Bericht Cybersicherheit für das Jahr 2021

Bericht Cybersicherheit für das Jahr 2021

Wien, 2022

Bundeskanzleramt

Bundesministerium
Inneres

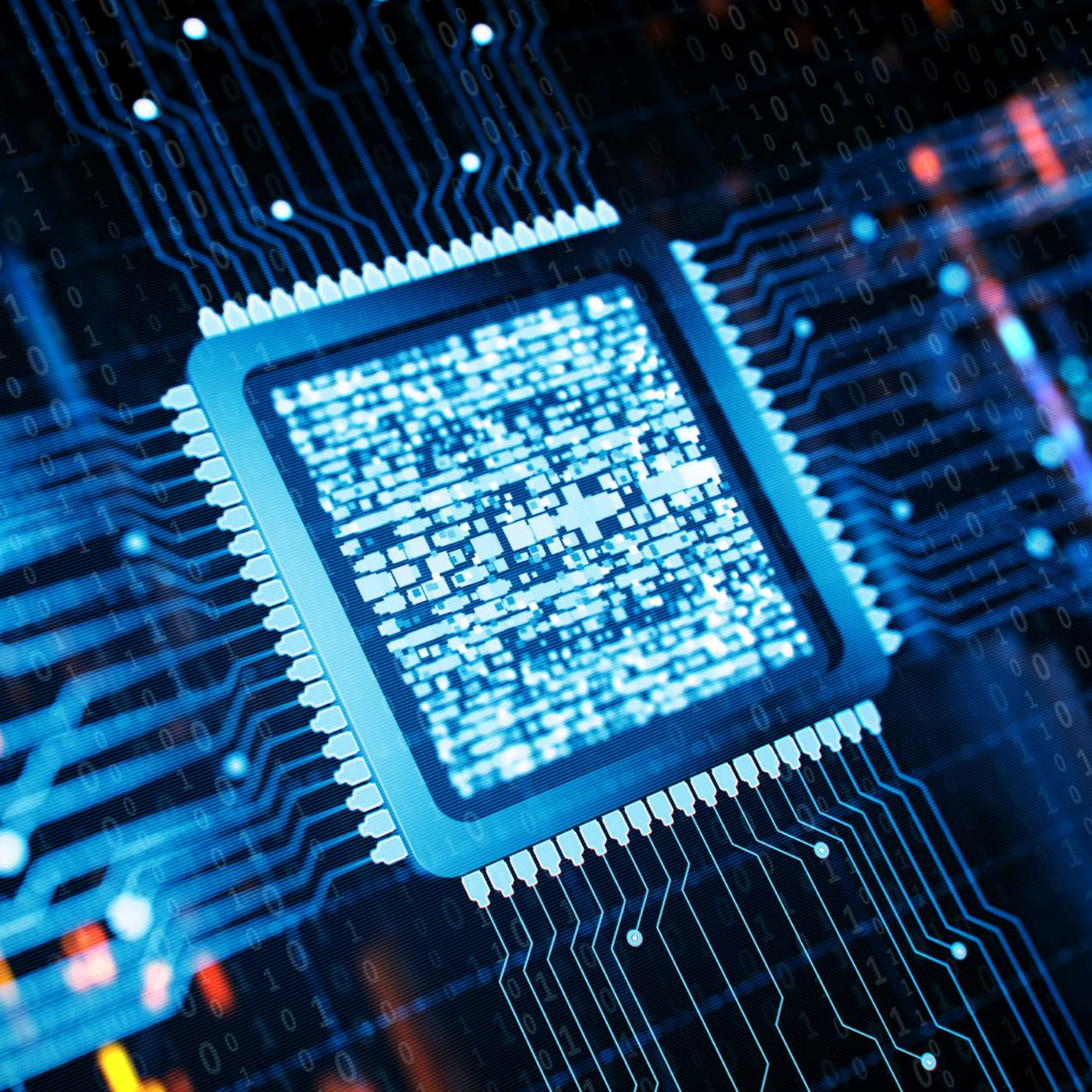
Bundesministerium
Landesverteidigung

Bundesministerium
Europäische und internationale
Angelegenheiten

Impressum

Medieninhaber, Verleger und Herausgeber:
Bundeskanzleramt
Ballhausplatz 2, 1010 Wien
bundeskanzleramt.gv.at
Fotonachweis: iStock
Layout: BKA Design & Grafik
Druck: Druckwerkstatt Handels GmbH
Wien, November 2022

Inhalt



Editor's note

„Habemus novum Cybersicherheit chartam!" hallte es an jenem Vorweihnachtsabend durch die Hallen des Bundeskanzleramtes, als die neue Österreichische Strategie für Cybersicherheit 2021 durch einen Umlaufbeschluss in Kraft gesetzt wurde. Nun, vielleicht nicht genau in diesen Worten – aber, es war vollbracht!

Nach kleinen Intermezzi wie einer Expertenregierung, einer Nationalratswahl, einem Cybervorfall im Bundesministerium für europäische und internationale Angelegenheiten und einer Pandemie konnten die Arbeiten erfolgreich finalisiert und der Bundesregierung zur Beschlussfassung vorgelegt werden. Der 22. Dezember 2021 würde den Mitwirkenden auf ewig in Erinnerung bleiben.

Mit dem Ansatz, die Strategie als Dokument UND als dynamische Plattform auszugestalten, wurde ein neuer, innovativer Weg beschritten – auch das gibt es in der öffentlichen Verwaltung (in Wirklichkeit viel öfter, als gemeinhin angenommen wird). Das erlaubt auch bei der Identifikation und Definition von Maßnahmen zur Umsetzung der Ziele der Österreichischen Strategie für Cybersicherheit 2021 eine starke Involvierung der Stakeholder. Auch die Plattform selbst wird permanent und kooperativ zwischen Behörden und Zielgruppen weiterentwickelt, was auch künftig zu interessanten und wertvollen Einsichten und Funktionalitäten führen wird.

Währenddessen wurde in Brüssel, unter reger Beteiligung der österreichischen Repräsentanten, um die genaue Ausgestaltung der NIS-2-Richtlinie (als Nachfolge zur EU Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union) verhandelt.

Zielte NIS1 noch darauf ab, die kritischen Infrastrukturen und die Betreiber wesentlicher Dienste bei der Erhöhung des Sicherheitsniveaus im Cyberraum zu unterstützen, wird mit NIS2 der Wirkungsbereich viel breiter sein. Eine Chance für Österreich und Europa als Ganzes gemeinsam cyberresilienter zu werden.

Aber das letzte Jahr war natürlich nicht nur von der strategischen Ebene geprägt: Auch im operativen Bereich gab es 2021 zumindest zwei Vorfälle, welche Österreich und der ganzen Welt ihre Abhängigkeiten in die Cyber Supply Chain sowie deren dramatische Verwundbarkeit aufzeigten. Plötzlich ging es nicht nur mehr darum, die eigenen Systeme abzusichern und zu härten – nein, auch die Anbieter von Software und sogar deren Subanbieter erwiesen sich als mitunter hochproblematische Einfallstore für Schwachstellen und Schadfunktionalitäten.

Mit Jahreswechsel 2020/2021 wurde bekannt, dass global agierende Softwareanbieter und sogar Anbieter von Sicherheitssoftware selbst infiltriert wurden und somit Schadsoftware an Kunden ausliefern würden. Das Betroffenen- und auch Schadensausmaß war vorerst unmöglich abzuschätzen und hat sich erst im Laufe des ersten Halbjahres 2021 eröffnet – es waren hauptsächlich Regierungsorganisationen oder diesen nahestehende. Eine staatliche Lenkung des Angriffs erscheint wahrscheinlich.

Doch sind es nicht immer nur gezielte Angriffe, welche aufgrund der komplexen Abhängigkeiten von und zwischen Software zu massiven Schäden führen können.

Die Entwicklung von Software ist aufwändig und kostenintensiv. Um zu verhindern, dass mit jedem neuen Produkt „das Rad neu erfunden würde“, nutzen Entwickler Funktionsbibliotheken, damit nicht-domänenspezifische Problemstellungen schnell und weitestgehend standardisiert gelöst werden können. Eine dieser Bibliotheken, Log4J, dient dazu, die in jeder hinreichend kompetent entwickelten Software notwendige Funktionalität des Loggings – also der Nachvollziehbarmachung der internen Abläufe zur Laufzeit des Pro-

grammes – umzusetzen. Leider wurde in dieser Software eine Schwachstelle übersehen, die dazu führte, dass plötzlich und mit einem Schlag hunderttausende Anwendungen potentiell gefährdet waren. Die Direktorin der U.S. Cybersecurity & Infrastructure Security Agency nannte diese Schwachstelle die wohl ernsteste ihrer Karriere. Am Ende stellte sich heraus, dass die Entwicklung und Wartung dieser zentralen Software von zwei Entwicklern betrieben wurde – als Open Source Projekt, gratis und in ihrer Freizeit. Diesen beiden ist keinesfalls ein Vorwurf zu machen, aber es zeigte sich deutlich, dass es Mechanismen braucht, auch Open Source Software strukturiert zu testen und Verantwortlichkeiten zu klären. Initiativen, wie das leider ausgelaufene EU-FOSSA 2 Bug Bounty Programm[1], könnten hier entsprechende Aufmerksamkeit generieren.

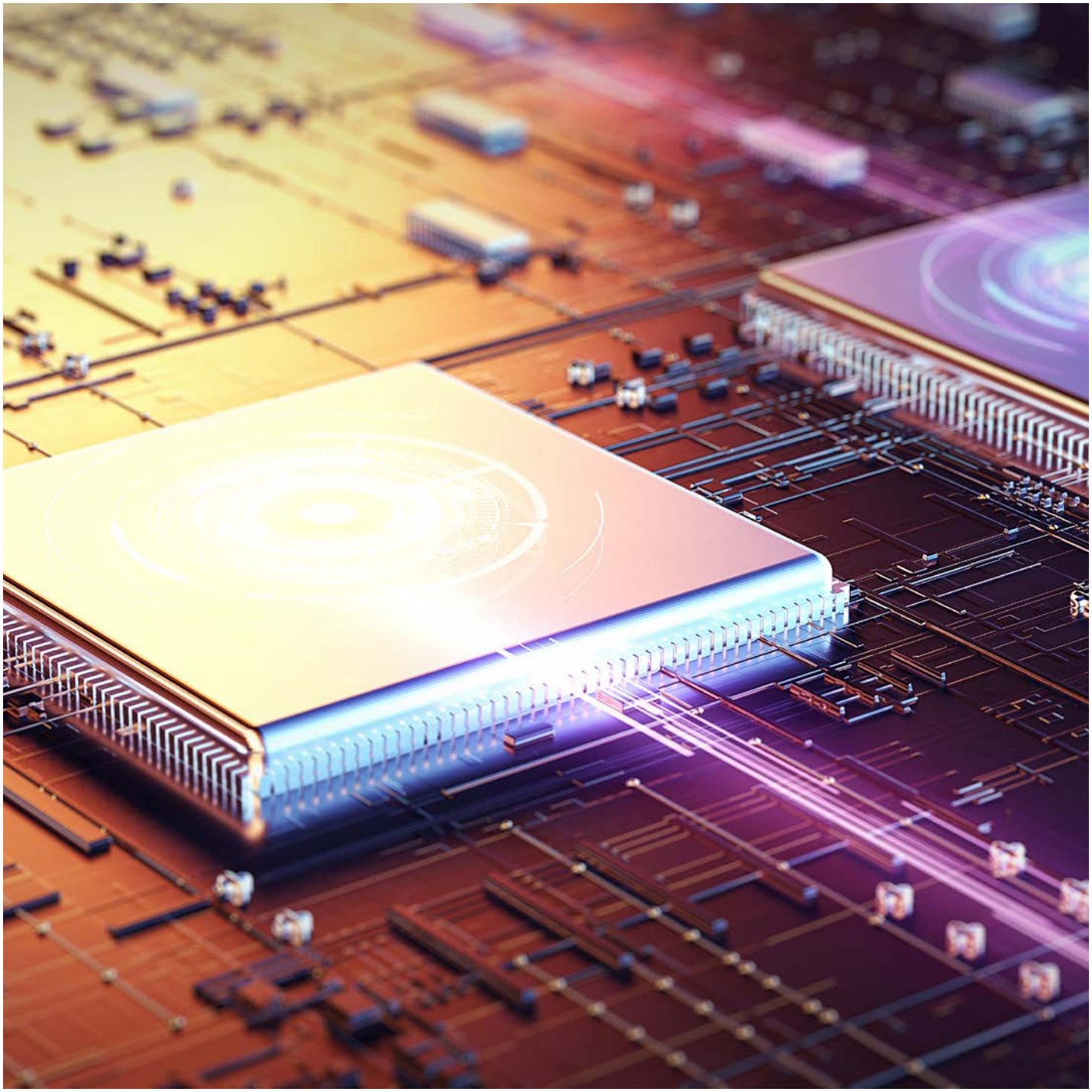
Eine Firma, die besonders darum bemüht war, keine Aufmerksamkeit zu erregen, bekam 2021 mehr als genug davon. Die Rede ist von der NSO-Group und ihrer von staatlichen Kunden eingesetzten Spyware „Pegasus". Diese wurde nämlich überraschenderweise nicht nur auf Mobiltelefonen von mutmaßlichen oder identifizierten Terroristen eingesetzt, nein, auch Politiker, Dissidenten, Menschenrechtsaktivisten und Journalisten wurden mit Hilfe der Software überwacht. In Österreich wurden offziell keine Infektionen bekannt. Schlussendlich wurde die NSO-Group sogar auf eine schwarze Liste der USA gesetzt, da der Spyware-Hersteller „gegen die Außenpolitik und die nationalen Sicherheitsinteressen der USA" gehandelt habe. Dass dies das Ende des Wirtschaftszweiges Spionagesoftware bedeutet, darf aber getrost bezweifelt werden.

Vieles gäbe es noch zu erzählen und einiges von dem was passiert ist, können die geneigten Leserinnen und Leser diesem Bericht entnehmen. Viel Vergnügen bei der Lektüre!

Nach all diesen Aufregungen des Jahres 2021 mit der Pandemie und den hohen Zahlen an Cyberangriffen ist klar: Das Jahr 2022 kann nur ein ruhigeres werd…

---

1 siehe https://ec.europa.eu/info/departments/informatics/eu-fossa-2_en



Einleitung

Die Österreichische Strategie für Cybersicherheit 2021 (ÖSCS 2021) legt fest, dass durch die Cyber Sicherheit Steuerungsgruppe (CSS) ein jährlicher Bericht zur Cybersicherheit in Österreich erstellt wird. Der letzte Bericht wurde im Juli 2021 vorgelegt.

Der aktuelle Bericht Cybersicherheit für das Jahr 2021 baut auf den Inhalten des letztjährigen Berichtes auf und ergänzt diesen um aktuelle Entwicklungen mit Schwerpunkten in den Bereichen internationale und operationelle Entwicklungen. Beobachtungszeitraum ist das Jahr 2021, einzelne aktuelle Entwicklungen im Jahr 2022 haben Eingang gefunden.

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

1
Cyberlage/ Bedrohung

Die Steigerung der digitalen Widerstandsfähigkeit Österreichs und die Gewährleistung von Cybersicherheit in der digitalen Welt insgesamt sind sowohl für unseren Wohlstand als auch für unsere Sicherheit von großer Bedeutung.

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

1.1 Lage Cybersicherheit – operative Ebene

In den letzten Jahren war Ransomware ein beständiges Problem für Wirtschaft und Gesellschaft. Auf die Verbesserung der Sicherheits- und Backup-Mechanismen reagierten die Cyberkriminellen mit immer neuen Wegen, um sich den illegalen Profit zu sichern. Nach Ultimaten und Drohungen mit der Löschung von Daten, ist die Androhung der Veröffentlichung von Datenbeständen hinzugekommen. An sich sind die Phänomene Datendiebstahl nicht neu, aber in der Kombination mit Ransomware und der Drohung mit gezielter Veröffentlichung von Interna sehen sich viele Unternehmen und Organisationen genötigt, auf die Forderungen der Täterschaft einzugehen.

Ransomware ein beständiges Problem für Wirtschaft und Gesellschaft

Neben den eigentlichen Schäden durch die Angriffe, welche Business Continuity- sowie Wiederherstellungskosten zur Folge haben, fürchten viele Opfer zu erwartende Reputationsschäden durch die angedrohte Datenveröffentlichung. Dies wird durch die direkt mit dem Vorfall zeitlich im Zusammenhang stehenden Veränderungen bei Aktienkursen und Verkaufszahlen bestätigt. Die Cyberkriminellen wiederum sind finanziell hoch motiviert und passen sich sehr schnell an neue Gegebenheiten oder veröffentlichte Schwachstellen an. Da diese größtenteils arbeitsteilig vorgehen, kann in diesem Zusammenhang auch von „criminal enterprises“ gesprochen werden.

Unter diesem Gesichtspunkt ist auch das Spektrum der Angriffe anders zu verstehen. Es ist von Tätergruppen mit hoher finanzieller Motivation und zumindest in Teilen mit einem tiefen technischen Verständnis auszugehen. Durch eben diese finanziellen Möglichkeiten der Angreiferinnen und Angreifer können diese auch auf „gray markets“ bzw. „black markets“ bisher unbekannte Schwachstellen (Zero-Days) einkaufen. Augrund der erwähnten Umstände, der Adaptionsfähigkeit der Täterschaft, der steigenden technischen Komplexität sowie der von Natur aus schlechteren Ausgangslage für Verteidiger (Defenders Dilemma), wird die Vorfallerkennung und -bearbeitung zu einem immer komplexeren und fordernden Aufgabengebiet. Dies stellt auch besonders die Cybersicherheit-Analysten vor die Aufgabe, ein breites Spektrum an Wissen und Fähigkeiten ständig parat und abrufbar zu haben.

In den folgenden Unterpunkten werden einige der „Highlights“ aus dem Themenbereich Cybersicherheit genauer beleuchtet.

1.1.1 Datenleaks & -diebstähle

Datenabflüsse durch nicht ausreichend gesicherte Systeme oder aufgrund von zu spät erkannten Sicherheitslücken scheinen bereits an der Tagesordnung zu stehen. So sahen sich im letzten Jahr eine Vielzahl an Serviceanbietern im Internet, insbesondere auch Social Media Anbieter, die von Natur aus über große Datenbestände verfügen, mit diesem Problem konfrontiert. Die Diversität der exfiltrierten Daten, sei es Art oder Qualität, schwankt dabei sehr stark. Auch 2021 setzte sich der Trend von Angriffen mit Diebstahl von Kunden- und Unternehmensdaten fort. Dabei ist mitunter nicht der einzelne entwendete Datensatz problematisch, sondern die Summe aus bereits veröffentlichten Datensätzen, die wiederum neue Angriffsvektoren wie Social-Engineering oder Password-Spraying ermöglichen.

Daten- und Cybersicherheit sind ein Überlebensfaktor für Unternehmen und Organisationen

Hinzu kommen noch die eingangs erwähnten „Datendiebstähle“ im Zuge von Ransomware-Kampagnen. Hierbei handelt es sich in vielen Fällen um Datenbestände, die auch aus der Sicht des Datenschutzes (General Data Protection Regulation [GDPR]) als besonders schützenswert gelten. Ein Faktor, der bisher noch wenig Beachtung gefunden hat, ist die bewusste Manipulation veröffentlichter Daten. So scheint ein Ansatz, im Zuge der veröffentlichten Datensätze bewusst manipuliertes, kompromittierendes Material unter die echten Daten zu mischen. Der Nachweis einer Manipulation ist schwierig, gleichzeitig ist mit breiter medialer Aufarbeitung zu rechnen. Die Reputation eines Unternehmen ist eng mit der wirtschaftlichen Überlebensfähigkeit verbunden. Daten- sowie Cybersicherheit sind somit ein Überlebensfaktor für Unternehmen und Organisationen.

Ransomware-Gruppierungen sind darüber hinaus dazu übergegangen, im Zuge der initialen Kompromittierung von Systemen, die finanziellen Kapazitäten des Opfers zu analysieren und die Lösegeldforderung an die Wirtschaftsleistung des Zieles anzupassen. Dies führte im Beobachtungszeitraum zu teils horrenden Forderungen.

1.1.2 Spyware Pegasus

Im Jahr 2021 wurde bekannt, dass die für Ermittlungsbehörden von der israelischen Firma NSO-Group vertriebene Software „Pegasus“ in diversen Ländern auch gegen Oppositionelle sowie Journalistinnen und Journalisten eingesetzt wurde. An die Öffentlichkeit gebracht wurde dies durch die NGO “Cititzen Lab” sowie Amnesty International.

Zweck der Software ist laut Firmenbeschreibung, den Ermittlungsbehörden direkten Zugriff auf Smartphones zu ermöglichen und somit die unterschiedlichen Verschlüsselungs- und Schutzmechanismen auszuhebeln. Dabei erfolgt eine Infektion ohne aktive Interaktion durch den Benutzer – der Empfang einer manipulierten Kurznachricht reicht aus. Die Software verfügt über diverse Tarnmechanismen und erlaubt auch, den Ausschaltvorgang zu unterbrechen, um weiterhin aktiv zu bleiben.

Das seit dem Jahr 2016 im Umlauf befindliche Überwachungstool bediente sich der Infektion bisher unbekannter Schwachstellen (Zero-Days, 0-Days), die eine Erkennung nahezu unmöglich machten. Durch Amnesty International wurde eine Open Source Software entwickelt, die die Erkennung einer Infektion mit der Überwachungssoftware anhand der Überprüfung eines erstellten Backups ermöglichte (MVT – Mobile Verification Tool).

Im Zuge der Veröffentlichung der Details zur Anwendung und der einsetzenden Länder, entwickelte sich eine breite zivilgesellschaftliche und mediale Front, die auch politische sowie wirtschaftliche Konsequenzen für das Unternehmen NSO-Group nach sich zog.

1.1.3 Log4j/Log4Shell

Ende des Jahres 2021 hat die als Log4j/Log4Shell benannte Schwachstelle in einer beliebten und weit verbreiteten Java-Bibliothek zu einer der weitreichendsten Sicherheitslücken der letzten Jahre geführt.

Bibliotheken werden in der Softwareentwicklung genutzt, um häufig benötigte Funktionalitäten über mehrere Entwicklungsprojekte nutzen zu können, ohne jedes Mal selbige

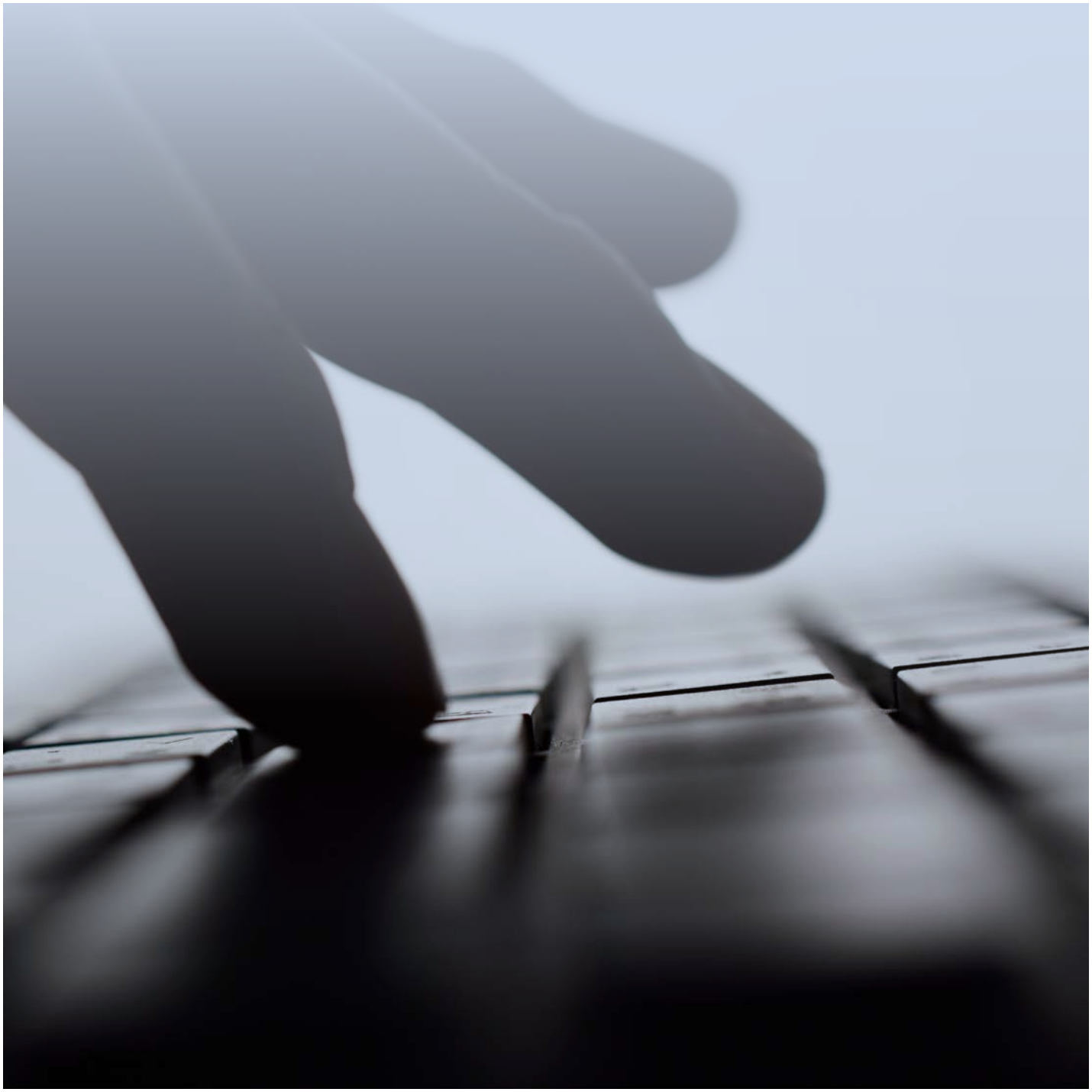
neu implementieren zu müssen. Die von der Schwachstelle betroffene Bibliothek stellte Logging- und Monitoring-Mechanismen zur Verfügung, beide sind integrale Bestandteile eines jeden Softwareprojektes. Das und die Möglichkeit als Free- und Open-Source ohne Lizenzkosten in eigene, auch kommerzielle Softwareprodukte einbinden zu können, hat zu einem hohen Verbreitungsgrad geführt. Welche Systeme tatsächlich betroffen waren, war in einem ersten Ansatz nicht festzustellen, da die Schwachstelle über die Bibliothek in unzähligen Produkten integriert wurde.

Die hohe Anzahl an potentiell gefährdeten Zielen und somit auch die Möglichkeit auf breiter Basis Systeme übernehmen zu können, führte zu einem Wettlauf zwischen Systemadministratoren und Angreifern, wobei die Geschwindigkeit, mit der dies erfolgte, ein selten dagewesenes Ausmaß erreichte.

Über die staatlichen Cybersicherheitsstukturen wurden potentiell betroffene Systeme in Österreich identifiziert und mit den Betreibern proaktiver Kontakt aufgenommen. Somit konnte nachhaltiger Schaden verhindert werden.

1.1.4 Advanced Persistent Threats (APT)

Bei Advanced Persistent Threats (APT) handelt es sich um zielgerichtete Cyberangriffe, die nicht nur für die öffentliche Verwaltung, sondern auch für Unternehmen und Organisationen eine zunehmende Bedrohung darstellen. APT zeichnen sich neben einem hohen personellen und finanziellen Background vor allem auch durch über das normale Maß hinausgehende technische Fähigkeiten aus. Wird ein System als lohnend identifiziert, wird oft mit Hartnäckigkeit und hohem Ressourceneinsatz vorgegangen. Ist ein solcher Angriff erfolgreich, halten sich APT oftmals sehr lange Zeit unbemerkt in den Systemen der Opfer auf. Mitunter werden Systeme, die der Sicherung oder Einbruchserkennung dienen, auch gezielt manipuliert, um so Sicherungsmechanismen gezielt auszuhebeln.



APT dienen häufig Spionagetätigkeiten. Sie stellen daher eine besondere Gefährdung in Bezug auf die Ausspähung von Staatsgeheimnissen aber auch Forschungs- und Entwicklungsergebnissen dar. Darüber hinaus können sie aber auch für Datenmanipulation oder Sabotage, beispielsweise im Bereich kritischer Infrastruktur, eingesetzt werden.

Sowohl die Erkennung als auch die Verteidigung vor solchen Angriffen gestaltet sich als schwierig. Wurde ein System kompromittiert, ist meist eine umfassende und herausfordernde Aufarbeitung und Säuberung notwendig.

Investitionen der kritischen Infrastruktur im Bereich Cybersicherheit auch 2021 steigend

Die Attribution von APT ist selbst unter großem Aufwand nur sehr eingeschränkt möglich. Technische Indikatoren können in vielen Fällen zwar bestimmten Tätergruppen zugeordnet werden, allerdings existieren auch auf dieser Ebene dokumentierte False-Flag-Angriffe. Die Zuordnung eines Angriffs kann daher immer nur in einem strategischen/politischen Kontext erfolgen.

1.2 Lage Cybersicherheit – Unternehmen und Sicherheitsdienstleister

Staatliche Stellen arbeiten im Bereich der Lagedarstellung und –beurteilung nach dem Kooperationsmodell mit den Bedarfsträgern zusammen.

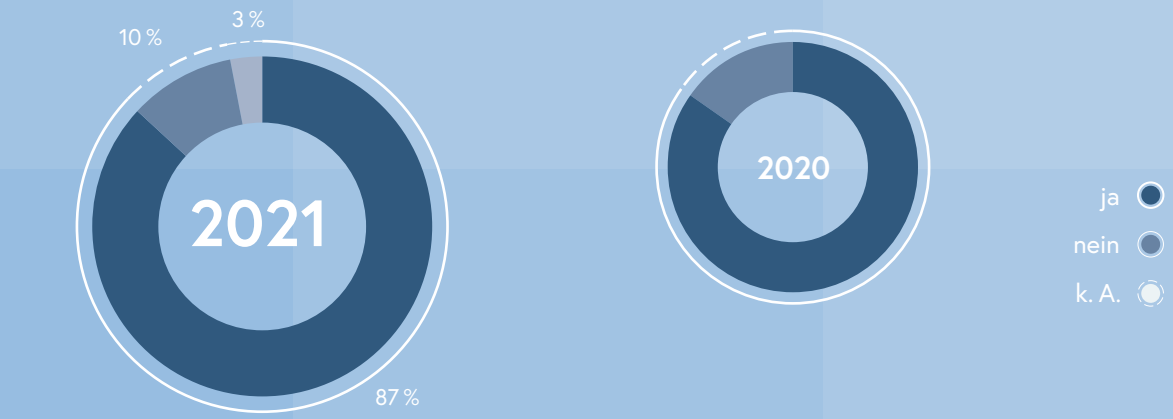
Folgedessen wurden zur Erstellung des vorliegenden Berichtes auch in diesem Berichtsjahr wieder Unternehmen der kritischen Infrastruktur und verfassungsmäßige Einrichtungen sowie führende private Unternehmen aus der Cybersicherheitsbranche eingeladen, aus eigener Perspektive zum Informationsaufkommen beizutragen und mit Expertise zu unterstützen. Auf diese Weise wird ein weitestgehend vollständiges Bild der Cyberlage in Österreich erstellt. Dabei liegt das Augenmerk nicht nur auf konkreten Vorfällen, sondern auch auf Trends und Entwicklungen im Sinne einer abstrakten Überblicksdarstellung.

1.2.1 Lageeinschätzung Unternehmen der kritischen Infrastruktur und verfassungsmäßige Einrichtungen

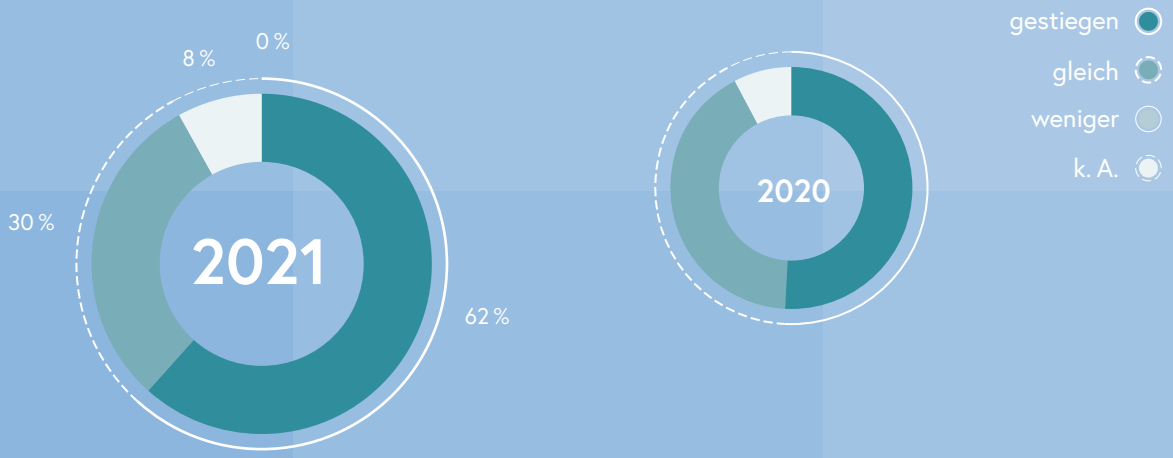
Wie schon in den Vorjahren, wurden auch im Berichtsjahr 2021 erneut bei der Mehrheit der befragten österreichischen Unternehmen der kritischen Infrastruktur Investitionen im Bereich der Cybersicherheit getätigt. Das Verhältnis von Firmen, die ihr Cybersicherheitsbudget erhöhten, zu Firmen, die gleich viel Budget für Cybersicherheit wie im Vorjahr vorgesehen haben, ist über mehrere Jahre hinweg konstant.

Erfreulich ist, dass kein Unternehmen das Budget für Cybersicherheit reduzierte. Durch die zielgerichteten Investitionen konnten mutmaßlich schwerwiegende IT-Sicherheitsvorfälle verhindert werden.

Wurden in Ihrer Firma 2021 neue IT-Security-Maßnahmen implementiert, welche die Erkennbarkeit von IT-Sicherheitsvorfällen erhöhen können?



Wie hat sich in Ihrer Firma im Jahr 2021 das für IT-Security zur Verfügung stehende Buget gegenüber dem Jahr 2020 verändert?



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

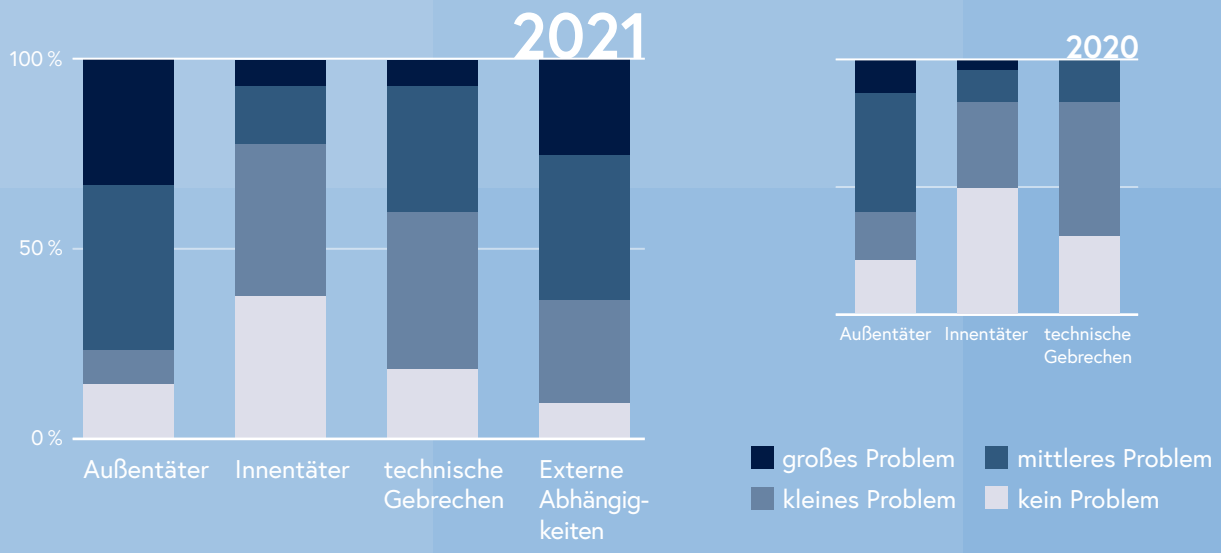
- Einführung von SIEM-, SOC-, EDR- oder ISMS-Lösungen,
- Optimierung der Firewall und Erweiterung der IDS/IPS-Systeme,
- Nutzung von Sandboxen, Nutzung von DNS-Filter,
- erweitertes Logging und ergänzende Monitoring-Tools sowie vermehrte Einführung von Multi-Faktor-Authentifizierung (MFA).

Hinzu kommen ergänzend Security Awareness Trainings für Mitarbeiterinnen und Mitarbeiter, Penetrationtests, Sicherheitsaudits, Phishing-Simulation, Zertifizierungen (z.B. ISO 27001) bzw. die Umsetzung diverser erweiterter Sicherheitskonzepte. Ergänzt wurde dies oftmals durch gezielte Personalrekrutierung für den Sicherheitsbereich.

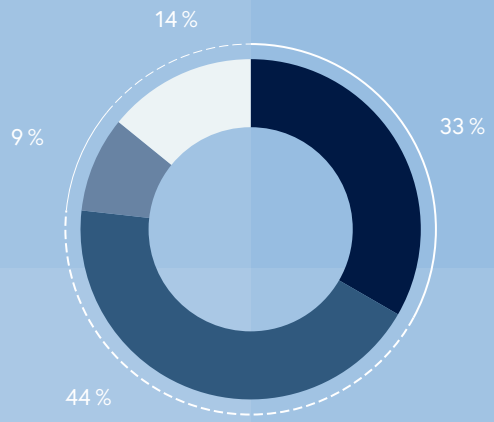
Auch 2021 werden primär Außentäter für Sicherheitsvorfällen verantwortlich gemacht. Externe, teils nicht kontrollierbare Abhängigkeiten durch Supply Chain (z.B. die Notwendigkeit, bestimmte Softwareprodukte zu nutzen), werden vermehrt als Risiko bzw. auch als Problem erkannt.

Technische Gebrechen resultieren bei den Befragten meist in kleineren bis mittleren Problemen – hier wurden über die letzten Jahre Maßnahmen zur Stärkung der Resilienz getroffen. Dementsprechend sind derartige Vorfälle im Vergleich zum Vorjahr weiter rückläufig.

Wie beurteilen Sie die „Vorfallsursache“?

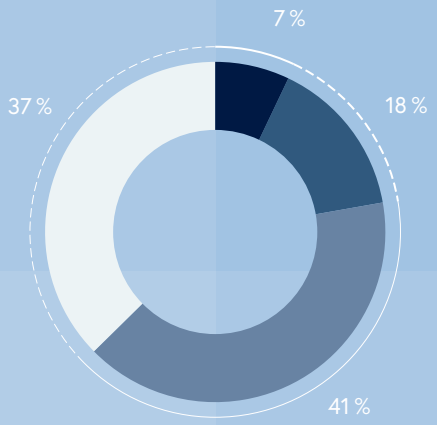


Wie beurteilen Sie die „Vorfallsursache“ Außentäter für das Jahr 2021?



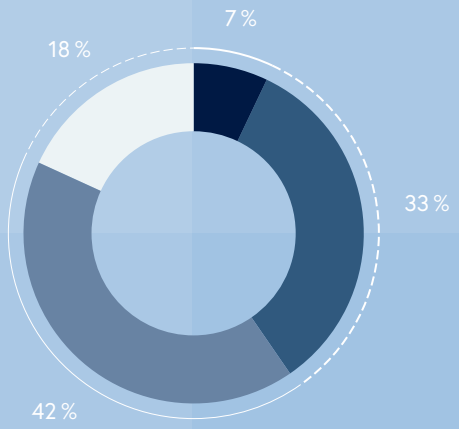
- großes Problem
- mittleres Problem
- kleines Problem
- kein Problem

Wie beurteilen Sie die „Vorfallsursache“ Innentäter für das Jahr 2021?



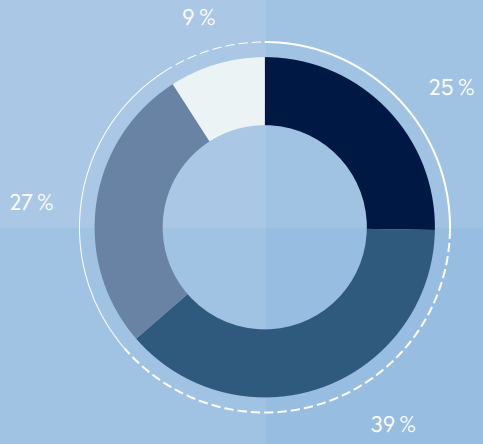
- großes Problem
- mittleres Problem
- kleines Problem
- kein Problem

Wie beurteilen Sie die „Vorfallsursache“ technische Gebrechen für das Jahr 2021?

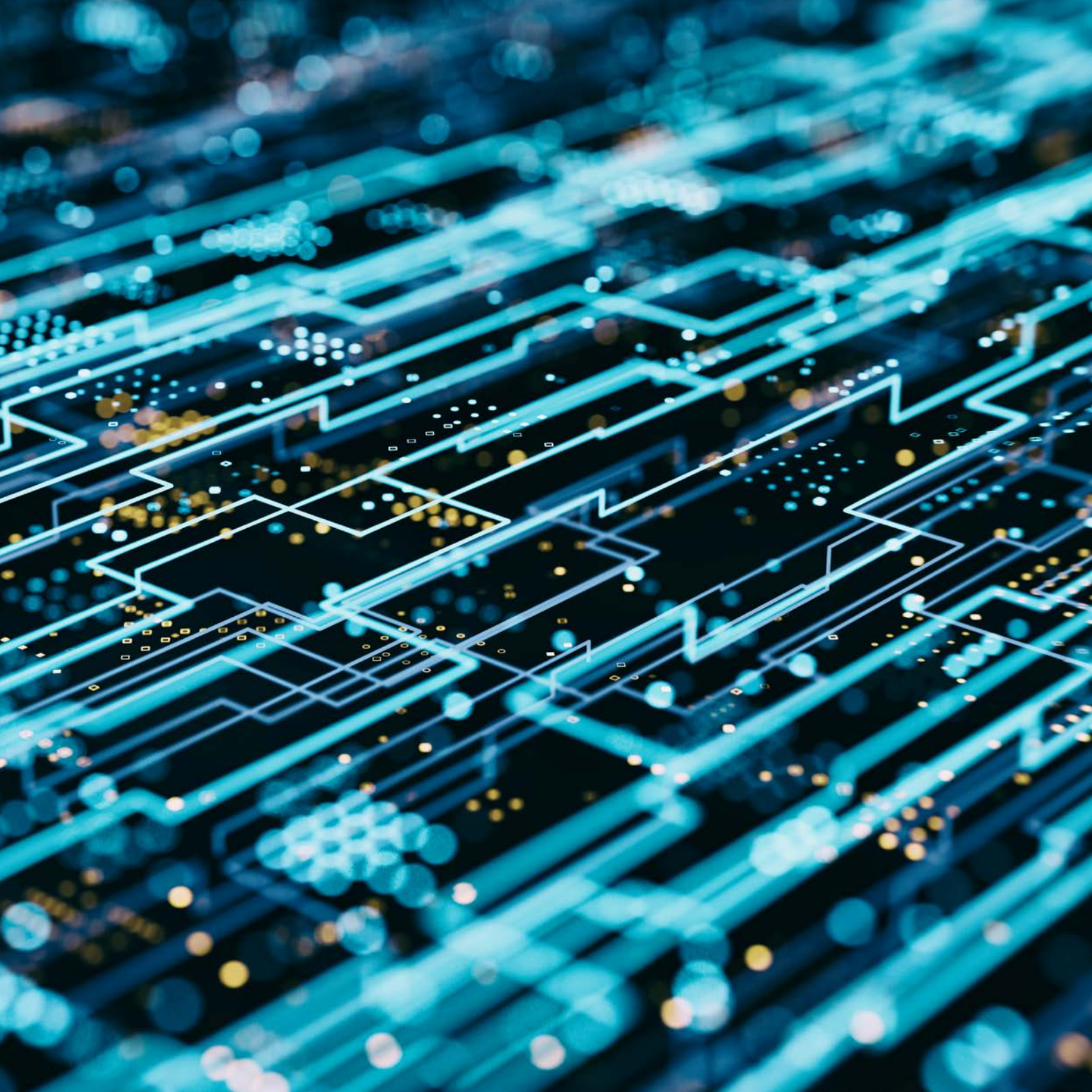


großes Problem
mittleres Problem
kleines Problem
kein Problem

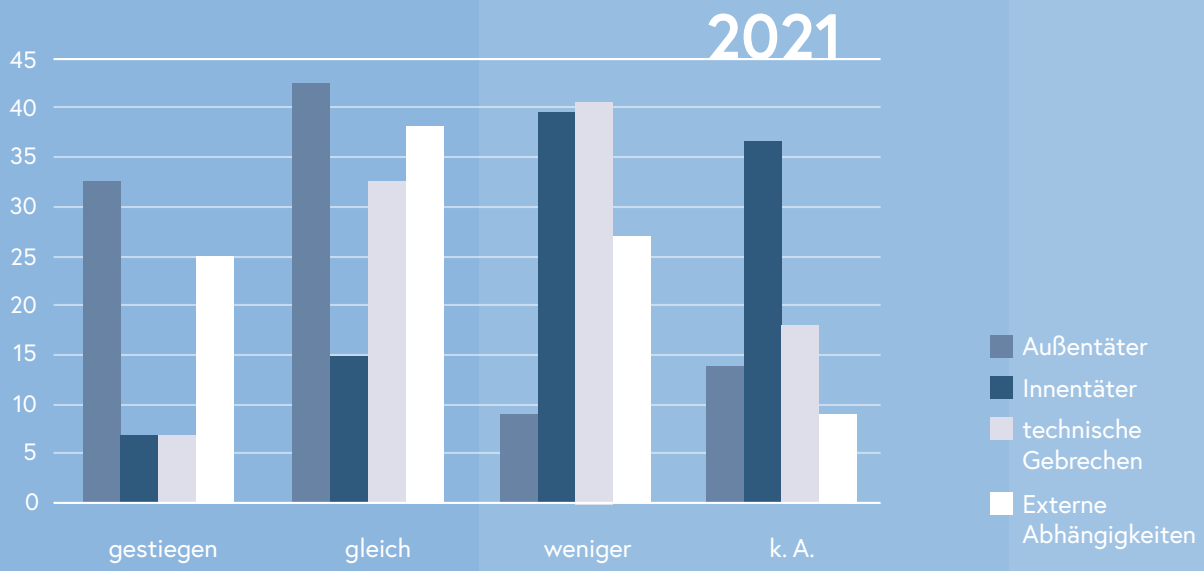
Wie beurteilen Sie die „Vorfallsursache“ Externe Abhängigkeiten (Lieferanten, Dienstleister, etc.) – „Supply Chain“ für das Jahr 2021?



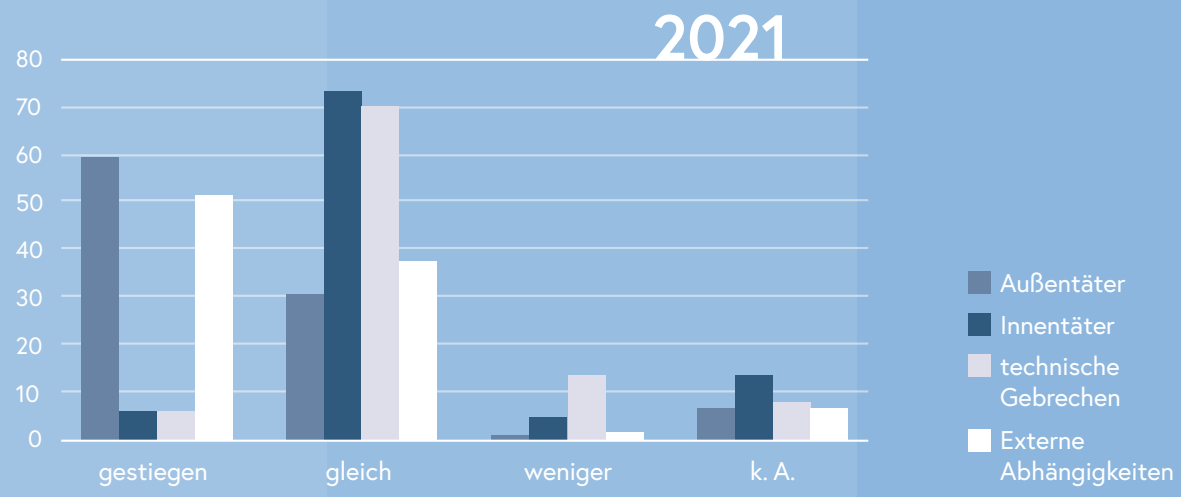
großes Problem
mittleres Problem
kleines Problem
kein Problem



„Vorfallsursachen“ im Vergleich für das Jahr 2021?



Welche Trends konnten Sie 2021 diesbezüglich gegenüber 2020 beobachten?



Abgefragt wurde ebenso, welche „Lessons Learned“ die Unternehmen der kritischen Infrastruktur und der verfassungsmäßigen Einrichtungen im Beobachtungszeitraum gezogen hatten.

Neben Awareness und deren Erhöhung waren es vor allem die Notwendigkeit der Analyse von Abhängigkeiten in der Lieferkette sowie der Identifikation von darin liegenden Schwachstellen.

Flächendeckendes Homeoffice erhöht den Bedarf an sicheren Remotezugängen massiv

Die Unternehmen führten weiter aus, dass Penetrationstests als Mittel der Schwachstellenanalyse immer wichtiger werden und vor allem dazu dienen, eigene Angriffsflächen nachhaltig zu reduzieren.

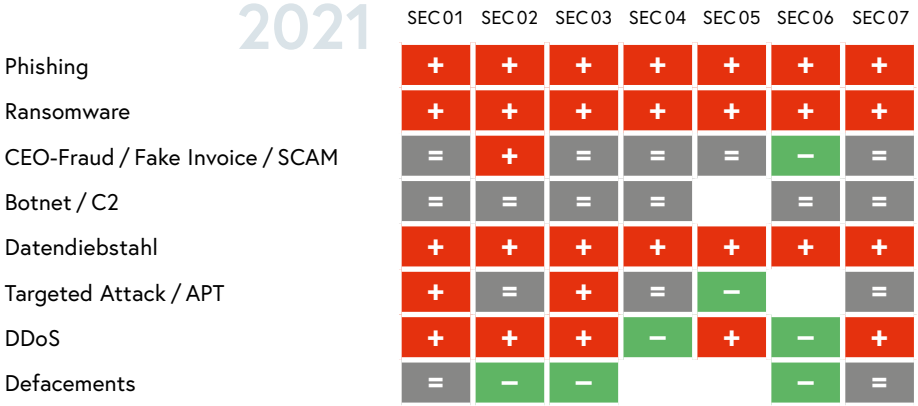
Die Erkennung und Bearbeitung von Vorfällen wird immer komplexer und zeitintensiver. Verwertbare Informationen aus Logging-, EDR- und SIEM-Systemen sollten daher eingeführt und betrieben werden. Hiezu ist die Qualifizierung eignenen Personals von besonderer Wichtigkeit, um einerseits die generierten Daten analysier- und verwertbar zu machen, aber auch um die Abhängigkeit von externen Dienstleistern zu reduzieren.

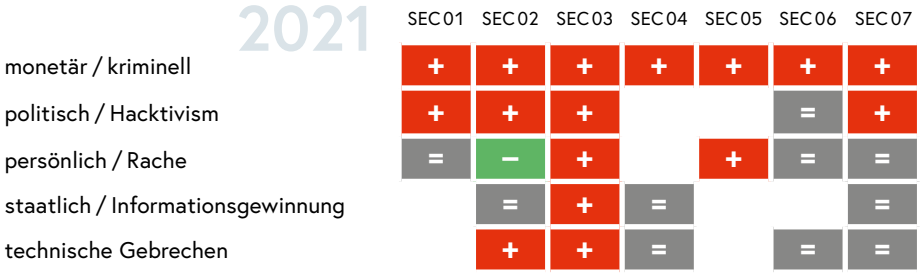
Mittlerweile verkürzt sich die Zeit zwischen Veröffentlichung und Ausnutzung von Schwachstellen dramatisch. Oft dauert es nur Stunden nach Bekanntwerden einer Vulnerabilität, bis automatisierte Angriffe auf potentiell verwundbare Systeme beginnen. Von daher kommt dem Schwachstellen- und Patchmanangement eine immer größere Rolle zu.

Zuletzt wurden auch die sich durch das Homeoffice und die sich daraus ergebende Angriffsoberfläche breitflächiger Fernzugänge als neue Bedrohung bzw. Herausforderung angeführt. Entsprechende Absicherungsmaßnahmen werden auch hier immer wichtiger.

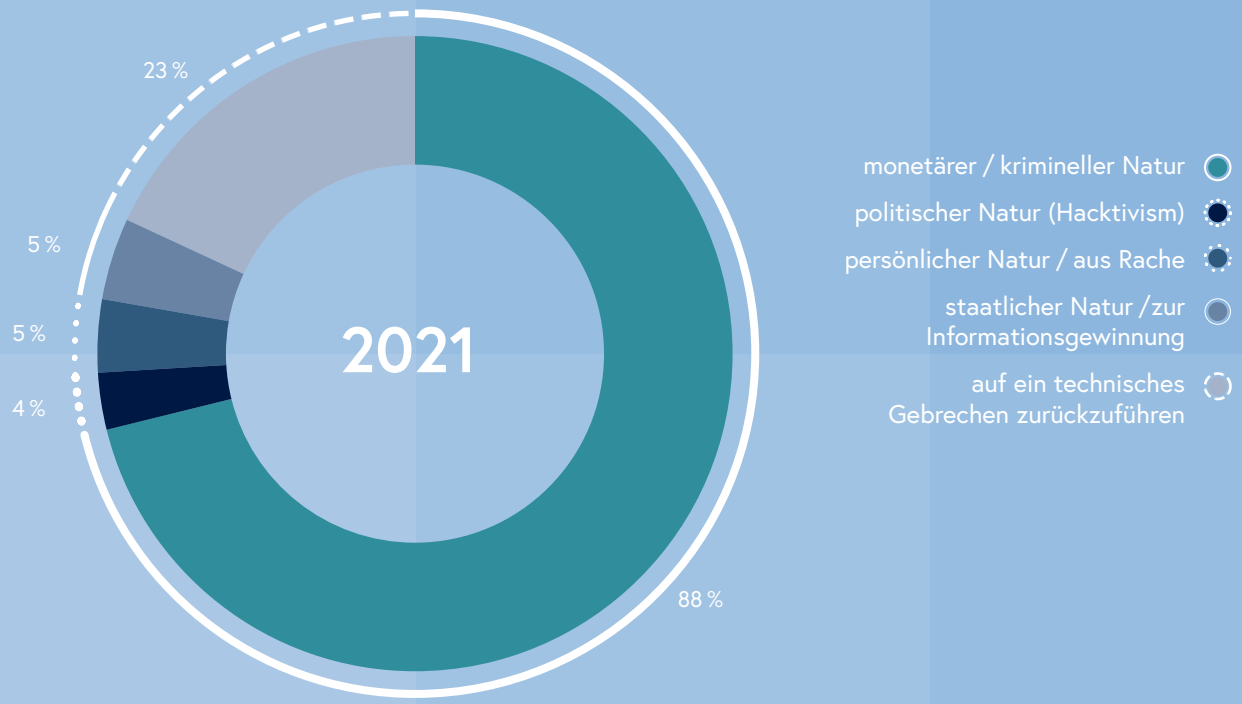
1.2.2 Lageeinschätzung führender privater Unternehmen aus der Cybersicherheitsbranche

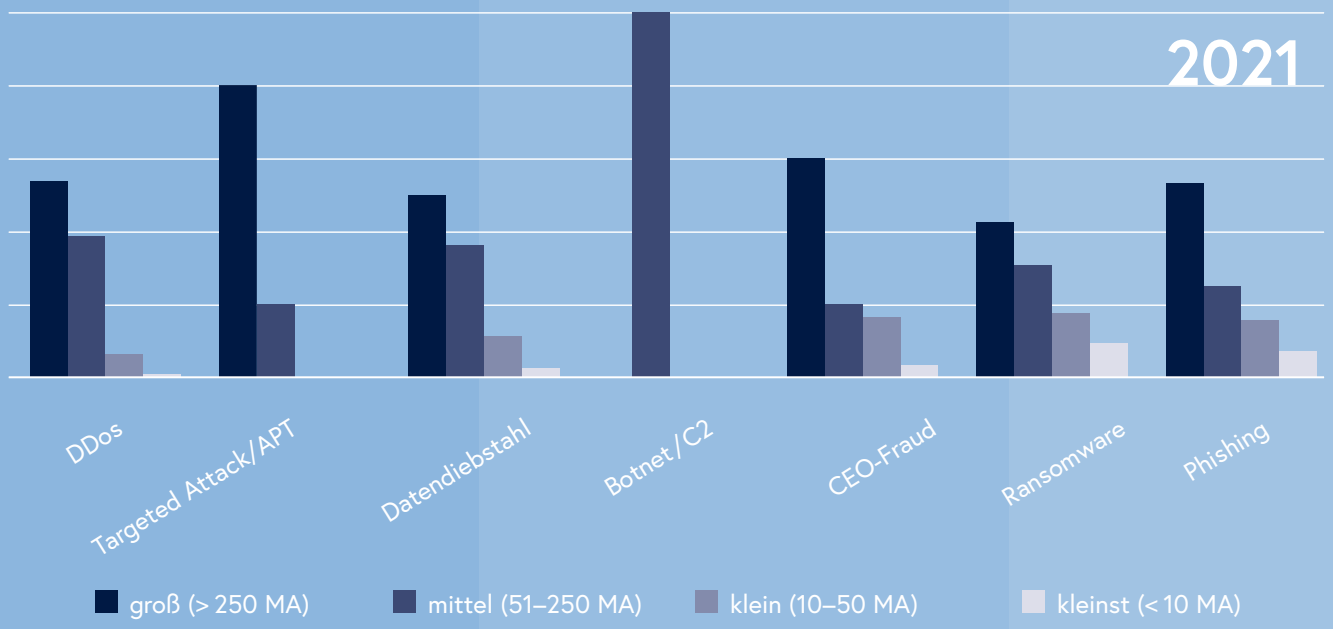
Aus den eingegangenen Beantwortungen der Befragung von führenden privaten Unternehmen aus dem Bereich der Sicherheitsdienstleister für das Jahr 2021 lassen sich nachfolgend angeführte Trends und Lessons Identified ableiten:





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




2021
DDos
Targeted Attack/APT
Datendiebstahl
Botnet/C2
CEO-Fraud
Ransomware
Phishing
groß (> 250 MA)
mittel (51–250 MA)
klein (10–50 MA)
kleinst (< 10 MA)

Phishing: Die Resilienz der Unternehmen in Bezug auf Phishing wird noch immer nicht als ausreichend beurteilt. Die Awareness der Mitarbeiterinnen und Mitarbeiter ist oft nicht ausreichend und entsprechendes Bewusstsein in Hinsicht auf Gefahren und Auswirkungen nicht ausreichend vorhanden. Gerade gezielte, auf das Unternehmen und deren Spezifika angepasste E-Mails haben immer noch eine hohe Durchschlagsqote. Auch wenn Awareness-Trainings diesen Angriffsvektor nicht vollständig eliminieren können, sind sie ein probates Mittel, um dieses Gefahrenpotential entsprechend zu reduzieren.

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

Gefährdung durch Phishing nimmt weiter zu

Ransomware: Die fehlende Netzsegmentierung stellt in vielen Unternehmen immer noch ein großes Problem dar und erhöht dadurch die Bedrohung der Ausbreitung von Schadsoftware im internen Netz (lateral movement). Als beliebte Angriffsfläche haben sich durch die Einführung von Homeoffice vermehrt bereitgestellten Remote Access Lösungen erwiesen. Weiterhin wird Sicherheit nur bis zum Perimeter gedacht – ist der Angreifer erst einmal im Netz, gibt es außer Virenscannern oft wenig, was ihn aufhalten könnte. Eine kohärente und umfassende Security Strategy, welche Risiken identifiziert, klassifiziert und Maßnahmen definiert, fehlt in den meisten Unternehmen. Grundsätzlich kann festgehalten werden, dass die Awareness zwar generell steigt, als ausreichend kann sie aber vor allem in Hinblick auf die Kritikalität des Cyberbereiches für die Erfüllung der Kernaufgaben jedenfalls nicht bezeichnet werden. Das zeigt sich auch darin, dass bis heute nicht jedes Unternehmen eine dezidierte Backup-Strategie vorweisen kann – auch ist eine unternehmensweite Umsetzung des Least-Privilege-Prinzip (nur die für die Erfüllung einer konkreten Aufgabe notwendigen Berechtigungen und Zugriffsrechte) eher die Ausnahme.

CEO-Fraud/Business Email Compromise (BEC)/Fake Invoice/SCAM: Aufgrund der mitunter hohen erzielbaren Summen erfreuen sich diese Angriffsvektoren hoher Beliebtheit und werden in ihren Ansätzen raffinierter und schwerer zu erkennen. So werden BEC oftmals auch für andere, weitreichendere Angriffe genutzt. Generell ist aber festzustellen, dass die Awareness für diese Art der Bedrohung weiter steigt. Die Problematik und die Gefahren von Social Engineering werden als ernst erkannt und werden in den Schulungsmaßnahmen entsprechend intensiv behandelt.

Botnet/C2: Ohne laufendes Security-Monitoring bleiben aktive Bots oft monatelang unentdeckt. Veraltete Betriebssysteme (Legacy Systeme) sind weiterhin exponiert und ohne weitere Absicherungsmaßnahmen im Einsatz und stellen somit ein willkommenes Einfallstor für Bots dar.

Investitionen in Cybersicherheit konnten schwerwiegende IT-Sicherheitsvorfälle verhindern

Datendiebstahl: Trotz steigender Anzeigenmoral muss die Dunkelziffer weiterhin als hoch angenommen werden. Datendiebstähle erfolgten im Berichtszeitraum häufig in Kombination mit Ransomware-Angriffen und stellen eine permanente Bedrohung dar.

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

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

1.3 Lage Cybercrime

Die Betrachtung der polizeilichen Kriminalstatistik lässt mit über 46.000 angezeigten Delikten im Jahr 2021 eine Steigerung von etwa 28% gegenüber dem Jahr 2020 erkennen. Die genauen Deliktszahlen werden jährlich im Frühjahr mit der polizeilichen Kriminalstatistik veröffentlicht. Eine tiefergehende Analyse und Beschreibung der kriminalpolizeilichen Phänomene erfolgt mit dem jährlichen Cybercrimereport des Bundeskriminalamtes.

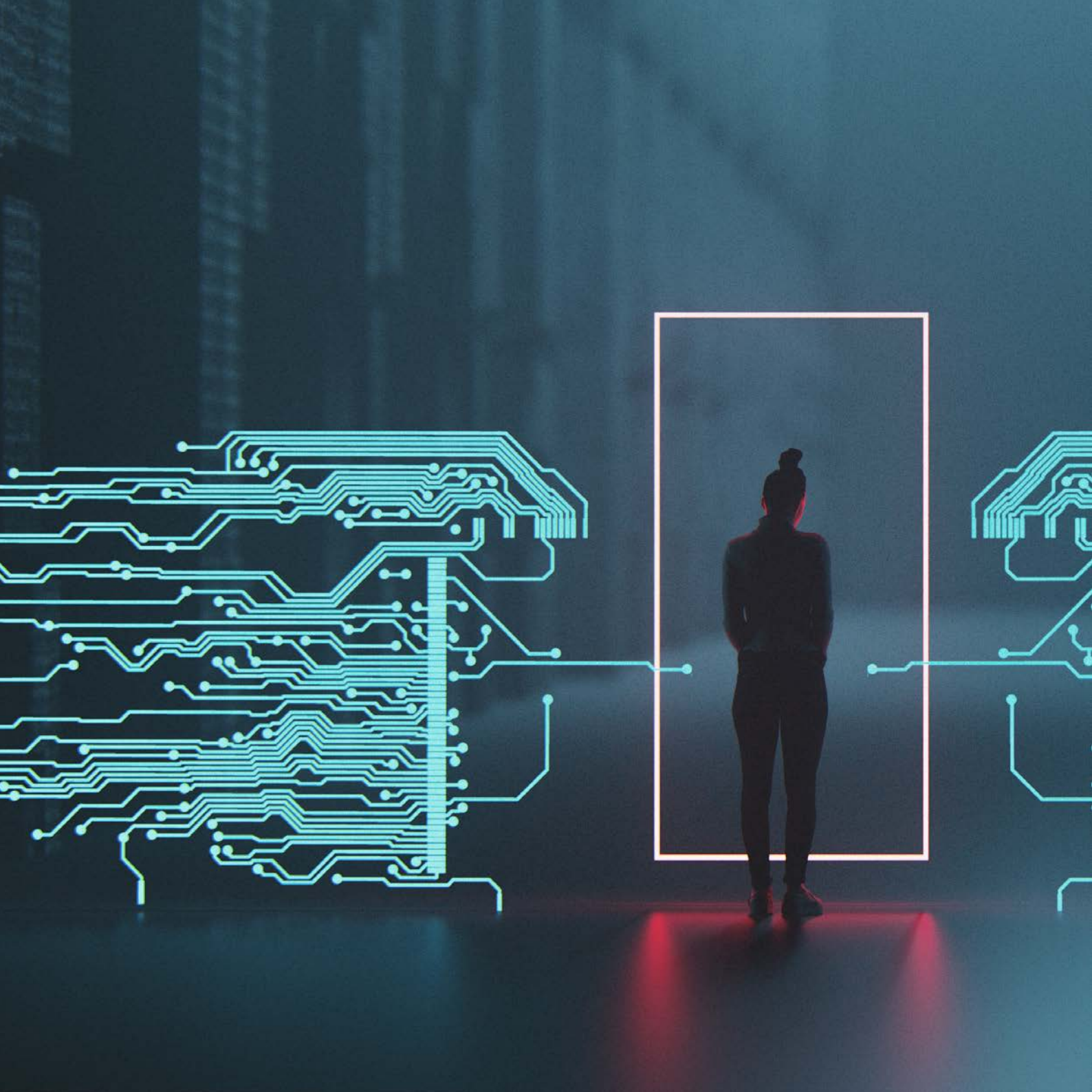
Der Begriff Cybercrime umfasst:

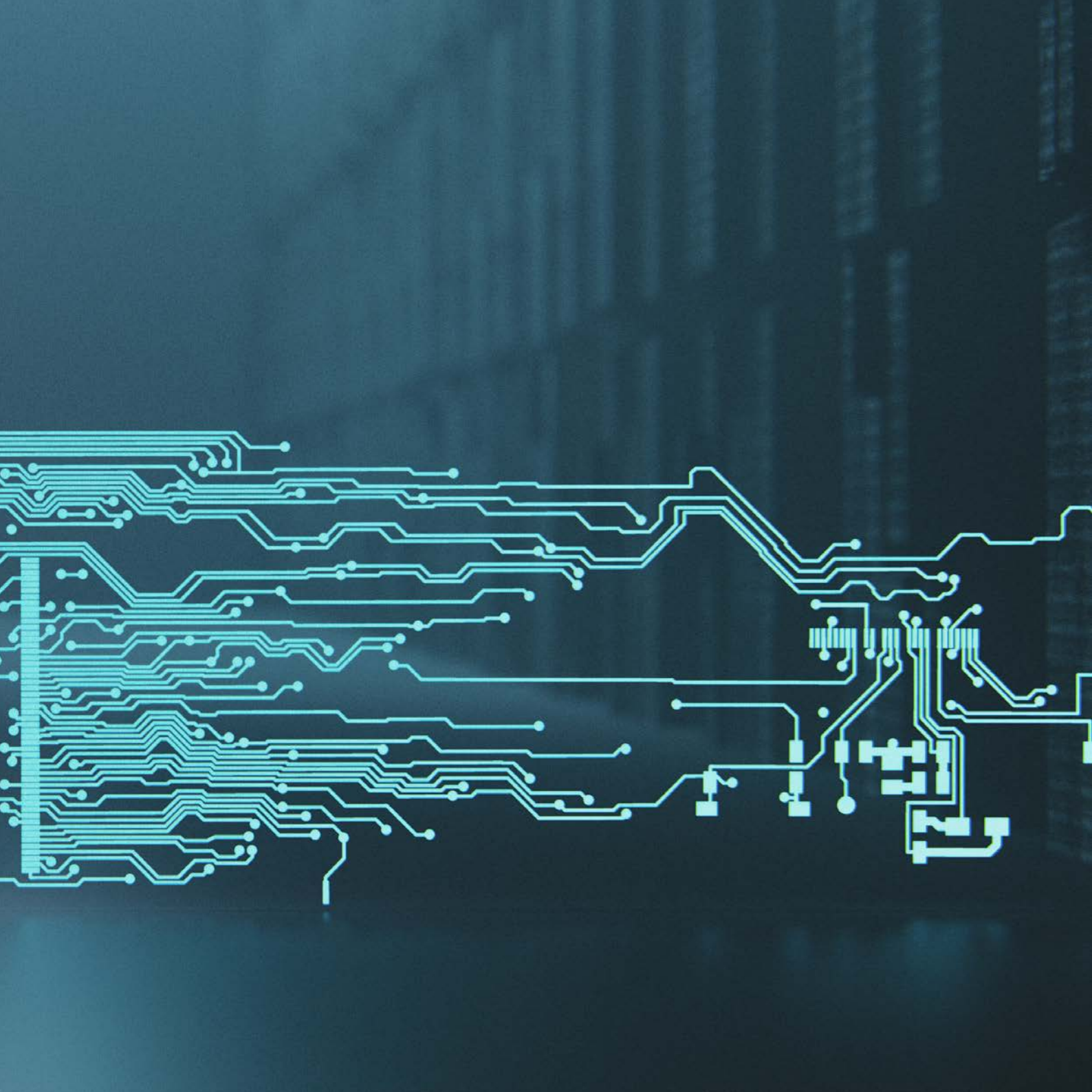
- Cybercrime im engeren Sinn,
- Internetbetrug und
- sonstige Kriminalität im Internet.

Cyberkriminalität im Jahr 2021 wieder enorm gestiegen

1.3.1 Cybercrime im engeren Sinn

Im Bereich der Cybercrime im engeren Sinn sind die Anzeigen im Jahr 2021 gegenüber dem Jahr 2020 um etwa 20% angestiegen. Darunter fallen Straftaten, bei denen Angriffe auf Daten oder Computersysteme unter Ausnutzung der Informations- und Kommunikationstechnik begangen werden. Beispiele dafür sind der widerrechtliche Zugriff auf ein Computersystem oder die Datenbeschädigung. Angriffe durch Schadsoftware, DDoS-Angriffe und widerrechtliche Zugriffe auf Computernetzwerke und -systeme lassen zu Jahresbeginn 2021 die Anzahl der Anzeigen hierzu signifikant steigen. Die Anzeigen im Bereich der Ransomware sind zunächst rückläufig, dafür steigt die Angriffsqualität (vermehrt durch Ausnützung aktueller Sicherheitslücken) und die jeweiligen Schadenshöhen in den einzelnen Fällen enorm. Laut den Zahlen in der Kriminalstatistik ist im Frühjahr 2021 außerdem ersichtlich, dass immer häufiger Cybermobbing-Vorfälle zur Anzeige gebracht werden. Im Zusammenhang mit Ransomware ist gegen Jahresmitte generell eine erhöhte Aktivität von unterschiedlichen Tätergruppen wahrnehmbar. Bei größeren Unternehmen steigt die Gefahr, dass zusätzlich zur Verschlüsselung auch noch mit der Veröffentlichung von Unternehmensdaten gedroht wird. Nach einem Schadensfall





ist gerade bei größeren Unternehmen damit zu rechnen, dass es trotz vorhandener Backups für mindestens drei bis sieben Tage zu Produktionsausfällen kommen kann. Gegen Jahresende ist die Anzahl von Meldungen und Anzeigen in Österreich zur Verbreitung von Schadsoftware stark angestiegen.

1.3.2 Internetbetrug

Den zahlenmäßig größten Faktor stellt der Internetbetrug dar. Dieser ist auch maßgeblich für den letztjährigen Anstieg der Delikte im Bereich der Cyberkriminalität verantwortlich. Fast die Hälfte der Internetdelikte fallen auf Betrugsdelikte: 2021 wurden 22.440 Fälle von Internetbetrug angezeigt, ein starkes Plus von 19,5%. Mit der fortschreitenden Digitalisierung verlagern sich Betrugsdelikte immer mehr ins Internet. Für die Täter ist es ein Leichtes, aufgrund technischer Anonymisierung sowie Verschleierung der Finanzflüsse Betrugshandlungen unerkannt und damit „sicher" durchzuführen. Zusätzlich können durch den weltweiten Zugang zum Internet immer mehr Menschen als potenzielle Opfer angesprochen werden. Der Bestellbetrug – sowohl käufer- als auch verkäuferseitig – ist der mit Abstand größte Bereich, gefolgt von unbefugten Abbuchungen von Bankkonten der Opfer. Hier waren vor allem die „FluBot"-Attacken, die Mitte des Jahres 2021 stark auftraten, verantwortlich. Aber auch der digitale Investmentbetrug schlug sich 2021 nieder.

1.3.3 Sonstige Kriminalität im Internet

Unter sonstiger Kriminalität im Internet versteht man alle Straftaten mit der Tatörtlichkeit im Internet, ausgenommen solche, die unter Cybercrime im engeren Sinn und Internetbetrug fallen sowie zusätzlich alle Straftaten nach § 207a StGB (Pornographische Darstellungen Minderjähriger) und § 208a StGB (Anbahnung von Sexualkontakten zu Unmündigen), unabhängig von der Tatörtlichkeit. Bei der „sonstigen Kriminalität im Internet" wurde im Jahr 2021 ebenfalls ein Anstieg der Delikte verzeichnet. Der Grund dafür liegt in der zunehmenden Verlagerung klassischer Strafrechtsdelikte ins Internet. Gleichzeitig werden sogenannte „Crime-as-a-Service"-Leistungen im Darknet angeboten. Dabei handelt es sich vorwiegend um Hackingtools oder Erpressungstrojaner. Ebenso wurde ein vermehrter Vertrieb von Falschgeld, Kinderpornographie, Kreditkartendaten

und gefälschten Urkunden wahrgenommen. Durch die im Darknet angebotenen Dienste steigen vor allem Erpressungen mit Ransomware und Massenerpressungsmails, meist begleitet von Geldforderungen in Bitcoin, sehr stark an.

1.4 Cyberlage Landesverteidigung

kritische Infrastrukturen durch Cyberangriffe stark bedroht

Auch die Ereignisse im Cyberraum 2021 haben gezeigt, dass die COVID19-Pandemie weiterhin massiv das Weltgeschehen beeinflusst. Hierbei waren Angriffe auf die kritische Infrastruktur im Gesundheitssektor, besonders im Hinblick auf die andauernde Pandemie, besonders besorgniserregend. Das Österreichische Bundesheer (ÖBH) ist laufend in Kontakt mit den nationalen Sicherheitsgremien, um die Sicherheit und Souveränität Österreichs auch in Krisensituationen aufrecht zu erhalten.

Die sich stetig erhöhende Gefahr im Cyberraum war 2021 besonders geprägt von Cyberangriffen auf kritische Infrastrukturen mit teilweise schwerwiegenden Auswirkungen auf die reale Welt. So begann bereits Ende 2020 ein Angriff, welcher weit in das Jahr 2021 andauerte. Dabei handelte es sich um die sogenannten „SolarWinds"-Hacks. Die Schwachstelle schlug international enorme Wellen – in den USA, wo die Software SolarWinds hauptsächlich zum Einsatz kommt – waren nach Medienangaben um die 250 Behörden und Ministerien betroffen. Den Angreifern gelang es dabei, durch ein Systemupdate eine Hintertür in der Software zu platzieren, wodurch sie mithilfe von Schadsoftware in die Zielnetze eindringen konnten. Das initiale Ziel der vermutlich staatsnahen Akteure war hierbei nicht wie bei Ransomware der finanzielle Mehrwert, sondern vertrauliche Informationen über die Ziele zu bekommen. Der Angriff verdeutlicht besonders gut, wie komplex der Bereich der Informations- und Cybersicherheit mittlerweile geworden ist. Es zeigt sich, dass es nicht mehr ausreichend ist, nur die eigenen Systeme abzusichern, sondern auch die Bewertung der gesamten Versorgungskette und Lieferanten („Supply-Chain") muss berücksichtigt werden.

Neben SolarWinds erlitt die USA auch zwei weitere massive Angriffe gegen ihre kritische Infrastruktur. Die Unternehmen „JBS“ (einer der größten Fleischproduzenten der Welt), sowie „Colonial Pipeline“ wurden Opfer von Ransomware. Die Angriffe hatten, neben enormen finanziellen Schäden für die Betroffenen, auch Auswirkungen auf die Bevölkerung. So sorgten beispielsweise Panik-Einkäufe bei den Tankstellen für Treibstoffknappheit in einem Teil der USA. Sowohl SolarWinds als auch die Ransomware-Angriffe auf die beiden Unternehmen wurden russischen Akteuren zugeschoben. Dies verdeutlicht, wie sehr geopolitische Konflikte mittlerweile auch in Friedenszeiten, zu einem Teil unter dem Radar der Öffentlichkeit, ausgetragen werden. Daher ist es für das Bundesministerium für Landesverteidigung/Österreichische Bundesheer (BMLV/ÖBH) unumgänglich, die nötigen Kompetenzen zur Abwehr dieser Gefahren auf die ressorteigenen und auch gesamtstaatlichen Systeme zu vertiefen und zu erweitern. International haben in den letzten Jahren nahezu alle Nationen ihre staatlichen, militärischen und zivilen Cybersicherheitskompetenzen weiter ausgebaut.

Ein weiterer Trend, der auch 2021 im Fokus des BMLV stand, ist die gezielte Beeinflussung der Öffentlichkeit durch Desinformationskampagnen. Vor allem durch die Covid19-Pandemie wurden sowohl national als auch international Kampagnen gegen Regierungen, Behörden, Institutionen und Einzelpersonen beobachtet. Das BMLV/ÖBH führt intensive nationale und internationale Medienbeobachtungen durch, um Spannungen in der Gesellschaft so früh wie möglich zu erkennen und auch entsprechend aufklärend reagieren zu können.

Es zeigt sich, wie in jedem Jahr, dass auch in der Landesverteidigung der Cyberraum immer mehr an Bedeutung gewinnt. So beginnen moderne Konflikte bereits weit vor Einsatz militärischer Truppen mit hybrider Einflussnahme unter bevorzugter Nutzung des Cyberraums. Auch die militärische Konfliktführung wird im Normalfall nur mehr mit Unterstützung von moderner Technologie, inklusive Angriffen und beeinflussendem Agieren im Cyberraum, Unterstützung der Truppen durch Drohnenaufklärung oder Battlemanagement mit Hilfe von künstlicher Intelligenz, durchgeführt. Auf EU-Ebene

wurde 2021 daher die „EU Military Vision and Strategy on Cyberspace as a Domain of Operations“ verabschiedet, welche eine verstärkte Nutzung von Cyberfähigkeiten im Rahmen von GSVP-Missionen und Operationen vorsieht.

Aufgrund all dieser Entwicklungen ist das ÖBH durch nationale und internationale Kooperationen aktiv mit dem Ausbau seiner Cyberverteidigungsfähigkeiten sowie der Erforschung moderner Technologien befasst.

2
Internationale Entwicklungen

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

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

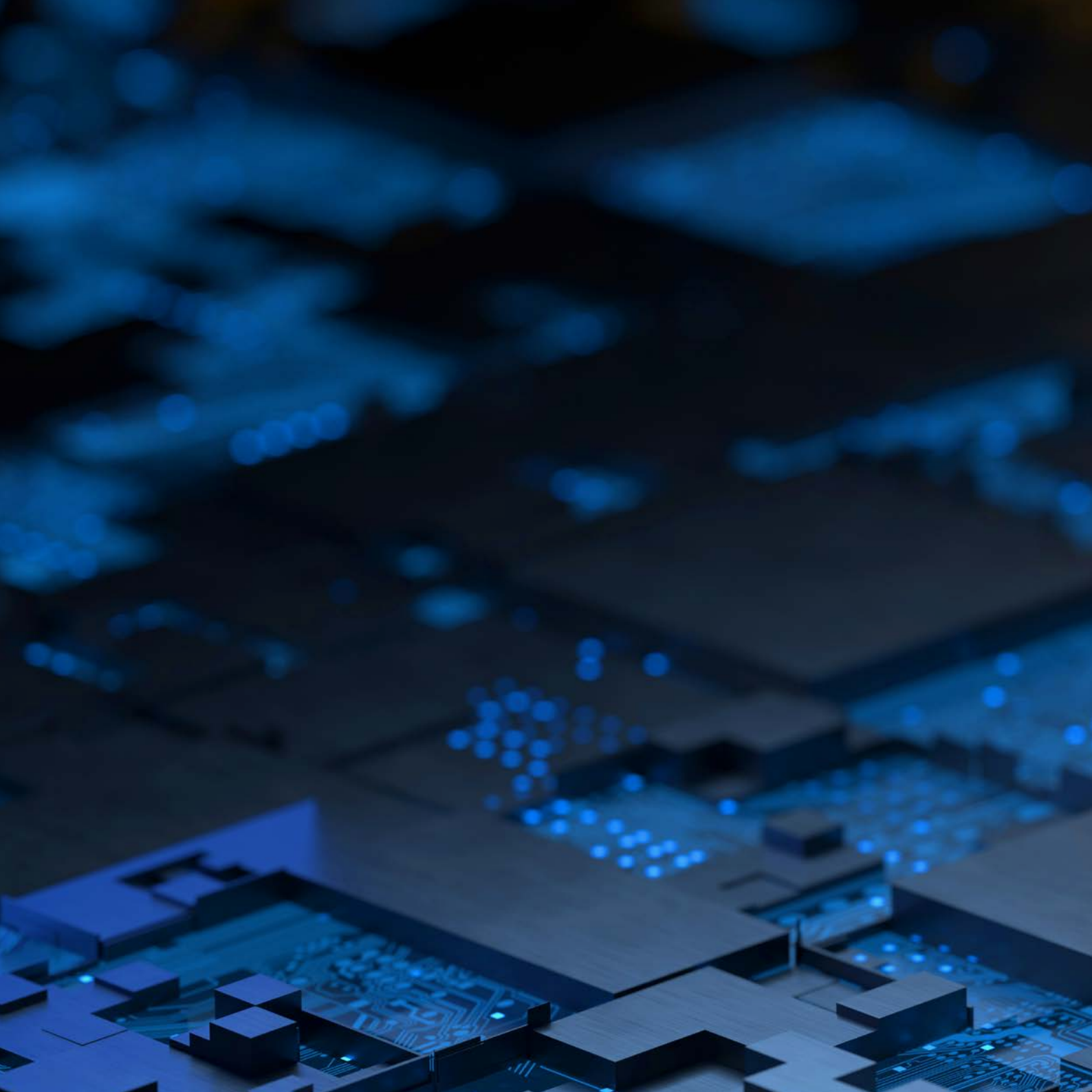
2.1 Europäische Union (EU)

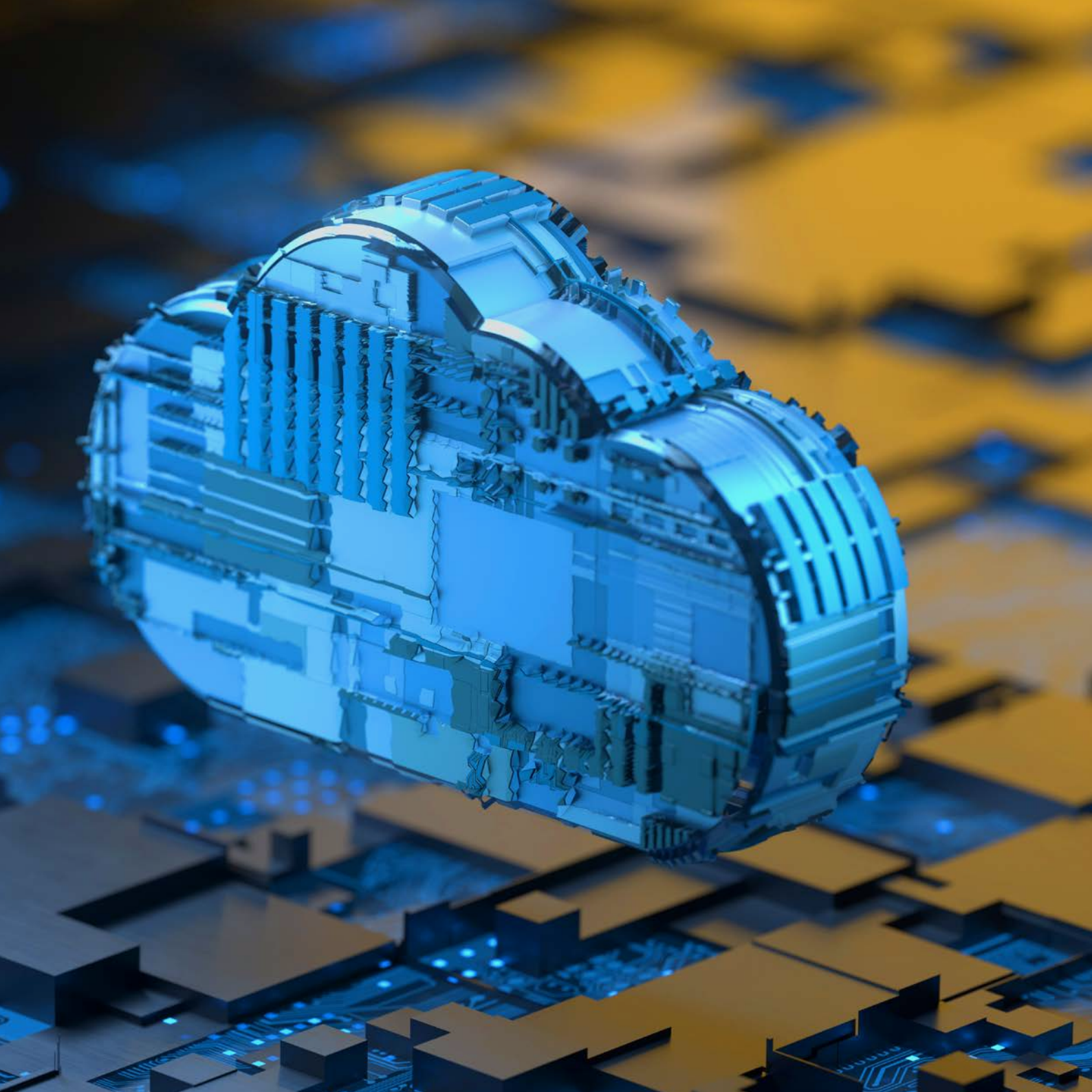
Cybersicherheit erfährt weiterhin eine zunehmende Bedeutung. Auch im Jahr 2021 war sie Thema in zahlreichen internationalen Organisationen und multilateralen Foren. Dabei wurde teilweise sehr kontroversiell diskutiert, vor allem die unterschiedlichen Auslegungen und Sichtweisen in Bezug auf Rechte und Pflichten, Regulatorien sowie Grenzen der Meinungsfreiheit stellten die Verhandler vor Herausforderungen.

Dabei werden die außen- und sicherheitspolitischen Maßnahmen vom Bundesministerium für europäische und internationale Angelegenheiten (BMEIA) koordiniert, dem Bundeskanzleramt (BKA) obliegt die Koordination der Cybersicherheit im Zusammenhang mit der Europäischen Union (EU). Im Allgemeinen engagiert sich Österreich auf internationaler Ebene für ein freies, offenes und sicheres Internet, wobei die Ausübung aller Menschenrechte auch im virtuellen Raum gewährleistet werden muss. Dabei muss auf ein angemessenes Gleichgewicht zwischen den Interessen der Strafverfolgung und der Achtung grundlegender Menschenrechte, wie dem Recht auf freie Meinungsäußerung und Informationsfreiheit sowie dem Recht auf Privatleben und Privatsphäre geachtet werden. Österreich setzt sich zudem bereits bei der Entwicklung neuer digitaler Technologien für die Einhaltung menschenrechtlicher Standards ein.

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 Angelegenheiten im Cyberrraum, insbesondere für die Cyberpolitik und die gesetzgeberischen Aktivitäten, zuständig. Sie legt die Cyberprioritäten und strategischen Ziele der EU als Teil eines umfassenden politischen Rahmens fest und gewährleistet eine Arbeitsplattform, die eine Harmonisierung und ein einheitliches Vorgehen in Fragen der Cyberpolitik ermöglicht.





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

Schlussfolgerungen des Rates zur EU-Cybersicherheitsstrategie für die digitale Dekade angenommen

Ingesamt gab es mit einer beeindruckenden Anzahl von 60 Sitzungen der HWP Cyber im Jahr 2021 so viele Sitzungen wie noch nie, was von der hohen Arbeitsintensität zur Weiterentwicklung der europäischen Cybersicherheitspolitik zeugt. Im Bereich der Verhandlung von Rechtsakten stand dabei die am 16. Dezember 2020 von der EU-Kommision vorgestellte NIS-2-Richtlinie im Vordergrund. Während die portugische Ratspräsidentschaft eine erste Lesung abschließen konnte und bei der Tagung des Rates der EU „Verkehr, Telekommunikation und Energie“ am 4. Juni 2021 einen Fortschrittsbericht vorlegte, gelang der slowenischen Ratspräsidentschaft das Erreichen einer allgemeinen Ausrichtung über die NIS-2-Richtlinie bei der Tagung des Rates der EU „Verkehr, Telekommunikation und Energie“ am 3. Dezember 2021. Siehe Kapitel 2.1.8.

Die HWP Cyber bereitete die „Schlussfolgerungen des Rates zur Cybersicherheitsstrategie der EU für die digitale Dekade“ vor, welche vom Rat am 22. März 2021 gebilligt wurden. Die Cybersicherheitsstrategie wurde am 16. Dezember 2020 von der EU-Kommission und dem Hohen Vertreter für Außen- und Sicherheitspolitik vorgelegt. Sie löst die Cybersicherheitsstrategie 2013 als neuen strategischen Referenzrahmen für Cybersicherheit auf EU-Ebene ab und legt den Rahmen für EU-Maßnahmen fest, mit denen Bürgerinnen und Bürger sowie Unternehmen der EU vor Cyberbedrohungen geschützt, sichere Informationssysteme gefördert und ein globaler, offener, freier und sicherer Cyberraum gewährleistet werden sollen. In den Ratsschlussfolgerungen werden die Prioritäten der Mitgliedstaaten festgelegt und bekräftigt, dass die Cybersicherheit für den Aufbau eines widerstandsfähigen, grünen und digitalen Europas von wesentlicher Bedeutung ist. Als zentrales Ziel wird das Erreichen der strategischen Autonomie unter Bewahrung einer offenen Wirtschaft festgehalten. Dazu gehört auch die Stärkung der Fähigkeit zur autonomen Entscheidungen

im Bereich der Cybersicherheit, um die digitale Führungsrolle der EU und ihre strategischen Kapazitäten zu stärken.

Des Weiteren nahm der Rat bezüglich der Joint Cyber Unit am 19. Oktober 2019 Schlussfolgerungen „zur Prüfung des Potenzials der Initiative für eine Gemeinsame Cyber-Einheit als Ergänzung zur koordinierten Reaktion der EU auf große Cybersicherheitsvorfälle und –krisen“ an, welche von der HWP Cyber vorbereitet wurden.

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

2.1.2 NIS-Kooperationsgruppe

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

Die NIS-Kooperationsgruppe nimmt ihre Aktivitäten auf der Grundlage von zweijährigen Arbeitsprogrammen wahr. Das Arbeitsprogramm für den Zeitraum 2020 bis 2022 beauftragt eine Bestandsaufnahme der bisher erbrachten Leistungen, eine Bewertung, deren Auswirkungen und die Identifikation von Verbesserungspotentialen. Ziel der NIS-Kooperationsgruppe ist es, die Umsetzung der NIS-Richtlinie weiterhin zu erleichtern, den Informationsaustausch weiter zu operationalisieren sowie eine strategische Diskussion über wichtige politische Dokumente für die Cybersicherheit in der EU, wie z.B. in Bezug auf 5G, künstliche Intelligenz oder das Internet der Dinge, zu ermöglichen.

Die NIS-Kooperationsgruppe traf sich im Jahr 2021 zu vier Plenarsitzungen und zu mehr als 23 Sitzungen im Rahmen ihrer Arbeitsbereiche („Work Stream Meetings“). Zu den umfangreichen Arbeiten im Bereich der Cybersicherheit von 5G-Netzen siehe Kapitel 2.1.5.

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 Widerstandsfähigkeit der EU und ihrer Mitgliedstaaten, dem gemeinsamen Vorgehen bei der Abwehr von hybriden Bedrohungen sowie der Verbesserung der strategischen Kommunikation und der Bekämpfung von Desinformation. Die Arbeitsgruppe dient der Koordinierung innerhalb des Rates und der Zusammenarbeit mit den anderen Organen, Diensten und Agenturen der EU. Böswillige Cyberaktivitäten stellen häufig Schlüsselelemente hybrider Bedrohungen dar und werden in diesem Kontext von den Arbeiten der HWP ERCHT umfasst.

Im zweiten Halbjahr 2021 begann die HWP ERCHT mit der Arbeit an einer „Hybrid Toolbox". Diese soll eine rasche, umfassende und maßgeschneiderte Reaktion der EU und ihrer Mitgliedstaaten auf hybride Bedrohungen ermöglichen. Die Stärkung der Fähigkeiten der EU zur Bewältigung hybrider Bedrohungen ist auch ein wichtiges Element im „Strategischen Kompass für Sicherheit und Verteidigung". Darüber hinaus enthalten aktuelle Vorschläge der Europäischen Kommission (EK) Maßnahmen, die für die Widerstandsfähigkeit der EU gegenüber hybriden Bedrohungen relevant sind, wie der Digital Services Act, die Richtlinie über Maßnahmen für ein hohes gemeinsames Maß an Cybersicherheit in der gesamten Union (NIS2), die Richtlinie über die Resilienz kritischer Einrichtungen (CER) oder der Cyber Resilience Act (CRA).

2.1.4 EU-Zertifizierungsrahmen (Cybersecurity Act)

Der bereits im Jahr 2019 in Kraft getretene Cybersecurity Act schafft unter anderem einen europäischen Zertifizierungsrahmen für die Cybersicherheit. Dieser legt einen Mechanismus fest, mit dem europäische Schemata für die Cybersicherheitszertifizierung geschaffen werden. In weiterer Folge soll der europäische Zertifizierungsrahmen für die Cybersicherheit bescheinigen, dass IKT-Produkte, -Dienste und -Prozesse, die nach einem solchen Schema bewertet wurden, den festgelegten Sicherheitsanforderungen

genügen. Anbietende und Herstellende können sich zukünftig freiwillig zu einer Cybersicherheitszertifizierung von IKT-Produkten, -Diensten und -Prozessen entscheiden. Ein Cybersicherheitszertifikat wird EU-weit anerkannt. Durch den Nachweis, dass ein Produkt die angegebenen Sicherheitsfunktionen erfüllt oder bestimmte Sicherheitsanforderungen einhält, kann Cybersicherheitszertifizierung wesentlich dazu beitragen, das Vertrauen in IKT-Produkte, -Dienste und -Prozesse zu stärken und damit das ordnungsgemäße Funktionieren des digitalen Binnenmarktes gewährleisten.

Die „Europäische Gruppe für die Cybersicherheitszertifizierung" (European Cybersecurity Certification Group [ECCG]) wurde durch den Cybersecurity Act eingesetzt und nahm ihre Arbeit im Jahr 2019 auf. Die ECCG setzt sich aus Vertreterinnen und Vertreter der nationalen Behörden für die Cybersicherheitszertifizierung oder Vertreterinnen und Vertreter anderer einschlägiger nationaler Behörden zusammen. Österreich wird in der ECCG durch das Bundesministerium für Digitalisierung und Wirtschaftsstandort (BMDW) und das strategische NIS-Büro des Bundeskanzleramtes (BKA) vertreten. Die ECCG traf sich im Jahr 2021 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 EU-Kommission und der ENISA ihre Arbeit fort. Die SCCG setzt sich aus Vertreterinnen und Vertreter aus akademischen Einrichtungen, Verbraucherschutzorganisationen, Konformitätsbewertungsstellen, Organisationen, die Normen entwickeln, Unternehmen, Handelsverbände und anderen zusammen und soll in strategischen Fragen der Cybersicherheitszertifizierung beraten.

Neben den bereits im Jahr 2019 von der EU-Kommission bei ENISA zur Ausarbeitung beauftragten möglichen Schemata für die Cybersicherheitszertifizierung (das ist einerseits das „European Union Common Criteria Scheme" [EUCC] sowie andererseits das „European Union Cybersecurity Certification Scheme on Cloud Services" [EUCS]) wurde im Jahr 2021 im Jänner ein drittes Schema für die Cybersicherheitszertifizierung

beauftragt. Dieses läuft unter dem Namen EU5G und hat die Cybersicherheit von 5G-Netzwerken zum Gegenstand. Das Schema soll sich beim Anwendungsbereich auf das GSMA Network Equipment Security Assurance Scheme sowie auf relevante Common Criteria-Schutzprofile für embedded Universal Integrated Circuit Card (eUICC) beziehen. Zu den umfangreichen Arbeiten im Bereich der Cybersicherheitszertifizierung von 5G-Netzen siehe Kapitel 2.1.5.

Alle drei Schemata befinden sich noch in Ausarbeitung, wobei ENISA seinen Entwurf für das EUCC bereits an die EU-Kommission übergeben hat.

2.1.5 Cybersicherheit von 5G-Netzen

Die Sicherheit der als „fünfte Generation des Mobilfunknetzes“ (5G) betitelten Technologie stand wie auch im Vorjahr im Fokus der Aufmerksamkeit von Cybersicherheitsbehörden. Hier wechselte 2021 der Fokus weg von der Schaffung genereller Sicherheitsmaßnahmen oder Regeln zur Erarbeitung möglicher Zertifizierungsschemata für 5G-Produkte und -Prozesse in der ECCG (siehe Kapitel 2.1.4).

2021 war es ebenfalls möglich, die am 29. Jänner 2020 vorgestellte „Cybersecurity of 5G networks EU Toolbox of risk mitigating measures”, im Folgenden „Toolbox“, vollends umzusetzen. Hier unterschied die Toolbox zwischen „technical measures“ und „strategic measures“.

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

Mit dem am 1. November 2021 in Kraft getretenen Telekommunikationsgesetz 2021 (TKG 2021) wurde der zweite Teil der aus der Toolbox stammenden Maßnahmen, die sogenannten „strategic measures“, umgesetzt. Diese beinhalten in § 45 eine eigene Bestimmung, wie mit etwaigen „Hochrisikolieferanten“ umgegangen werden kann. Ein

Hochrisikolieferant ist demnach jemand, bei „dem davon auszugehen ist, dass er mit hoher Wahrscheinlichkeit die für ihn in der EU geltenden einschlägigen Normen, insbesondere im Bereich der Informationssicherheit und des Datenschutzes, nicht oder nicht ständig einzuhalten in der Lage ist“. Hierbei wird auch die Möglichkeit geschaffen, einen Hersteller von der Lieferung sicherheitsrelevanter Komponenten oder Netzbestandteile ganz oder teilweise – etwa eingeschränkt auf bestimmte sicherheitsrelevante Geschäftsbereiche, Waren- oder Dienstleistungsgruppen oder einzelne Hard- und Softwarekomponenten sowie auf einen bestimmten Zeitraum oder ein bestimmtes geografisches Gebiet – auszuschließen. Darüber entscheidet die Bundesministerin für Landwirtschaft, Regionen und Tourismus (BMLRT) aus Gründen der nationalen Sicherheit nach Befassung eines eigens eingerichteten Expertengremiums.

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

Der Work Stream der NIS-Kooperationsgruppe „on the cybersecurity of 5G networks” (NIS CG 5G Work Stream) beschäftigte sich im letzten Jahr vor allem mit der Einsetzbarkeit von Open RAN für die europäischen Telekommunikationsnetze. Bei Open-RAN (RAN steht für „Radio Access Network“) handelt es sich um eine Initiative, die zum Ziel hat, die Interoperabilität im Zugangsnetz (RAN) der Mobilfunknetze zu verbessern bzw. zu fördern. Dabei soll durch die Definition von zusätzlichen Standards und Schnittstellen eine Diversifizierung der RAN-Hersteller und bessere Unabhängigkeit von den bisherigen Herstellern erreicht (Stichwort Vendor-Lock-In) und somit die in der 5G Toolbox geforderte „diversity of suppliers“ umgesetzt werden.

Für die Definition und Ersichtlichmachung relevanter Standards und Organisationen spielt der 2020 gegründete Sub-Work-Stream „SubGroup on 5G standardisation and certification” eine große Rolle. 2021 wurden die bestehenden Standards gesammelt und kategorisiert. Die Erkenntnisse der Arbeitsgruppe wurden an die „EU 5G Ad-hoc Working Group“ der ENISA innerhalb der ECCG übergeben. Diese richtete in Folge drei

spezifische (Sub)-Work Streams ein, die sich mit der „Ist"-Übersetzung bestehender Elemente der von der GSMA entwickelten Zertifizierungsschemata NESAS, SAS-SM, SAS-UP und eUICC in ein EU-Äquivalent befassen und eine risikobasierte Definition von Sicherheits- und Zertifizierungsanforderungen für teilnehmerbezogene Anwendungsfälle des 5G-Ökosystems erarbeiten. Das daraus resultierende EU-5G-Zertifizierungsschema muss unter anderem im Einklang mit dem Cybersecurity Act (CSA, Verordnung (EU) 2019/881) entwickelt werden. Der NIS CG 5G Work Stream dient weiterhin als Schnittstelle zum Informationsaustausch zwischen den einzelnen Gruppen.

Überdies fand am 30. September 2021 und 1. Dezember 2021 die dritte „Prague 5G Security Conference" virtuell statt. Diesmal wurden zwei neue „Prague Proposals" vorgestellt, einer über „Telecomunications Supplier Diversity" und ein anderer über „Cyber Security of EDTs" („Emerging Disruptive Technologies"). Ersterer thematisiert das bereits in der 5G Toolbox angeführte Problem der Abhängigkeit von wenigen Herstellern, zweiteres informiert über mögliche zukünftige Cybersicherheitsprobleme bei EDTs, wie etwa „Artificial Intelligence („AI"), „Quantum Communication Infrastructure" („QCI"), „Big Data Advanced Analytics" („BDAA") sowie „Autonomous Systems und Massive Internet of Things" („IOT").

2.1.6 Cyberdiplomatie

Die Cyber Diplomacy Toolbox der EU sieht diplomatische und politische Maßnahmen vor, wie im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik der EU (GASP) koordiniert auf Völkerrechtsverletzungen im Cyberraum reagiert werden kann. Sie kam auch 2021 zum Einsatz, indem staatliche Akteure hinter schwerwiegenden Cyberangriffen öffentlich angeprangert wurden. So wurden im vergangenen Jahr EU-Erklärungen zum Cyber Supply Chain-Angriff SolarWinds mit weltweit potenziell 18.000 Opfern, zur Ausnutzung einer Sicherheitslücke im Microsoft-Exchange-Server zum Zweck der Industriespionage sowie zur Ghostwriter-Kampagne im Vorfeld der Bundestagswahlen in Deutschland veröffentlicht. Die Toolbox umfasst neben präventiven, kooperativen und stabilisierenden auch restriktive Maßnahmen. Letztere wurden erstmals 2020 gegen

Personen und Einrichtungen im Rahmen des Cybersanktionenregimes verhängt und sehen Einreiseverbote und das Einfrieren von Vermögenswerten vor. Eine konkrete Attribution eines Cyberangriffs ist nicht für alle in der Cyber Diplomacy Toolbox enthaltenen Maßnahmen Voraussetzung.

Ein wichtiger Teil der Cyberdiplomatie auf EU-Ebene ist die Erarbeitung gemeinsamer Positionen und Strategien zu Cyberthemen auf internationaler Ebene, allen voran in Zusammenarbeit mit den Vereinten Nationen (siehe Kapitel 2.2). Denn Standard- und Normensetzung für neue Technologien und den Cyberraum sind längst geopolitische Konfliktzonen und die Zunahme an Cyberangriffen durch staatlich gelenkte Akteure verstärkt die geopolitische Polarisierung. Die im März 2021 angenommenen Ratsschlussfolgerungen zur Cybersicherheitsstrategie der EU unterstreichen die Bedeutung der Cybersicherheit für den Aufbau eines widerstandsfähigen, grünen und digitalen Europas. Mit dem Anspruch einer EU-Führungsrolle auf internationaler und regionaler Ebene soll die EU-Vision für das globale und offene Internet verankert und dabei sichergestellt werden, dass neue Technologien auf Menschen und den Schutz ihrer Privatsphäre fokussieren und ihr Einsatz rechtmäßig und ethisch erfolgt.

Zur Stärkung der internationalen Zusammenarbeit Österreichs in Angelegenheiten der Cyberdiplomatie hat das BMEIA einen Sonderbeauftragten für Cyber-Außenpolitik und Cyber-Sicherheit eingesetzt, der seine Tätigkeit im Mai 2021 aufgenommen hat. Zu seinen Aufgaben zählen die Delegationsleitung in multilateralen Verhandlungen und die Durchführung bilateraler Cyber-Dialoge sowie die Mitwirkung am EU-Netzwerk der Cyberbotschafter.

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

Am 28. Juni 2021 trat die Verordnung (EU) 2021/887 des Europäischen Parlaments und des Rates vom 20. Mai 2021 zur Einrichtung des Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit (European Cybersecurity Industrial, Technology and Research Competence Centre [ECCC]) und des Netzwerks nationaler Koordinierungszentren (National Coordination Centres [NCC]) in Kraft. Mit der Verordnung werden das ECCC, welches seinen Sitz in Bukarest haben wird, sowie das Netzwerk der NCCs („Netzwerk“) eingerichtet. Das ECCC soll eine tragende Rolle bei der Umsetzung des Programms Digitales Europa (Verordnung (EU) 2021/694) einnehmen und zur Umsetzung von Horizont Europa beitragen. Es erstellt des Weiteren einen Rahmen für die Steigerung und Koordinierung von Investitionen in die Cybersicherheit zwischen der EU, den Mitgliedstaaten und, indirekt, der Industrie. In diesem Zusammenhang ist es der Auftrag des ECCC und des Netzwerks, die EU zu unterstützen bei:

- der Stärkung ihrer Führungsrolle im Bereich der Cybersicherheit, um das Vertrauen und die Sicherheit, einschließlich der Vertraulichkeit, Integrität und Zugänglichkeit von Daten, zu steigern;
- der Förderung der Abwehrfähigkeit und Zuverlässigkeit der Netz- und Informationssysteme, darunter der kritischen Infrastruktur und der gängigen Hard- und Software;
- der Steigerung der globalen Wettbewerbsfähigkeit und hoher Standards der Cybersicherheitsbranche der EU und der Verwandlung der Cybersicherheit in einen Wettbewerbsvorteil für andere Wirtschaftszweige der EU.
- Der Verwaltungsrat (Governing Board) des ECCC fand sich im Jahr 2021 drei Mal informell und ein erstes Mal formell und sich konstituierend im Oktober 2021 zusammen. Im Vordergrund standen in erster Linie die Annahme administrativer Entscheidungen, die nötig sind, um das ECCC in Betrieb nehmen zu können.

Bei dem Netzwerk soll jeder Mitgliedstaat ein NCC benennen, das sich für die Entwicklung neuer Cybersicherheitskapazitäten und den weiteren Kompetenzausbau einsetzen wird. In Österreich wird das nationale Koordinierungszentrum vom BKA in Kooperation mit der Österreichischen Forschungsförderungsgesellschaft (FFG) betrieben. Ziele des NCC sind insbesondere die:

- Verbesserung der Cyberabwehrfähigkeit,
- Entwicklung und Markteinführung neuer europäischer Cybersicherheitstechnologien,
- Unterstützung von Start-ups und Klein- und mittlere Unternehmen (KMU) im Bereich Cybersicherheit,
- Förderung von Forschung und Innovation im Bereich der Cybersicherheit,
- Stärkung der Kompetenzen und der Kooperation im Bereich der Cybersicherheit,
- Stärkung der digitalen Souveränität Europas.

2.1.8 NIS-2-Richtlinie

Am 16. Dezember 2020 wurde von der EU-Kommission neben einer neuen EU-Cybersicherheitsstrategie unter anderem auch der Vorschlag für eine neue Richtlinie über Maßnahmen für ein hohes gemeinsames Maß an Cybersicherheit in der gesamten Union (NIS-2-Richtlinie [NIS2]) vorgestellt. NIS2 soll die bisherige Richtlinie aus dem Jahr 2016 ersetzen und substantiell verbessern. Die verfolgten Ziele sind grundsätzlich dieselben und werden fortgeschrieben. Konkret sollen die Cybersicherheitskapazitäten in der EU verbessert werden, eine intensivere Zusammenarbeit zwischen den Mitgliedstaaten stattfinden sowie eine Verbesserung der Cyberresilienz öffentlicher und privater Einrichtungen erreicht werden. Insgesamt soll das Cybersicherheitsniveau in der EU weiter erhöht werden. Dieses hohe gemeinsame Niveau an Cybersicherheit innerhalb der EU wird durch folgende Maßnahmen gefördert:

NIS2 wird die bisherige Richtlinie ersetzen und substantiell verbessern

- Die Mitgliedstaaten haben nationale Cybersicherheitsstrategien zu verabschieden sowie zuständige Behörden, zentrale Anlaufstellen und CSIRTs (Computer Security Incident Response Teams in Europe) zu benennen.
- Die Cyberresilienz von Unternehmen soll gestärkt werden und alle relevanten Sektoren umfassen. Alle öffentlichen und privaten Einrichtungen im gesamten Binnenmarkt, die wichtige Funktionen für die Wirtschaft und die Gesellschaft als Ganzes erfüllen, sollen als sogenannte wesentliche und wichtige Einrichtungen verpflichtet werden, angemessene Cybersicherheitsmaßnahmen zu ergreifen (insbesondere durch die Einrichtung eines Cybersicherheitsrisikomanagements sowie durch die Meldepflicht von IT-Sicherheitsvorfällen und Cyberbedrohungen).
- Bei den Sektoren im Binnenmarkt, die bereits unter die Richtlinie fallen, sollen resillienzsteigernde Maßnahmen gefördert werden. Dies wird durch die stetige Angleichung des De-facto-Anwendungsbereichs, der Sicherheitsanforderungen und Meldepflichten bei IT-Sicherheitsvorfällen, der Bestimmungen für die nationale Aufsicht und Durchsetzung sowie der Kapazitäten der zuständigen Behörden in den Mitgliedstaaten erreicht.

- Die gemeinsame Lageerfassung sowie die kollektive Vorsorge und Reaktionsfähigkeit soll verbessert werden, indem Maßnahmen zur Stärkung des Vertrauens zwischen den zuständigen Behörden gesetzt und der Informationsaustausch gestärkt wird. Darüber hinaus werden Regeln und Verfahren für den Fall großflächiger Sicherheitsvorfälle oder Krisen festgelegt (Cybersicherheitskrisenmanagement): NIS2 enthält erstmals die Pflicht zur Festlegung eines nationalen Rahmens für das Cybersicherheitskrisenmanagement und sieht die Einrichtung eines europäischen Netzwerks der Verbindungsorganisationen für Cyberkrisen (European Cyber Crises Liaison Organisation Network [EU-CyCLONe]) vor. Dieses soll die koordinierte Bewältigung großer Cybersicherheitsvorfälle und -krisen unterstützen und den regelmäßigen Informationsaustausch zwischen Mitgliedstaaten und EU-Organen gewährleisten.

NIS2 wird im EU-Parlament im Ausschuss für Industrie, Forschung und Energie (ITRE) behandelt, wo der unter dem Berichterstatter (MEP Bart Groothuis [NL; ALDE]) erarbeitete Entwurf des Verhandlungsmandats am 28. Oktober 2021 von ITRE angenommen (70 Stimmen; 3 Gegenstimmen; 1 Enthaltung) und die Zustimmung zur Aufnahme der Verhandlungen mit dem Rat erteilt wurde. Dieses Verhandlungsmandat wurde in der Plenarsitzung am 10. November 2021 bekanntgegeben.

Im Rat der EU wurde die NIS2 in der Horizontal Working Party on Cyber Issues behandelt (s. Kapitel 2.1.1). In der unter dem slowenischen Ratsvorsitz am 3. Dezember 2021 erreichten „Allgemeinen Ausrichtung“ wurde ein verstärktes Augenmerk auf einen risikobasierten und verhältnismäßigen Ansatz im Hinblick auf den Anwendungsbereich, die Pflichten und Strafen gelegt. Eine Harmonisierung zu sektorenspezifischen Bestimmungen (DORA und CER) ist ebenso erfolgt. Ferner wurden Bestimmungen betreffend die Amtshilfe und Gerichtszuständigkeit sowie Territorialität verbessert.

2.2 Vereinte Nationen (VN)

Seit der erstmaligen Auseinandersetzung des 1. Komitees (Abrüstung und internationale Sicherheit) der Generalversammlung der Vereinten Nationen (VN-GV) mit dem Thema Cybersicherheit im Jahr 1998 beschäftigt sich die VN-GV mit zunehmender Intensität mit dieser Thematik. Die Staaten verfolgen in diesem Rahmen das Ziel, die aus der Nutzung des Cyberraumes entstehenden Risiken für die internationale Sicherheit und Stabilität zu minimieren. Im Zuge der Verhandlungen gelang es, vier prioritäre Handlungsbereiche zu identifizieren, die für die Etablierung und Durchsetzung eines internationalen Normengerüstes für den Cyberraum besonders wichtig sind:

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

Nach einigen pandemiebedingten Verschiebungen 2020 war 2021 hinsichtlich der Konfliktverhütung im Cyberraum ein besonders ereignisreiches Jahr. Die zwei 2018 durch die VN-GV initiierten und parallel, aber nominell unabhängig voneinander agierenden Arbeitsgruppen konnten ihre Arbeiten im ersten Halbjahr abschließen und jeweils substanzielle Abschlussberichte vorlegen, die im Konsens angenommen wurden. Österreich brachte sich hierbei aktiv in die Arbeiten der Open-Ended Working Group (OEWG) zu Cybersicherheit ein, die allen Mitgliedstaaten offenstand. In der aus lediglich 25 Mitgliedern bestehenden Gruppe von Regierungsexpertinnen und Regierungsexperten (GGE) war Österreich nicht vertreten, verfolgte die Debatten aber dennoch mit.

Inhaltlich bedeutsam ist, dass im Abschlussbericht der OEWG alle Mitgliedstaaten erstmals die Geltung des bestehenden Völkerrechts, insbesondere der Satzung der VN, im Cyberraum klargestellt haben, wenngleich hinsichtlich der genauen Anwendbarkeit von Völkerrecht (vor allem der Menschenrechte und des humanitären Völkerrechts) nach

wie vor teils große Auffassungsunterschiede bestehen. Weitere Übereinstimmung zeigte sich in Bezug auf die Notwendigkeit von Kapazitätenaufbau sowie die Wichtigkeit von vertrauensbildenden Maßnahmen.

Für Österreich, die EU und gleichgesinnte Staaten bilden die im Konsens angenommenen Empfehlungen der OEWG und der GGE die Grundlage für die Arbeiten der auf Betreiben von Russland und China lancierten neuen OEWG zu Cybersicherheit 2021–2025. Die erste Sitzung der neuen OEWG im Dezember 2021 ging mangels Konsens zur Teilnahme von Vertreterinnen und Vertretern aus Zivilgesellschaft, Privatsektor und Forschung ohne Einigung auf Verfahrensregeln zu Ende. Offen bleibt auch, wie sich die neue OEWG zu der von über 50 Mitgliedstaaten, darunter Österreich, propagierten Ausarbeitung eines handlungsorientierten Aktionsplans (Programme of Action) zu Cybersicherheit verhalten wird.

Der Bereich der internationalen Cybersicherheit findet sich ebenso in der 2018 lancierten Abrüstungsagenda des Generalsekretärs der VN (VN-GS) wieder. Im dazugehörigen Implementierungsplan sind der Cybersicherheit zwei Aktionsbereiche gewidmet. Einer bezieht sich auf die friedliche Konfliktbeilegung, der andere auf die Stärkung sich entwickelnder Normen im Cyberraum. 2021 wurden die dahingehenden Implementierungsmaßnahmen durch die Staaten fortgesetzt.

Unterstützt wird die Umsetzung der Abrüstungsagenda durch das Büro der VN für Abrüstungsfragen (United Nations Office for Disarmament Affairs [UNODA]). Das Institut der VN für Abrüstungsforschung (United Nations Institute for Disarmament Research [UNIDIR]) trägt mit der Veröffentlichung wissenschaftlicher Publikationen zu den internationalen Cybersicherheitsdiskussionen bei.

Im VN-Sicherheitsrat setzte Estland das Thema Cybersicherheit im Juni 2021 erneut auf die Tagesordnung und veranstaltete eine virtuelle Offene Debatte mit hochrangiger

Teilnahme, an der sich auch Österreich mit einer nationalen schriftlichen Stellungnahme beteiligte.

Das von VN-GS Guterres 2018 einberufene High-level Panel on Digital Cooperation (HLPDC) legte im Jahr 2019 konkrete Empfehlungen zur Stärkung der Zusammenarbeit zwischen Regierungen, dem Privatsektor, der Zivilgesellschaft, internationalen Organisationen, der Wissenschaft, der technischen Gemeinschaft und anderen relevanten Stakeholdern im digitalen Raum vor. Darauf aufbauend erarbeitete VN-GS Guterres im Jahr 2020 einen Bericht („Road Map for Digital Cooperation"), der unter dem Titel „Connect, respect, protect" unter anderem die Einsetzung eines „Tech-Envoys" des VN-GS vorsieht. Die Stelle soll im Frühjahr 2022 besetzt werden.

Im Kontext der VN in Genf arbeitet die Internationale Fernmeldeunion (ITU) an Richtlinien für die Nutzung ihrer „Globalen Cybersicherheitsagenda" (GCA), die darauf abzielt, das Vertrauen und die Sicherheit in der Informationsgesellschaft zu stärken, aber von westlichen Staaten aufgrund der potenziellen Zunahme von staatlicher Kontrolle im digitalen Raum teilweise sehr kritisch gesehen wird. Eine der Empfehlungen im Entwurf der Richtlinien, rechtliche Regelungen zur Bewältigung globaler Cybersicherheitsfragen in der ITU zu entwickeln, wird 2022 im Mittelpunkt der Diskussionen im ITU Rat und der ITU Plenipotentiary Konferenz in Bukarest (26. September bis 14. Oktober 2022) stehen.

Das Sekretariat des Internet Governance Forums (IGF) hat seinen Sitz in Genf. Mit der Einrichtung des „Leadership Panels" und laufenden Debatten über eine Reform des Forums, wie in der „Common Agenda" des VN-GS vorgeschlagen, wird die Bedeutung des IGF als Inkubator für neue Initiativen im Bereich der Cybersicherheit voraussichtlich zunehmen.

Anlässlich der 11. WTO-Ministerkonferenz (MC11) 2017 in Buenos Aires wurde eine gemeinsame Initiative zu e-Commerce ins Leben gerufen. Die Arbeiten schreiten voran. Allerdings gibt es bei ganz wesentlichen Themen noch keine Aussicht auf Einigung, da

die Positionen der EU und anderer Teilnehmer sehr weit auseinander liegen. Das betrifft insbesondere die Themen Datenflüsse, aber auch Cybersicherheit und Quellcodes.

Cyberkriminalität hat sich rasch zu einer globalen und äußerst profitablen Verbrechenssparte entwickelt. Das VN-Büro für Drogen- und Verbrechensbekämpfung (UNODC) in Wien stellt weiterhin einen unverzichtbaren Bestandteil in der effektiven weltweiten Bekämpfung von Cyberkriminalität dar. Durch das „Global Programme on Cybercrime" unterstützt UNODC Mitgliedstaaten mit dem Aufbau von Kapazitäten, der Prävention und Bewusstseinsschaffung in der Bekämpfung von Cyberkriminalität. Österreich beteiligt sich seit 2020 mit freiwilligen Beiträgen an der Umsetzung von Initiativen in diesem Bereich.

Die 2010 im Bereich Cyberkriminalität eingerichtete „Intergouvernementale Expertengruppe" (IEG) trat im April 2021 zum siebten und letzten Mal zusammen. Eine Verlängerung des Mandates, wie von vielen Staaten gewünscht, scheiterte an der Minderheitsposition, dass die Arbeitsgruppe im Lichte der Etablierung des Ad hoc-Komitees (AHC) zur Ausarbeitung einer neuen VN-Konvention (sh. unten) hinfällig geworden sei. Die Arbeit der IEG wurde mit der konsensualen Annahme von 61 Empfehlungen und Schlussfolgerungen abgeschlossen.[2]

Der Anstieg von Cyberkriminalität als Folge der Covid-Pandemie wurde quer durch alle Gremien thematisiert, einschließlich der Kommission für Verbrechensverhütung und Strafrechtspflege (CCPCJ) und der Suchtstoffkommission (CND). Das Thema wurde auch im 2022–2025 Arbeitsplan der CCPCJ priorisiert und wird den Schwerpunkt der ersten thematischen Diskussion im Rahmen der 31. Tagung der CCPCJ im Mai 2022 stellen.

Zusätzlich zu den Diskussionen rund um Cybersicherheit im 1. Komitee der VN-GV wurde die Frage der Verhandlung einer VN-Konvention zur Bekämpfung der Cyberkriminalität

2 V2102595.pdf (unodc.org)

weiterhin im 3. Komitee der VN-GV (soziale, humanitäre und kulturelle Angelegenheiten) behandelt. In Folge der Schaffung des Ad hoc-Komitees (AHC) zur Ausarbeitung eines umfassenden internationalen Übereinkommens über die Bekämpfung der Nutzung von Informations- und Kommunikationstechnologien zu kriminellen Zwecken (VN-Cybercrime-konvention) im Jahr 2019 zog sich der Prozess der Einigung auf die Arbeitsmodalitäten des neuen AHC bis zum Mai 2021 hin. Das finale Ergebnis sieht einen Verhandlungsprozess vor, der zur Hälfte am VN-Standort in Wien und zur Hälfte in New York bis ins Jahr 2024 andauern soll. Dank einer speziellen Klausel in den Modalitäten können neben VN-Mitgliedstaaten auch NGOs und der Privatsektor an diesem Prozess mitwirken. UNODC fungiert als Sekretariat für den Verhandlungsprozess.

Im Rahmen der 47. Tagung des VN-Menschenrechtsrats (VN-MRR) im Juni 2021 brachte Österreich als einer der Hauptsponsoren (neben Südkorea, Brasilien, Dänemark, Marokko und Singapur) erfolgreich die zweite und diesmal inhaltliche Resolution zum Thema „Neue und aufkommende Technologien und Menschenrechte“ ein. OHCHR (VN-Büro für Menschenrechte) wird darin mit zwei Arbeitssträngen beauftragt, nämlich der Abhaltung von Expertenseminaren zur Implementierung der VN Guiding Principles on Business and Human Rights in Tech-Unternehmen sowie der Kontaktaufnahme mit der ITU und dem Ausloten von Möglichkeiten auf Ebene der Expertinnen und Experten, wie sichergestellt werden kann, dass technische Normen stets auch menschrechtlichen Standards entsprechen.

Die von Österreich im September 2021 als einer der Hauptsponsoren eingebrachte Resolution zum "Recht auf Privatsphäre im digitalen Zeitalter" thematisiert die Auswirkungen der fortschreitenden Nutzung privater Daten durch Algorithmen auf das Recht auf Privatsphäre. Die Resolution fordert nunmehr Staaten und Unternehmen dazu auf, den Schutz der Menschenrechte im Verlauf des gesamten Lebenszyklus („design, development, deployment and use“) von Künstlicher Intelligenz (KI) miteinzubeziehen, um Risiken zu minimieren. An die Pegasus-Enthüllungen anknüpfend, behandelt die Resolution auch den Einsatz von Technologien, die durch private Unternehmen entwickelt werden und

deren Auswirkungen auf die Arbeit von Menschenrechtsverteidigern oder Journalisten teilweise beträchtlich sind. Zudem dürfe der Schutz der Privatsphäre von Entwicklern nicht als Hemmnis für Innovation dargestellt werden.

Die im September 2020 während der 45. Tagung des VN-MRR von Österreich eingebrachte Resolution zur Sicherheit von Journalistinnen und Journalisten verurteilte erstmals die vorsätzliche und völlige Abschaltung des Internets als Verstoß gegen Menschenrechtsstandards.

2.3 NATO

Als militärisch-politisches Bündnis mit einem starken Fokus auf Sicherheit und gemeinsame Verteidigung befasst sich die North Atlantic Treaty Organization (NATO) seit der Verabschiedung ihres geltenden Strategischen Konzepts (2010) und der Anerkennung des Cyberraums als operative Domäne vermehrt mit den Verteidigungsaspekten von Cybersicherheit. Im Zuge der aktuellen Beschäftigung mit den Chancen und Gefahren durch aufkommende und bahnbrechende Technologien wurde der NATO die Bedeutung von gesicherten Daten (dabei besonders in Zusammenhang mit Big Data, KI, Autonomie, Quantentechnologie und Weltraum) und somit erforderlicher Schutzmaßnahmen verstärkt bewusst. Als Reaktion auf die geänderte Bedrohungslandschaft und zwischenzeitlich erfolgten Maßnahmen im Bereich der Widerstandsfähigkeit führte die NATO eine Überarbeitung ihrer Cyberverteidigungspolitik aus dem Jahr 2014 durch, welche beim Gipfeltreffen im Juni 2021 im Rahmen des Treffens der NATO-Staats- und Regierungschefs angenommen wurde.

Österreich kooperiert hier als Partnerland unverändert eng mit der NATO und beteiligt sich auf technischer Ebene an Sitzungen des NATO-C3 (Consultation, Command and Control)-Boards sowie jenen im Zusammenhang mit einschlägigen Smart Defence-Projekten.

Seit 2013 stellt das Bundesministerium für Landesverteidigung (BMLV) einen Offizier im „NATO Cooperative Cyber Defence Center of Excellence“ (CCDCoE) in Tallinn. Ziel der Zusammenarbeit ist die Steigerung der Fähigkeiten zur Cyberverteidigung. Das dadurch zugängliche Kursangebot wird durch die österreichischen Ressorts umfassend in Anspruch genommen und die angebotenen Übungen zur Überprüfung der nationalen Fähigkeiten im internationalen Vergleich genutzt. Ergänzend entsendet Österreich auch einen Mitarbeiter des BMLV in das „European Centre of Excellence for Countering Hybrid Threats“ in Helsinki, an dem sich auch die NATO-Mitgliedstaaten beteiligen.

2.4 Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE)

Als größte zwischenstaatliche Sicherheitsorganisation der Welt befindet sich die Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) im Bereich der internationalen Cybersicherheitspolitik in einer Doppelrolle. Einerseits unterstützt sie die Umsetzung der auf Ebene der VN getroffenen Beschlüsse (insbesondere den Kapazitätenaufbau durch ihre exekutiven Strukturen, vor allem das Sekretariat in Wien und das weite Netz an Feldmissionen). Andererseits übernahm die OSZE bei der Ausarbeitung vertrauensbildender Maßnahmen (VBM) im Cyberraum eine Vorreiterrolle. Die Annahme der 16 VBM stellt global gesehen den ambitioniertesten Versuch zur Steigerung der internationalen Kooperation im Feld der Cybersicherheit außerhalb der VN dar. Ziel ist es, durch Austausch von Informationen, die Etablierung von Kommunikationskanälen und den Aufbau von Kapazitäten zwischenstaatliche Spannungen, die aus der Nutzung des Cyberraumes entstehen, zwischen den teilnehmenden Staaten der OSZE zu minimieren. Die OSZE-Arbeit konzentriert sich darüber hinaus auf die Wahrung und Stärkung der Menschenrechte im Cyberraum sowie die Bekämpfung von Desinformation und Hassrede.

Für die Weiterentwicklung und Implementierung der VBM vorrangig zuständig ist die Informelle Arbeitsgruppe zu Cyber (Cyber-IWG). Das der OSZE zugrundeliegende Sicher-

heitsverständnis leitet auch die Arbeit der Cyber-IWG: Die Thematik wird unter Berücksichtigung politisch-militärischer, wirtschaftlicher und menschenrechtlicher Aspekte behandelt. 2021 setzte die Cyber-IWG ihre Aktivitäten im Rahmen der „adopt a CBM (Confidence Building Measure)"-Initiative fort, im Zuge derer Staaten oder Staatengruppen die Umsetzung der VBM vorantreiben. Wichtige Schritte in diesem Zusammenhang sind die Einrichtung eines Netzwerkes von Kontaktpersonen, regelmäßige Überprüfungen der Kommunikationskanäle sowie die Vorbereitung einer effektiven Zusammenarbeit im Falle einer Cyberkrise. Österreich treibt gemeinsam mit Belgien, Estland, Finnland, Italien und Schweden die Umsetzung der CBM 14 zu Public-Private-Partnerships voran und stellte im November 2021 die österreichische Cybersicherheitsplattform als ein Modell dafür vor.

Neben der institutionalisierten Behandlung der Thematik durch die Cyber-IWG setzen seit einigen Jahren die jeweiligen Vorsitzstaaten der OSZE die Cybersicherheit auf ihre Vorsitzagenda und halten regelmäßig Cybersicherheitskonferenzen ab. Im Jahr 2021 fand diese Konferenz mit den Schwerpunktthemen „Neue Technologien und Konfliktprävention sowie Auswirkungen auf die humanitäre Lage und Menschenrechte" in Stockholm als Teil des 2021 Stockholm Forum on Peace and Development statt.

2.5 Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD)

Die „Working Party on Security in the Digital Economy" (WPSDE) ist eine von vier Arbeitsgruppen unter dem „Committee on Digital Economy" der OECD. Ziel ist die Entwicklung evidenzbasierter Richtlinien für digitale Sicherheit und praktischer Leitlinien, um Vertrauen in die digitale Transformation aufzubauen und die Widerstandsfähigkeit, Kontinuität und Sicherheit kritischer Aktivitäten zu unterstützen. Der Schwerpunkt liegt auf dem Management digitaler Sicherheitsrisiken für wirtschaftliche und soziale Aktivitäten und auf der Verbesserung von Sicherheit bei digitalen Produkten und Dienst-

leistungen. Dabei wird auf die Expertise aus OECD- und Partnerländern, Wirtschaft, Zivilgesellschaft und der technischen Internet-Community gesetzt. Die WPSDE trifft sich normalerweise zweimal im Jahr in Paris und organisiert Workshops und Konferenzen. Aufgrund der Pandemie waren 2021 Treffen nur virtuell möglich – dafür wurde zu den zwei regulären Sitzungen eine weitere abgehalten.

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

Wie im Bericht des letzten Jahres schon angeführt, wurde die Überarbeitung der OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity aus dem Jahr 2015 weitergeführt. Dabei wurde der ursprüngliche Bericht in eigene Unterkapitel getrennt, die separat erscheinen werden: eine Recommendation on digital security risk management, eine Recommendation on national digital security strategies, eine Recommendation on the digital security of products und eine Recommendation on vulnerability treatment. Diese Dokumente werden getrennt bearbeitet und können hoffentlich 2022 finalisiert und veröffentlicht werden.

Auch drei zusätzliche Reports mit sehr interessanten Themenbereichen wurden vorgestellt, die ebenfalls Q1/2 2022 finalisiert werden sollen: „Enhancing the Securing communication networks: Infrastructure“, „Security of the DNS: An introduction for policy makers” und „Security of Routing”.

In der Arbeitsgruppe wurde zudem diskutiert, bei Veröffentlichungen oder Reports vermehrt den Begriff „Cyber“ (statt oder neben „digital“) in den Dokumenten anzuführen, um für mehr Sichtbarkeit in der öffentlichen Wahrnehmung zu sorgen. Als neuer Chair der Arbeitsgruppe wurde der Schweizer Delegierte des Bundes für Cybersicherheit, Florian Schütz, bestellt.

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

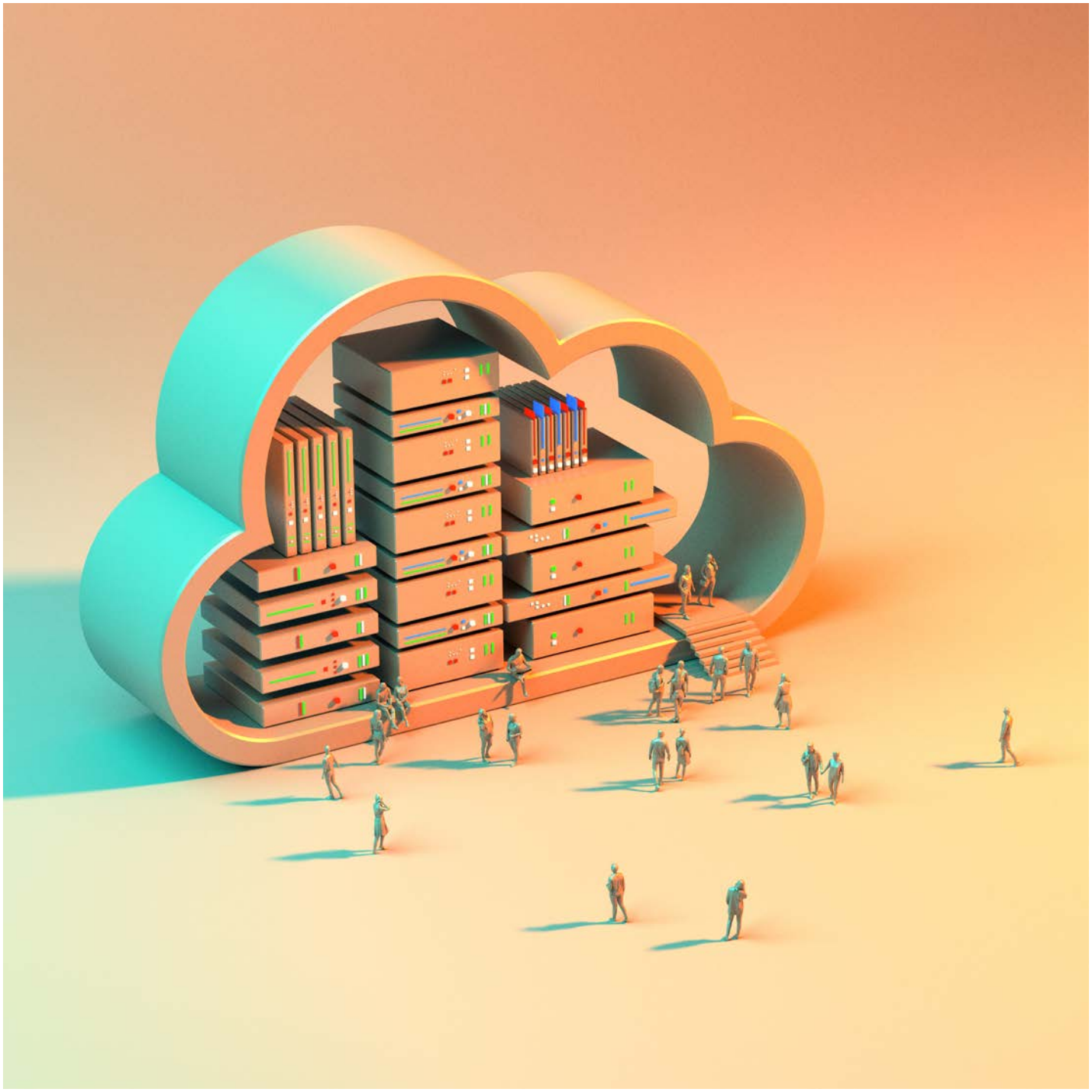
2.6 Europarat

Den Kern der Aktivitäten des Europarates im Bereich Cybersicherheit bildet die „Budapest-Konvention“ aus 2001, die mit aktuell 66 Ratifikationen (2021 Schweden) eine Bedeutung weit über Europa hinaus erlangt hat. Hauptzweck ist die Verfolgung einer gemeinsamen Strafrechtspolitik zum Schutz der Gesellschaft vor Cyberkriminalität, insbesondere durch entsprechende gesetzliche Regelungen und die Förderung internationaler Zusammenarbeit.

Die Umsetzung der Konvention wird über kapazitätsbildende Projekte unterstützt, die durch ein Cybercrime-Programmbüro des Europarates in Bukarest (C-PROC) koordiniert werden. Hierzu gehören auch die Beratung bei einschlägigen Legislativmaßnahmen und Hilfe bei der Ausbildung von Richtern und Staatsanwälten. Darüber hinaus werden die Projekte „iProceeds-2“ in Südosteuropa mit Fokus auf Erträgen aus Cyberkriminalität, das „Cyber South“ in Nordafrika, das weltweit agierende und in Zusammenarbeit mit Interpol durchgeführte „GLACY+“ sowie „Cyber East“, das auf die Verbesserung der Partnerschaftsstrukturen mit östlichen Staaten abzielt und durch das Europäische Nachbarschaftsinstrument finanziert wird, unterstützt.

Das „Octopus Project“ fördert außerdem die Umsetzung der Budapest-Konvention und damit zusammenhängender Standards. Die sogenannten „Oktopus-Konferenzen” dienen Expertinnen und Experten sowie Organisationen als wichtige Plattform im Bereich Cyberkriminalität. Die letzte Konferenz von 16. bis 18. November 2021 befasste sich anlässlich des 20-jährigen Bestehens der Budapest-Konvention mit dem Thema Zusammenarbeit im Rahmen bestehender Instrumente sowie mit Herausforderungen der COVID-19-Pandemie.

Am 17. November wurde im Ministerkomitee des Europarats zudem das Zweite Zusatzprotokoll zur Budapest-Konvention verabschiedet. Dieses befasst sich mit internationaler Rechtshilfe und dem damit verbundenen grenzüberschreitenden Zugang zu elektronischen Beweismitteln. Im Laufe von 2022 wird es zur Unterzeichnung aufgelegt.



Seit 2012 werden zudem Leitfäden („Guidance Notes“) zur Budapest-Konvention erarbeitet und veröffentlicht. Diese sollen den Vertragsstaaten die effektive Anwendung und Umsetzung erleichtern. Der bislang letzte derartige Leitfaden behandelte die Thematik der Beeinflussung von Wahlen.

Zu den weiteren Instrumenten des Europarats zählt die 2018 modernisierte Datenschutzkonvention des Europarates (ETS 108) sowie die Lanzarote-Konvention zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch. Diese leistet einen wesentlichen Beitrag zum Online-Schutz von Kindern.

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

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

Das Netzwerk arbeitet primär online, die Kommunikation erfolgt über ein Webportal, Mailinglisten und ein Instant Messaging System. Die Treffen des CNW dienen dem Informationsaustausch bezüglich der Dienste, Tätigkeiten und Kooperationsfähigkeiten der CSIRTs, ebenso werden auf freiwilliger Basis Informationen zu relevanten Sicherheitsvorfällen ausgetauscht und aus Übungen gewonnene Erkenntnisse zur Sicherheit von Netz- und Informationssystemen erörtert. Zentrale Aufgabe des CNW ist der Auf- und Ausbau von Vertrauen zwischen den Mitgliedstaaten und die Förderung der raschen und

wirksamen operativen Zusammenarbeit zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der EU.

Die ersten beiden Treffen 2021 wurden noch rein virtuell abgehalten, erst das dritte fand hybrid statt. Im März wurde im Policy-Teil erstmals der Entwurf der zweiten Version der NIS Direktive vorgestellt und diskutiert, die primären Themen auf der technischen Ebene waren die Vorgänge rund um den EMOTET-Takedown und der Lieferkettenangriff über SolarWinds. Beim zweiten Treffen im Juni 2021 gab es eine gemeinsame Session mit der NIS Kooperationsgruppe und dem EU Cyber Crisis Liaison Organisation Networks (CyCLONe) Chair, auf technischer Ebene wurden unter anderem aktuelle Vorfälle im Bereich Ransomware und Desinformation besprochen. Das Treffen im November 2021 fand in Ljubljana und online statt. Es fand wieder eine „shared session" statt, dieses Mal mit CyCLONe.

Auf technischer Seite war 2021 geprägt von der Zusammenarbeit bei der Behandlung von Schwachstellen (herausragend waren MS Exchange und diverse Firewalls/VPNs), während auf der Policy-Seite der Entwurf der NIS2 Direktive dominierte.


152.68
123.05
279.82
977.65
555.74
73.79

3
Nationale Akteure

3.1 Cyber Security Center (CSC)

Durch die Reform des BVT (Bundesamt für Verfassungsschutz und Terrorismusbekämpfung) und der Entstehung der DSN (Direktion für Staatsschutz und Nachrichtendienst) mit 1. Dezember 2021, wurden die bisherigen Agenden der Abteilung II/BVT/5 zwischen der DSN und der Sektion IV des BMI aufgeteilt. Das Cyber Security Center (CSC) der DSN fungiert auch künftig als operative Koordinierungsstelle für Meldungen und Anfragen zu Angriffen auf die Systeme und Infrastruktur von verfassungsmäßigen Einrichtungen sowie solchen, die der kritischen Infrastruktur zuzuordnen sind. Dabei liegt der Fokus verstärkt auf zielgerichteten Angriffen sowie deren technischer Vorfallsbearbeitung. Dafür bedient sich das CSC eines breiten Spektrums an Fähigkeiten und Techniken wie beispielweise Cyber Threat Intelligence, Incident Response, Malware Analysis und Reverse Engineering. Im Zuge der Tätigkeit ergibt sich zwangsläufig auch die Taxonomie und Beschäftigung mit neuen Phänomen im Cyberbereich und der Reaktion auf aktuelle Trends. Um einen Erfahrungs- und Wissensaustausch zu ermöglichen und zu fördern, setzt das CSC auch auf die Schwarmintelligenz der Cybersecurity Community, zu der auch Stakeholder aus der Wirtschaft sowie der Forschung zählen. Ziel dabei ist, gemeinsam die Resilienz und die Kommunikation in diesem Bereich zu fördern. Ebenso findet der Austausch mit Partnerdiensten statt, um die eigenen Erkenntnisse zu teilen und eine globale Sicht auf die Materie zu erhalten.

3.2 Cybercrime Competence Center (C4)

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

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

Derzeit befindet sich das C4 in einer Umstrukturierung. Aufbauend auf den bestehenden Strukturen werden Ressourcen des C4 erweitert und gliedern sich künftig in folgende Bereiche:

3.2.1 Zentrale Aufgaben

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

3.2.2 IT-Beweissicherung

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

3.2.3 IT-Ermittlungen

Zur adäquaten Bekämpfung von High-Tech-Crime werden operative Unterstützungsteams die bestehenden Ermittlungsbereiche erweitern und auch in mobiler Form zur Verfügung stehen. Spezialisierte Ermittlungseinheiten für die Fachrichtungen Darknet wie auch Kryptowährungen/Blockchain (mitunter zuständig für die Sicherstellung und Verwertung von Kryptowährungen) sind für die Bereitstellung der notwendigen Expertise bei Ermittlungen notwendig. Ebenfalls der Bereich des „Complex Cybercrime", bei dem auf Cybercrime-Delikte und Massenphänomene eingegangen wird, deren Ermittlungsansätze zum weitaus überwiegenden Teil im digitalen Bereich liegen, mit einem hohen Schadenspotential und internationalen Zusammenhängen, wird künftig abgedeckt.

3.2.4 Entwicklung & Innovation

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

3.2.5 Digitales Beweismittelmanagement

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

3.2.6 Meldestelle & ZASP

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

3.3 Direktion IKT&Cyber

Die Cyberkräfte sind jene Elemente im Österreichischen Bundesheer (ÖBH), welche die anderen Teilstreitkräfte (Land- und Luft) aber auch alle Führungsebenen (vom Ministerium bis zum Gruppenkommandanten) miteinander verbinden und damit die Kommunikations- und Führungsfähigkeit herstellen. Damit können nicht nur Informationen aus elektronischen Systemen (Radar, elektronische Lagekarten, etc.) übermittelt werden, sondern auch der Betrieb und Einsatz durch Sprachübertragung gesichert werden.

In der neu aufgestellten Direktion IKT&Cyber werden diese Elemente der IKT- und Cyberkräfte zusammengeführt. Die Direktion IKT&Cyber bildet hierbei das Kompetenzzentrum des ÖBH für Informations- und Kommunikationstechnologie, Cyberverteidigung, Elektronische Kampfführung (EloKa) und MilGeoWesen im Einsatz-, Übungs- und Friedensbetrieb.

Auch hierarchisch liegt alles in einer Hand: Von den militärstrategischen Planungsaufgaben im Cyberraum über Führungsaufgaben bis zur Bereitstellung der IKT-Services. Damit sind Planung und Umsetzung der Vorgaben im IKT-Bereich näher zusammengerückt und die Ablaufzeiten und Bedürfnisse können besser optimiert werden.

Die Kernaufgaben der Direktion IKT&Cyber sind die Zurverfügungstellung von interoperablen, sicheren und innovativen Leistungen und IKT-Services für den Einsatz im In- und Ausland, die Sicherstellung für den wirkungsorientierten Verwaltungsbetrieb und die Aufrechterhaltung der Führungsüberlegenheit im Cyberraum. Die Direktion IKT&Cyber ist durchgehend mit Bedrohungen aus dem Cyber- und Informationsraum sowie auch mit hybriden Bedrohungsformen konfrontiert und hat zeitnah auf Bedrohungen im Einsatz und im Normbetrieb zu reagieren.

3.3.1 Cyber-Truppe

Die Cyber-Truppe begegnet Angriffen im Cyberraum. Das bedeutet: Sie beherrscht das volle Spektrum des Kampfes in Computernetzwerken (Verteidigung, Ausnützung, Angriff). Die Cyber-Truppe ist für die Sicherstellung des Schutzes der IKT-Systeme und der darin vorhandenen Informationen verantwortlich und hat diese bei Cyber-Angriffen aufrechtzuerhalten bzw. deren Schutzzustand wiederherzustellen. Bei Bedarf unterstützt sie den Schutz von IKT-Systemen der verfassungsmäßigen Einrichtungen sowie kritische Infrastrukturen. Die Cyber-Truppe übernimmt, im Falle eines souveränitätsgefährdenden Angriffs im Cyberraum, diese Aufgabe auch selbstständig.

3.3.2 IKT-Truppe

Die IKT-Truppe plant, errichtet und betreibt die IKT-Systeme des Bundesheeres. Sie stellt im Alltag sowie bei Übungen und Einsätzen im In- und Ausland die erforderliche Informations- und Kommunikationstechnologie für die Truppe bereit. Über die ortsfesten IKT-Infrastrukturen hinaus werden verlegbare und mobil gehaltene Infrastrukturen bedarfsgerecht eingesetzt und in militärisch gesicherte Netzwerke angebunden. Ein eigenständiger Betrieb ist ein wesentliches Fähigkeitsmerkmal. Übergänge in andere Netze und/oder ein Zugang in das Internet können technisch geschaffen und betrieben werden.

3.3.3 EloKa-Truppe

Die Fernmeldetruppe EloKa hat speziell für das elektromagnetische Spektrum die Aufgabe, Informationen unter Nutzung technischer Mittel zu erfassen, zu identifizieren, auszuwerten und für die jeweilige Führungsebene aufzubereiten. Elektromagnetische Signale sind technisch zu analysieren, zu speichern und zu nutzen, um Truppen vor feindlicher elektromagnetischer Wirkung zu schützen, sowie einem Aggressor/Gegner die ungehinderte Nutzung des elektromagnetischen Spektrums durch Störungen zu verwehren.

3.4 Abwehramt (AbwA)

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

3.5 Heeres-Nachrichtenamt (HNaA)

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

3.6 GovCERT, CERT.at und Austrian Energy CERT

GovCERT Austria

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 BKA angesiedelt, die Erbringung operativer und operationeller Leistungen erfolgt im Rahmen einer Public-Private-Partnership mit CERT.at. Das GovCERT stellt den CERT Point of Contact für Österreich in Bezug auf die Netze der öffentlichen Verwaltung dar und steht mit internationalen Organisationen und Ansprechpartnern wie der European GovCERT Group oder der Central European Cyber Security Plattform (CECSP) im engen Austausch.

CERT.at

Bereits seit März 2019 nimmt CERT.at die Rolle des nationalen Computer-Notfallteams gemäß NISG wahr. CERT.at versteht sich als Kontaktpunkt für sicherheitsrelevante IKT-Ereignisse in Österreich und dient als vertrauenswürdige und anerkannte Informationsdrehscheibe innerhalb österreichischer Organisationen und Unternehmen im Bereich der Cybersicherheit. Dazu nutzt CERT.at sein Kontaktnetzwerk zu internationalen CERTs und anderen Cybersecurity-Organisationen sowie eigens dafür entwickelte Software wie z.B. das Open Source Produkt „IntelMQ“[3]. Weiters informiert CERT.at über Social Media und Mailinglisten über aktuelle Bedrohungen und Schutzmaßnahmen.

AUSTRIAN ENERGY CERT

Das Austrian Energy CERT (AEC) ist ein brancheneigenes Computer Emergency Response Team für die österreichische Energieindustrie. Im Jahr 2020 wurde es als sektorenspezifisches Computer-Notfallteam gemäß NISG für den Sektor „Energie“ akkreditiert. Das Ziel des AEC ist die Stärkung der IT-Sicherheitskompetenz des Energiesektors und die Erhöhung der Resilienz des Sektors gegenüber Cyberattacken. Zu den Aufgaben gehört neben dem Security Incident Management die Bearbeitung von täglich eingehenden

3 https://github.com/certtools/intelmq

Anfragen und Sicherheitsmeldungen, die Durchführung von Schulungstätigkeiten, die Teilnahme an internationalen Cybersicherheitsübungen oder die Mitarbeit bei der Erstellung technischer Sicherheitskonzepte für die Elektrizitäts- und Erdgaswirtschaft. Darüber hinaus erfüllt das AEC die Rolle des primären Ansprechpartners (Single Point of Contact) bei nationalen und internationalen Security Incidents im Energiesektor. Damit wird neben der schnellen und effizienten Kommunikation auch die Koordination der IT-Sicherheitsexpertinnen und -experten und Behörden innerhalb der Branche gewährleistet.

Gemeinsam erfüllen die drei CERTs die Aufgaben gemäß NISG und decken damit die Vorgaben der europäischen Richtlinie für Netz- und Informationssicherheit sowie die Empfehlungen der EU Agentur ENISA für die Erhöhung der IT-Sicherheit bei kritischen Infrastrukturen ab. Sie stellen auch die österreichischen Mitglieder des CSIRTs-Netzwerk der EU. Alle drei werden in erster Linie bei Sicherheitsbedrohungen und -ereignissen aktiv, dies geschieht durch Verständigung von betroffenen Stellen oder auf Basis eigener Recherchen. Darüber hinaus führen alle drei Computer-Notfallteams auch vorbeugende Maßnahmen wie Früherkennung, Öffentlichkeitsarbeit, Beratung und Unterstützung im Anlassfall sowie auf Anfrage durch. Die Aufgabenbereiche der CERTs sind im NISG festgeschrieben.

So sieht das Gesetz in der Umsetzung unter anderem für Betreiber wesentlicher Dienste sowie Anbieter digitaler Dienste eine Meldeverpflichtung für schwerwiegende Sicherheitsvorfälle vor. Diese verpflichtenden Meldungen werden von den Betroffenen an bestimmte, sektorenspezifische Meldestellen (sektorenspezifische Computer-Notfallteams) gesendet und von dort an das Bundesministerium für Inneres (BMI) weitergeleitet. Auf freiwillige Meldungen trifft dies ebenfalls zu, allerdings können diese Meldungen vor der Weiterleitung an das BMI von den Sektor-CERTs anonymisiert werden.

Für die Einrichtungen der öffentlichen Verwaltung – mit Ausnahme jener im IKDOK vertretenen – nimmt GovCERT Austria die Entgegennahme und Weiterleitung solcher Meldungen vor. Zusätzlich kann GovCERT Austria auch Frühwarnungen, Alarmmeldun-

gen, Handlungsempfehlungen und Bekanntmachungen vornehmen, erste allgemeine technische Unterstützung bei der Reaktion auf einen Sicherheitsvorfall leisten, Risiken, Vorfälle und Sicherheitsvorfälle beobachten und analysieren sowie die Lage beurteilen. Das NISG sieht zur Wahrnehmung dieser Meldestellenfunktion die Etablierung eigener Branchen- oder Sektoren-CERTs in jedem Sektor vor. Wurde in einem Bereich noch kein eigenes CERT etabliert (aktuell existieren nur das GovCERT und das AEC als Sektoren-CERTs), werden die Aufgaben des Computer-Notfallteams und die der Meldestelle durch CERT.at wahrgenommen. CERT.at hat dafür eine Meldeplattform unter https://nis.cert.at eingerichtet. Dort können auch von jeder Organisation freiwillige Meldungen eingetragen werden, die helfen, ein besseres Cyberlagebild zu schaffen.

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 2021 erfolgreich fort. Insbesondere konnten im Jahr 2021 die Ermittlungen der Betreiber wesentlicher Dienste auf Grundlage der NIS-Verordnung abgeschlossen werden. Im Hinblick auf die Vertretung Österreichs in der NIS-Kooperationsgruppe sowie in anderen EU-weiten und internationalen Gremien für die Sicherheit von Netz- und Informationssystemen, denen strategische Aufgaben zugewiesen sind, wurden umfangreiche Aktivitäten gesetzt. Hierzu sei auf das Kapitel 2.1 verwiesen. Schwerpunkt bildete dabei die Koordinierung und Vertretung der österreichischen Position in den Verhandlungen zur NIS-2-Richtlinie.

3.8 Operative Netz- und Informationssystemsicherheit

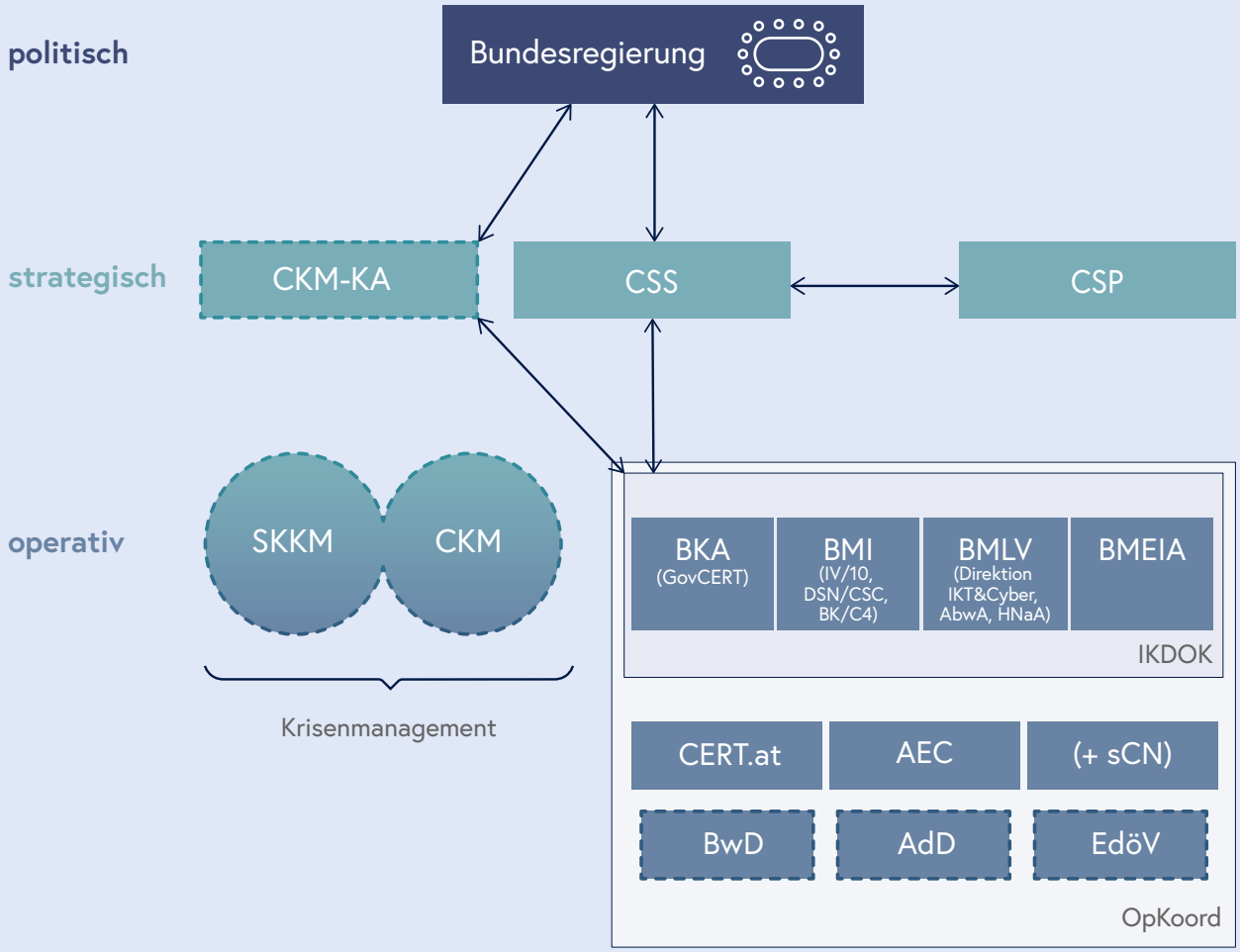
Am 30. November 2021 wurde das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) im Zuge einer umfassenden Reform aufgelöst und als Direktion für Staatsschutz und Nachrichtendienst (DSN) neu gegründet. Die Aufgaben, die bis zu diesem Zeitpunkt von der Abteilung II/BVT/5 wahrgenommen worden waren, wurden in der Folge zwischen dem DSN und der Sektion IV des Bundesministeriums für Inneres (BMI) aufgeteilt. Im Zuge dieser Kompetenzteilung wurde in der Sektion IV des BMI die Abteilung IV/10 „Netz- und Informationssystemsicherheit" neu gegründet.

Vorrangige Aufgabe dieser neuen Abteilung ist die Wahrnehmung der Funktion der operativen NIS-Behörde für Österreich. Dies beinhaltet im Wesentlichen die Umsetzung der Vorgaben des Netz- und Informationssystemsicherheitsgesetzes (NISG) gegenüber Betreibern wesentlicher Dienste, Anbietern digitaler Dienste sowie Einrichtungen der öffentlichen Verwaltung. Dazu zählen unter anderem die regelmäßige Überprüfung der Einhaltung der verpflichtenden Sicherheitsvorkehrungen bei betroffenen Unternehmen und Organisationen, sowie der Betrieb einer Meldesammelstelle für Meldungen über Sicherheitsvorfälle und eines Single-Point-of-Contacts zur Kommunikation mit den NIS-Behörden anderer Mitgliedsstaaten der EU bei grenzüberschreitenden Cybervorfällen.

Darüber hinaus übernimmt die Abteilung IV/10 hinkünftig auf Basis der Regelungen im NISG die koordinierende Rolle innerhalb der gesamtstaatlichen Operativen Koordinierungsstruktur (OpKoord) und des Inneren Kreises der Operativen Koordinierungsstruktur (IKDOK), die bisher durch das CSC im BVT ausgefüllt wurde. Weiters unterstützt die Abteilung im Rahmen der im NISG normierten Aufgabenstellungen berechtigte Unternehmen und Organisationen im Bereich der Cyberprävention durch ein umfassendes Angebot an Beratungen, Workshops, Vorträgen und Publikationen für deren Mitarbeiterinnen und Mitarbeiter.

Legende

- - - - - anlassbezogen
AbwA ..... Abwehramt
AdD ..... Anbieter digitaler Dienste
AEC..... Austrian Energy CERT (=sCN für Sektor „Energie“)
BK..... Bundeskriminalamt
BKA..... Bundeskanzleramt
BMEIA ..... Bundesministerium für europäische und internationale Angelegenheiten
BMI ..... Bundesministerium für Inneres
BMI IV/10... Abteilung Netz- und Informationssicherheit
BMLV..... Bundesministerium für Landesverteidigung
BwD ..... Betreiber wesentlicher Dienste
C4 ..... Cybercrime Competence Center
CERT.at ..... nationales Computer-Notfallteam
CKM..... Cyberkrisenmanagement
CKM-KA.... CKM-Koordinationsausschuss
CSC ..... Cyber Security Center
CSP..... Cyber Sicherheit Plattform
CSS ..... Cyber Sicherheit Steuerungsgruppe
DSN ..... Direktion für Staatsschutz und Nachrichtendienst
EdöV..... Einrichtungen der öffentlichen Verwaltung
GovCERT.. Government Computer Emergency Response Team Austria
HNaA..... Heeresnachrichtenamt
IKDOK ..... Innerer Kreis der Operativen Koordinierungsstruktur
OpKoord... Operative Koordinierungsstruktur
sCN..... sektorenspezifisches Computer-Notfallteam
SKKM..... Staatliches Krisen- und Katastrophenschutzmanagement


politisch
Bundesregierung
strategisch
CKM-KA
CSS
CSP
operativ
SKKM
CKM
Krisenmanagement
BKA
(GovCERT)
BMI
(IV/10,
DSN/CSC,
BK/C4)
BMLV
(Direktion
IKT&Cyber,
AbwA, HNaA)
BMEIA
IKDOK
CERT.at
AEC
(+ sCN)
BwD
AdD
EdöV
OpKoord

4
Nationale Strukturen

4.1 Innerer Kreis der Operativen Koordinierungsstruktur (IKDOK)

Mit 29. Dezember 2018 trat das Netz- und Informationssicherheitsgesetz (NISG) in Kraft. Dieses bildet im Bereich der Cybersicherheit die wichtigste Grundlage zur interministeriellen Zusammenarbeit in Österreich. Ein unmittelbares Ergebnis ist die Etablierung einer dauerhaften Struktur zur Koordination auf der operativen Ebene „Operative Koordinierungsstruktur – OpKoord" sowie, darin enthalten, eine interministerielle Struktur zur Koordination auf der operativen Ebene im Bereich der Sicherheit von Netz- und Informationssystemen „Innerer Kreis der Operativen Koordinierungsstruktur – IKDOK". Während die OpKoord vorrangig die Erörterung eines gesamtheitlichen Lagebildes vornimmt, das auch freiwillige Meldungen miteinbezieht, liegen die Hauptaufgaben des IKDOK bei der Erfassung und Bewertung des Lagebildes über Risiken, Vorfälle und Sicherheitsvorfälle sowie in der Unterstützung des Koordinationsausschusses im Cyberkrisenmanagement (CKM).

Dem IKDOK, unterstützt durch die OpKoord, kommt dabei im Krisenfall die Funktion einer direkten Schnittstelle zum gesamtstaatlichen CKM zu. Dabei orientiert sich das CKM hinsichtlich anzuwendender Mechanismen und Prozesse stark an den bereits bewährten und erprobten Abläufen des staatlichen Krisen- und Katastrophenschutzmanagements (SKKM). Anfang 2020 wurde der IKDOK und das CKM einer ersten harten Bewährungsprobe unterzogen, als ein Cyberangriff auf eine verfassungsmäßige Einrichtung ohne bleibende Schäden abgewehrt und eine Bereinigung des betroffenen Netzwerks erfolgreich koordiniert und durchgeführt werden konnte.

Der IKDOK setzt sich heute aus Vertreterinnen und Vertretern des BMI (IV/10, DSN/CSC, BK/C4), BKA (GovCERT), BMEIA und BMLV (AbwA, IKT&Cyber und HNaA) zusammen. Das BMI (IV/10) koordiniert dabei die Arbeiten im Gremium und leitet die Gespräche. Der IKDOK erstellt monatlich ein IKDOK- und ein OpKoord-Lagebild, welches der jeweiligen Zielgruppe zur Verfügung gestellt wird.

4.2 CERT-Verbund Austria

Der CERT-Verbund Austria wurde 2011 als Kooperation aller damals existierenden österreichischen CERTs des öffentlichen Bereichs und jener der privaten Sektoren gegründet. Intention war die Bündelung der verfügbaren Kräfte zur optimalen Nutzung des gemeinsamen Know-hows der CERTs. Die Teilnahme am CERT-Verbund Austria ist freiwillig. Jeder einzelne Teilnehmer verpflichtet sich zu regelmäßigem Informations- und Erfahrungsaustausch, zur Identifikation und Zurverfügungstellung von Kernkompetenzen sowie zur Förderung der CERTs in allen Sektoren – im Sinne eines gemeinschaftlich geführten und auf Kooperation basierenden Verbundes.

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

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

Da die Corona Situation für den zehnjährigen Jubiläumstag im November 2021 nicht absehbar war, wurde bereits im Sommer ein Social Event abgehalten. Dieses wurde nach der langen Zeit der hauptsächlich online durchgeführten CERT-Verbund-Treffen sehr gut angenommen und hat wesentlich dazu beigetragen, die Zusammenarbeit zu stärken.

Seit der Gründung des CERT-Verbundes Austria haben sich die aktuell 17 mitwirkenden Teams in 50 Sitzungen getroffen und sind auch außerhalb der regelmäßigen Treffen

über sichere Kommunikationskanäle in ständigem Austausch miteinander. So können über Organisations- und Unternehmensgrenzen hinweg sehr rasch Lagebilder erstellt und Maßnahmen abgestimmt werden.

Cyber Sicherheit Plattform

4.3 Cyber Sicherheit Plattform (CSP)

Als fixer Bestandteil des österreichischen Cyber-Ökosystems fungiert die Cyber Sicherheit Plattform (CSP) seit nunmehr sechs Jahren als zentrale strategische Austausch- und Kooperationsplattform zwischen Wirtschaft, Wissenschaft und öffentlicher Verwaltung. Sie genießt das Vertrauen aller relevanter Stakeholder und dient dem Erfahrungs- und Informationsaustausch im Bereich Cybersicherheit mit besonderem Fokus auf kritische Infrastrukturen. Die CSP leistet wichtige Beiträge bei der Weiterentwicklung der österreichischen Cybersicherheitsstrategie und der Ausgestaltung des legistischen Rahmens zur Cybersicherheit in Österreich (Stichwort NIS, NIS2). Als sektorübergreifendes Kooperationsmodell findet die CSP weit über Österreich hinaus Beachtung und wurde beispielsweise 2021 im Rahmen der Confidence Building Measures Arbeitsgruppe der OSZE vorgestellt. Beteiligungen bei internationalen Arbeitsgruppen wie der ENISA oder der UNODC Cyber Crime Convention runden das Gesamtbild ab. Auch 2022 wird die CSP ihren Beitrag zur Gestaltung der Cybersicherheit in Österreich leisten und im Rahmen des nationalen Koordinierungszentrums für Cybersicherheit (NCC, siehe auch Kapitel 2.1.7) einen wesentlichen Bestandteil der österreichischen Cybersecurity Competence Community (CCC) bilden.

4.4 Austrian Trust Circle (ATC)

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

Die wesentlichen Ziele des ATC sind:

- Das Schaffen einer Vertrauensbasis, um im Ernstfall gemeinsam agieren zu können;
- Vernetzung und Informationsaustausch in und zwischen den Sektoren der kritischen Infrastruktur und der öffentlichen Verwaltung;
- Kontaktaustausch zwischen den CERTs und den teilnehmenden Unternehmen, Organisationen und Behörden;
- Unterstützung zur Selbsthilfe in den Sektoren im Bereich IT-Sicherheit;
- Operative Kontakte zu den CERTs beispielsweise
  - bei der Information über und
  - bei der Behandlung von Sicherheitsvorfällen in den Organisationen;
  - zu Expertinnen und Experten für das BKA im Krisenfall.

Neben regelmäßigen Treffen innerhalb der einzelnen Sektoren-Circles, die aufgrund der Corona-Situation 2021 leider nicht stattfinden konnten, wird der Austausch zwischen den Sektoren inklusive der öffentlichen Verwaltung einmal im Jahr im Rahmen einer zweitägigen Veranstaltung gefördert. Zumindest dieses Treffen konnte 2021 unter der Einhaltung der behördlichen Vorgaben abgehalten werden, was einen wichtigen Austausch zu sicherheitsrelevanten Themen ermöglichte.

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 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 Kooperationspartnern (Bundesministerien, Landesregierungen, Behörden, Universitäten, Fachhochschulen, Forschungsinstitute, Unternehmen, Vereine und Interessensvertretungen) laufend erweitert. Es beinhaltet aktuelle Meldungen und Warnungen, Informatives, Beratung sowie weiterführende Informationen sowohl für Einsteigerinnen und Einsteiger als auch für Expertinnen und Experten.

2021 umfassten die Aktivitäten auf dem IKT-Sicherheitsportal insgesamt die Erstellung von 130 Newsartikeln, 24 Publikationseinträgen und 68 Veranstaltungseinträgen. Jedes Monat wurde ein Schwerpunktthema zu aktuellen Trends festgelegt, wozu insgesamt 107 Fachbeiträge veröffentlicht wurden. Dies waren beispielsweise im März die IT-Sicherheit im Homeoffice, im Mai das digitale Amt und sichere digitale Behördenwege sowie im Oktober ein wiederkehrender Schwerpunkt zum „European Cyber Security Month“ (ECSM) und den österreichischen Aktivitäten, die im Zuge dessen veranstaltet wurden. Des Weiteren wurde der Cybermonitor, eine statistische Aufbereitung der zwölf wesentlichsten Gefährdungen im Bereich der IKT- und Cybersicherheit, grunderneuert und neu gestaltet. Der Cybermonitor bietet zu den jeweiligen Kategorien eine grafische Darstellung zur Entwicklung der Gefährdungslage und zeigt dadurch aktuelle Trends auf.

5 Cyberübungen

5.1 Blue OLEx 2021

Am 12. Oktober 2021 veranstaltete die ENISA gemeinsam mit dem rumänischen National Cyber Security Directorate (DNSC) die dritte Blue OLEx-Cyberübung. Primäres Ziel der Übung war es, die im Rahmen des CyCLONe festgelegten Standard Operating Procedures für große, grenzüberschreitende Cybervorfälle zu testen und zu beüben. Die Übung fand aufgrund der Covid-19-Pandemie in einem Hybridformat in Bukarest und online statt.

Bei der Übung handelte es sich um eine sogenannte Tabletop-Exercise. Das bedeutet, dass das Übungsszenario lediglich in der Theorie durchgespielt wurde und es zu keinen tatsächlichen Einschränkungen an den betroffenen Einrichtungen kam. Das Übungsszenario konzentrierte sich auf Sicherheitsvorfälle im Bereich der schienengebundenen Verkehrsinfrastruktur und des Energiesektors in mehreren europäischen Ländern. Im Zuge der Übung wurden Einspielungen zu verschiedenen Beeinträchtigungen des Regelbetriebs, wie Störungen in der Energieversorgung, Manipulationen der Schienen-Signalsysteme, langandauernde Stromausfälle und begleitende Desinformationskampagnen bearbeitet und entsprechende Maßnahmen und Reaktionen abgeleitet.

An der Übung nahmen hochrangige Behördenvertreterinnen und -vertreter aus insgesamt 22 EU-Mitgliedsstaaten teil. Seitens der EU waren Personen aus der EK und der ENISA involviert. Die österreichische Delegation war online an die Übung angebunden, vertreten waren Teilnehmerinnen und Teilnehmer aus der Zentralstelle des BMI, der DSN und dem BKA.

5.2 KSÖ Planspiel

Das Kompetenzzentrum Sicheres Österreich (KSÖ) veranstaltete am 20. und 21. September 2021 gemeinsam mit dem Austrian Institute of Technology (AIT) ein länderübergreifendes Cybersicherheits-DACH-Planspiel, in dem in hybrider Form die Abwehr von Cyberangriffen realitätsnahe durchgespielt wurde. Der Fokus des Planspiels lag auf cyberphysischen und begleitenden Informationsmaßnahmen. Im Rahmen der Übung kamen im Raiffeisen Forum in Wien sowie – online zugeschaltet – in der Schweiz und Deutschland die unterschiedlichsten technischen und strategischen Spielerinnen und Spieler, Beobachterinnen und Beobachter sowie und Multiplikatorinnen und Mutliplikatoren zusammen. Bei der Übung, die vom BMI gefördert wurde, übten die acht spielenden Teams in Wien gemeinsam mit der nationalen Koordinierungsstruktur für die Cybersicherheit (IKDOK/OpKoord) als auch mit Partnerinnen und Partnern vom schweizerischen nationalen Zentrum für Cybersicherheit (NCSC) und dem deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) in einem herausfordernden Szenario. Dieses Bedrohungsszenario wurde von Expertinnen und Experten des AIT in der „AIT Cyber Range“ umgesetzt.

Das Szenario der Übung war aus gegebenem Anlass der aktuellen politischen und gesellschaftlichen Situation in Angesicht der Covid-19-Pandemie angepasst. Im Rahmen der Übungsannahmen versuchte eine Gruppe von militanten Impfgegnern einen fiktiven internationalen Pharmakonzern, der eine Schlüsselfunktion bei der Bekämpfung einer Pandemie spielt, durch verschiedenartige Cyberangriffe sowie massive Desinformationskampagnen in die Knie zu zwingen. Die teilnehmenden Teams agierten dabei als Mitarbeiterinnen und Mitarbeiter des angegriffenen Konzerns und versuchten gemeinsam, die Angriffe abzuwehren und den Regelbetrieb wiederherzustellen. Die teilnehmenden Behördenvertreterinnen und -vertreter unterstützten den Konzern dabei im Rahmen ihrer realen Aufgabenstellungen und erprobten und optimierten damit die nationalen und internationalen Melde- und Kommunikationswege.

5.3 milCERT Interoperability Exercise 2021 (MIC21)

Das milCERT (militärisches Computer Emergency Readiness Team) des BMLV hat bei der heuer erstmalig stattfindenden Übung MIC21, organisiert durch die European Defence Agency (EDA), erfolgreich teilgenommen und dabei den dritten Platz in der Gesamtwertung erreicht. Darüber hinaus wurde die Spezialwertung "Situation Reports" durch das österreichische Team gewonnen.

Zusammenarbeit und Informationsaustausch sind ein Schlüsselfaktor bei der Bekämpfung von Bedrohungen im Cyberraum. Daher setzte die EDA bei der neuen Übungsserie den Fokus auf eben diese Themen. Die teilnehmenden Teams mussten in einer virtuellen Umgebung live stattfindende Angriffe auf typische militärische IT-Umgebungen (z.B. Büroumgebung, Befehls-Infrastruktur/„C2“, Kommunikationssysteme, kritische Infrastruktur sowie Sensor- und Waffensysteme) erkennen, diese analysieren und relevante Bedrohungen aufzeigen. Darüber hinaus mussten regelmäßig Berichte, sogenannten „Situation Reports“ (SITREP) erstellt werden, welche ebenfalls bewertet wurden. Diese SITREPS sind insofern relevant, als dass sie die Auswirkungen der erkannten Angriffe (z.B. „Denial of Service“ (DoS), Kompromittierung mit Schadsoftware oder vollständige Übernahme) gegenüber der militärischen Führung darstellen. Diese muss anhand der Informationen im Ernstfall gegebenenfalls über mögliche weitere Maßnahmen oder Alternativen entscheiden. Neben der Qualität der Berichte wurde auch der Zeitfaktor, nämlich wie schnell ein Angriff erkannt und gemeldet werden kann, sowie die Genauigkeit gewertet.

Das primäre Ziel der Übung war es, milCERTs innerhalb der EU näher zusammenzubringen, um die Zusammenarbeit sowie den Informationsaustausch zu stärken. Darüber hinaus sollten auch gemeinsam Cybersicherheitsvorfälle erkannt und gelöst werden. Daher war es genauso wichtig, neben der „eigenen Infrastruktur“ (das virtuelle Übungsnetzwerk) auch die Partner im Hinterkopf zu behalten. Typische Erkennungsmerkmale für Angriffe, sogenannte „Indicators of Compromise“ (IoC), mussten den anderen milCERTs zur Verfügung gestellt werden. Diese konnten somit im Anschluss in den eigenen Um-

gebungen danach suchen und so eventuell übersehene Angriffe retrospektiv erkennen und geeignete Gegenmaßnahmen einleiten.

Wie der estnische Verteidigungsminister, Kalle Laanet, als virtueller Gastgeber in seiner Rede bemerkte, „haben die zivilen CERTs innerhalb der EU bereits sehr gute Kontakte aufgebaut und kontinuierlich verbessert. Im Gegensatz dazu ist dies bei militärischen CERTs noch nicht der Fall. Dies ist unter anderem aufgrund ihrer sensiblen Umgebung zwar verständlich, dennoch ist es wichtig, Möglichkeiten zur Vertrauensbildung zu schaffen, um den Informationsaustausch zu verbessern. Diese Live-Fire Übung sorgt genau dafür."

Planspiele sind ein ganz entscheidender Faktor bei der Erhöhung der gesamtstaatlichen Resilienz

Das österreichische milCERT ist bestrebt, auch weiterhin an dieser Übungsserie teilzunehmen und den Informationsaustausch über Cyberangriffe mit Partnern auf EU-Ebene zu verbessern. Denn nur gemeinsam wird es künftig möglich sein, den Herausforderungen im Cyberraum effektiv begegnen zu können.

5.4 Locked Shields 2021 (Red Team)

Seit beinahe zehn Jahren nimmt Österreich an der internationalen Cyber-Übung "Locked Shields" teil, die von der NATO-Schulungseinrichtung "Cooperative Cyber Defence Center of Excellence" organisiert wird. Bisher war Österreich als verteidigendes Team ("Blue Team") stets unter den besten Fünf der teilnehmenden Nationen und Organisationen.

Die Abordnung der Direktion IKT&Cyber war heuer allerdings nur im Red Team vertreten, wird aber 2022 in einem gemeinsamen Joint-Team mit Deutschland auch wieder im verteidigenden Blue Team teilnehmen.

Die diesjährige Übung involvierte mehr als 5.000 virtualisierte Systeme, die gegen mehr als 4.000 Angriffe verteidigt werden mussten. Darüber hinaus mussten pro Team mehr als 150 komplexe IT-Systeme instandgehalten werden. Die "Blue Teams" mussten Vor-

fälle melden, strategische Entscheidungen treffen, sich forensischen, gesetzlichen und medialen Herausforderungen stellen und sich gegen Cyber-Feinddarsteller durchsetzen.

Dieses Jahr lag der Fokus der Übung auf dem Verbessern der Kommunikation zwischen technischen Expertinnen und Experten, zivilen und militärischen Teilnehmerinnen und Teilnehmern und den Führungsebenen. Das NATO-Center kreierte dieses technische und strategische "Spiel", um die Umsetzung der Befehlskette im Fall eines schweren Cybervorfalls mit Auswirkungen auf Zivilisten und auch auf das Militär zu proben.

5.5 Common Roof 2021

Von 2. bis 19. November 2021 fand in der Schwarzenberg-Kaserne in Wals-Siezenheim die multinationale Übung "Common Roof 21" statt. Das Übungsszenario war ein Erdbeben im Rheintal in der Schweiz mit Auswirkungen auf Deutschland und Österreich. Zur Unterstützung der zivilen Infrastruktur und zur Aufrechterhaltung des staatlichen Krisenmanagements wurde ein interoperables, militärisches Führungsnetz errichtet und gegen Cyberbedrohungen geschützt.

Das Bereitstellen eines Notfallkommunikationsnetzwerkes zur Aufrechterhaltung der Führungsfähigkeit war ein unverzichtbarer Bestandteil der militärischen Einsatzführung. Die Herausforderung lag dabei in der Schaffung von sicheren Übergängen zu anderen militärischen und zivilen IT-Netzwerken. Dafür wurden die Interoperabilitätsstandards und Betriebsabläufe unter dem Begriff "Federated Mission Networking" spezifiziert.

Im Mittelpunkt der Übung standen die multinationale und gemeinsame Betriebsführung, in welcher IT-Service-Management und IKT-Sicherheitsprozesse durchgeübt und evaluiert wurden. Dazu wurden die Teilnetze Österreich, Deutschland und Schweiz miteinander verbunden, zentral überwacht und gesteuert.

Im Übungsszenario wurden darüber hinaus unterschiedlichste Einlagen eingespielt, welche im Ernstfall betrieblich gemeinsam koordiniert werden mussten. Somit konnte die zivil-militärische und trinationale Zusammenarbeit zur Unterstützung von Einsatzkräften bei einer Katastrophenlage bestmöglich unterstützt werden.

Insgesamt nahmen 150 Personen aus Deutschland, der Schweiz und Österreich an der gemeinsamen Übung teil. Die ca. 55 Übungsteilnehmerinnen und -teilnehmer aus Österreich waren großteils IT-Expertinnen und Experten der Direktion IKT&Cyber des Österreichischen Bundesheeres. Die Leitung erfolgt durch die neu geschaffene Abteilung IKT&Cyber Einsatz.

5.6 Multilateral Cyber Defence Exercise 2021

Das "Military University Institute" in Lissabon führte die diesjährige "Cyber Phalanx" durch. 130 Teilnehmerinnen und Teilnehmer aus der EU und NATO wurden als Führungskräfte in operativen Planungsprozessen sensibilisiert. Mit dabei waren auch die Cyberexpertinnen und -experten des ÖBH. Die "Multi-Lateral Cyber Defense Exercise" fand auf der Cyber-Range des Forschungsinstituts CODE in München von 4. bis 8. Oktober 2021 statt. Die Cyberteams wurden nicht nach Nationalitäten gebildet, vielmehr lag das Schwergewicht auf der Durchmischung der Gruppen nach individuellen Fertigkeiten. Außerdem bewies sich jedes Teammitglied als Teamleiter.

National und international gewonnene Erkenntnisse aus Kooperationen und Zusammenarbeit sind im Ernstfall von höchster Bedeutung. Die Teilnehmerinnen und Teilnehmer werden im Umgang mit grenzüberschreitenden Bedrohungen trainiert, was zu einer Erhöhung des Cybersicherheitsschutzes führt und die Leistungsfähigkeit für die Abwehr von Cyberangriffen auf kritische Infrastrukturen stärkt.

Sowohl für militärische Organisationen wie auch Behörden, Unternehmen und andere Organisationen ist das Abhalten realitätsnaher Übungen im Cyberraum alternativlos. Denn nur was regelmäßig geübt wird, kann im Einsatzfall auch tatsächlich funktionieren.

6
Die neue Österreichische Strategie für Cybersicherheit 2021

Im Jahr 2021 konnte die neue Österreichische Strategie für Cybersicherheit 2021 (kurz ÖSCS 2021) verabschiedet werden. Sie dient der langfristigen Schaffung eines sicheren Cyberraumes, ist als Beitrag zur Steigerung der Resilienz Österreichs und der Europäischen Union (EU) zu sehen und wird im gesamtstaatlichen Ansatz umgesetzt.

Die ÖSCS 2021 ist eine Weiterentwicklung der ÖSCS 2013 und baut auf dessen nationalen Strukturen und Grundsätzen auf. Der Veröffentlichung gingen intensive Zusammenarbeit und die Führung zahlreicher Gespräche mit Stakeholdern auf nationaler, europäischer und internationaler Ebene voraus. Zudem wurden bei der Entwicklung der Strategie Expertinnen und Experten aus den Bereichen Wirtschaft, Bildung, Forschung und Entwicklung sowie des Bundes miteingebunden.

Bundesregierung beschließt am 22.12.2021 ein erneuertes, umfassendes und proaktives Konzept zum Schutz des Cyberraums und der Menschen im virtuellen Raum – die ÖSCS 2021

Strategische Dokumente tendieren dazu, lange gültig zu bleiben. Dies stellt für hochdynamische Themen wie Cybersicherheit eine besondere Herausforderung dar. Von daher wurde entschieden, die ÖSCS 2021 in ein strategisches Rahmenwerk und einen dynamischen, webseitengestützen Maßnahmenkatalog aufzuteilen.

Das Dokument ÖSCS 2021 stellt den langfristigen strategischen Überbau dar und spezifiziert die Ausgangslage, Herausforderungen und Chancen. Es beinhaltet die Vision der ÖSCS 2021 und definiert zwölf Ziele zur Verwirklichung eben dieser. Zielgruppen der ÖSCS 2021 sind Gesellschaft, Wirtschaft, Bildung, Forschung und Entwicklung sowie der öffentliche Sektor.

Cybersicherheit kann nicht regional gedacht werden, daher ist die ÖSCS 2021 in die „Europäische Cybersicherheitsstrategie für die digitale Dekade“ eingebettet. Vervollständigt wird das strategische Grundlagendokument durch die Spezifizierung der Maßnahmenerhebung und des Maßnahmenmanagements zu Umsetzung der Strategie sowie des Steuerungs- und Monitoringprozesses.

Der zweite Teil ist ein webseitengestütztes, datenbankbasiertes Managementtool. Dieses erlaubt die Ehebung, Verwaltung, Steuerung und das Monitoring von Maßnahmen zur Umsetzung der Ziele der ÖSCS 2021 und damit ein agiles und zeitnahes Reagieren auf sich ändernde Rahmenbedingungen, Herausforderungen oder Bedrohungen. Die Besonderheit ist, dass die Ressorts und die Zielgruppen jeweils den eigenen Wirkungsbereich betreffende Maßnahmen einmelden und mit detaillierten Umsetzungsplänen hinterlegen. Die Vorgabe dabei ist, dass jede Maßnahme dabei zumindest einem Ziel sowie einer Zielgruppe zugeordnet werden muss. Dies erlaubt auch eine Abdeckungsmessung über die strategischen Vorgaben.

Die Überwachung der Umsetzung der ÖSCS schließlich obliegt der Cyber Sicherheit Steuerungsgruppe. Auf Grundlage der Umsetzungspläne wird halbjährlich ein Fortschrittsbericht erstellt und – soweit möglich – veröffentlicht.