum (NCC) vom BKA in Kooperation mit der Österreichischen Forschungsförderungsgesellschaft (FFG) betrieben (siehe 3.9).

Der Verwaltungsrat (Governing Board) des ECCC fand sich im Jahr 2023 unter Teilnahme des Bundeskanzleramts vier Mal zusammen. Dabei erarbeitete das ECCC gemeinsam mit den Mitgliedstaaten einen Entwurf für das Arbeitsprogramm Cybersicherheit 2025 bis 2027 des EU-Förderprogrammes „Digitales Europa“ (DEP) entlang der 2023 verabschiedeten Strategischen Agenda und überführte die Arbeitsgruppen des ECCC-Verwaltungsrats in folgende neue Struktur: Es gibt nun Arbeitsgruppen zu 1. Community Building, 2. Boost application process, 3. International awareness, 4. Strategic advice, 5. Cyber Skills sowie 6. Cyber Hubs.

Das NCC nahm an Sitzungen des NCC-Netzwerkes und von ECCC-Arbeitsgruppen aktiv teil. Diese umfassten insbesondere die ECCC-Arbeitsgruppen zu Cybersecurity Skills (Nr. 5) und zur Einrichtung der Europäischen Kompetenzgemeinschaft (Nr. 1).

---

7 Verordnung (EU) 2021/694

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 beschaffen gemeinsam mit dem ECCC mit DEP-Mitteln Infrastruktur. Diese Projekte sollen in weiterer Folge bei der Durchführung des Cyber Solidarity Acts (siehe 2.1.1) unterstützen.

2.1.8 Cybersecurity Skills

Die Europäische Kommission hat am 18. April 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 Akteurinnen und Akteuren unterbreitet. Diese politische Willensbekundung wurde in den Ratsschlussfolgerungen zur Cyberabwehrpolitik im Mai 2023 durch die Mitgliedstaaten begrüßt. In der gemeinsamen Mitteilung wird die Gründung eines sogenannten EDICs (Europäisches Digitales Infrastrukturkonsortium) durch interessierte Mitgliedstaaten vorgeschlagen, um die Initiative zu implementieren und einen Beitrag zum Schließen der Fachkräftelücke im Bereich der Cybersicherheit zu leisten.

2.1.9 Cyberverteidigung

Im Rahmen der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP) der EU sieht der 2022 veröffentlichte Strategische Kompass der EU eine gemeinsame Stärkung der unionsweiten Sicherheit und Verteidigung vor, mit einem deutlichen Schwerpunkt auf den Cyberraum. Zur Stärkung der EU-weiten Kapazitäten und Fähigkeiten zur Cyberverteidigung wurde deshalb 2023 die von allen Mitgliedstaaten gemeinsam ausgearbeitete EU Cyber Defence Policy veröffentlicht. Diese verbindet bestehende Elemente der Cybersicherheit, unter Einbeziehung der Cyberverteidigungssektoren, auf nationaler und auf EU-Ebene. Die Cyber Defence Policy beruht auf den folgenden drei Säulen: Kooperation und Koordination innerhalb der EU, Sicherung des EU-Verteidigungssektors sowie Investitionen in Cyberabwehrfähigkeiten. Zur Verwirklichung werden zurzeit mehrere Maßnahmen umgesetzt.

Um die operative Kooperation und Koordination voranzutreiben, wird in den kommenden Jahren ein gemeinsames EU Cyber-Lage- und Koordinierungszentrum aufgebaut und ein Netzwerk für nationale militärische CERTs eingerichtet. Zur Stärkung der Interoperabilität und zur Vorbereitung auf Notfälle werden gemeinsame Normen und Standards etabliert und ein Rahmen zur Übung und Simulation von Cybervorfällen erstellt. Österreich beteiligt sich in diesem Zusammenhang unter anderem an den folgenden Projekten der EU-Verteidigungsinitiative „Permanent Structured Cooperation (PESCO)": Cyber Rapid Response Teams (CRRT), Cyber Ranges Federation (CRF) und Cyber and Information Domain Coordination Centre (CIDCC). Des Weiteren werden die gemeinsame strategi-

sche Vorausschau und Folgenabschätzung kritischer Cybertechnologien und emergenter Technologien ausgebaut, um auf zukünftige Bedrohungen besser vorbereitet zu sein.

Auch Österreich nimmt durch das Bundesministerium für Landesverteidigung (BMLV) und dem Österreichischen Bundesheer (ÖBH) an diesen und anderen Maßnahmen im Rahmen der GSVP teil und beteiligt sich aktiv an der Mitgestaltung der Cyberverteidigungspolitik der EU, zum Schutz des österreichischen und europäischen Cyberraums. Diese Vorhaben unterliegen dem Grundsatz der zivil-militärischen Zusammenarbeit, da militärische Mittel der Mitgliedstaaten die bestehenden Prozesse und Vorhaben zusätzlich ergänzen, um das Gesamtniveau der EU-weiten Cybersicherheit nachhaltig zu heben.

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 in zunehmender Intensität mit dieser Thematik. Die Staaten verfolgen in diesem Rahmen das Ziel, die aus der Nutzung von Informations- und Kommunikationstechnologie (IKT) 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 staatliches Verhalten im Cyberraum“ die Grundlage für die Arbeiten der neuen OEWG 2021 bis 2025. Diese hielt 2024 drei substanzielle sowie eine informelle Sitzung ab und einigte sich im Juli 2024 im Konsens auf den Dritten Jährlichen Fortschrittsbericht. Letzterer bildet gleichzeitig einen Fahrplan für die weitere Arbeit der Gruppe im vergangenen Jahr der OEWG 2025. Frankreich setzt sich gemeinsam mit einer überregionalen Gruppe von Staaten, darunter Österreich und die gesamte EU, für ein Aktionsprogramm der Vereinten Nationen zu Cybersicherheit ein. Dieses „UN Programme of Action“ zielt auf die Etablierung eines Mechanismus zur Förderung von praktischen Umsetzungsmaßnahmen ab. 2024 gelang die Einrichtung eines globalen Netzwerkes von nationalen Kontaktpersonen für Cybersicherheit nach Vorbild der OSZE, das als vertrauensbildende Maßnahme wirken soll.

Österreich brachte sich 2024 erneut insbesondere in den Beratungen über die verschiedenen Aspekte der Anwendung des Völkerrechts auf Cyberaktivitäten ein. Einen wertvollen Beitrag zu den Diskussionen zum Völkerrecht auf internationaler Ebene leistete Österreich durch die Veröffentlichung des nationalen Positionspapiers zur Anwendung des Völkerrechts auf Cyberaktivitäten im Mai 2024. Dabei wurde ein szenariobasierter, praktischer Ansatz gewählt, der in der internationalen Gemeinschaft auf großen Zuspruch stieß und Österreich eine Vorbildfunktion einnehmen ließ.

Im Herbst 2024 nahmen die Mitgliedstaaten außerdem den VN-Zukunftspakt an, der auf die Anstrengungen zur dringenden Bewältigung der zunehmenden und vielfältigen Cyberbedrohungen verweist.

In Vorbereitung auf den VN-Zukunftsgipfel im September 2024 wurden in der ersten Jahreshälfte in New York Verhandlungen über den VN-Pakt zu Fragen der digitalen Kooperation („Global Digital Compact“) durchgeführt. Der Pakt, der auch Bestimmungen zu Cybersicherheit enthält, wurde auf Ebene der Staats- und Regierungschefs als Annex zum Zukunftspakt am 22. September angenommen. In die Verhandlungen flossen auch zwei Resolutionen der VN-GV zu künstlicher Intelligenz sowie Empfehlungen des vom VN-GS seit 2023 eingesetzten High Level Advisory Board on Artificial Intelligence (HLAB AI) ein.

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 relevanten Akteurinnen und 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. Dem im Sommer 2022 durch den VN-GS eingerichteten, 15-köpfigen „IGF Leadership Panel“ gehörte 2022 bis 2024 auch die Bundesministerin für EU und Verfassung Karoline Edtstadler als einzige westliche Regierungsvertreterin an.

Cyberkriminalität hat sich rasch zu einer globalen und äußerst profitablen Verbrechenssparte entwickelt und war 2024 weltweit weiter im Steigen begriffen, u. a. in Form von Ransomware-Angriffen, Online-Betrug und Diebstahl von Kryptowährungen. Der Anstieg von Cyberkriminalität wurde 2024 quer durch alle Gremien thematisiert, einschließlich der Kommission für Verbrechensverhütung und Strafrechtspflege (CCPCJ). Das VN-Büro für Drogen- und Verbrechensbekämpfung (UNODC) in Wien ist eine tragende Säule der effektiven weltweiten Bekämpfung von Cyberkriminalität. Durch das „Global Programme on Cybercrime“ unterstützt UNODC Mitgliedstaaten beim Aufbau von Kapazitäten, der Prävention und Bewusstseinsschaffung in der Bekämpfung von Cyberkriminalität. Öster-

reich beteiligt sich seit 2020 mit freiwilligen Beiträgen an der Umsetzung von Initiativen in diesem Bereich.

Am 24. Dezember 2024 konnte die VN-GV die VN-Cybercrimekonvention im Konsens annehmen. Die Verhandlungen über den Text hatten von Februar 2022 bis August 2024 in Wien und New York stattgefunden. Österreich hat sich in den Verhandlungen zusammen mit seinen internationalen Partnerinnen und Partnern erfolgreich dafür eingesetzt, dass die VN-Konvention starke menschenrechtliche Bestimmungen enthält, um zu verhindern, dass sie von Staaten zur Legitimierung repressiver Maßnahmen missbraucht werden kann. Als Sekretariat für die Umsetzung der Konvention wird UNODC fungieren, womit die VN-Kompetenz im Zukunftsfeld der Cybersicherheit sowie auch der Amtssitz Wien weiter gestärkt werden. Die Konvention wird 2025 in Hanoi, Vietnam, zur Unterzeichnung aufliegen und tritt 90 Tage nach der Ratifizierung durch den 40. Mitgliedstaat in Kraft. Österreich wird sich gemeinsam mit Gleichgesinnten für einen effektiven, inklusiven und transparenten Umsetzungsmechanismus einsetzen.

Auch der VN-Menschenrechtsrat beschäftigt sich mit Cyberthemen, u. a. mit den (von Österreich unterstützten) Resolutionen zu Neuen Technologien und Menschenrechten, zur Sicherheit von Journalistinnen und Journalisten im digitalen Raum, zum Recht auf Privatsphäre im digitalen Zeitalter, zur Bekämpfung von Cyberbullying und zu „Technology-facilitated Gender-based Violence“.

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 von künstlicher Intelligenz auf die Menschenrechte. Die Resolution konnte im Konsens verabschiedet werden.

2.3 Organisation des Nordatlantikvertrages (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, Krisenprävention und -management sowie kooperative Sicherheit.

Als Reaktion auf die sich entwickelnde Cyber-Bedrohungslandschaft hat die NATO die Cyberverteidigung in ihren strategischen Rahmen integriert. Das Bündnis hat Mechanismen zur Erkennung, Prävention und Reaktion auf Cyberbedrohungen 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 Cyberverteidigungsfähigkeiten.

Die Cyber-Defence-Strategie der NATO umfasst Governance, Fähigkeitenaufbau und Zusammenarbeit mit internationalen Partnerinnen und Partnern sowie dem privaten Sektor. Die Governance-Struktur des Bündnisses erleichtert die politische, militärische und technische Koordination, wobei das Cyber Defence Committee (CDC) 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 Cyberverteidigungsbemühungen der NATO. Kooperative Initiativen mit der EU, den Vereinten Nationen (VN) und der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) sowie das Engagement mit Industrie und Wissenschaft verbessern die Kapazität des Bündnisses, Cyberbedrohungen effektiv zu adressieren. Das Engagement der NATO für ein freies, offenes und sicheres Umfeld für Cyberaktivitäten, ausgerichtet an internationalem Recht und Normen, untermauert den 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 Committee 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 Cyberverteidigung, der Prävention, Resilienz und Reaktion ausbalanciert, gewährleistet die Bereitschaft des Bündnisses, Cyberbedrohungen zu bekämpfen und abzumildern. Durch kontinuierliche Anpassung, Zusammenarbeit und Investitionen in Cyberfähigkeiten 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)

Als größte zwischenstaatliche Sicherheitsorganisation der Welt befindet sich die Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) im Bereich Cybersicherheit 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, engl. CBM) in Hinblick auf Cyberaktivitäten eine Vorreiter-

rolle. 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 der 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 umfassende 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 weiterhin einen besonderer Schwerpunkt bildeten.

2024 setzte die Cyber-IWG ihre Aktivitäten im Rahmen der „Adopt a CBM"-Initiative fort, im Zuge derer Staaten oder Staatengruppen die Umsetzung der VBM vorantreiben. Wichtige Schritte in diesem Zusammenhang sind die Einrichtung eines Netzwerkes von Kontaktpunkten, regelmäßige Überprüfungen der Kommunikationskanäle sowie die Unterstützung einer effektiven Zusammenarbeit im Falle einer Cyberkrise.

Im Rahmen der „Adopt a CBM"-Initiative treibt Österreich gemeinsam mit Belgien, Estland, Finnland, Italien und Schweden die Umsetzung der VBM 14 zu Public-Private-Partnerships (PPP) voran. PPP umfassen die Zusammenarbeit und den Informationsaustausch zwischen Unternehmen, der Wissenschaft und der öffentlichen Verwaltung und stellen einen Schlüsselfaktor für die Gewährleistung der Cybersicherheit und Cyberresilienz dar.

2024 riefen die VBM-14-Koadoptoren eine neue Veranstaltungsreihe ins Leben, um tiefergehende Einblicke in die jeweiligen nationalen Ansätze zur Umsetzung zu geben. Österreich machte mit einem Side-Event des BMEIA und BKA am 4. November 2024 den Auftakt und stellte verschiedene Aspekte der Umsetzung von PPP im österreichischen Cyberökosystem vor. Als zentrale PPP-Plattform wurde den OSZE-Teilnehmerstaaten die Cyber-Sicherheit-Plattform (CSP) präsentiert. Weiters gab es Vorträge zum nationalen CERT, der Austria Cyber Security Challenge (CTF-Wettbewerb als Maßnahme zum Kapazitätenaufbau/Nachwuchsförderung), der Arbeitsgruppe zu Coordinated Vulnerability Disclosure (CVD) und den Bildungsaktivitäten der „Epicenter.Academy".

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 jährliche Cybersicherheitskonferenzen ab. Im Jahr 2024 fand diese Konferenz mit dem Schwerpunktthema „Stärkung der nationalen Cyberresilienz“ im Vorsitzland Malta 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. 2024 wurde das Dokument zu „Safe Harbours and Guidance for Vulnerability Researchers“ zur Veröffentlichung freigegeben. Auch wurde beschlossen, 2025 „guiding principles for vulnerability researchers“ zu erarbeiten.

2.6 Europarat

Den Kern der Aktivitäten des Europarates im Bereich Cybersicherheit bildet die „Budapest-Konvention“ aus dem Jahr 2001, die mit aktuell 78 Ratifikationen und laufend neuen Beitritten eine Bedeutung weit über Europa hinaus erlangt hat. Hauptzweck ist die Verfolgung einer gemeinsamen Strafrechtspolitik zum Schutz der Gesellschaft vor Cyberkriminalität, insbesondere durch entsprechende gesetzliche Regelungen und die Förderung internationaler Zusammenarbeit. Die Konvention wurde um zwei Zusatzprotokolle erweitert. Seit 2006 ist das erste Zusatzprotokoll betreffend die Kriminalisierung von rassistischen und fremdenfeindlichen Handlungen durch Computersysteme in Kraft. Österreich hat 2003 unterzeichnet. Seit 12. Mai 2022 liegt das zweite Zusatzprotokoll zur Budapest-Konvention zur Unterzeichnung auf, das sich mit internationaler Rechtshilfe und dem damit verbundenen grenzüberschreitenden Zugang zu elektronischen Beweismitteln befasst. Es wurde bislang von 46 Staaten, darunter Österreich, unterzeichnet sowie von zwei Staaten ratifiziert. 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 2024 gemeinsame Europarats- und EU-Projekte unterstützt. „Cyber South+" und „Cyber East+" zielen darauf ab, die Strukturen in der südlichen und östlichen Nachbarschaft Europas zu verbessern. Seit 2023 läuft, aufbauend auf ein früheres Projekt, das weltweit agierende Projekt „GLACY-e" mit Fokus auf den Kapazitätsaufbau in Afrika, Asien/Pazifik und Lateinamerika. 2024 wurden Projekte zur Erleichterung der Umsetzung des zweiten Zusatzprotokolls zur „Budapest-Konvention" sowie zu elektronischen Beweismitteln neu gestartet. Diese sind CyberSPEX, mit Fokus auf die Kooperation zwischen EU-Mitgliedstaaten und sonstigen Vertragsstaaten der „Budapest-Konvention", CyberSEE, mit Fokus auf Südosteuropa und die Türkei, sowie CyberUA, zur Stärkung der Kapazitäten betreffend elektronische Beweismittel zu Kriegsverbrechen und schweren Menschenrechtsverletzungen in der Ukraine.

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.

Seit 2012 wurden zudem bislang 13 Leitfäden (Guidance Notes) zur Budapest-Konvention erarbeitet und veröffentlicht. Diese sollen den Vertragsstaaten die effektive Anwendung und Umsetzung erleichtern.

Am 5. September 2024 wurde die Rahmenkonvention zu künstlicher Intelligenz und Menschenrechte, Demokratie und Rechtsstaatlichkeit des Europarates in Vilnius zur Unterzeichnung aufgelegt. 14 Unterzeichnungen gibt es bisher, darunter die EU für ihre 27 Mitgliedstaaten.

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 Netzwerk der Computer-Security-Incident-Response-Teams (CSIRTs-Netzwerk oder CNW) wurde durch die EU-Richtlinie 2016 / 1148 (NIS-1-Richtlinie) geschaffen, welche dessen Tätigkeitsbereich festgelegt. Die EU-Richtlinie 2022 / 2555 (NIS-2-Richtlinie) hat, basierend auf den Erfahrungen der ersten Jahre, die Aufgaben des CNW etwas erweitert.

Das CSIRTs-Netzwerk setzt sich aus Vertreterinnen und Vertretern der CSIRTs der Mitgliedstaaten und dem CERT der EU-Institutionen (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, Austrian Energy CERT (AEC) und das Austrian HealthCERT (AHC) vertreten.

Das Netzwerk arbeitet primär online, die vertretenen CSIRTs kooperieren laufend miteinander. Auf freiwilliger Basis werden Informationen zu relevanten Sicherheitsvorfällen ausgetauscht und Erkenntnisse zur Sicherheit von Netz- und Informationssystemen erörtert.

Die Treffen des CNW dienen dem Informationsaustausch bezüglich der Dienste, Tätigkeiten und Kooperationsfähigkeiten der CSIRTs. 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. 2024 fanden diese Treffen im Jänner in Brüssel, im Mai in Gent und im September in Budapest statt. Im Juni 2024 wurde die vertiefte Zusammenarbeit, sowohl im Tagesgeschäft als auch bei größeren Vorfällen, im Rahmen der Übung Cyber Europe 2024 geprobt.

2.8 Andere Gremien, Foren und Initiativen

Freedom Online Coalition

Die „Freedom Online Coalition“ ist eine informelle Gruppierung 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 42 Mitgliedstaaten umfasst.

International Counter Ransomware Initiative

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 knapp 70 Mitgliedern zählen vor allem gleichgesinnte Staaten, aber auch Organisationen wie Interpol und die 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 vier Gipfeltreffen in Washington, zuletzt zwischen 30. September und 3. Oktober 2024. 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 ein: International Counter Ransomware Task Force (ICRTF), Policy Pillar und Diplomacy and Capacity Building Pillar.

Österreich setzt sich für eine Einbindung der Westbalkanstaaten (von denen bislang nur Albanien Mitglied ist) in die Initiative ein. Das BMEIA veranstaltete dazu gemeinsam mit dem Bundeskriminalamt am 6. Juni 2024 einen Workshop für die Westbalkanstaaten in Wien, um diesen die CRI näherzubringen. An der Veranstaltung nahmen Vertreterinnen und Vertreter von Bosnien und Herzegowina, Kosovo, Nordmazedonien und Serbien teil. Vertreterinnen und Vertreter des US-amerikanischen Außenministeriums und des FBI stellten die CRI vor und Albanien präsentierte seine Erfahrungen als bislang einziges regionales Mitglied der CRI.

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

Die Verbreitung und der Missbrauch von Spionagesoftware stellen eine steigende Sicherheitsbedrohung dar. Daher hat sich Österreich am 22. September 2024 dem von den USA initiierten Joint Statement zum Thema angeschlossen, das ein Bekenntnis zu folgenden Themen umfasst: Verhütung des Exports von Software, Technologie und Ausrüstung an Endabnehmerinnen und -abnehmer, die Güter für bösartige Cyberaktivitäten nutzen; Informationsaustausch; Zusammenarbeit mit Partnerinnen und Partnern in Industrie und Zivilgesellschaft in Hinblick auf Bewusstseinsbildung und Standard-Setting; und internationales Engagement. Besonders häufig werden Journalistinnen und Journalisten, Juristinnen und Juristen sowie Menschenrechtsverteidigerinnen und Menschenrechtsverteidiger Opfer des Missbrauchs derartiger Werkzeuge. Ein von Österreich mitunterstütztes Side-Event am 4. Oktober 2024 am Rande der 57. Sitzung des VN-Menschenrechtsrates widmete sich dieser Thematik.

3 Nationale Akteure

3.1 Verfassungsschutzrelevante Cybersicherheit

Die Direktion Staatsschutz und Nachrichtendienst (DSN) fungiert als operative Koordinierungsstelle für Meldungen und Anfragen zu Angriffen auf Systeme und Infrastrukturen von verfassungsmäßigen Einrichtungen sowie auf Systeme von Unternehmen der kritischen Infrastruktur. Hierfür bedient sich die DSN eines breiten Spektrums an Fähigkeiten und Techniken, wie beispielsweise Cyber Threat Intelligence, Malware Analysis und Reverse Engineering. Im Zuge der Tätigkeit ergibt sich die Taxonomie und Beschäftigung mit neuen Phänomenen im Cyberbereich und die Reaktion auf aktuelle Trends. Um einen Erfahrungs- und Wissensaustausch zu ermöglichen und zu fördern, setzt die DSN auf die Zusammenarbeit mit Strafverfolgungsbehörden und der Cybersicherheitscommunity, zu der Stakeholder aus Wirtschaft und Forschung zählen. Ziel ist es, gemeinsam die Resilienz und die Kommunikation im Bereich der Cybersicherheit zu fördern. Ebenso findet ein Austausch mit ausländischen Sicherheitsbehörden statt, um die eigenen Erkenntnisse zu teilen und eine globale Sicht auf Bedrohungen zu gewinnen.

Im Berichtsjahr 2024 wurden unterschiedliche verfassungsschutzrelevante Phänomene behandelt. Diese stellen Weiterentwicklungen von bereits in der Vergangenheit behandelten Bedrohungen dar. Dies sind vor allem Advanced Persistent Threat (APT), Hacktivistinnen und Hacktivisten, Private-Sector-Offensive-Actors (PSOA) und Ransomware-Gruppierungen. Sie stellen die nachrichtendienstliche Bearbeitung des Aufgabenspektrums Cybersicherheit vor anhaltende und dynamische Herausforderungen. Zusätzlich spielen auch geopolitische Konflikte eine große Rolle in der Cyberdomäne.

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 Bezirks- bzw. Regionalebene stehen Cybercrimeermittlerinnen und -ermittler sowie Cybercrimeforensikerinnen und -forensiker als erste Ansprechpersonen zur Verfügung.

Im Jahr 2024 erfolgte die Umstrukturierung des C4 mit einer Erweiterung der Ressourcen und gliedert sich nun wie folgt:

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-Forensik sowie die Automotive-IT.

3.2.3 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 Schadenspotenzial 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 Internetdienstanbieterinnen und -anbietern 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 und Innovation

Aufgabe ist die Unterstützung von digitaler Forensik und digitalen Ermittlungen mit wissenschaftlicher Expertise sowie die bedarfsorientierte Entwicklung von Tools und Skripten, die international auch für andere Strafverfolgungsbehörden zur Verfügung 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 Direktion 6 – IKT & Cyber – führt die Cyberkräfte des Österreichischen Bundesheeres (ÖBH). Die Cyberkräfte umfassen die IKT-Truppe, die Cyber-Truppe und die Elektronischer Kampf (EloKa)-Truppe. Das sind jene Elemente im ÖBH, welche die anderen Teilstreitkräfte (Land und Luft), aber auch alle Führungsebenen miteinander verbinden und damit die Kommunikations- und Führungsfähigkeit herstellen. Sie beobachten und bewerten die Lage im Cyberraum, ergreifen alle erforderlichen Maßnahmen zum Schutz der militärischen Netze und stehen auf Anforderung gesamtstaatlich bereit. Die Cyberkräfte sind dafür verantwortlich, dass jede Art der Kommunikation und Datenübertragung im ÖBH in eigenen Netzwerken reibungslos stattfinden kann. Sie sorgen permanent für die Informationshoheit und Kontrolle über die eigenen Systeme. Im Einsatz ist es überlebenswichtig, dass sichere Verbindungen bestehen und Informationen schnell und sicher zur richtigen Zeit am richtigen Ort sind. 2024 konnten die Restrukturierungsmaßnahmen im BMLV abgeschlossen werden und somit wurde die Direktion 6 in die Neustruktur des Ressorts übergeleitet.

Organisatorisch besteht die Direktion IKT & Cyber aus den drei Abteilungen

- IKT & Cyber Planung (IKTCyPl),
- IKT & Cyber Einsatz (IKTCyE) und
- IKT Bereitstellung und Nutzungsmanagement (IKTBstg&NuMngt).

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

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

Die **Abteilung IKTBstg&NuMngt** nimmt neben Digitalisierung, Architekturentwicklung sowie Informations- und Wissensmanagement auch die Einsatzkoordination und -auswertung sowie die Aufgabe des Kampfes im Informationsumfeld (psychologische Kampfführung) wahr.

Neben den angeführten Abteilungen sind fünf Fachbereiche im IKT & Cyber-Sicherheitszentrum zusammengefasst, die sich primär mit der Umsetzung der planerischen Vorgaben und der Implementierung beschaffter Systeme beschäftigen. Die Mitarbeiterinnen und Mitarbeiter des IKT & Cyber-Sicherheitszentrums 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 Beiträgen zur 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 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, das gesamtstaatliche und auch nachrichtendienstliche Informationen zur Cyberbedrohungslandschaft 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 Teams (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 und ist an zahlreichen nationalen und europäischen Forschungsprojekten 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-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.

Das Austrian HealthCERT wurde durch einen Beschluss der Bundes-Zielsteuerungskommission zur Stärkung der Cybersicherheitskompetenz des Gesundheitssektors gegründet und ist seit November 2024 als sektorenspezifisches CERT benannt. Zusätzlich ist das Austrian HealthCERT im Gesundheitstelematikgesetz rechtlich verankert.

Zu den Hauptaufgaben zählen die Beobachtung und Analyse von Cybersicherheitsbedrohungen sowie die Bearbeitung von Meldungen zu Sicherheitsvorfällen mit Bezug zum Gesundheitssektor. Darauf aufbauend werden Warnungen und Handlungsempfehlungen zeitnahe bereitgestellt.

Ergänzend zu diesen Leistungen agiert das Austrian HealthCERT als nationale und EU-weite Informationsdrehscheibe und erbringt damit einen wichtigen Beitrag zur Erhöhung der Resilienz des Gesundheitssektors gegenüber Cyberbedrohungen.

Gemeinsam erfüllen die vier 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)-Netzwerks der EU (siehe 2.7). Die genannten vier 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 vier 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 Betreiberinnen und Betreiber wesentlicher Dienste sowie Anbieterinnen und 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, 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 2024 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 Kapitel 2.1). Ein Schwerpunkt bildete dabei die Koordinierung und Vertretung der österreichischen Position in den Verhandlungen zum Cyber Resilience Act sowie zur Umsetzung der NIS-2-Richtlinie.

3.8 Operative Netz- und Informationssystemsicherheit - Abteilung IV/S/2 - Netz- und Informationssystemsicherheit (NIS)

Mit 1. Juli 2022 wurde die Abteilung IV/S/2 – Netz- und Informationssystemsicherheit (NIS) im Bundesministerium für Inneres eingerichtet. Die Abteilung und ihre nachgeordneten Referate erfüllen die Funktion der operativen NIS-Behörde für Österreich. Diese Tätigkeit umfasst ein breites Spektrum an Aufgabenstellungen, deren wesentliche Zielsetzung die Sicherstellung des Sicherheitsniveaus von Betreiberinnen und Betreibern wesentlicher Dienste nach dem NISG idgF und die Erhöhung der gesamtstaatlichen Resilienz in Österreich ist.

Im Jahr 2024 wurden umfangreiche organisatorische Vorbereitungsmaßnahmen in Erwartung der nationalen Umsetzung der europäischen Richtlinie 2022/2555 im Netz- und Informationssystemsicherheitsgesetz 2024 (NISG 2024) gesetzt. Ziel der diesbezüglichen Aktivitäten war die Planung und Schaffung einer neuen Organisationseinheit, die künftig die Funktionen sowohl der operativen als auch der strategischen NIS-Behörde, des Nationalen Koordinierungszentrums Cybersicherheit (NCC-AT) und des nationalen Cyber-Hubs für Österreich[8], wahrnehmen sollte. Aufgrund der vorläufigen Nicht-Annahme des Entwurfs zum NISG 2024 mussten diese Maßnahmen gestoppt und teilweise rückabgewickelt werden.

8 Ein nationaler Cyber-Hub ist eine Einrichtung, die laut dem EU-Rechtsakt zur Cybersolidarität (EU Cyber Solidarity Act) von allen Mitgliedstaaten implementiert werden kann und dessen Aufgabe es ist, Informationen zu Cyber-Bedrohungen und -Vorfällen zu erkennen, zu aggregieren, zu analysieren und an Bedarfsträgerinnen und -träger weiterzugeben. Das Europäische Cybersicherheitswarnsystem (European Cybersecurity Alert System) soll ein europaweites Netzwerk nationaler und grenzüberschreitender Cyber-Hubs werden.

Im Zentrum der Tätigkeiten der Abteilung steht derzeit – wie bisher – die behördliche Aufsicht über die Umsetzung der Vorgaben des Netz- und Informationssystemsicherheitsgesetzes (NISG) durch Betreiberinnen und Betreiber wesentlicher Dienste, Anbieterinnen und Anbieter digitaler Dienste sowie Einrichtungen der öffentlichen Verwaltung. Unter NIS 1 wurden ca. 100 Unternehmen bzw. Organisationen, die wesentliche Dienste erbringen, identifiziert.

Darüber hinaus nimmt die Abteilung eine koordinierende Rolle innerhalb der gesamtstaatlichen Operativen Koordinierungsstruktur (OpKoord) und ihres Inneren Kreises der Operativen Koordinierungsstruktur (IKDOK) wahr und unterstützt darüber hinaus die dem NISG unterworfenen Entitäten im Bereich der Bewusstseinsbildung (Awareness) hinsichtlich möglicher Bedrohungen im Cyberraum.

Ebenfalls in der operativen NIS-Behörde ist das Programm zur Umsetzung des EU-Cybersicherheitspakets 2020 und 2023 angesiedelt. Das Bundesministerium für Inneres verfolgt eine schnelle und vollständige Umsetzung, um die gesamtstaatliche Cyber-Resilienz Österreichs zu erhöhen und einen effizienten Aufgabenvollzug sicherzustellen. Im Programm sind insbesondere Projekte zur Optimierung des Vollzugs im Zusammenhang mit Meldevorgängen und dem Informationsaustausch bzw. Informationsfluss sowie Projekte zu technischen Vorhaben, z. B. der Aufbau eines Sensornetzwerkes in Österreich, gebündelt. Im Programm koordiniert werden die Kommunikationsmaßnahmen, die notwendig sind, um weitreichend über Vorhaben und deren Inhalte zu informieren. Parallel dazu betreut das Programm auch Agenden in Zusammenhang mit neuen EU-Rechtsakten im Bereich der Cybersicherheit, die aus operativer Sicht in Österreich umzusetzen sein werden.

Die Arbeit der operativen NIS-Behörde ist organisatorisch auf drei Referate verteilt.

3.8.1 Referat IV/S/2/a (Recht und Audit)

Das Referat IV/S/2/a (Recht und Audit) erfüllt einen wesentlichen Teil der Aufgabenstellungen der operativen NIS-Behörde. Die Hauptaufgaben umfassen folgende Bereiche:

- Regelmäßige Überprüfung der Umsetzung verpflichtender Sicherheitsmaßnahmen bei den dem NISG unterstellten Unternehmen und Organisationen
- Anlassbezogene Überprüfung dieser Umsetzungen durch die Behörde im Rahmen von Einschauen
- Sicherstellung des notwendigen Sicherheitsniveaus durch Aussprechen von Empfehlungen und bescheidmäßigen Anordnungen
- Verfahrensführung im Rahmen des NISG
- Feststellung der mit der Durchführung der Überprüfungen beauftragten qualifizierten Stellen
- Allgemeine und sektorspezifische Risikoanalysen
- Teilnahme an Arbeitsgruppen auf nationaler und internationaler Ebene

Im Rahmen der behördlichen Aktivität werden auch Empfehlungen und bescheidmäßige Anordnungen zur Umsetzung oder Anpassung von Sicherheitsvorkehrungen ausgesprochen. In den vergangenen Jahren gab es rund 2.300 Empfehlungen. Im Fokus standen vor allem Themen der technischen Umsetzung, z. B. im Bereich der „Sicherheitsarchitektur", „Systemwartung" oder das „Erkennen von und die Reaktion auf Vorfälle" sowie der organisatorischen Rahmenbedingungen, z. B. im Bereich der „Risikoanalyse" oder des „Umgangs mit Dienstleisterinnen und Dienstleistern, Lieferantinnen und Lieferanten sowie Dritten".

Zu den Aufgaben des Referats zählt auch das Einbringen von Sachverhaltsdarstellungen an Verwaltungsstrafbehörden. Der überwiegende Teil der Sachverhaltsdarstellungen beruhte auf Fristversäumnissen und Feststellungen von Nicht-Umsetzungen von Sicherheitsmaßnahmen im Sinne des NISG und der Netz- und Informationssystemsicherheitsverordnung (NISV).

3.8.2 Referat IV/S/2/b (Cyberlagezentrum, Prävention, Kommunikation)

Das Referat IV/S/2/b (Cyberlagezentrum, Prävention, Kommunikation) vereint eine Vielzahl von Aufgaben innerhalb der operativen NIS-Behörde. Ein Schwerpunkt liegt auf der ressortinternen und ressortübergreifenden Koordination sowie auf der Erstellung des gesamtstaatlichen Cyberlagebildes. Zudem werden IKDOK- und OpKoord-Lagebilder sowie Sonderlagebilder regelmäßig erstellt und den Bedarfsträgerinnen und Bedarfsträgern innerhalb des Bundesministeriums für Inneres sowie den anderen Ressorts, den Betreiberinnen und Betreibern kritischer Infrastruktur und wesentlicher Dienste zur Verfügung gestellt. Um die Qualität der Arbeit und die Akzeptanz der Partnerinnen und Partner sicherzustellen, wird laufend ein Feedback von der jeweiligen Zielgruppe eingeholt. Darüber hinaus werden Beiträge zu Cybersicherheit für andere ressortinterne Lagebilder erstellt.

Zudem wird die „Meldesammelstelle“ und der „Single Point of Contact“ – als zentrale Anlaufstelle für NIS-Behörden anderer Mitgliedstaaten der EU – vom Referat betreut. Ein wesentlicher Bestandteil dieser Tätigkeit ist die Analyse und Weiterverarbeitung der einlangenden Pflicht- und Freiwilligenmeldungen.

Die Zahl der Pflicht- und Freiwilligenmeldungen wächst stetig an. 2020 sind 36 Meldungen eingelangt, im Jahr 2024 stieg die Zahl auf 168 Meldungen.

Abbildung 10: Übersicht Meldungsaufkommen: Pflichtmeldungen und Freiwillige Meldungen von 2020 bis 2024

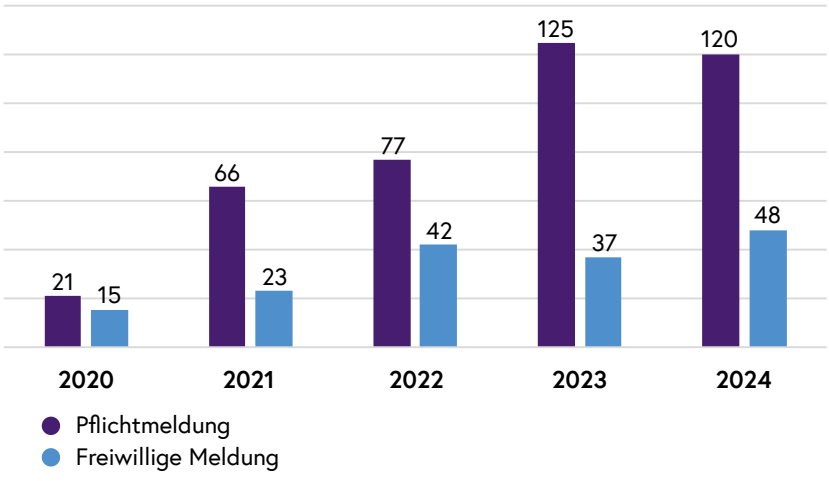


Abbildung 10: Übersicht Meldungsaufkommen: Pflichtmeldungen und Freiwillige Meldungen von 2020 bis 2024

Der Fachbereich Awareness im Referat IV/S/2/b ist für die Planung, Koordination und Durchführung von Awarenessveranstaltungen, Workshops und Beratungen bei Betreiberinnen und Betreibern wesentlicher Dienste, Anbieterinnen und Anbietern digitaler Dienste, Einrichtungen der öffentlichen Verwaltung und weiteren Unternehmen oder Organisationen sowie für die Konzeption und Erstellung von Unterlagen und Publikationen verantwortlich.

Im Jahr 2024 wurden 82 Awarenessveranstaltungen bzw. -beratungen mit einer durchschnittlichen Bewertung (Schulnoten) von 1,08 durchgeführt.

Auch Aufgaben auf nationaler sowie auf EU-Ebene im Bereich der operativen Cybersicherheit werden vom Referat IV/S/2/b wahrgenommen. Hierzu zählen die Abhaltung regelmäßiger bzw. anlassbezogener Sitzungen der operativen Koordinierungsstrukturen gemäß NISG sowie die Kooperation im Rahmen von EU-CyCLONe (European Cyber Crisis Liaison Organisation Network) zur Bewältigung großer, grenzüberschreitender Cybersicherheitsvorfälle mit Vertreterinnen und Vertretern der EU-Mitgliedstaaten.

3.8.3 Referat IV/S/2/c (NIS Technische Einrichtungen)

Das Referat IV/S/2/c (NIS Technische Einrichtungen) ist die technische Fachstelle der operativen NIS-Behörde. Das Referat konzipiert und begleitet die Entwicklung spezifischer IKT-Lösungen, die zur Erfüllung der Anforderungen des NIS-Gesetzes erforderlich sind, sowie IT-Anwendungen, die die operative NIS-Behörde gezielt in ihren Aufgaben unterstützen.

Zu den IKT-Lösungen nach dem NISG zählen unter anderem:

Meldeanalysesystem: Zur Analyse von Meldungen zu Cybersicherheitsvorfällen kümmert sich das Referat um den technischen Betrieb eines Meldeanalysesystems (§ 11 NISG). Dieses reichert eingehende Meldungen zu Cybersicherheitsvorfällen mit Informationen aus Open Source Intelligence (OSINT) an und unterstützt die Erstellung von Lagebildern zur Cybersicherheitslandschaft in Österreich.

IOC-Frühwarnsystem: Das Referat ist verantwortlich für die Konzeption, den Aufbau sowie den kontinuierlichen fachlichen Betrieb eines IOC-Frühwarnsystems (§ 13 NISG). Indicators of Compromise (IOCs) sind erkennbare Merkmale oder Spuren, die auf eine potenzielle oder bereits erfolgte Sicherheitsverletzung hinweisen. Das IOC-Frühwarnsystem dient der frühzeitigen Erkennung und Analyse von sicherheitsrelevanten Vorfällen in den IT-Infrastrukturen der NIS-Normunterworfenen, die hauptsächlich österreichische Unternehmen der kritischen Infrastruktur sind.

Zur Unterstützung der operativen Tätigkeiten der NIS-Behörde entwickelt und betreibt das Referat verschiedene IKT-Lösungen, darunter Anwendungen zur Verwaltung von

Stammdaten und Prüfberichten. Zudem ist das Referat für den Aufbau der erforderlichen IT-Infrastruktur sowie die Verwaltung der Schnittstellen zu anderen BMI-Anwendungen und für den technischen Input im European Network of SOC (ENSOC) verantwortlich.

ENSOC ist ein von der Europäischen Union gefördertes Projekt, das einen grenzüberschreitenden Cyber-Hub entwickelt. Dieser Hub ermöglicht den Austausch von Cyber Threat Intelligence (CTI) mit derzeit sechs anderen EU-Mitgliedstaaten.

3.9 Nationales Koordinierungszentrum für 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 vor Cyberbedrohungen zu schützen. Zudem soll die Exzellenz in der Forschung gesichert und die Wettbewerbsfähigkeit der europäischen Industrie ermöglicht werden.

Das Bundeskanzleramt setzte das NCC-AT in Kooperation mit der Österreichischen Forschungsförderungsgesellschaft (FFG) um und erfüllte 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.

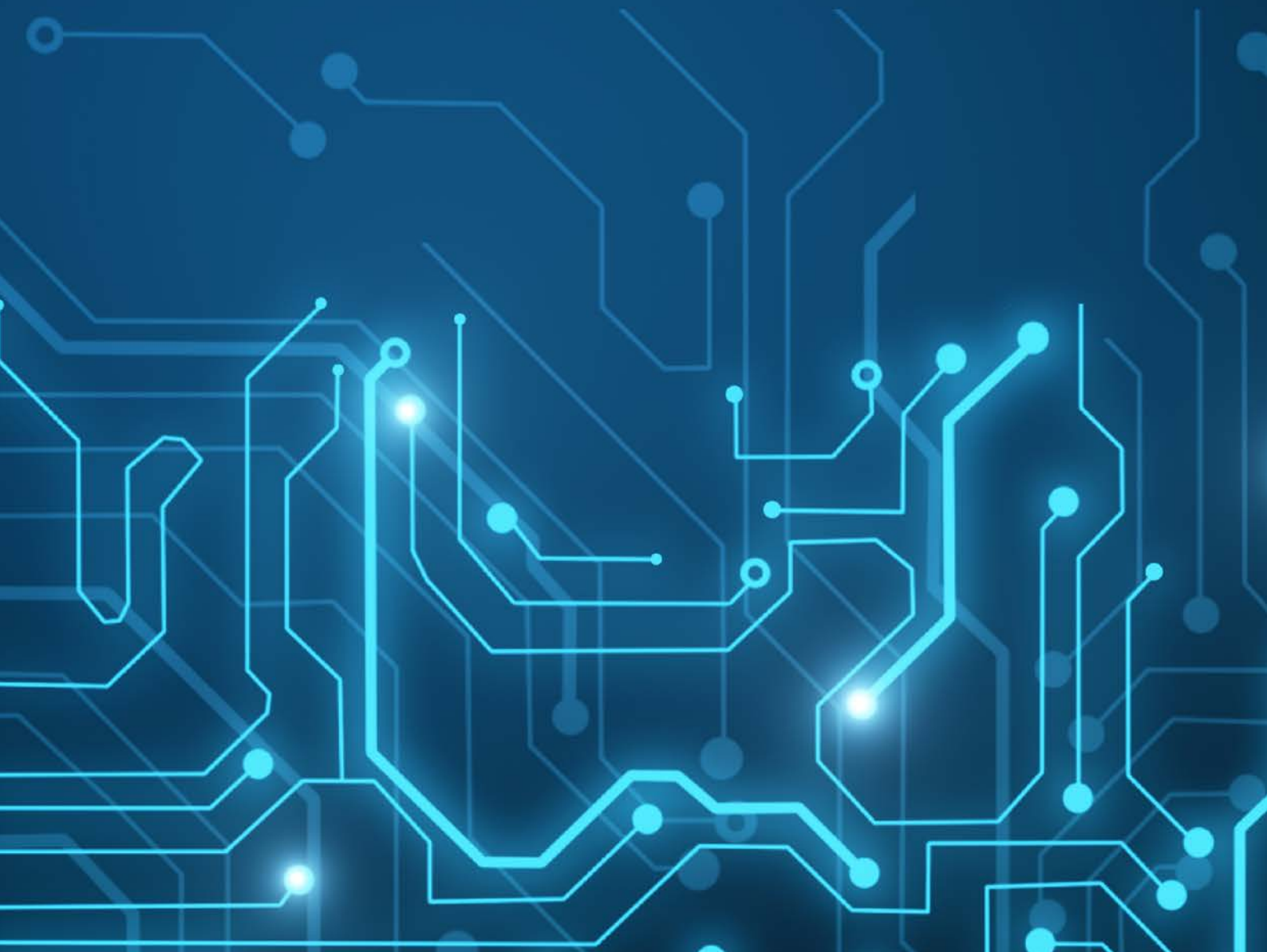
Der Auf- und Ausbau des NCC-AT und die Umsetzung eines in dem Zusammenhang stehenden EU-Projektes standen 2024 im Fokus und bildeten die Basis für folgende Aktivitäten:

- 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),
- zweite Ausschreibungsrunde der FFG-Förderschiene „Cyber Security Schecks“ in Höhe von zwei Millionen Euro zur Unterstützung von kleinen und mittleren Unternehmen (KMU), insbesondere im Anwendungsbereich der NIS-2-Richtlinie bei der Umsetzung von technischen Cybersicherheitslösungen,
- Online-Veranstaltung „NCC-AT Community Event“: Wege zur effektiven Cybersicherheit für KMU in Kooperation mit der Wirtschaftskammer Österreich (WKÖ),

- Einrichtung eines NCC-AT Beirates,
- Vernetzungstätigkeiten auf europäischer und nationaler Ebene sowie
- Mitwirkung an strategischen Arbeiten im NCC-Netzwerk und in ECCC-Arbeitsgruppen.

Diesbezüglich wird auf das Kapitel 2.1.7 verwiesen.

4 Nationale Strukturen



4.1 Innerer Kreis der Operativen Koordinierungs-strukturen (IKDOK)

Das Netz- und Informationssicherheitsgesetz (NISG) stellt die Grundlage zur ressortübergreifenden Zusammenarbeit im Bereich der Sicherheit von Netz- und Informationssystemen in Österreich dar. Dieses Gesetz ist damit die Rechtsgrundlage für die Operative Koordinierungsstruktur (OpKoord) und den Inneren Kreis der Operativen Koordinierungsstruktur (IKDOK). Der IKDOK setzt sich aus Vertreterinnen und Vertretern des Bundesministeriums für Inneres (Operative NIS-Behörde – IV/S/2, Direktion Staatsschutz und Nachrichtendienst — DSN, Cybercrime Competence Center – C4), des Bundeskanzleramts (Büro für strategische Netz- und Informationssystemsicherheit – I/8, GovCERT), des Bundesministeriums für europäische und internationale Angelegenheiten (BMEIA) sowie des Bundesministeriums für Landesverteidigung (Abwehramt – AbwA, Direktion IKT & Cyber, Heeres-Nachrichtenamt – HNaA) zusammen. Die Abteilung IV/S/2 des BMI übernimmt dabei administrative und koordinierende Aufgaben des Gremiums und leitet die Sitzungen.

Die anlassbezogen bzw. 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 sind die Erfassung und Bewertung eines monatlichen Lagebildes über Risiken, Vorfälle und Sicherheitsvorfälle, die Erstellung von situativen Lagebildern, der regelmäßige Austausch sowie die 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.

Auswahl von Tätigkeiten des IKDOK für das Jahr 2024

Die Arbeit von OpKoord und IKDOK findet im Rahmen von wöchentlichen Jour Fixes (online) und monatlichen Lagebildsitzungen (in Präsenz) statt. Im Beobachtungszeitraum wurden folgende Sitzungen abgehalten:

- 45 IKDOK Jour Fixes,
- zwölf Lagebild-Sitzungen und
- zehn Fragestunden mit den Bundesländern zu den aktuellen Lagebildern.

Gemäß seiner primären Aufgabenstellung wurden in diesem Zusammenhang 26 anlassbezogene bzw. regelmäßige Lagebilder erstellt, die sich wie folgt gliedern:

- Zwölf IKDOK Lagebilder
- Zwölf OpKoord Lagebilder
- Ein Sonderlagebild

- Ein Teillagebild nach Bundes-Krisensicherheitsgesetz (B-KSG)

Um die Qualität der Arbeit sicherstellen zu können, wird laufend Feedback von den jeweiligen Zielgruppen eingeholt. Im Bereich der OpKoord-Lagebilder wurde die Arbeit des Gremiums im Jahr 2024 mit 4,5 von 5 Sternen bewertet.

Einbindung des neu geschaffenen Austrian Health CERT (AHC) in das Gremium

Am 22. November 2024 trat der Bescheid zur Feststellung des Austrian Health CERT (AHC) in Kraft. In der Folge nehmen Vertreterinnen und Vertreter des AHC seit November 2024 an den OpKoord Jour Fixes im Rahmen der monatlichen Lagebildsitzungen teil.

4.2 CERT-Verbund Austria

Das 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. Ziel war, die verfügbaren Kräfte zu bündeln und das gemeinsame Know-how der CERTs optimal zu nutzen. Die Teilnahme am CERT-Verbund Austria ist freiwillig. Teilnehmende verpflichten sich zu regelmäßigem Informations- und Erfahrungsaustausch, zur Identifikation und Bereitstellung von Kernkompetenzen sowie zur Förderung der CERTs in allen Sektoren – im Sinne eines kooperativen, gemeinschaftlich geführten Verbundes.

Einer der Unterschiede zwischen einem klassischen IT-Sicherheitsteam und einem CERT ist, dass die Kommunikations- und Zusammenarbeitsbereitschaft mit Dritten ein Teil des Kernauftrags ist. Ein CERT soll Schnittstellen nach außen bieten, sich vernetzen und mit anderen Teams zusammenarbeiten. International sind die CERTs weltweit im FIRST (Forum of Incident Response and Security Teams) sowie in Europa in der Task Force CSIRT (Einsatzkommando) und im 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 2024 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 bzw. persönlich, wenn es die Situation erfordert. So können über Organisations- und Unternehmensgrenzen hinweg Lagebilder rasch erstellt und Maßnahmen abgestimmt werden.

4.3 Cyber Sicherheit Plattform (CSP)

Als fester Bestandteil des österreichischen Cyber-Ökosystems fungiert die Cyber Sicherheit Plattform (CSP) seit sieben Jahren als bisher zentrale strategische Austausch- und Kooperationsplattform zwischen Wirtschaft, Wissenschaft und öffentlicher Verwaltung. Sie genießt das Vertrauen aller relevanten Stakeholder und dient dem Erfahrungs- und Informationsaustausch im Bereich Cybersicherheit mit besonderem Fokus auf kritische Infrastrukturen. Die CSP leistet wichtige Beiträge bei der Weiterentwicklung der österreichischen Cybersicherheitsstrategie und der Ausgestaltung des legistischen Rahmens zur Cybersicherheit in Österreich. Beteiligungen von Mitgliedern der CSP an internationalen Arbeitsgruppen wie der ENISA oder der UNODC Cyber Crime Convention runden das Gesamtbild ab. Auch 2025 wird die CSP die Cybersicherheit in Österreich mitgestalten und im Rahmen des Nationalen Koordinierungszentrums für Cybersicherheit (siehe 3.9 – NCC) eine zentrale Rolle in der österreichischen Cybersecurity Competence Community (CCC) einnehmen.

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 Ereignis- und Reaktionsteam für Computersicherheit) mit Unterstützung des Bundeskanzleramts (BKA) gegründet und später durch das GovCERT erweitert. Die Zielgruppen 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 für einen „Trust Circle“ notwendige Vertrauen zu schaffen, verpflichten sich alle Teilnehmenden, den Code of Conduct einzuhalten und das Traffic-Light-Protokoll (TLP) gemäß der Definition des Forum of Incident Response and Security Teams (FIRST) zu befolgen.

Die wesentlichen Ziele des ATC sind:

- 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 die Behandlung,
  - 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, jährlich im Rahmen einer zweitägigen Veranstaltung gefördert. 2024 fand diese in Pörtschach statt.

In den vergangenen beiden Jahren lag der Schwerpunkt der behandelten Themen bei den Vorbereitungen zur NIS-2-Richtlinie. Der Trust Circle wurde genutzt, um die aus der NIS-2-Richtlinie erwarteten Vorgaben mit den Praxiserfahrungen der Teilnehmenden zu vergleichen. Im Finanzbereich waren DORA und die daraus entstehenden Aufgaben für Unternehmen ein wichtiges Thema.

Der Trust Circle wurde auch 2024 um weitere Mitglieder erweitert. 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 Praxis. Aufgrund des Wachstums des ATC und um den Teilnehmenden aus den Bundesländern einen regelmäßigen Austausch zu ermöglichen, wurden die Circle-Treffen ab 2024 hybrid (online und vor Ort bei CERT.at in Wien) abgehalten.

4.5 IKT-Sicherheitsportal

Das IKT-Sicherheitsportal „onlinesicherheit.gv.at“ ist eine interministerielle Initiative in Kooperation mit der österreichischen Wirtschaft und fungiert als zentrales Internetportal für Themen rund um die Sicherheit in der digitalen Welt. Die Initiative verfolgt als strategische Maßnahme der Nationalen IKT-Sicherheitsstrategie und der Österreichischen Strategie für Cybersicherheit (ÖSCS) das Ziel, durch Sensibilisierung und Bewusstseinsbildung der betroffenen Zielgruppen sowie durch Bereitstellung zielgruppenspezifischer Handlungsempfehlungen, die IKT- und Cybersicherheitskultur in Österreich zu fördern und nachhaltig zu stärken.

Das Informations- und Serviceangebot wird im Rahmen regelmäßiger Redaktionssitzungen mit den 40 Kooperationspartnerinnen und -partnern (Bundesministerien, Landesregierungen, Behörden, Universitäten, Fachhochschulen, Forschungsinstitute, Unternehmen, Vereine und Interessensvertretungen) laufend erweitert. Es beinhaltet aktuelle Meldungen und Warnungen, Informatives, Beratung sowie weiterführende Informationen sowohl für Einsteigerinnen und Einsteiger als auch für Expertinnen und Experten.

2024 umfassten die Aktivitäten auf dem IKT-Sicherheitsportal die Erstellung von 128 Newsartikeln, 13 Publikationseinträgen, 66 Veranstaltungseinträgen und zehn Videos. Jeden Monat wurde ein Schwerpunktthema zu aktuellen Trends festgelegt, wozu jeweils ein Video sowie Fachbeiträge und Interviews veröffentlicht wurden. Themenschwerpunkte waren beispielsweise „Künstliche Intelligenz“, „Digitale Ausweise & Wallets“, „Sicherer Onlinehandel & Gütezeichen“ sowie im Oktober ein wiederkehrender Schwerpunkt zum

„European Cyber Security Month“ (ECSM) und den österreichischen Aktivitäten, die im Zuge dessen veranstaltet wurden. Zudem gab es im Rahmen des „Safer Internet Days 2024“ einen eigenen Schwerpunkt, der damit verbundene Aktivitäten hervorhob. Zusätzlich zum Schwerpunkt wird künstliche Intelligenz auch als Querschnittsthema bei allen weiteren Themenschwerpunkten mitberücksichtigt. Darüber hinaus wurden ausgewählte Artikel inhaltlich aktualisiert sowie erneuert und teilweise mit Informationsgrafiken ergänzt, um eine noch verständlichere Aufbereitung der Inhalte zu erreichen.

Mit mittlerweile 18 verlinkten Online-Ratgebern von unterschiedlichen Organisationen wird – je nach Art des Ratgebers – eine Möglichkeit zur eigenständigen Prüfung der persönlichen Kompetenz oder zum Umsetzungsgrad eines Themenbereichs geboten. So dient der „Fake-Shop-Simulator“ zur Sensibilisierung gegenüber betrügerischen Online-Shops und der „Cyber Security Check“ zur Überprüfung der bestehenden Cybersicherheitsmaßnahmen in einem Unternehmen.

Des Weiteren wurde der Cybermonitor – eine statistische Aufbereitung der zwölf wesentlichsten Gefährdungen im Bereich der IKT- und Cybersicherheit – laufend aktualisiert. Der Cybermonitor bietet zu den jeweiligen Kategorien, beispielsweise Phishing oder Schwachstellen, eine grafische Darstellung der Entwicklung der vergangenen Jahre und zeigt dadurch bestehende Trends der Gefährdungslage auf.

Durch die kontinuierliche Veröffentlichung multimedialer Inhalte in diversen Formaten wie Newsartikel, Fachbeiträge, Interviews und Videos, inklusive ausgewählten statistischen Kennzahlen, konnte die Reichweite gemeinsam mit gezielter Suchmaschinenoptimierung für das Kalenderjahr 2024 auf 1.283.779 Besuche um 31,5 Prozent gegenüber dem Vorjahr (2023) gesteigert werden.

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. Das unter Verantwortung des Bundesministeriums für Finanzen stehende K-PASS unterstützt primär österreichische Unternehmen und Forschungseinrichtungen bei der Entwicklung neuer Technologien und der Gewinnung des erforderlichen Wissens, um die digitale Sicherheit Österreichs zu erhöhen und Wertschöpfung zu generieren. Ziel ist die Schaffung marktnaher Forschungsergebnisse zu digitaler Sicherheit für sämtliche Sicherheitsanwenderinnen und -anwender bzw. Bedarfsträgerinnen und -träger, beispielsweise die Polizei oder Feuerwehr, aber auch sicherheitsrelevante Unternehmen wie der Verbund oder der Flughafen Wien-Schwechat.

Daten und Fakten-Box:

Budget	5 Mio. € für jährliche Ausschreibungen
Rechtliche Grundlage	Verwaltungsübereinkommen zwischen BKA und BMF
Programmeigentümer	BMF
Programmabwicklung	FFG
Erfolgreich geförderte Projekte	10
Programmstart / Zweite Ausschreibung	23. Oktober 2024 bis 13. Februar 2025
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

5.1 Cyber Europe 2024

Die Agentur der Europäischen Union für Cybersicherheit (ENISA) veranstaltet seit dem Jahr 2010 breit angelegte, grenzüberschreitende Cyberübungen unter dem Namen „Cyber Europe“ im Zwei-Jahres-Rythmus. Die Übungen simulieren Cybersicherheitsvorfälle, die sich im Verlauf der Übung zu Cyberkrisen entwickeln können. Die Vorfälle folgen dabei realistischen Szenarien, die von realen Ereignissen und Bedrohungen inspiriert sind. Die Cyber Europe bringt Cybersicherheits-Expertinnen und -Experten aus dem öffentlichen und privaten Sektor der EU und der EFTA sowie europäische Institutionen, Einrichtungen und Agenturen zusammen, um deren technische und operative Fähigkeiten zu stärken.

Die Cyber Europe 2024 war die siebte Ausgabe dieser paneuropäischen Übungsreihe und fand am 19. und 20. Juni 2024 statt. Das Szenario konzentrierte sich in diesem Jahr primär auf Cyberangriffe auf die Energieinfrastruktur der EU-Mitgliedstaaten, wobei auch die digitale Infrastruktur und die öffentliche Verwaltung von den Angreiferinnen und Angreifern als sekundäre Ziele ins Visier genommen wurden, um den Druck zu erhöhen und Chaos zu stiften. Hintergrund des gewählten Übungsszenarios ist, dass laut ENISA Cyberangriffe auf die Energie- und Rohstoffinfrastruktur seit 2017 permanent zunehmen und 2022 schließlich einen Rekordwert erreicht haben. Da die Energieinfrastruktur für moderne Volkswirtschaften von entscheidender Bedeutung ist, sind Elektrizitäts-, Öl- und Gasunternehmen für Cyberkriminelle ein attraktives Ziel.

Szenario der Cyberübung

Im Übungsszenario ist die Energieinfrastruktur der EU-Mitgliedstaaten angesichts der anhaltenden geopolitischen Spannungen zwischen der Union und dem fiktiven Staat Voltaros zu einem Hauptziel für Cyberangriffe geworden. Es besteht der Verdacht, dass APT-Akteurinnen und -Akteure (Advanced Persistent Threats) sowie andere kriminelle Gruppen zusammenarbeiten, um das Machtgleichgewicht zugunsten ihrer politischen Verbündeten in Voltaros zu verschieben, indem sie kritische Infrastrukturen angreifen.

Übungsteilnahme im Rahmen des IKDOK

Die Cyber Europe 2024 ermöglichte es, im Rahmen des Inneren Kreises der Operativen Koordinierungsstruktur (IKDOK) die Standard Operating Procedures (SOP) und die Abläufe gemäß Geschäftsordnung in der Praxis zu testen. Bereits kurze Zeit nach Übungsbeginn verlangte das Szenario eine Einberufung des IKDOK, wobei erste Informationen zur Lage ausgetauscht wurden. Aufgrund der zunehmenden Dynamik der Ereignisse wurden in der Folge regelmäßige Lageupdates für alle an der Übung beteiligten IKDOK-Organisationen erstellt und verteilt. Die zugrundeliegenden Informationen beschränkten sich dabei nicht nur auf die nationale Situation, auch Meldungen aus dem CSIRTs Network (Europäisches Netzwerk der Computernotfallteams) und dem EU-CyCLONe (Europäisches Netzwerk

der Verbindungsorganisationen für Cyberkrisen) waren wesentlicher Bestandteil des Informationsaustausches. Der Nutzen einer Vernetzung über Landesgrenzen hinaus wird selten so deutlich wie hier in der Cyberdomäne.

Eine Neuerung bei der Cyber Europe 2024 war die Einbeziehung und der Informationsaustausch mit dem Bundeslagezentrum, das durch das Bundes-Krisensicherheitsgesetz (B-KSG) neu eingerichtet wurde. Im Bundeslagezentrum laufen im Krisenfall alle Fäden zusammen. Neben dem durch den IKDOK erstellten Cyberlagebild erhält das Bundeslagezentrum auch zusätzliche Lagebilder aus anderen Bereichen. Im Rahmen der diesjährigen Übung war dies das Lagebild aus dem österreichischen Energiesektor.

Die Cyber Europe 2024 zeigte neuerlich, dass die bestehende Vertrauensbasis und die darauf aufbauende, eingespielte Kooperation der IKDOK Organisationen ein wesentliches Element für die Bewältigung kritischer Situationen darstellt.

5.2 KSÖ-Planspiel 2024

Das Kompetenzzentrum Sicheres Österreich (KSÖ) und das Austrian Institute of Technology (AIT) veranstalteten am 6. und 7. November 2024 gemeinsam die siebte Auflage ihres Cyber-Planspiels. Ziel dieser Cyberübung war, dass Vertreterinnen und Vertreter österreichischer und internationaler Behörden und Unternehmen gemeinsam die Bewältigung eines fiktiven hybriden Angriffs auf Staat, Wirtschaft und Gesellschaft trainieren. Konkret sollte durch diese Übung die Fähigkeit zur Reaktion auf komplexe, koordinierte Angriffe verbessert werden, um die Geschäftskontinuität in kritischen Situationen sicherstellen zu können.

Das KSÖ-Planspiel 2024 richtete sich an Sicherheitsakteurinnen und -akteure sowie Expertinnen und Experten aus verschiedenen Ländern (Österreich, Deutschland und Italien) und aus betroffenen Sektoren und Branchen (Finanzsektor, Industrie, IT-Dienstleisterinnen und -Dienstleister). Auch Behörden aus den genannten Ländern sowie CERTs und GOV-CERTs (Computer Emergengy Response Team) waren beteiligt.

Szenario der Cyberübung

Die Teilnehmenden vertraten während dieser Cyberübung nicht ihre jeweiligen realen Unternehmen, sondern verkörperten Mitarbeitende des fiktiven Industrieunternehmens OptiTeq und der fiktiven OeBank, die jeweils Ziel einer massiven Cyberangriffswelle waren. Um die Angriffe abzuwehren, mussten die Teilnehmenden Bedrohungen richtig erkennen und entsprechende Gegenmaßnahmen ergreifen. Zu den Herausforderungen zählten der Schutz sensibler Daten, die Verteidigung gegen Ransomware-Angriffe, die Eindämmung von gefälschten Informationen und Desinformationskampagnen sowie die

Verhinderung von finanziellen Diebstählen. Parallel dazu wurden die Teilnehmenden mit physischen Angriffsvektoren auf Produktionsanlagen und gefälschten Banktransaktionen konfrontiert.

Übungsteilnahme im Rahmen des IKDOK

Das KSÖ-Planspiel 2024 ermöglichte es, Prozesse und Abläufe im Inneren Kreis der Operativen Koordinierungsstruktur (IKDOK) zu trainieren und zu optimieren. Während die Mitarbeiterinnen und Mitarbeiter der teilnehmenden Firmen verschiedene Rollen in den fiktiven Unternehmen „OptiTeq" und „OeBank" verkörperten, nahm der räumlich getrennte Behördenbereich, der sich aus Vertreterinnen und Vertretern des IKDOK und der Finanzmarktaufsicht (FMA) zusammensetzte, in der Übung seine jeweils tatsächlichen Funktionen wahr.

Weil anfangs die Informationen auf Behördenseite nur langsam und vereinzelt eintrafen, beschränkten sich die Aktivitäten des IKDOK in dieser Phase auf seine Funktion als Informationsdrehscheibe. Aufgrund der Eskalation der Ereignisse mit Fortschreiten der Cyberübung wurde es erforderlich, die betroffenen Unternehmen direkt einzubinden. Zu diesem Zweck wurde der IKDOK zur Operativen Koordinierungsstruktur (OpKoord) erweitert, im Rahmen derer auch externe Personen teilnehmen durften. Im Zuge der OpKoord-Sitzungen zeichnete sich rasch ein klares Bild über die wahren Ausmaße der Ereignisse ab. Diese Informationen waren die Basis für ein umfassendes Lagebild, das in der Folge permanent fortgeschrieben und regelmäßig an die Bedarfsträgerinnen und Bedarfsträger verteilt werden konnte.

Das KSÖ-Planspiel 2024 präsentierte sich als eine aufwendig geplante Übung, die sich nicht bloß auf Cyberangriffe beschränkte, sondern ein umfassendes hybrides Szenario präsentierte, das mit Fortschreiten des Planspiels auch eine physische Komponente beinhaltete. Diese Elemente, die von einfachen Einbrüchen und Sabotageakten bis hin zu verheerenden Brandanschlägen reichten, stellten die Teilnehmerinnen und Teilnehmer vor große Herausforderungen. Die etablierte Kooperation in IKDOK und OpKoord konnte aber auch unter diesen Rahmenbedingungen zu einer Bewältigung der Situation beitragen.

5.3 Locked Shields

2024 nahmen Expertinnen und Experten des Militärischen Cyberzentrums (MilCyZ) erneut an der größten Cyber-Verteidigungsübung der Welt, der „Locked Shields", teil. Gemeinsam mit Cyberspezialistinnen und -spezialisten aus der Schweiz und der National Guard Vermont übten Expertinnen und Experten des BMLV als Combined Blue Team die Verteidigung gegen einen hybrid agierenden, staatlichen Gegner. Im Fokus der Verteidigung von Computernetzwerken und -systemen standen neben den militärischen Systemen zum

Beispiel Militärische Führungs- und Informations-Systeme sowie Luftabwehrsysteme, aber auch Satellitensysteme sowie kritische Infrastruktur. Besonders durch die Übungsleitung hervorgehoben wurde die Initiative des Blue Teams. Der Austausch mit anderen Nationen war ein wichtiger Beitrag eines gemeinsamen, nationenübergreifenden Handelns.

5.4 Crossed Swords

Die Übung „Crossed Swords" wird jährlich vom Cooperative Cyber Defence Centre of Excellence (CCDCoE) in Tallinn durchgeführt. Ziel der Übung ist es, Cyber-Spezialistinnen und -Spezialisten in Anlehnung an die „Cyber Kill Chain" darin auszubilden, in einem krisenhaften Umfeld offensive Cyber-Operationen erfolgreich durchzuführen. Ein weiterer Fokus liegt auf der Schulung militärischer Kommandoelemente in der Führung offensiver Cyberraum-Fähigkeiten. Die Übung unterstützt auch die Entwicklung anderer bereichsbezogener operativer und taktischer Fähigkeiten im Zusammenhang mit dem Cyberraum, z. B. Informationsoperationen.

200 Teilnehmende aus 40 Ländern nahmen daran teil, um in einem Bereich, der heutzutage von großer Bedeutung ist, zu üben und zu experimentieren. Die Übungsteilnehmerinnen und -teilnehmer bildeten ein Cyber-Hauptquartier mit Planungsstab, militärische Cyber-Operatorinnen und -Operatoren, Expertinnen und Experten für digitale Forensik und Spezialistinnen und Spezialisten anderer Einheiten, die Teil ihrer jeweiligen nationalen Cyber-Streitkräfte sind.

Die Übung profitiert von der Unterstützung durch Partnerinnen und Partner aus Wissenschaft und Industrie, die es ermöglichen, das Vorhaben authentisch und an die aktuellen Herausforderungen der realen Welt angepasst zu gestalten.

5.5 Military Interoperability Conference (MIC)

20 Leiterinnen und Leiter militärischer Computernotfallteams (MilCERTs) aus zwölf EU-Mitgliedstaaten nahmen 2024 am operativen Track der Military CERT Interoperability Conference (MIC) 2024 bei der Europäischen Verteidigungsagentur (EDA) teil. Dieser szenariobasierte Austausch diente der gemeinsamen Vorbereitung auf eine Cyberkrise und konzentrierte sich auf die Werkzeuge und Verfahren, die das Militär Europas benötigt, um rasch und adäquat gemeinsam reagieren zu können.

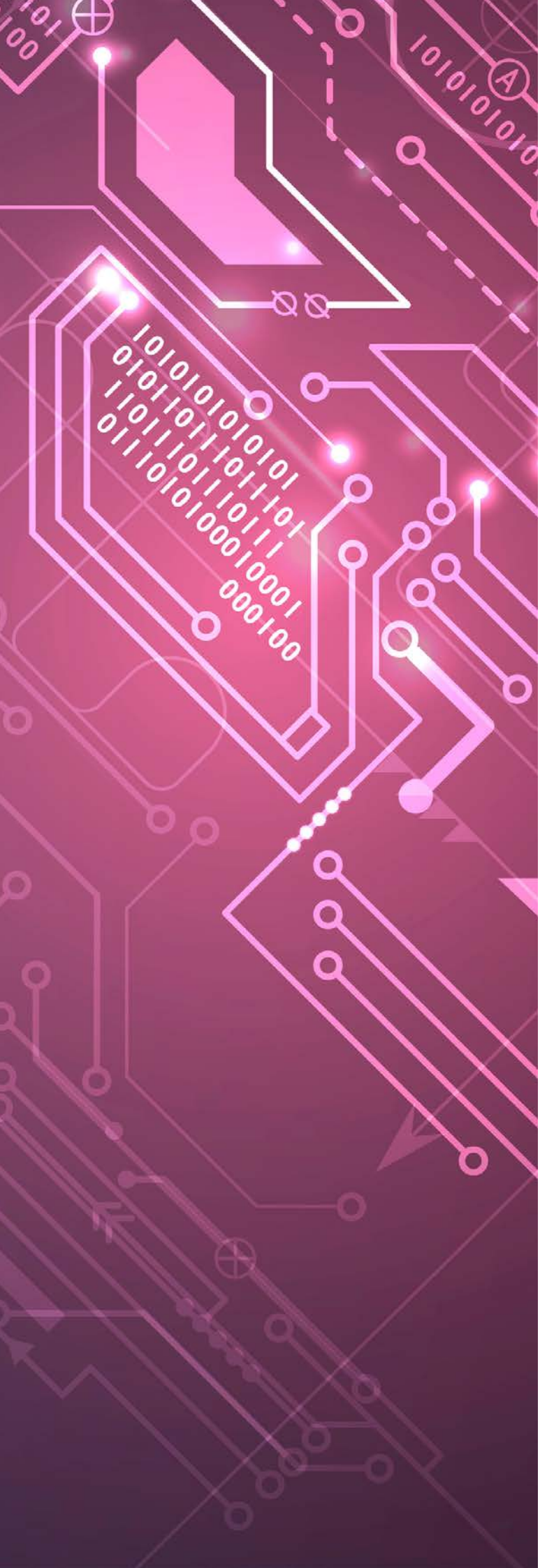
Im Vorfeld wurde im Rahmen eines technischen Tracks, der auf einer Cyberrange abgehalten wurde, unter regem Austausch an kreativen Lösungen zur gemeinsamen Bewältigung von Cybervorfällen gearbeitet.

Im Fokus waren vor allem zentrale Themen wie der Informationsaustausch, die Entwicklung neuer Handlungsanweisungen und der Überprüfung von Mechanismen zur Reaktion auf Vorfälle im Kontext einer eskalierenden Krise im Cyberspace.

5.6 Cyber Range Exercise

Das Militärische Cyberzentrum (MilCyZ) der Direktion IKT & Cyber des ÖBH veranstaltete wie im Vorjahr eine Cyberübung für fortgeschrittene Cyber-Expertinnen und -Experten. Auf einer extern bereitgestellten Cyberrange fand eine Schulung durch Cyber-Spezialistinnen und -Spezialisten mit anschließender Blue- und Redteam-Übung statt. Im Zuge dieser Übung wurden Cyber-Verteidigungs- und -Angriffssimulationen unter Ausbildungsbedingungen absolviert.

6 Zusammenfassung



Der Cybersicherheitsbericht für das Jahr 2024 fasst auch in seiner aktuellen Ausgabe Einschätzungen, Entwicklungen und Aktivitäten im Bereich der Cybersicherheit in Österreich zusammen und stellt diese in fünf Kapiteln dar. Der Bericht zeigt abermals, dass Cybersicherheit auch weiterhin ein zentrales Thema für Wirtschaft, Gesellschaft und Verwaltung bleibt.

Die Cyberlage auf operativer Ebene zeigt, dass das Jahr 2024 vor allem von einer hohen Bedrohung durch Ransomware-Angriffe geprägt war, die sich zunehmend auch auf kritische Infrastrukturen wie das Gesundheitswesen und den Finanzsektor auswirkten. Angreiferinnen und Angreifer konzentrierten sich dabei primär auf die Ausnutzung unentdeckter Schwachstellen in Software und Systemen. Besonders bemerkenswert erscheint in diesem Zusammenhang die fortschreitende Resilienz krimineller Akteurinnen und Akteure, da Gruppen wie LockBit trotz vorübergehender Stilllegung durch internationale Strafverfolgungsbehörden bereits kurze Zeit später wieder aktiv waren.

Im Jahr 2024 nahm auch die Zahl der Cyberangriffe durch nichtstaatliche Akteurinnen und Akteure sowie Hacktivistinnen und Hacktivisten deutlich zu. Dies zeigte sich vor allem durch eine Verstärkung von DDoS-Attacken und der Veröffentlichung gestohlener Daten. Auch hat sich die Rolle von Cyberangriffen in geopolitischen Konflikten weiter intensiviert, wobei besonders der fortwährende Angriffskrieg Russlands gegen die Ukraine als treibende Kraft hinter der Zunahme von Cyberaktivitäten festgemacht werden kann. Spill-Over-Effekte führen dazu, dass sich Konflikte und Cyberaktivitäten auch über nationale Grenzen hinweg ausbreiten und unbeteiligte Dritte in Mitleidenschaft ziehen können. Solche Effekte stellen eine große Herausforderung für die Cybersicherheit in Österreich dar.

Positiv hervorzuheben ist, dass im Berichtsjahr 2024 neuerlich bei der Mehrheit der befragten österreichischen Unternehmen aus dem Bereich der kritischen Infrastruktur umfassende Investitionen im Bereich der Cybersicherheit getätigt wurden. Insgesamt bestätigt sich der Trend, dass Ausgaben für IT-Sicherheit auf einem hohen Niveau gehalten werden. Ein entscheidender Trend in diesem Bereich ist der vermehrte Einsatz von künstlicher Intelligenz (KI), der die Sicherheit von Unternehmen durch Optimierungen im Bereich von SEC-Monitoring, Logauswertungen und vorzeitiger Bedrohungserkennung erhöhen konnte.

Die alljährliche Befragung von Sicherheitsdienstleisterinnen und -dienstleistern in Österreich zeigt, dass die meisten Einsätze im Beobachtungszeitraum Ransomware, Phishing sowie CEO-Fraud galten. Dabei zeigt sich bei Ransomware eine gleichbleibende Tendenz auf sehr hohem Niveau, wohingegen bei Phishing durchwegs starke Zunahmen zu verzeichnen waren. Die polizeiliche Kriminalstatistik lässt im Jahr 2024 einen leichten Rückgang von 5,4 Prozent gegenüber dem Jahr 2023 erkennen, wobei Internetbetrug zahlenmäßig den größten Faktor im Bereich der Cyberkriminalität darstellt – mehr als

die Hälfte der erfassten Anzeigen im Bereich der Internetkriminalität entfallen demnach auf Betrugsdelikte. Von großer Bedeutung für die künftige Entwicklung erscheint auch die Beobachtung, dass auch Angreiferinnen und Angreifer zunehmend auf künstliche Intelligenz (KI) zur Optimierung ihrer Angriffshandlungen zugreifen.

Die militärische Kriegsführung verändert sich durch die zunehmende Nutzung von Informations- und Kommunikationstechnologien kontinuierlich. Eine sich wandelnde Sicherheitslandschaft schafft dabei neue Gefahren. Das Österreichische Bundesheer (ÖBH) investiert in die Kooperationen mit Industrie- und Forschungseinrichtungen, um die neuesten Entwicklungen schnell in die eigenen Strukturen und Fähigkeiten zu integrieren. Aus Sicht des Verfassungsschutzes stellen Advanced Persistent Threats (APTs) und Hacktivismus eine entscheidende Bedrohung für die Cybersicherheit dar. Russische, chinesische, iranische und nordkoreanische Nachrichtendienste sind im Cyberraum aktiv und verfolgen dabei strategische und monetäre Interessen.

Die Europäische Union (EU) setzte auch im Jahr 2024 ihre Bemühungen zur Stärkung der Cybersicherheit fort, insbesondere durch die Arbeit der Horizontal Working Party on Cyber Issues (HWP Cyber) und der NIS-Kooperationsgruppe. Ein wichtiger Meilenstein war die Verabschiedung des Cyber Resilience Acts (CRA) und des Cyber Solidarity Acts (CSoA). Der CRA soll verbindliche Cybersicherheitsanforderungen für Produkte mit digitalen Elementen einführen, während der CSoA ein europäisches Cyber-Warnsystem und einen Notfallmechanismus vorsieht. Das Europäische Kompetenzzentrum für Industrie, Technologie und Forschung im Bereich der Cybersicherheit erlangte im Jahr 2024 nach intensiven Aufbauaktivitäten seine finanzielle Autonomie und ist nun in der Lage, seinen Auftrag vollumfänglich zu erfüllen. In den Vereinten Nationen (VN) wurde der VN-Zukunftspakt durch die Mitgliedstaaten angenommen.

Abbildungsverzeichnis

Bundesministerium für Inneres
Herrengasse 7, 1010 Wien
post@nis.gv.at
bmi.gv.at