Bericht Cybersicherheit für das Jahr 2020

Bericht Cybersicherheit für das Jahr 2020

Wien, 2021

Bundeskanzleramt

Bundesministerium
Inneres

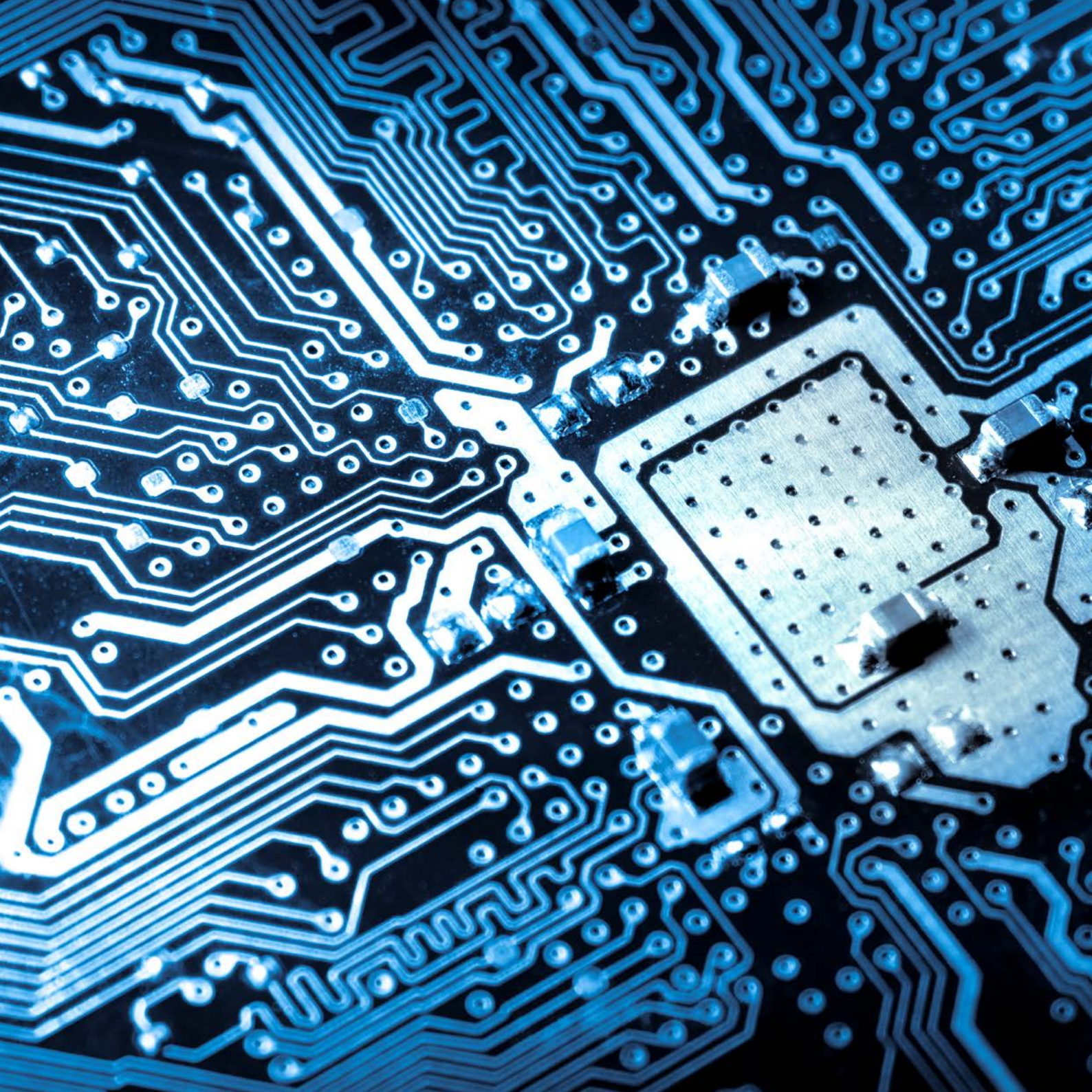
Bundesministerium
Landesverteidigung

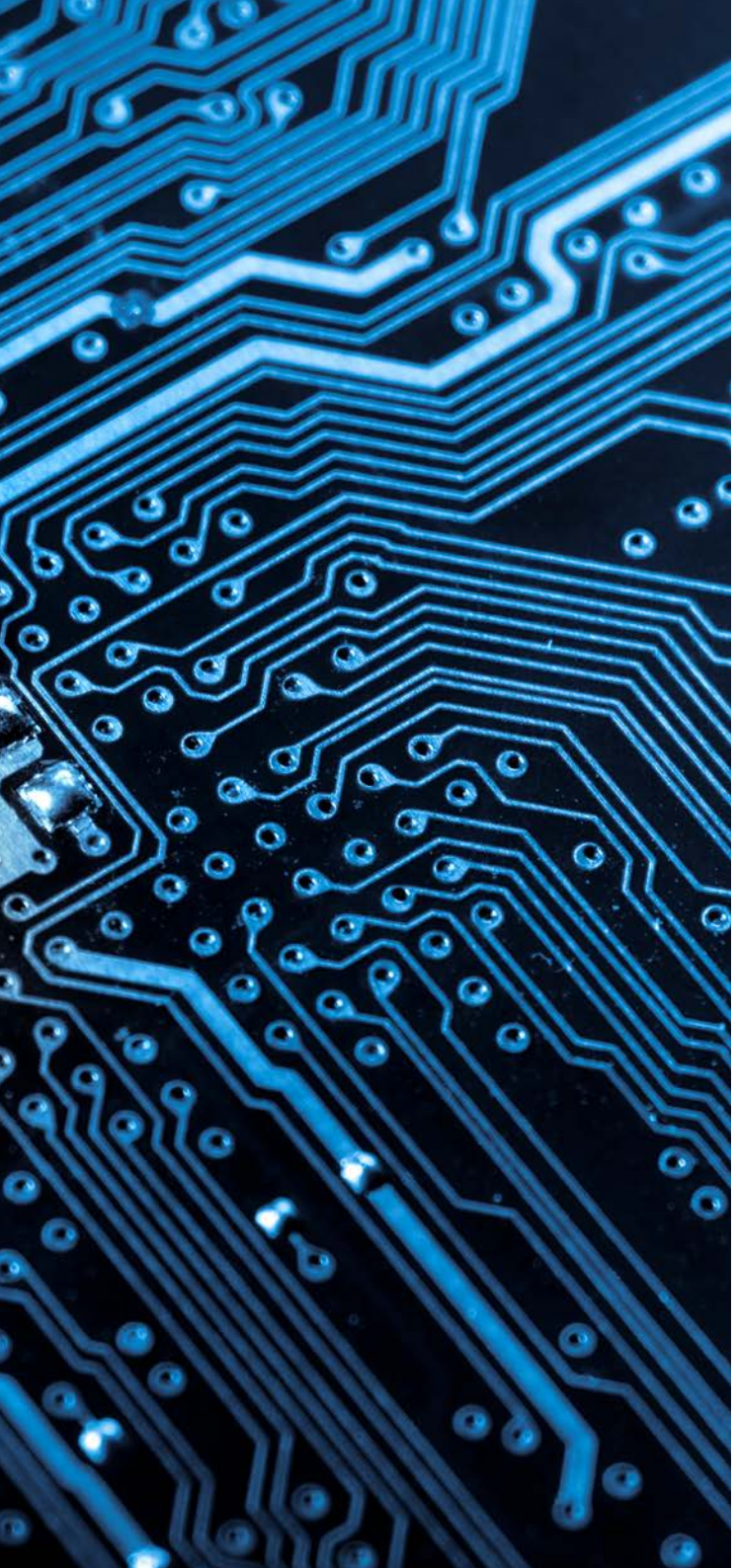
Bundesministerium
Europäische und internationale
Angelegenheiten

Impressum

Medieninhaber, Verleger und Herausgeber:
Bundeskanzleramt
Ballhausplatz 2, 1010 Wien
bundeskanzleramt.gv.at
Fotonachweis: iStock
Layout: BKA Design & Grafik
Druck: Druckerei Walla GmbH
Wien, Juli 2021

Inhalt





Editor's note

Das vergangene Jahr war vor allem von der Pandemie bestimmt. Über kein anderes Thema wurde so oft berichtet, nichts wurde so oft diskutiert und nichts hat unser aller Leben mehr beeinflusst, geprägt und bestimmt als das Corona-Virus.

Ja, man könnte sogar versucht sein, Corona als das einzig relevante Thema im Berichtszeitraum zu identifizieren und mit diesen ersten Zeilen den nunmehr vorliegenden Cybersicherheitsbericht als bereits abgeschlossen anzusehen.

Spoiler-Alert! Ganz so war es dann doch nicht und diesen ersten Seiten folgen noch ein paar mehr.

Auch wenn es schon wie Ewigkeiten her zu sein scheint, so war es zu Beginn des Jahres 2020, als der bisher größte Cyberangriff auf eine österreichische staatliche Institution, namentlich das Bundesministerium für europäische und internationale Angelegenheiten, stattfand. Erstmalig wurden die gesamtstaatlichen Cybersicherheitsstrukturen aktiviert. Ein ad-hoc gebildetes Team bestehend aus Expertinnen und Experten des Bundesministeriums für europäische und internationale Angelegenheiten, des Bundesministeriums für Inneres, des Bundesministeriums für Landesverteidigung und des Bundeskanzleramtes, inklusive Government Computer Emergency Response Team Austria, konnte letztendlich das weltweit verteilte IT-System absichern. Alle dachten, dieses Ereignis wäre der Höhepunkt des Jahres gewesen – das war Anfang Februar.

In der Retrospektive scheint dies amüsant, hatte doch wenige Wochen später die Pandemie Österreich und die ganze Welt in ihrem Würgegriff. Und doch war es maßgeblich das Virus und nicht die CIOs und CDOs, welches der Digitalisierung in noch nie gekannter Weise Vorschub leistete. Homeoffice war plötzlich nicht mehr nur eine Lösung für einige Exoten und hippe Unternehmen, sondern wurde zur Norm. Unternehmen entdeckten Onlineplattformen und neue Medien als Interaktionskanäle mit ihren Kunden und Videokonferenzen wurden zu einem Renner. Ein paar Datenschutzpannen, wie zum Beispiel bei Zoom, waren da schnell als Petitessen abgetan.

Eine Chance tat sich auf! Nicht nur für die Wirtschaft und die Forschung, nein, auch die Verwaltung sprang auf und zeigte ihre Agilität. Diese zeigten übrigens auch die Cyberkriminellen, welche wieder einmal bewiesen, wie situationselastisch und schnell sie auf veränderte Rahmenbedingungen reagieren können. Passenderweise wurde auch gleich eine veritable Sicherheitslücke im auch in Österreich weit verbreiteten Netscaler / VPN-Gateway einer renommierten Firma bekannt, welche derart unangenehm war, dass sie wenig schmeichelhaft „Shitrix“ getauft wurde. Mehrere Lücken sollten folgen - das Rennen 2020 war eröffnet und würde auch die österreichischen Cybersicherheitsteams das ganze Jahr über auf Trab halten.

Cyberkriminellen wird ja oftmals nachgesagt, sie hätten keinen Ethos und keine Ehre. Öffentlichkeitswirksam dem widersprechend gelobten deren selbsternannte Sprachrohre Krankenhäuser und Forschungseinrichtungen natürlich nicht anzugreifen, da es ja schließlich um Menschenleben ginge. Kurz darauf kam es in Deutschland zum ersten, mit einem Cyberangriff in Zusammenhang stehenden Todesfall. Es war aber nicht der vielfach prognostizierte Hack einer Insulinpumpe oder eines Herzschrittmachers, welcher hierfür verantwortlich war. Am Ende war es ein unscheinbares, durch einen Kryptotrojaner verschlüsseltes Krankenhausverwaltungssystem, dessen Ausfall dazu führte, dass eine

Notfallpatientin in ein anderes Krankenhaus umgeleitet werden musste – dies kostete Zeit, Zeit die sie nicht mehr hatte. Österreichische Krankenhäuser blieben, zumindest von derartigen Angriffen, vorerst verschont.

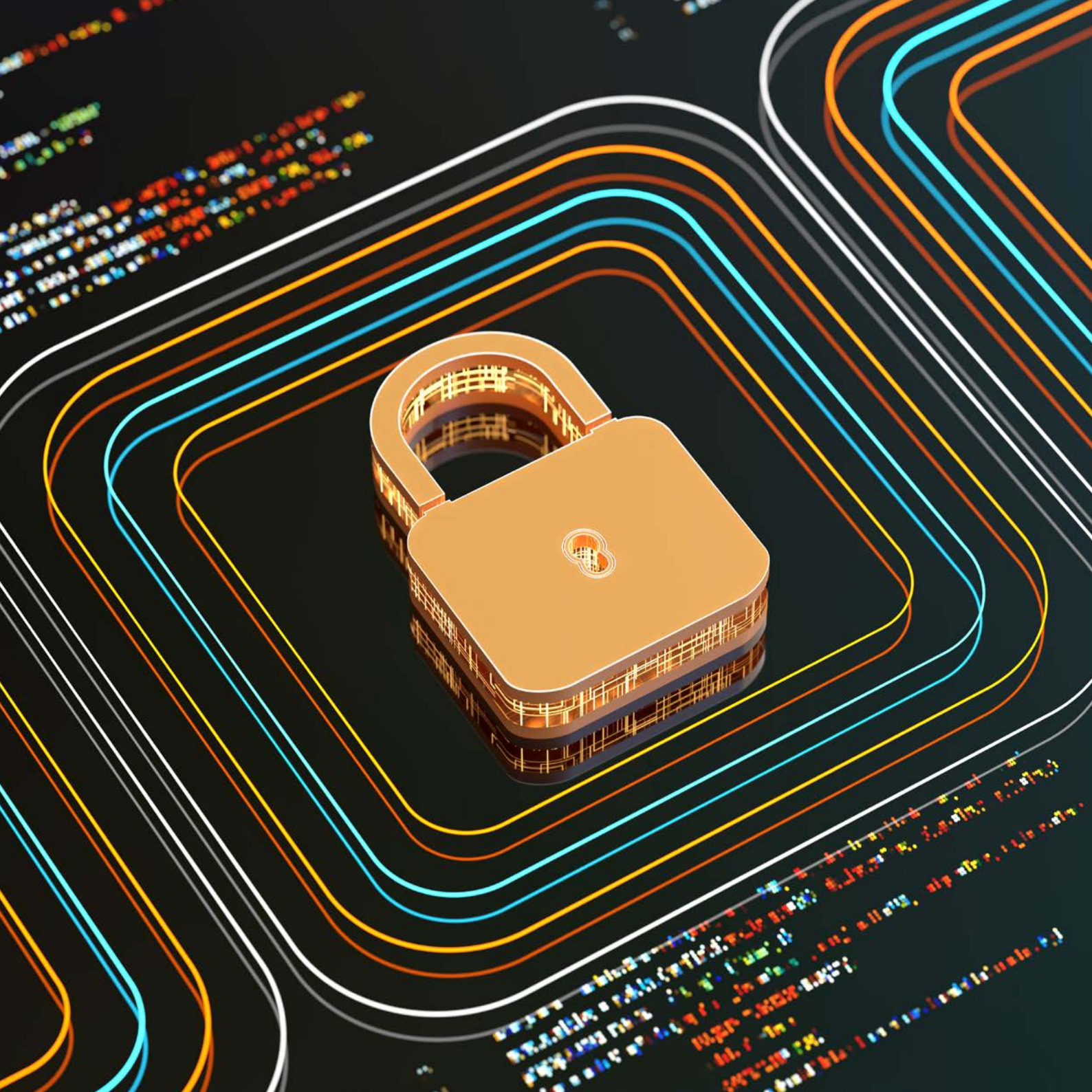
Nicht verschont wurden aber eine Vielzahl an Klein- und Mittelbetrieben, welche sich einer wahren Flut an Verschlüsselungsmalware und Erpressungstrojanern gegenübersahen. Und war es bisher noch möglich, sich mit guten Backup- und Restoreprozessen zu schützen, hatten die Cyberkriminellen gelernt und ihr Erpressungsrepertoire um die Veröffentlichung von Firmen- und Privatdaten bei Nichtbezahlung des Lösegeldes erweitert.

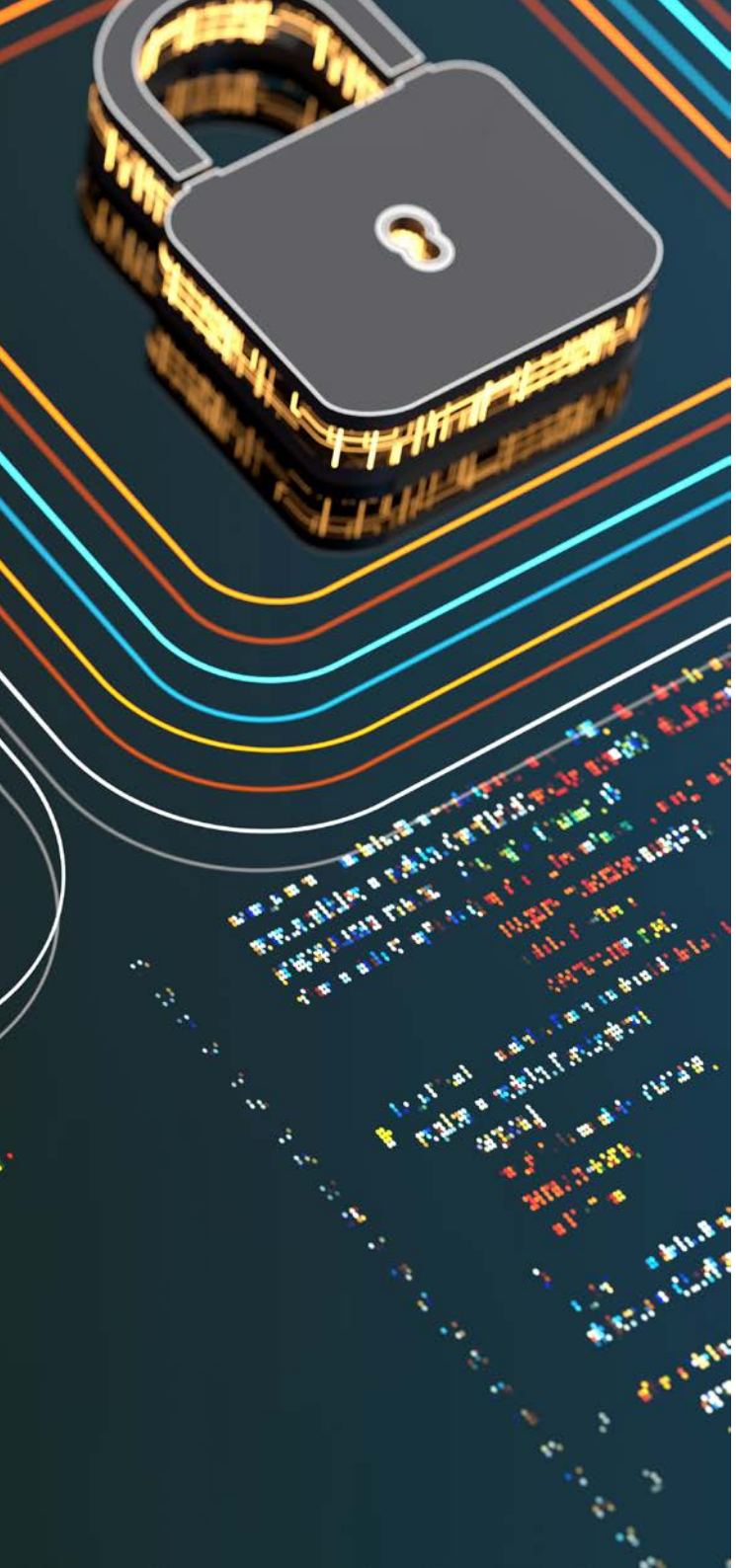
Der erste Lockdown hatte kurzfristig in der Verwaltung eine Art Schockstarre ausgelöst. Alle Treffen wurden abgesagt, Reisen waren unmöglich, Gremienarbeit undenkbar. Doch war diese Paralyse nur von kurzer Dauer und schnell ging es, sicherheitshalber gleich mit erhöhtem Tempo, weiter. Gerade auf EU-Ebene hat der Umstieg auf Videokonferenzlösungen in den Arbeitsgruppen dazu geführt, dass in viel kürzeren Intervallen getagt wurde und somit die Arbeiten zur Einrichtung des Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung und des Netzes nationaler Koordinierungszentren bereits 2020 abgeschlossen werden konnten. Nebenbei wurde auch gleich die Cybersicherheitsstrategie der EU für die digitale Dekade vorgestellt. Und der Vorschlag der Europäischen Kommission zu einer neuen Richtlinie über Maßnahmen für ein hohes gemeinsames Maß an Cybersicherheit in der gesamten Union – also der NIS-2-Richtlinie – angenommen. Formell soll diese die geltende NIS-Richtlinie aus dem Jahr 2016 ersetzen und substantiell verbessern. Informell soll NIS 2 im Cybersicherheitsbereich den Turbo zünden. Nach und nach wurde sogar erkannt, dass Videokonferenzen, welche über mehrere Stunden gingen, die eine oder andere Pause guttäte.

Noch viel mehr gebe es anzuführen, vieles von dem, was passiert ist, kann diesem Bericht entnommen werden. Das Jahr 2020 war, auch wenn es auf den ersten Blick nicht so scheinen mag, gerade für den Bereich der Cybersicherheit so viel mehr als nur Corona.

Und als wäre all das nicht schon spannend und aufregend genug gewesen, wurde gegen Jahresende ein Cybersicherheitsvorfall bekannt, welcher der Welt ihre Abhängigkeiten in die Cyber Supply Chain sowie deren dramatische Verwundbarkeit aufzeigte. Wieder einmal war Weihnachten keine Zeit der Besinnung, der Einkehr und des Innehaltens. Denn eines war klar: SolarWinds SUNBURST würde auch an Österreich nicht einfach vorbeigehen …

Aber das ist eine andere Geschichte und soll ein andermal erzählt werden.





Einleitung

Die Österreichische Strategie für Cybersicherheit (ÖSCS) legt fest, dass durch die Cyber Sicherheit Steuerungsgruppe (CSS) ein jährlicher Bericht zur Cybersicherheit in Österreich erstellt wird. Der letzte wurde im November 2020 vorgelegt.

Der aktuelle Bericht Cybersicherheit für das Jahr 2020 baut auf den Inhalten des letztjährigen Berichts auf und ergänzt diesen um aktuelle Entwicklungen mit Schwerpunkten in den Bereichen der internationalen und operationellen Entwicklungen. Beobachtungszeitraum ist das Jahr 2020, einzelne aktuelle Entwicklungen im Jahr 2021 haben Eingang gefunden.

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

1 Cyberlage / Bedrohung

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

1.1 Lage Cybersicherheit – operative Ebene

1.1.1 Operatives Lagebild – Überblick

Der Berichtszeitraum 2020 begann mit einem Cybersicherheitsvorfall in einer verfassungsmäßigen Einrichtung, der es zum ersten Mal seit Inkrafttreten des Netz- und Informationssystemsicherheitsgesetzes (NISG) notwendig machte, eine Cyberkrise festzustellen. Daraufhin aktivierte der damalige Bundesminister für Inneres, Dr. Wolfgang Peschorn, das staatliche Cyberkrisenmanagement (CKM), was dazu führte, dass eine Stabsstruktur durch die Mitglieder des Inneren Kreises der Operativen Koordinierungsstruktur (IKDOK) eingerichtet wurde. Alle Gremien und Einsatzstrukturen arbeiteten hochprofessionell und effizient und konnten somit die Krise rasch unter Kontrolle bringen. Die ersten Risikominimierungsmaßnahmen erfolgten zeitnah. Durch dieses schnelle und zielgerichtete Vorgehen konnte der Angreifer in seinen Tätigkeiten nachhaltig gestört, die strukturierte Bereinigung des Systems vorbereitet und mit Anfang Februar durchgeführt werden.

Cybersicherheitsvorfall im BMEIA aktivierte erstmalig die gesamtstaatlichen Cybersicherheitsstrukturen

Die Ausrufung einer Gesundheitspandemie im Frühjahr 2020 führte weltweit zu einem massiven Anstieg von Phishing- und Betrugsversuchen mit Pandemieködern als (sogenanntes „Event based“) Social Engineering. Gleichzeitig erfolgte häufig ein Absenken der Perimeter-Cybersicherheit in Unternehmen und anderen Einrichtungen, um den massiv erhöhten Bedarf an Teleworking/Homeoffice, entstanden durch Einschränkung der Bewegungsfreiheit durch Lockdowns, zu bewältigen.

Angriffe mit Ransomware oder mittels DDoS (Distributed Denial of Service) wurden im Berichtszeitraum seitens der Täterinnen und Täter weiterentwickelt. Die Kriminellen hinter Ransomware fordern nun nicht mehr „nur“ Lösegeld für Entschlüsselung, sondern drohen auch mit der Veröffentlichung von erbeuteteten Daten.

Die Corona-Pandemie hatte im vergangenen Jahr nicht nur Auswirkungen auf die Gesundheit und die Wirtschaft, sondern auch auf den Cyberbereich. SARS-CoV-2-Themen waren dabei Köder für Social Engineering-Angriffe und Betrugstatbestände.

Bei DDoS-Angriffen wird hingegen „Schutzgeld“ gefordert. Nach einem Angriff auf die IT-Infrastruktur als „Warnschuss“ oder „Beweis“ wird mit der Lahmlegung aller im Internet erreichbaren Dienste des oder der Angegriffenen gedroht, sollte nicht die in der entsprechenden Erpresser-E-Mail geforderte Summe in Form von Kryptowährung bezahlt werden.

Ein massives Risiko für Unternehmen und verfassungsmäßige Einrichtungen stellen Abhängigkeiten von Cloud-Infrastrukturen und IT-Fernzugängen für das Teleworking dar.

International ist ein Trend zu Angriffen auf das schwächste Glied und damit eine Infektion der eigentlichen Ziele innerhalb der digitalen Lieferkette (Cyber Supply Chain) festzustellen.

1.1.2 Effekte von SARS-CoV-2 im Cyberspace

Das Homeoffice mit dem damit verbundenen Teleworking hat vor allem zu Beginn der Pandemie für Störungen in Teleworking-Lieferketten (Supply Chain) von IT-Systemen geführt. Unternehmen waren oft gezwungen, ihre eigenen Cybersicherheitsbarrieren abzusenken, um den Bediensteten den Zugriff auf ihre Arbeitsplätze von außerhalb zu ermöglichen. Dies führte zu einer enorm vergrößerten Angriffsfläche und damit auch zu neuen Angriffsvektoren. Die Bedrohungslage wurde noch zusätzlich durch eine fast zeitgleich bekannt gewordene Sicherheitslücke in hierfür notwendiger Software (RDP Gateways) verschärft. Im Berichtszeitraum kam es in Österreich in diesem Zusammenhang zu keinen schwerwiegenden Cybersicherheitsvorfällen in kritischen Infrastrukturen oder Einrichtungen der öffentlichen Verwaltung. Dennoch ist die Gefahr für Systeme durch das abgesenkte Sicherheitsniveau weiterhin vorhanden und dauerhaft hoch.

Obwohl zu Beginn der Krise Cyberkriminelle medienwirksam den “Verzicht” des Angriffs auf Organisationen des Gesundheitsbereichs verkündet hatten, wurde dieses Versprechen nicht eingehalten: Sowohl Krankenhäuser als auch Impfstoffforschungseinrichtungen wurden Ziele von teilweise massiven Cyberangriffen und Spionage.

1.1.3 Advanced Persistant Threats (APTs)

Advanced Persistant Threats (APTs) stellen sowohl für die öffentliche Verwaltung als auch für Unternehmen in Österreich eine permanente und steigende Bedrohung dar. Das vorrangige Ziel von APTs dient der Beschaffung von Informationen im Kontext von Wirtschafts- und Industriespionage oder politisch motivierter Ausspähung. Darüber hinaus erlauben APTs den Angreifenden, Computernetzwerke in Verwaltung, Produktions- und Lieferketten zu sabotieren. Dies kann von Reputationsverlust bis zur vollständigen Unbrauchbarkeit der Systeme führen.

Im Netzwerk des österreichischen Bundesministeriums für europäische und internationale Angelegenheiten (BMEIA) wurde, nach Hinweis durch das Government Computer Emergency Response Team (GovCERT), mit Jahreswechsel Schadsoftware festgestellt. Gleich nachdem die Unregelmäßigkeiten bekannt wurden, konnte die Vorfallserstreaktion innerhalb der Linie gestartet und eine Erstanalyse durch GovCERT und dem Cyber Security Center (CSC) des Bundesamtes für Verfassungsschutz und Terrorismusbekämpfung (BVT) vorgenommen werden. Nach Erkennen der Dimension des Vorfalls durch erfolgreiche Entschlüsselung von Teilen der Schadsoftware am 3. Jänner 2020 wurden die vorgesehenen Krisenmechanismen für derartige Vorfälle initiiert.

Am 7. Jänner 2020 wurden die Einsatzstrukturen mit Vertreterinnen und Vertretern aus dem Bundesministerium für Inneres (BMI, Bundesamt für Verfassungsschutz und Terrorismusbekämpfung [BVT], Cyber Crime Competence Centrum [C4]), Bundesministerium für Landesverteidigung (BMLV, Militärisches Computer Emergency Readiness Team [Mil-CERT], Heeres-Nachrichtenamt [HNaA], Abwehramt [AbwA]); Bundeskanzleramt (BKA), Government Computer Emergency Response Team (GovCERT) und Bundesministerium für europäische und internationale Angelegenheiten (BMEIA) aktiviert. Dieses Team setzte sich mit der konkreten Bearbeitung des Vorfalls auseinander. Die Einsatzführung erfolgte, wie in derartigen Fällen vorgesehen, durch das BMI. Seitens BMEIA wurde ein österreichischer Dienstleister beauftragt, welcher in die Einsatzstrukturen integriert wurde.

Nach Vorliegen einer Gesamtübersicht über Ausmaß und Schweregrad wurde am 7. Februar 2020 die Bereinigung initiiert, welche in einem konzertierten Vorgehen über die Zentralstelle und allen Vertretungsbehörden erfolgte. Das BMEIA-Netzwerk ist sowohl global als auch dezentral (über eine Vielzahl an Zeitzonen) und weist einen hohen Anteil an mobilen IKT-Geräten auf. Dies stellte eine besondere organisatorische und logistische Herausforderung in der Vorbereitung und Durchführung des Bereinigungsvorgangs dar. Mit 9. Februar 2020 konnte dieser weitestgehend ohne Vorkommnisse abgeschlossen werden.

Der Angriff und die durch den Akteur eingesetzten Verhaltensmuster (TTP) kennzeichnen einen Advanced Persistent Threat (APT). Ein strafrechtliches Ermittlungsverfahren ist anhängig. Im Zuge des Cybervorfalls wurden zahlreiche Maßnahmen eingeführt, die die Resilienz des Netzwerks nachhaltig stärken.

1.1.4 DDoS mit Erpressungsversuchen

Im Berichtszeitraum kam es national wie international zu mehrere Wellen von DDoS-Angriffen (Distributed Denial of Service), vor allem im Banken- und Finanzsektor und auf Internet Service Provider (ISP). Die Angriffe erfolgten mit dem zusätzlichen Ziel, das Opfer zu erpressen. Die neue Methode der Täterschaft besteht darin, jene IT-Komponenten und Services des Opfers, welche aus dem Internet erreichbar sind, durch einen DDoS geringerer Bandbreite zu attackieren. Gleichzeitig ergeht per E-Mail ein Erpresserschreiben, welches in weiterer Folge mit „weit stärkerem“ DDoS droht, sollte das Opfer nicht per Kryptowährung bezahlen. Nach vorliegenden Informationen kam es zu keinen unmittelbaren Folgeangriffen. Erst gegen Ende des Jahres wurden jene Unternehmen, die dem ersten Erpressungsversuch nicht Folge geleistet hatten, erneut angegriffen. Hierbei handelte es sich in einigen Fällen jedoch um Trittbrettfahrer, welche in den in Deutsch verfassten Erpresserschreiben die Namen bekannter Tätergruppen (unter anderem Fancy Bear, Lazarus) verwendeten.

Dieses Phänomen tritt weltweit und zunehmend auch in unterschiedlichen Sektoren, oftmals mit identen Erpesserschreiben, auf. Lediglich die Adressen der Kryptowährungen

(oftmals Bitcoin) und die Absender-E-Mail-Adressen variieren. Es ist letztendlich nicht feststellbar, ob es sich dabei um nur eine Tätergruppe oder mehrere handelt.

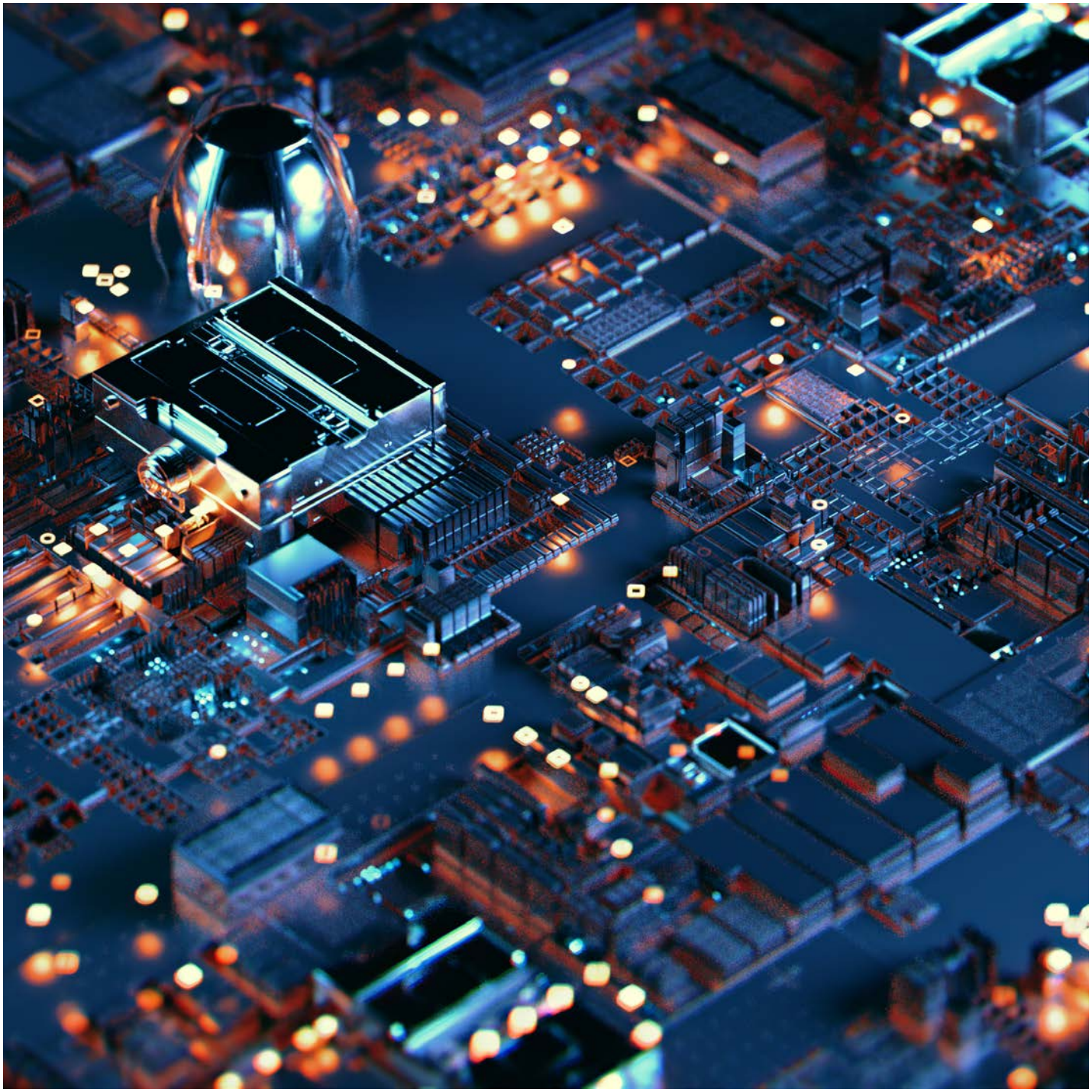
Diese Form der digitalen Wegelagerei wird durch die zunehmende Vernetzung und die Einbindung von, meist gering gesicherten, Internet of Things (IoTs) in Botnetze einen weiter ansteigenden Trend erfahren.

1.1.5 Eindringen in Computer-Netzwerke

SolarWinds: Gegen Jahresende 2020 wurde ein Cybersicherheitsvorfall bekannt, welcher die Abhängigkeit innerhalb der Cyber Supply Chain und deren Verwundbarkeit dramatisch offenlegte. Der mutmaßlich initiale Vorfall ereignete sich beim US-amerikanischen Unternehmen SolarWinds, welches im Bereich von Software-Lösungen für die Computer-Netzwerkverwaltung tätig ist.

Einem Angreifer war es gelungen, in das Unternehmensnetzwerk von SolarWinds einzudringen und die Software-Update-Infrastruktur zu kompromittieren. Damit wurde Kunden, die Updates der, in ihrer Integrität verletzten, aber mit der Signatur von SolarWinds versehenen Software-Suite Orion heruntergeladen hatten, eine Backdoor installiert. Eine erste Schadensanalyse durch SolarWinds ergab, dass es 18.000 potentielle Opfer des Supply Chain-Angriffs gab, darunter auch einige österreichische Unternehmen, die aber nicht zu den verfassungsmäßigen Einrichtungen oder den kritischen Infrastrukturen zählen.

Das, im Zuge des Angriffs kompromittierte, Software-Produkt Orion wird neben einer Reihe von US-Regierungsbehörden auch vom Großteil der Fortune-500-Unternehmen eingesetzt. Daher wurde durch die US-Cybersicherheitsbehörde CISA eine Notfallwarnung ausgesprochen, die eine sofortige Einstellung der Nutzung der Plattform empfahl. Attacken unter anderem auf das US-Finanzministerium und die Telekommunikationsbehörde NTIA, die zum US-Handelsministerium gehört, sind Resultat dieses Angriffs. In Österreich ist diese Software-Plattform wenig verbreitet.



Die Kompromittierung der Update-Infrastruktur wie bei SolarWinds war nicht der erste bekannt gewordene Sicherheitsvorfall über diesen Angriffsvektor, aber in seiner Tragweite und den Auswirkungen wohl der kritischste.

Software AG: Ein weiterer schwerwiegender Cybersicherheitsvorfall ereignete sich beim Unternehmen Software AG, dem zweitgrößten Softwareunternehmen Deutschlands. Dieses wurde Anfang Oktober 2020 Opfer eines Cybererpressungsangriffs. Dabei wurden Daten im Unternehmensnetzwerk aus dem System entwendet und danach unbrauchbar gemacht. Die exfiltrierten Daten wurden danach für Angriffe auf Kunden der Software AG genutzt. Außergewöhnlich und brisant ist dieser Fall, weil die Software AG Produkte für Operating Technology (OT, ~Industrie 4.0), jener Schnittstelle zwischen Software und Produktionshardware anbietet und diese meist mit Fernwartungszugängen versehen sind.

Die Angreifer verfügen nun möglicherweise auch über Zugangsdaten zu deren Kunden. Auf der im TOR-Netzwerk befindlichen Plattform, die für die Veröffentlichung der erbeuteten Daten genutzt wird/wurde, befanden sich auch Daten österreichischer Unternehmen. Diese wurden durch ein zeitnahes Warnschreiben des IKDOK darüber in Kenntnis gesetzt und Mitigationsmöglichkeiten kommuniziert.

Cloudbasierte Datenbanken und Speicher: Vorfälle im Berichtszeitraum haben gezeigt, dass solche Systeme (unter anderem Amazon S3 Buckets, Redis, Elasticsearch, MongoDB) von den Täterinnen und Tätern systematisch gesucht, schnell entdeckt und anschließend ausgenutzt werden können. In diesem Kontext sollte auch der SolarWinds-Vorfall beurteilt werden.

1.1.6 Ransomware

Allgegenwärtig und für große Schäden verantwortlich war im Berichtszeitraum auch das Phänomen Ransomware. Die Funktionalität von Ransomware wurde oft erweitert, um aus dem befallenen Computernetzwerk Daten zu entwenden. Zeigte sich das Opfer nicht zahlungswillig, so wurde mit der Veröffentlichung der entwendeten Daten gedroht.

Die Höhe des geforderten Lösegelds bemisst sich meist an der finanziellen Situation des Opfers, diese wird im Zuge offener Quellenrecherche durch die Angreifer erhoben. Als Angriffsvektor dient in den meisten Fällen eine Kombination aus gezieltem Social Engineering und einem mit einem Schadcode versehenen MS-Office-Dokument als Anhang einer E-Mail.

1.1.7 Andere Schadcodes

Die Malware **EMOTET** wurde nach einer mehrmonatigen Pause im Sommer des Berichtszeitraums wieder aktiv und löste erneut eine weltweite Malspam-Welle aus. Die Fähigkeiten der Schadsoftware wurden in dieser Pause weiterentwickelt. Eine der zentralen Schutzmaßnahmen gegen EMOTET ist es, Microsoft Office das Ausführen von Makros zu verbieten oder nur vertrauenswürdige, signierte Makros zu erlauben. Office-Dokumente mit Makros sind ausführbare Dateien und sicherheitstechnisch mit .EXE-Dateien vergleichbar. Durch das Eingreifen in bestehende E-Mail-Kommunikation erzeugt EMOTET den Anschein von Legitimität und bringt so das Opfer dazu, Dateien herunterzuladen und zu öffnen.

Der Code verfügt auch über die Funktionalität, weitere Schadcodemodule nachzuladen. Darunter fallen Ransomware, Tools zur Datenextraktion bzw. zum -diebstahl oder Software zur Einbindung des befallenen Systems in ein Botnetzwerk.

1.1.8 Schwachstellen

Auch dieser Berichtszeitraum war geprägt von zahlreichen kritischen Schwachstellen, wobei für österreichische Unternehmen bzw. die öffentliche Verwaltung folgende besonders herausfordernd waren.

CITRIX/NetScaler: Nach Veröffentlichung der Exploit-Codes am 10. Jänner 2020 kam es zu zahlreichen Angriffen auf Unternehmen und Behörden (öffentlich diskutiert wurden in diesem Zusammenhang auch die Auswirkungen auf den Elektronischen Akt [ELAK] in der öffentlichen Verwaltung).

RDP Gateway: Microsoft veröffentlichte am 14. Jänner 2020 Patches für zwei kritische Lücken in RDP Gateway (CVE-2020-0609 und CVE-2020-0610), die beide potentiell zu Remote Code Execution (RCE) führen können. Seit dem 23. Jänner 2020 ist ein Exploit öffentlich auf GitHub verfügbar. RCE wurde bisher zwar demonstriert, aber der Code noch nicht veröffentlicht.

Microsoft Server Message Block 3.1.1 (SMBv3): Die Lücke kann über das Netzwerk ausgenützt werden und ermöglicht die Ausführung beliebiger Befehle mit Systemrechten. Außerdem ist die Schwachstelle mutmaßlich wurmfähig, kann sich also selbst weiterverbreiten. Betroffen waren SMBv3-Clients und Server mit Windows 10 Versionen 1903/1909.

Netlogon Remote Protocol (CVE-2020-1472 alias Zerologon): Erfolgreiche Angreifer konnten ganze Windows-Domänen übernehmen. Zu der von Microsoft im August gepatchten Lücke wurde ein Proof-of-Concept veröffentlicht.

Weitere kritische Schwachstellen fanden sich in mehreren Versionen des Oracle WebLogic Servers. Sie wiesen eine kritische, via Internet ausnutzbare Schwachstelle auf (CVE-2020-14750) in SAP NetWeaver AS Java (CVE-2020-6287) bei F5 K52145254 TMUI RCE Vulnerability (CVE-2020-5902), Palo Alto PAN-OS (CVE-2020-2021) und im Dezember 2020 wurde mit Kerberos Bronze Bit Attack (CVE-2020-17049) ein weiterer Designfehler in den Windows Authentication-Protokollen gefunden.

In Bezug auf die oben bereits angeführte Cyber Supply Chain-Problematik ergibt sich das Dilemma zwischen sofortigem Einspielen (die Standard-Empfehlung) des Updates oder der Duchführung eines Code-Reviews, um einen möglicherweise eingebetteten Schadcode oder andere systemstörende Fehler zu erkennen, bevor sie Schaden im eigenen Netzwerk anrichten. Code-Reviews sind jedenfalls zeit- und kostenintensiv und erfordern oftmals vertragliche Ergänzungen mit dem Softwarehersteller.

1.1.9 Veröffentlichung von Daten

Der Trend bei der Veröffentlichung von Daten (Data Leaks) in Form von entwendeten Zugangsdaten ist weiterhin ungebrochen. So wurden beispielsweise persönliche Daten von (auch österreichischen) Kundinnen und Kunden der IT-Sicherheitstrainingsfirma SANS öffentlich zugänglich gemacht.

Wie schon in den voranstehenden Punkten Ransomware, DDoS und andere Schadcodes angeführt, wurde die Drohung und oftmals durchgeführte (teilweise) Veröffentlichung von erbeuteten Daten eine Erweiterung des Geschäftsmodells von Cyberkriminellen, um ihren Forderungen mehr Nachdruck zu verleihen. Betroffen sind dabei nicht nur das primäre Opfer selbst, sondern auch dessen Partner in der Cyber Supply Chain.

1.1.10 Legacy IT-Infrastruktur

Im Herbst 2020 wurde mutmaßlich der Quellcode von WindowsXP geleakt und in einem Internetforum zum Kauf angeboten. Viele ältere Systeme, „vererbte" IKT-Infrastruktur (Legacy Systems), darunter oft Operating Technology (OT), verwenden WindowsXP als Betriebssystem. Gerade OT sieht sich damit konfrontiert, dass kaum Updates für das darunterliegende Betriebssystem bereitgestellt werden. Das stellt die Betreiber dieser veralteten Technologie vor ein enormes Sicherheitsproblem. Der End-of-Life-Cycle wurde für das Microsoft Betriebssystem Windows XP, beginnend mit 8. April 2014, sukzessive zurückgefahren und ist seit langem beendet. Das bedeutet, dass entdeckte Lücken herstellerseitig nicht mehr gepatcht werden. Darüber hinaus ist auch der Support für das Betriebssystem Microsoft Windows 7 am 14. Jänner 2020 ausgelaufen.

„Legacy Systems" stellen häufig ein Einfallstor für Cyberkriminelle dar. Durch den weiter anhaltenden und durch die COVID-19 Krise beschleunigten Trend der Anbindung vieler dieser veralteten Systeme an das Internet (unter anderem Industrie 4.0) werden diese Systeme zu bevorzugten Zielscheiben. Einem Bericht des Magazins Heise zur Folge sind noch mindestens 100 Millionen Windows-7-PCs am Netz, das entspricht ca. 18 Prozent

aller Windows-Rechner weltweit. Auch in Österreich sind unzählige dieser veralteten IT-Systeme in Verwendung und über das Internet erreichbar.

1.2 Lage Cybersicherheit – Unternehmen und Sicherheitsdienstleister

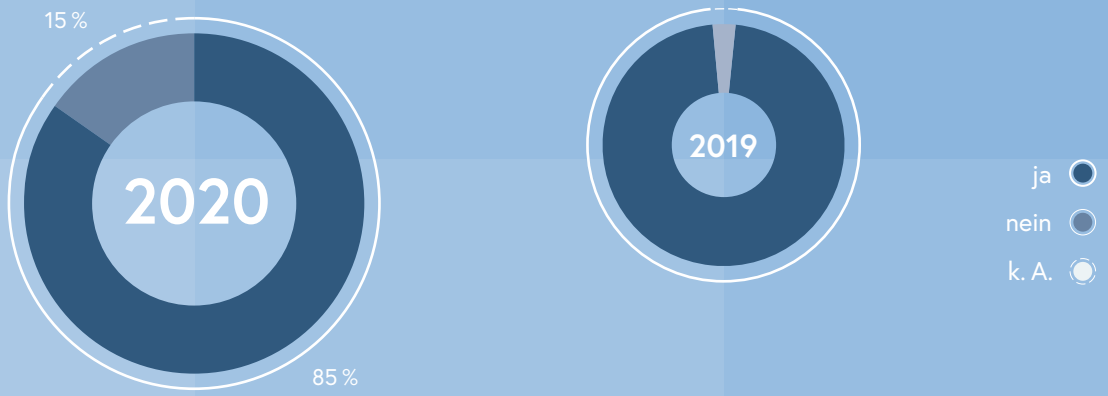
Investitionen in Cybersicherheit konnten schwerwiegende IT-Sicherheits-vorfälle verhindern

Um als Staat sowohl einen Überblick über die Cyberlage zu haben, als auch zeitnah kritischen Entwicklungen gegensteuern zu können, kooperieren die staatlichen Cybersicherheitsstrukturen eng mit den verfassungsmäßigen Einrichtungen, den Betreibern der kritischen Infrastruktur und den Betreibern wesentlicher Dienste. Zur Erstellung des vorliegenden Berichts wurden auch in diesem Berichtsjahr führende Stakeholder eingeladen, Einschätzungen zu den Entwicklungen abzugeben und somit zum Lagebild beizutragen. Auf diese Weise soll ein valider und weitestgehend vollständiger Überblick über Chancen, Bedrohungen und Trends in der Dimension Cyber in Österreich geschaffen werden.

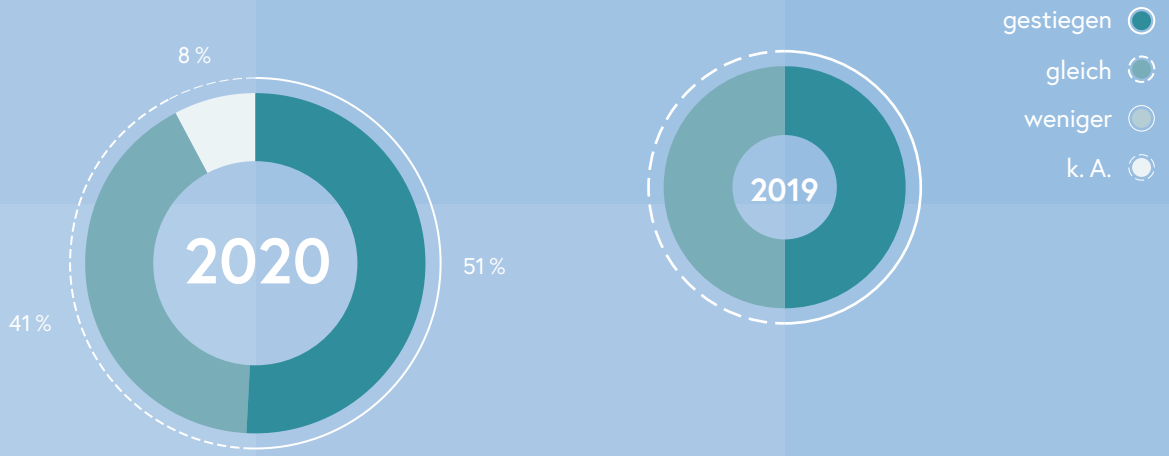
1.2.1 Unternehmen der kritischen Infrastruktur und verfassungsmäßige Einrichtungen

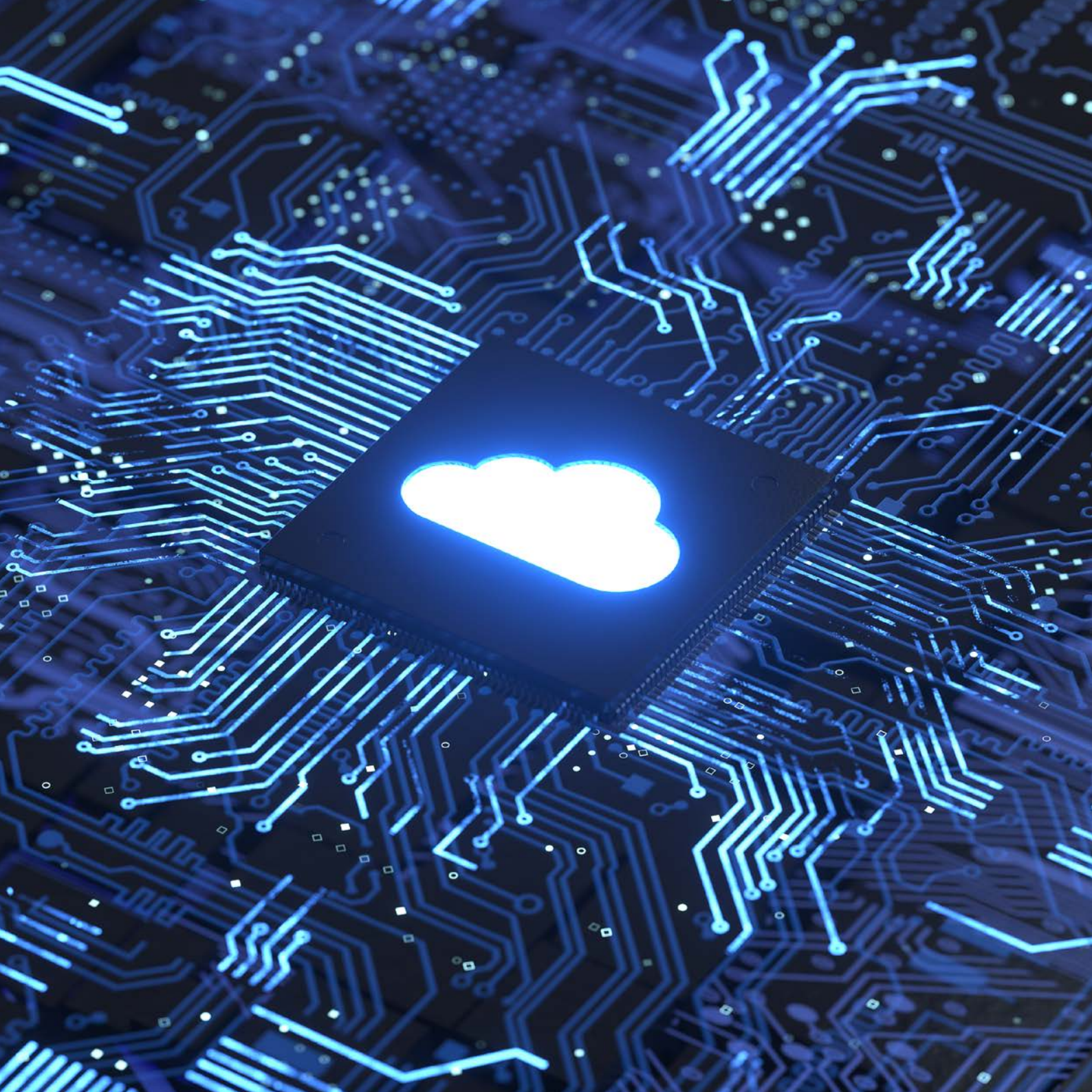
Bei der Mehrheit der befragten österreichischen Unternehmen der kritischen Infrastruktur wurden im Jahr 2020 Investitionen im Bereich der Cybersicherheit vorgenommen. Dabei hat sich das Verhältnis von Firmen, die ihr Budget im Berichtszeitraum erhöhten, gegenüber solchen Firmen, die das Budget auf Vorjahresniveau hielten, leicht verbessert. Keines der befragten Unternehmen verminderte das Budget für Cybersicherheit. Insgesamt bestätigt sich der Trend, dass die Ausgaben für IT-Sicherheit über die Jahre auf gleichem Niveau blieben. Diese Investitionen konnten mutmaßlich schwerwiegende IT-Sicherheitsvorfälle verhindern.

Wurden in Ihrer Firma 2020 neue IT-Security-Maßnahmen implementiert, welche die Erkennbarkeit von IT-Sicherheitsvorfällen erhöhen können?



Wie hat sich in Ihrer Firma im Jahr 2020 das für IT-Security zur Verfügung stehende Buget gegenüber dem Jahr 2019 verändert?





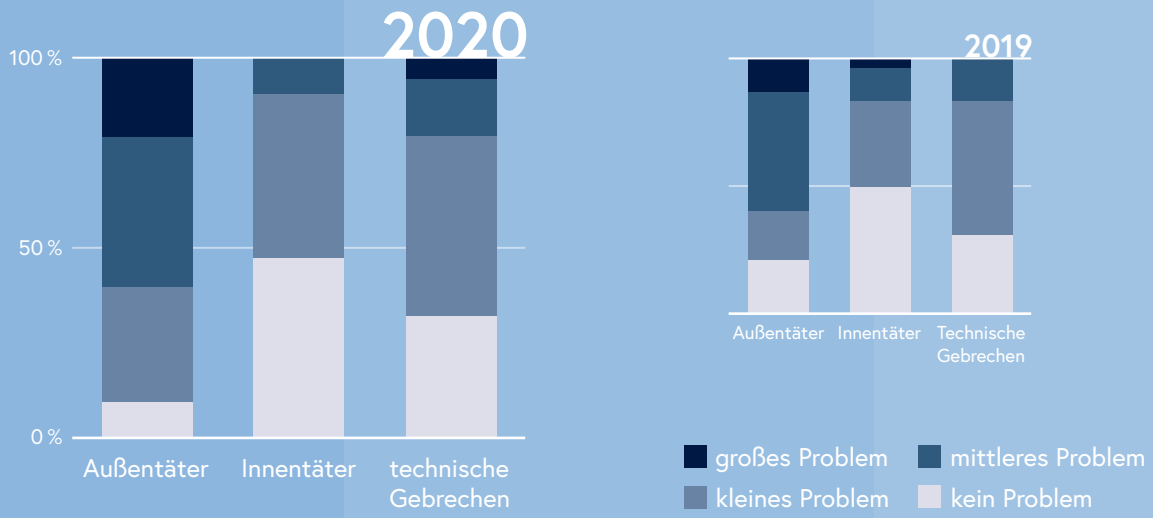
Die im IT-Bereich getroffenen Sicherheitsmaßnahmen umfassten im Berichtszeitraum unter anderem verstärktes Monitoring der On-Premise- und Cloud-Systeme, die Implementierung und Erweiterung von Security Information and Event Management-Lösungen (SIEM) sowie erweitertes Logging, die Einrichtung von Security Operations Centers (SOC), Next Generation Firewalls und Next Generation Mail Gateways, Ransomware Scanner, Endpoint Detection, Cloud Access und DNS-Filtering, regelmäßige Penetrationstests und Schwachstellen-Scans, die Verbesserung von Information Security Management Systems (ISMS), die Zertifizierung nach ISO 27001 sowie zahlreiche Awareness-Maßnahmen und Schulungen von Mitarbeiterinnen und Mitarbeitern.

Wie in den Vorjahren gelten ein konzernweites IT-Risikomanagement, ein ISMS nach ISO27001/27019 und Awareness-Schulungen als die effektivsten Mittel, um Sicherheitsvorfälle erfolgreich zu vermeiden bzw. ihren Schaden zu minimieren.

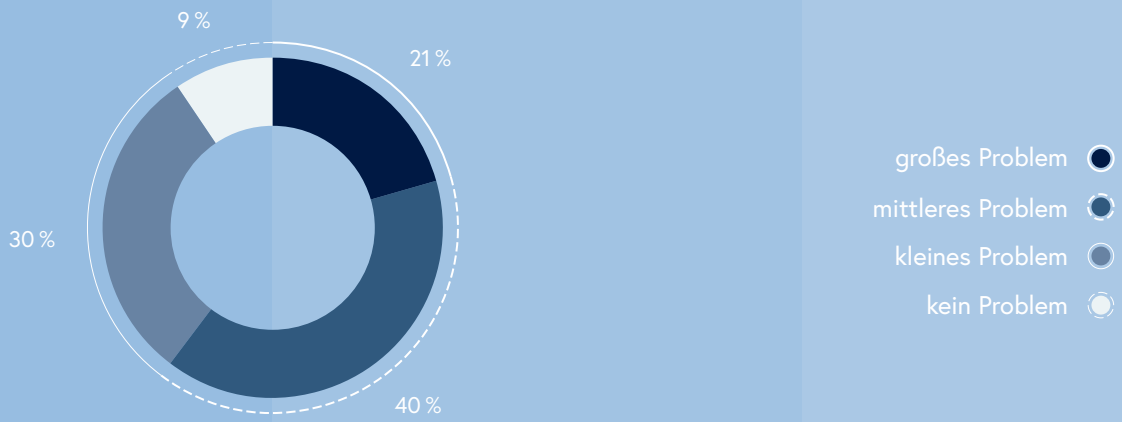
Gute Cybersicherheitsexpertise im eigenen Team zu haben, gilt als Schlüssel zum Erfolg; daher wurde viel in die Aus-, Fort- und Weiterbildung investiert

Die Einschätzung von Vorfallsursachen zeigt auch für 2020 im Großen und Ganzen ein dem vorjährigen Berichtsjahr vergleichbares Bild. Demnach sind primär Außentäter oder technische Gebrechen Vorfallsverursacher. Innentäter waren nur bei einer geringen Anzahl von Vorfällen involviert. Allerdings sind im Vergleich zu 2019 Verschiebungen dahingehend zu verzeichnen, dass die Gefährdung durch Außentäter stark zugenommen hat, die Gefährdung durch Innentäter aber eher gleich geblieben ist. Die Gefahr eines technischen Gebrechens wird als gleichbleibend problematisch eingeschätzt. Der Office-Bereich bzw. Windows-Geräte sind die primären Bereiche, die für Angriffe genutzt werden.

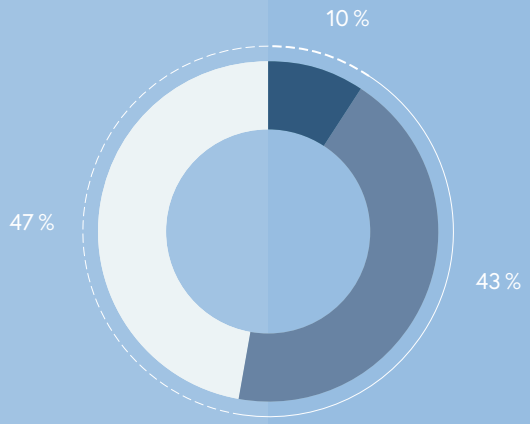
Vorfallsursachen



Wie beurteilen Sie die „Vorfallsursache“ Außentäter für das Jahr 2020?

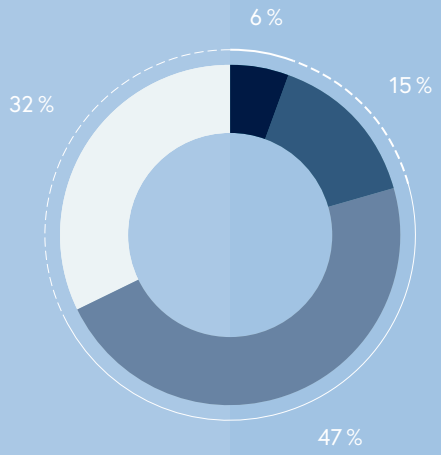


Wie beurteilen Sie die „Vorfallsursache“ Innentäter für das Jahr 2020?



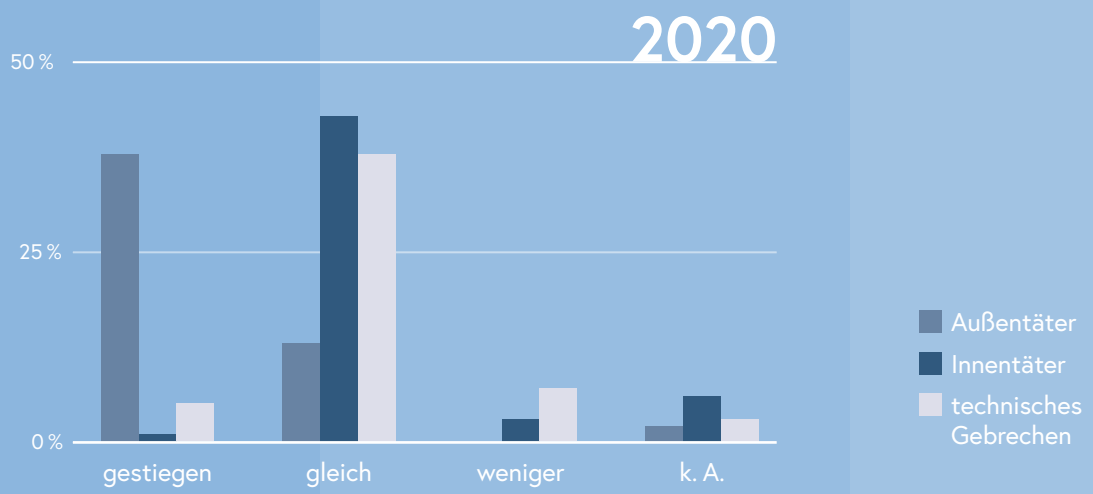
- großes Problem
- mittleres Problem
- kleines Problem
- kein Problem

Wie beurteilen Sie die „Vorfallsursache“ technisches Gebrechen für das Jahr 2020?



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

Welche Trends konnten Sie 2020 diesbezüglich gegenüber 2019 beobachten?



Rückmeldungen von „Lessons Learned“ zeigen folgende Trends:

Den Rückmeldungen zufolge beschäftigten sich befragte Organisationen 2020 intensiv mit neuen regulatorischen Maßnahmen, wie der Datenschutzgrundverordnung (DSGVO) oder der Umsetzung des NISG, das 2019 in Kraft getreten ist. Darüber hinaus kann erneut festgestellt werden, dass am Thema Cloud kein Weg vorbeiführt. Der Druck, Cloud-Dienste zu nutzen, steigt weiter an, obwohl wesentliche Fragen bezüglich Datenschutz und Datensicherheit weiterhin ungelöst sind. Aus Sicht der Befragten gibt es für die rechtlichen Fragen oft keine zufriedenstellenden Regulatorien. Die Realität und die rechtlichen Rahmenbedingungen klaffen hier stark auseinander. Dabei kann eine unternehmenseigene Cloud-Strategie helfen, viele der aufkommenden Probleme bereits vor dem erstmaligen Auftreten zu adressieren. Firmen werden besipielsweise akut mit komplexen Herausforderungen konfrontiert, wenn internationale Softwarehersteller mit großer Marktdurchdringung zu einer „Cloud first“ oder „Cloud only“-Strategie wechseln. Die schwierige und rechtlich nicht vollends geklärte Problematik in Bezug auf die Datenübermittlung in die USA (DSGVO) stellt in diesem Zusammenhang Firmen vor Herausforderungen. Als unbefriedigend wird angeführt, dass es keine einheitliche Vorgangsweise aller EU-Staaten in Bezug auf die Cloud-Lösungen gibt. Dies hat sich 2020 vor allem auch in Hinblick auf die Corona-Pandemie im Zusammenhang mit Videokonferenzsystemen (unter anderem Zoom, MS-Teams) gezeigt.

Als große Herausforderung wird zunehmend die Wahrung der eigenen Handlungsfähigkeit aufgrund des Trends zum ausschließlich cloudbasierten Management von Sicherheitskomponenten inklusive der damit verbundenen Supply Chain-Risiken gesehen. So wird angemerkt, dass der durch die DSGVO erhoffte Bedeutungsschub für eine eigenständige europäische IT-Security-Industrie weitestgehend ausgeblieben ist, während die Geschäftserfolge der amerikanischen und israelischen Industrie drastisch zugenommen haben. Ein zunehmend unüberschaubarer Kreis an Cybersicherheitskompetenzzentren in Österreich und der EU, mit teils unterschiedlichen Vorgaben und Empfehlungen bezüglich

Stand der Technik etc., hat die Situation nicht vereinfacht. In dieser Hinsicht werden Standardisierungen und Konsolidierungen erhofft.

Operative Sicherheit wurde bisher meist nur am Rande als Cybersicherheitsthema verstanden. Mit Inkrafttreten des NISG fanden ganzheitliche Konzepte und Risikobewertungen größere Verbreitung. In diesem Zusammenhang gewannen Business Continuity Management (BCM) sowie Notfallpläne an Bedeutung und fanden Einzug in aktualisierte Strategien. Organisatorische Weiterentwicklungen im Zusammenhang mit ISMS wurden angestoßen und die Wichtigkeit von SOCs als unverzichtbar erkannt. Auch haben aktuelle Vorfälle in den Unternehmen dazu geführt, Prozesse einer neuerlichen bzw. vermehrten Qualitätssicherung zu unterziehen. In diesem Kontext wurden in den Unternehmen vermehrt Chief Information Security Officers (CISOs) installiert und Notfallorganisationen geschaffen.

Incident Response Playbooks oder „Checklisten-Security" werden als Erfolgsfaktor zur Bewältigung von Cybersicherheitsvorfällen gesehen. Hilfreich waren auch die Ergebnisse aus externen und internen Audits. Die Komplexität und die damit verbundene Spezialisierung wird als weiter zunehmend wahrgenommen, auch aufgrund der hohen Anzahl von Lieferanten im IT-Security-Bereich und einer immer komplexeren Supply Chain. Die Unternehmen gehen daher davon aus, dass zusätzliche dedizierte Ressourcen für diesen Bereich bereitzustellen sein werden, um ein angemessenes Sicherheitsniveau auch entlang der Lieferkette garantieren zu können.

Security Berater sehen sich immer häufiger als „Übersetzer" der Themen für die Chief Information Officers (CIOs) und IT-Abteilungen – analog zu den IT-Beratern für die Business-Abteilungen. Maßnahmen zur Sicherung von IT-Systemen und Informationssicherheit bedürfen höchster Priorität und Management Commitment, um bei schnell ändernden Gefährdungslagen sicher und situationsangepasst handeln zu können.

Im Sektor liegt ein verstärkter Fokus auf Vulnerability Management und Threat Intelligence, um vorhandene Schwachstellen zeitnah zu schließen und Lücken in der eigenen Verteidigung erkennen und adressieren zu können. Die Reduktion von Domain Admins bzw. granularere Berechtigungsvergaben werden dabei als Mittel der Wahl zur Reduktion von Konfigurationsfehlern und deren Auswirkungen gesehen. In diesem Zusammenhang gewinnen Zero-Trust-Systeme an Relevanz.

Geleakte Passwörter, fehlendes Account-Lifecycle-Management, fehlende Daten- und Servicequalität in der Corporate IT (durch Dienstleister), fehlende Durchsetzung und Überwachung von Sicherheitsrichtlinien sowie nicht zeitnahes Umsetzen von Empfehlungen aus Security Audits werden als die Treiber von Cyberrisiken für die Unternehmen gesehen.

Auch binden stark steigende Compliance- und Dokumentationsaufwände zunehmend operative Betriebsressourcen und senken dadurch die Effektivität von IT-Securitypersonal.

Als Hauptrisikofaktor wird nach wie vor der Mensch, d. h. „die Mitarbeitenden", angesehen. In den nächsten Jahren wird nach Einschätzung der befragten Unternehmen der Bedarf an Bewusstseinsbildung (Cyber-Awareness) für die Mitarbeiterinnen und Mitarbeiter stark steigen und es wird zu einer Weiterentwicklung der IT-Security-Services von derzeit eher technisch geprägten Bereichen hin zu einem gesamtheitlichen System mit Trainings- und Schulungsmaßnahmen kommen müssen.

COVID-19-bedingt bedarf es derzeit verstärkter Vermittlung entsprechender Cyber Security Awareness, vor allem für Mitarbeiterinnen und Mitarbeiter im Homeoffice. Sogenannte Shadow-IT (also nicht offiziell zur Verfügung gestellte und entsprechend abgesicherte IKT-Infrastruktur) im Homeoffice-Bereich erhöht das Risikopotential erheblich.

Die hohe Bedeutung einer ausreichenden Absicherung von externen Zugängen (z. B. über 2FA), welche verstärkt durch Homeoffice verwendet werden, wurde durch die Befragten festgehalten.

Der Markt der Cyberrisikoversicherungen wird trotz Hype in den einschlägigen Medien als äußerst beschränkt beurteilt, was an den sehr unterschiedlichen Prämienhöhen und -leistungen festgemacht wird. Auch liegen laut Befragung noch keine konkreten Erfahrungswerte in Bezug auf Kosten und Nutzen vor.

Als deutlicher Trend und positiv konnotiert wird die Auslagerung von SOC-Diensten an professionelle externe Dienstleister wahrgenommen. Als einschränkend stellt sich hier lediglich die zunehmende Abhängigkeit von Dritten dar, welche vor allem im Notfall kaum eigenständiges und autarkes Handeln erlaubt. Die Auslagerung von Sicherheitsdienstleistungen sei jedenfalls „gesamtheitlich und nicht nur ökonomisch zu beurteilen", wird festgestellt.

Durch regelmäßige Cyberübungen in den Unternehmen, sowohl auf strategischer als auch operativer Ebene, wurde einerseits das Verständnis auf Managementebene gestärkt, als auch das Zusammenspiel der Incident Response Teams verbessert.

Auslagerungen von SOC-Diensten an professionelle externe Dienstleister sind ein aktueller Trend

Analysen von Angriffen auf Mitbewerber bildeten die Grundlage für konkrete Maßnahmen zur Erhöhung der Sicherheit, sowohl prozessuale als auch verfahrenstechnische Verbesserungen wurden implementiert. Ein Schwergewicht wurde auf die Optimierung der Kommunikationsprozesse bei Cybervorfällen gelegt.

COVID-19 hat gezeigt, dass die Zusammenarbeit trotz Homeoffice funktioniert, wobei die Einhaltung der Meldewege und Meldepflichten als wesentlich beurteilt wird. Was es braucht, sind eine abteilungsübergreifende Kommunikation und multidimensionale Betrachtungsweisen. Der offene Informationsaustausch über Sicherheitsvorfälle lässt das gesamte österreichische Unternehmensumfeld resilienter und reaktionsfähiger werden. Frühzeitige Informationen über Angriffe sind für die Einleitung entsprechender Abwehrmaßnahmen entscheidend, was einerseits funktionierende Kommunikationsstrukturen, andererseits aber auch ein hohes Maß an Vertrauen bedingt.

Der Fachkräftemangel im Bereich Cybersicherheit bleibt weiterhin Thema und wird durch die voranschreitende Digitalisierung als auch die gegenwärtige Krise weiter verschärft. Dieser Mangel an qualifiziertem Personal führt auch dazu, dass dringend durchzuführende, sicherheitsbezogene Tätigkeiten, wie beispielsweise die Kontrolle der Arbeitsergebnisse von Fremdfirmen durch Auftraggeberpersonal nicht in entsprechender Tiefe und Qualität erfolgen können.

Flächendeckendes Homeoffice erhöht den Bedarf an sicheren Remotezugängen massiv

Die neue Arbeitsweise erfordert aber auch inhaltliche und organisatorische Anpassungen sowie redundante Internetanbindungen und flächendeckend mobile Arbeitsplätze. Damit ergeben sich auch neue Herausforderungen im Bereich der Administration und der Durchsetzung der IT-Sicherheitsvorgaben. Die Anforderungen und Aufwände im Sicherheitsbereich steigen durch diese technischen und organisatorischen Maßnahmen. Für das mit der technischen Umsetzung betraute Personal bedeutet das zudem eine dahingehende Fähigkeitenentwicklung.

Die voranschreitende Vernetzung von Produktions-IT und Operating Technologie (OT) erfordert entsprechende Netzwerkplanungen und Absicherungskonzepte. Gerade kritische OT erfordert erhöhte Aufwände und Aufmerksamkeit, um bei einem Cybersicherheitsvorfall schnelle Eindämmung (Containment) und rasche Herstellung der Kontrolle sicherstellen zu können. Laut den Rückmeldungen der befragten Unternehmen stellt diese enge Vernetzung und die Notwendigkeit, den Betrieb der OT zu jedem Zeitpunkt, auch unabhängig von der IT sicherstellen zu müssen, eine besondere Herausforderung dar. Legacy-IoT, also aus den Updatezyklen herausgefallene IoT-Geräte, werden als hohes Risiko und in der Absicherung als besonders herausfordernd wahrgenommen.

Aufgrund von bekannt gewordenen schwerwiegenden Cybersicherheitsvorfällen mit internationalen Auswirkungen, rückt die Cyber Supply Chain erneut in den Fokus der Firmen. Dabei sind nicht nur Abhängigkeiten zu Cloud-Dienstleistern zu beurteilen, sondern auch die Cybersicherheit bei Lieferanten, Kunden und Partnern. Die umfassende Absicherung der gesamten Produktionskette und die vereinheitlichte Definition

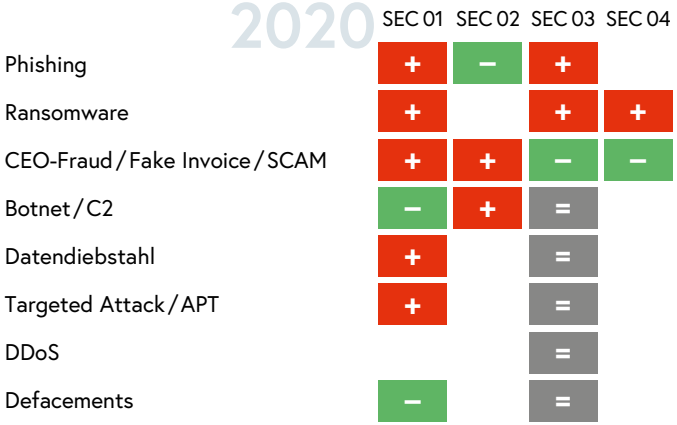
und Anwendung von Sicherheitsstandards gilt hierbei als besonders schwierig. Dabei sind nicht nur offensichtliche Abhängigkeiten, wie bei zugekauften IT-Leistungen (z. B. Office IT und Produktions OT) zu beurteilen, sondern auch nicht offensichtliche Abhängigkeiten (z. B. jene von Telekomprovidern) in die Risikobewertung und die Business Continuity-Planungen mit aufzunehmen. Neben funktionierenden Backup- und Wiederherstellungsprozessen, Absicherungskonzepten und Krisenplänen sind dies vor allem konkrete Planungen, wie im Falle des Ausfalls von kritischen Produktionssystemen der Betrieb weiter aufrecht erhalten werden kann. Da entlang der Cyber Supply Chain jeder Teilprozess durch ungenügende Absicherung alle anderen Teilnehmer gefährden kann, wird ein gemeinsames Verständnis und der Wille, Mindeststandards hochzuhalten, als besonders wichtig erachtet. Die befragten Unternehmen sehen hier allerdings oftmals bei Herstellern von produktionsnahen Systemen oder gar „menschennahen" Medizinprodukten noch Verbesserungsbedarf.

Künstliche Intelligenz (KI) wird von Unternehmen einerseits als Möglichkeit, die eigene Cybersicherheit zu steigern, gesehen, andererseits wird damit aber auch eine Erhöhung des Bedrohungspotentials durch kriminelle Nutzung befürchtet. Die durch KI-Nutzung erhöhte Angriffsgeschwindigkeit erfordert KI-unterstützte Abwehrsysteme. Damit ergibt sich jedoch ein Kontrollverlust über die eigenen Systeme und Maßnahmen, welcher kritisch beurteilt wird.

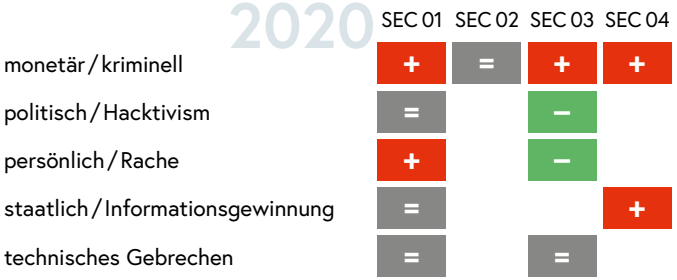
1.2.2 Führende private Unternehmen aus der Cybersecurity-Branche

Die Befragung von führenden privaten Unternehmen aus dem Bereich der Sicherheitsdienstleister wies auch für das Berichtsjahr 2020 eine vergleichsweise geringe Rücklaufquote auf. Aus den eingegangenen Beantwortungen zur Erhebung lassen sich aber dennoch einige Trends und Lessons Identified ableiten.

Trends bei bearbeiteter Vorfallsart

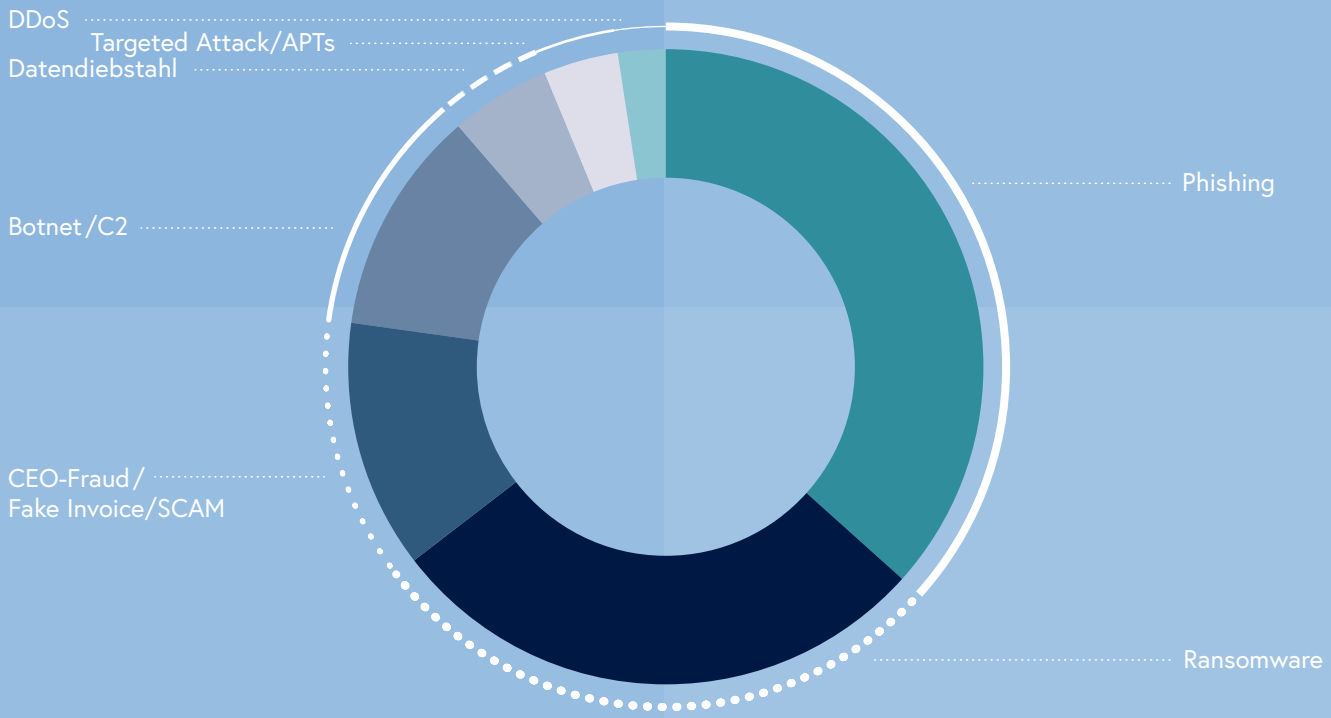


Trends bei bearbeiteten Motivationen

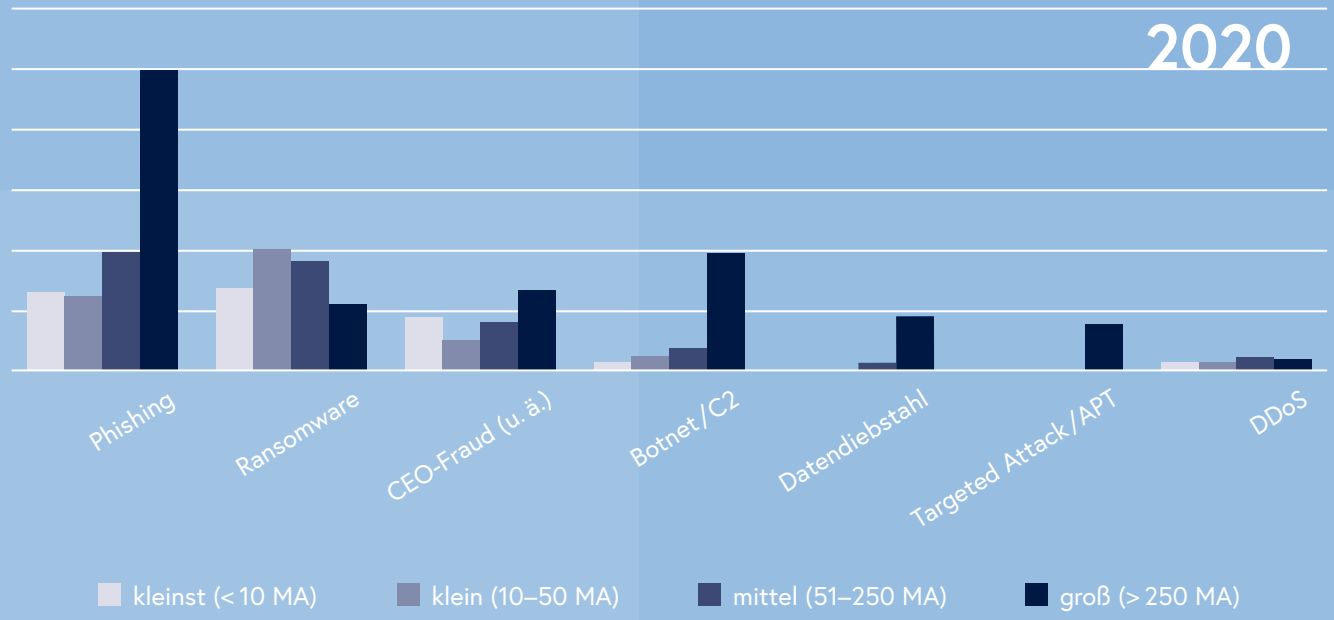


Folgende Vorfallsarten waren im Berichtszeitraum bei den rückmeldenden privaten Unternehmen aus dem Bereich der Sicherheitsdienstleister evident:

Vorfallsarten im Berichtszeitraum



Vorfallsarten im Berichtszeitraum nach Unternehmensgröße aufgeschlüsselt



Phishing

Die Resilienz der Unternehmen in Bezug auf Phising wird als nicht ausreichend beurteilt. Die Awareness der Mitarbeiterinnen und Mitarbeiter ist oft nicht vorhanden, um gezielte Angriffe zu erkennen. Die Möglichkeiten von Awareness-Trainings sind hier aber limitiert, der Angriffsvektor durch solche nicht vollkommen auszuschließen.

Dabei wird, nach dem Motto „Detection & Visibility is key", die Sichtbarmachung möglicher Cybersicherheitsvorfälle im eigenen Netzwerk als Schlüsselfähigkeit gesehen. Nicht nur um etwaige Phishing-Angriffe zu erkennen, sondern auch, um nach erfolgreichen Angriffen die Auswirkungen konkret festmachen und beurteilen zu können (z. B. Accountinformationen geleakt, Zugriffe auf VPN-Services, Verlust von Daten, etc.).

Ransomware

Aufgrund des Homeoffice wurden Remote Access-Lösungen breitflächig ausgerollt. Damit steigt jedoch auch die Angriffsfläche für Ransomware-Attacken weiter an. Die fehlende Netzsegmentierung stellt in diesem Zusammenhang immer noch ein großes Problem dar. Ist ein Eintrittstor gefunden, verbreitet sich die Ransomware im Netz und über die Netzgrenzen hinaus und setzt sich an unterschiedlichen Stellen fest. Somit sind die Angreifer in der Lage, jederzeit über unterschiedliche Eintrittspunkte Zugriff auf die Systeme zu erhalten, Daten zu exfiltrieren oder auch zu verschlüsseln. Reaktionen auf derartige Angriffe treten oft vereinzelt auf, da aufgrund des hohen Drucks zur Reaktion kaum Zeit für tiefgreifende Analysen bleibt. Eine umfassende, unternehmensweit geltende Cyberstrategie in Zusammenwirken mit definierten und geübten Prozessen sowie einem hohen Awareness Level reduziert die Wahrscheinlichkeit erfolgreicher Angriffe bzw. deren Auswirkungen massiv. Zero-Trust-Umgebungen gewinnen in diesem Zusammenhang an Bedeutung.

Als größte Fehler beim Umgang mit Ransomware-Bedrohungen werden fehlende Backup- und Business-Continuity-Strategien bezeichnet.

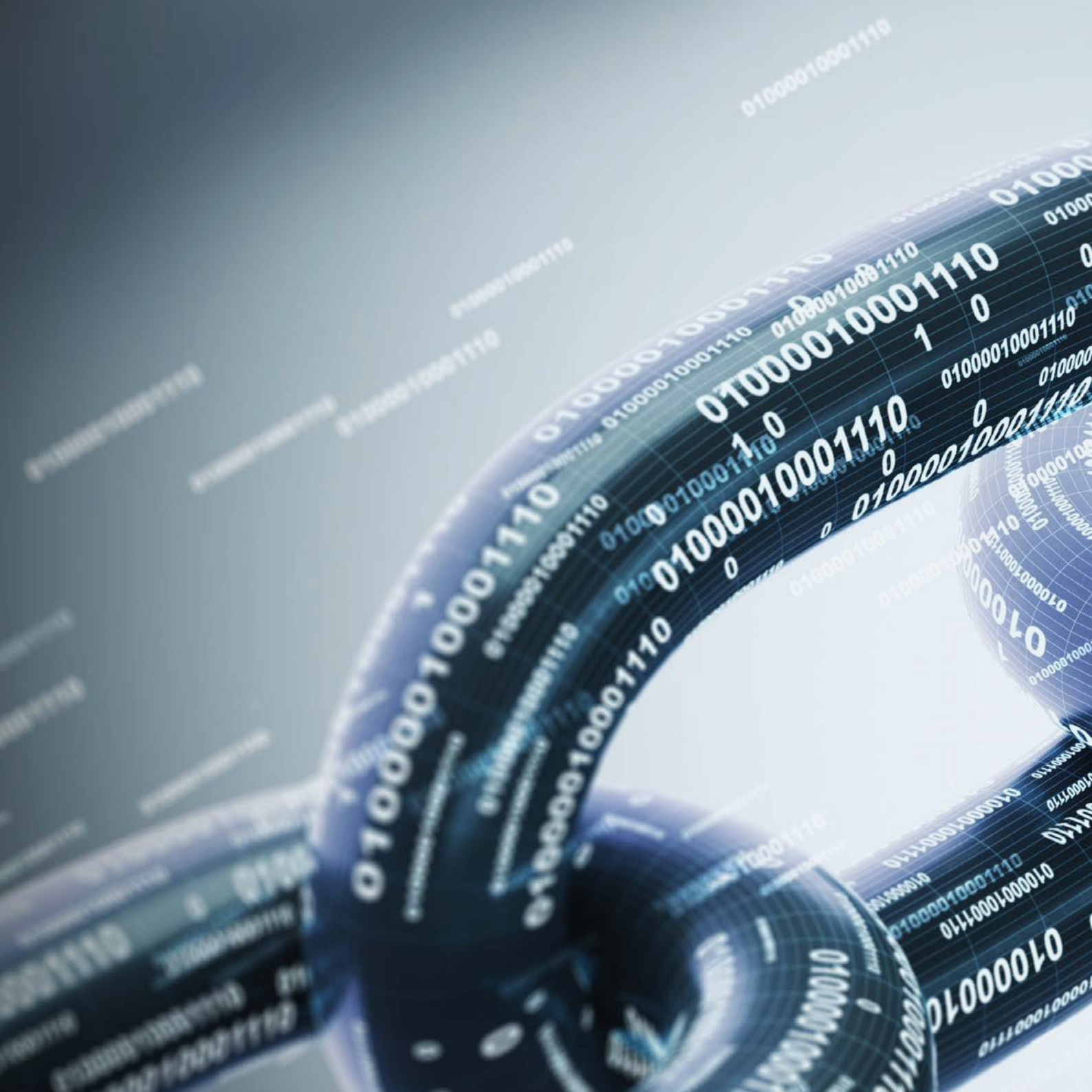
CEO-Fraud / Business E-Mail Compromise (BEC) / Fake Invoice / SCAM
Diese Angriffsvektoren werden immer perfider und gezielter und BEC erfolgt meist in Kombination mit anderen zeitgleich durchgeführten Angriffen. Die Awareness für diese Art der Bedrohung ist aber im Steigen begriffen.

Botnet/C2
Ohne laufendem Security Monitoring bleiben aktive Bots oft monatelang unentdeckt. Veraltete Betriebssysteme (Legacy Systeme) sind weiterhin im Einsatz und häufigstes Einfallstor für Bots und deren Betreiber.

Datendiebstahl
Datendiebstähle erfolgten im Berichtszeitraum häufig in Kombination mit Ransomware-Angriffen und sind eine permanente Bedrohung. Die Dunkelziffer muss als hoch angenommen werden.

Targeted Attack/APT
Die Anzahl registrierter gezielter Angriffe bei den befragten Unternehmen steigt, ist aber im Gesamtvolumen immer noch gering. 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 Webservice her möglich ist, können CDNs (Content Delivery Networks) vor DDoS-Angriffen schützen bzw. diese zumindest regional eindämmen.



1.3 Lage Cybercrime

1.3.1 Zuständige Ermittlungsbehörden

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 Cyber Crime Competence Center (C4) in der Abteilung 5 des Bundeskriminalamtes angesiedelt. In jeder der neun Landespolizeidirektionen sind spezialisierte Assistenzbereiche für den Cybercrime- und Forensikbereich 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.

1.3.2 Tätigkeiten

Im C4 des BMI werden laufend Maßnahmen gesetzt, um den europäischen und internationalen Austausch im Bereich der Bekämpfung von Cyberkriminalität zu intensivieren. Dies betrifft vornehmlich die Zusammenarbeit mit dem European Cybercrime Centre (EC3) von Europol sowie mit INTERPOL's Digital Crime Center (IDCC). Darüber hinaus erfolgt eine enge Kooperation im Rahmen der European Cybercrime Task Force (EUCTF), hier speziell bei den Operational Actions (OAs) aus den Operational Action Plans (OAPs) und den multinationalen Joint Investigation Teams (JIT), bei der European Cybercrime Training and Education Group (ECTEG), der European Multidisciplinary Platform Against Criminal Threats (EMPACT) sowie beim G7-24 / 7-Netzwerk.

Bekämpfung von Cyberkriminalität durch europäische und internationale Zusammenarbeit

Diese Kooperationen stärken die europäische und internationale Zusammenarbeit in vielen Bereichen, wie zum Beispiel die erfolgreiche Arbeit der ehemaligen SOKO Clavis. Internationale Cybercrime-Gruppierungen, Ermittlungen im Darknet und die Nachverfolgung von Kryptowährungen können nur im internationalen Verbund erfolgen.

Im Jänner 2020, noch vor Beginn der Pandemie, konnte in Wien eine große Kryprowährungskonferenz mit internationaler Beachtung ausgerichtet werden.

1.3.3 Phänomene im vergangenen Jahr

Zu Jahresbeginn 2020 stiegen die schadsoftwareunterstützten Angriffe auf Computersysteme und IKT-Netzwerke erneut an. Auch das bereits im Vorjahr aufgetauchte Phänomen von widerrechtlichen Zugriffen mittels alter, wiederverwendeter E-Mail-Adressen und Online-Accounts Sozialer Medien, sowie Zahlungs- und Webshopping-Dienstleistern, hielt weiter an.

Erpressungsversuche auf Unternehmen mittels pornografischer Darstellungen Minderjähriger in Verbindung mit Kontaktdaten und Lichtbildern der Erpressten läuteten das neue Jahr ein. Auch nahmen widerrechtliche Zugriffe auf Online-Accounts aufgrund von Datenleaks zu.

Die Phänomene Internetbetrug, insbesondere Delikte mit COVID-19-Bezug, Datenleaks und DDoS-Angriffe stellten im Beobachtungszeitraum die größten Herausforderungen im Bereich Cybercrime dar.

Internetbetrug

Generell musste über die letzten Jahre ein sehr starker Anstieg bei Anzeigen im Bereich von Internetbetrug und Erpressung über das Tatmedium Internet verzeichnet werden. Aufgrund zunehmender Arbeitsteilung (Crime-as-a-Service) und der Vernetzung der Tätergruppen vor allem im Ransomware-Bereich wird eine erfolgreiche Strafverfolgung zunehmend erschwert.

Stromkunden wurden Opfer von Fraud Calls, wobei seitens der Täter mit richtiger Nennung der IBAN, der Höhe der letzten Stromrechnung und weiteren wahrheitsgemäßen Details agiert wurde.

Mit Jahresmitte wurde ein Anstieg von CEO-Frauds beobachtet.

Der im Herbst erneut aufgetretene Cyber Trading Fraud/Investment Scam erzeugte finanzielle Schäden in Millionenhöhe. Erstkontakt erfolgte über Telefon, Online-Werbung, Social Media oder E-Mails – anschließend wurden die Opfer unter falscher Versprechung hoher Gewinne (unter anderem in den Bereichen Forex Trading, Handel mit binären Optionen oder bei Investitionen in Kryptowährungen) zu immer höheren Investments gedrängt.

Phishing-Attacken ein großer Angriffsvektor

Im Bereich Phishing E-Mails/-Websites ist für den Berichtszeitraum der Betrug mit FinanzOnline zu erwähnen: E-Mails mit der falschen Absendeadresse finanzOnline@bmf.gv.at versprachen Steuerrückerstattungen von über tausend Euro. Folgte man dem Link, gelangte man auf eine Phishing-Website, welche die Eingabe von persönlichen Informationen und Kreditkartendaten forderte.

Darüber hinaus waren alle größeren Bankinstitute in Österreich von Phishing der Zugangsdaten für eBanking betroffen. Unter anderem wurden mittels Android-Applikationen mobile TANs für das Online-Banking entwendet. Besonders im Rahmen der Anubis Android-Malware waren mehrere Phishing- und Malware-Verbreitungskampagnen im Umlauf. Nur wenn die Phishing-Seite per Android-Webbrowser besucht wurde, war zur Eingabe der Daten und zum Download einer „Sicherheits-App" aufgefordert worden.

Unabhängig von COVID-19 waren Trading-Fraud/Anlagebetrügereien in Verbindung mit Kryptowährungen zu verzeichnen, wobei weiterhin massiv mit hohen Investitionsgewinnen im Zusammenhang mit Kryptowährungen wie Bitcoins geworben wurde.

Im Spätsommer 2020 wurden auch SMS-Nachrichten vermehrt zum Daten-Phishing verwendet: Es kursierten mehrere Spam-Kampagnen, die einen Hinweis auf eine angebliche „Zustellbenachrichtigung" und weiterführende Links enthielten. Hierbei wurde zu Portonachzahlungen von 1,50 Euro aufgefordert, wobei wahres Ziel der Täterschaft das Phishing von Kreditkartendaten war.

In der Vorweihnachtszeit stieg auch wieder die saisonal beobachtbare Anzahl an kriminellen Webshops (Fake- und Phishing-Shops) deutlich an. Auch waren wieder zahlreiche Spamwellen mit Erpressermails (Sextortion) und E-Mails mit Phishing von Bankdaten im Umlauf.

Ebenso wurde ab Mitte November vielfach versucht, WhatsApp-Accounts von Usern zu stehlen, um damit weitere Betrugshandlungen durchzuführen.

Delikte mit Bezug zu COVID-19

Das erste Quartal des Vorjahres war von der Pandemie geprägt: Nach Neuregistrierung mehrerer tausender Domains wurde im Zusammenhang mit COVID-19 eine starke Zunahme betrügerischer Websites mit dem Ziel Phishing bzw. der Verbreitung von Schadsoftware beobachtet.

In Erpressermails forderten die Absender von ihren Opfern die Zahlung eines Geldbetrages von 4.000 USD in Form von Bitcoins, widrigenfalls deren Familien mit dem Coronavirus infiziert werden würden.

Mittels Malspam/Phishing/Ransomware wurde im Namen von Paket-Zustelldiensten versucht, Opfer zum Öffnen von mit Malware hinterlegten Links zu bewegen. Hierbei wurde auf veränderte Zustellzeiten aufgrund von Corona verwiesen. Durch Öffnen des Links bzw. Dateianhangs wurde die Schadsoftware (unter anderem AZORult, Emotet, Nanocore RAT, Trick-Bot) am Zielcomputer installiert.

Vermutlich in direktem Zusammenhang mit den Ausgangsbeschränkungen stehend, erfolgte eine massive Abnahme angezeigter Delikte. Die absoluten Zahlen dürften jedoch nicht die Realität widerspiegeln.

Generell erfuhr der Bereich Cybercrime durch das allgemeine Social Distancing einen Anstieg von Scam/Lovescam/Stranded Travellers.

Sowohl in Fakeshops als auch über legitime Plattformen wurde ein Cybercrime-Anstieg im Zusammenhang mit dem Verkauf von Desinfektionsmitteln und Atemschutzmasken festgestellt.

Datenleaks

Mitte des Jahres fand eine Verschiebung von Ransomware-Angriffen hin zu Datenleaks mit Lösegelderpressung statt.

DDoS-Angriffe im Banken- und Finanzsektor

Die Anzahl von Einbrüchen in Computernetzwerke von Unternehmen nahm zu. Unbekannte Täter extrahierten vermehrt Unternehmensdaten und erpressten Lösegeld. Im Fall von Nichtzahlung wurden Daten über entsprechende Websites veröffentlicht. Durch die Häufung verschiedener Datenleaks erhöhte sich auch die Anzahl der Anzeigen zu widerrechtlichen Zugriffen auf Benutzerkonten bei Online Service Providern (OSP). Die Zugangsdaten wurden von den Tätern meist in betrügerischer Absicht verwendet. Die entwendeten Daten lösen oftmals auch Jahre später Folgekriminalität aus.

DDoS-Angriffe

National wie international wurden ab Herbst mehrere Wellen von DDoS-Angriffen vor allem im Banken- und Finanzsektor und auf ISPs gemeldet. In einigen Fällen handelt es sich um Trittbrettfahrer, die in den Erpresserschreiben Namen bekannter Tätergruppen (unter anderem Fancy Bear, Lazarus) verwendeten. Beobachtet wurden dort bis zu 100 GBit/s. Den Erpresserschreiben folgten in seltenen Fällen Folgeangriffe, die aber dann tatsächlich mit noch deutlich höheren Bandbreiten waren.

1.4 Cyberlage Landesverteidigung

Die Ereignisse im Jahr 2020 haben gezeigt, dass neben der COVID-19-Pandemie Terrorismus und Cyberangriffe ein zunehmendes Risiko für Österreichs Sicherheit und Souveränität darstellen. Diese Cyberangriffe betrafen potentiell sowohl Privatpersonen, kleine und mittlere Unternehmen, aber auch große und namhafte Betriebe. Nicht zuletzt waren auch Einrichtungen der öffentlichen Verwaltung betroffen. Eine der Kernaufgaben des Österreichischen Bundesheeres (ÖBH) ist die Sicherheit und Souveränität Österreichs auch in Krisensituationen aufrechtzuerhalten und sich entsprechend vorzubereiten, um den verfassungsmäßigen Auftrag erfüllen zu können.

Terrorismus und Cyberangriffe ein zunehmendes Sicherheitsrisiko

Daher legt das BMLV/ÖBH auch einen immer größer werdenden Fokus auf die militärische Landesverteidigung im Cyberraum. Dies umfasst sowohl Maßnahmen der Informations- und Kommunikationstechnologie-Sicherheit (IKT), als auch alle Maßnahmen zur Abwehr von Cyberangriffen auf die militärischen IKT-Systeme. Im Cyberverteidigungsfall wird auch die kritische Infrastruktur Österreichs unterstützt. Das BMLV/ÖBH ist aufgrund seiner Bedeutung nicht nur für Kriminelle oder sogenannte „Script Kiddies“ ein lohnendes Ziel, sondern vor allem auch für staatliche Akteure. Da solche Angriffe jederzeit und ohne Vorwarnzeit durchgeführt werden können, hat die Vorbereitung auf Einsätze auch im Cyberraum einen hohen Stellenwert. Der Einsatz von gut ausgebildeten Expertinnen und Experten zum Schutz von IKT-Systemen ist daher unverzichtbar.

Dies konnte das BMLV/ÖBH zu Beginn des Jahres bei der Bekämpfung des Cyberangriffes auf das BMEIA beweisen. Im Zuge des Assistenzeinsatzes leistete das BMLV durch das Bereitstellen von Cyberexpertinnen und -experten sowohl aus dem IKT und Cybersicherheitszentrum (IKT&CySihZ), dem Abwehramt (AbwA) als auch dem Heeres-Nachrichtenamt (HNaA) einen wesentlichen Beitrag zur erfolgreichen, gesamtstaatlichen Behandlung des Vorfalles.

2020 war vor allem durch die COVID-19-Pandemie geprägt, was sich auch massiv auf das BMLV/ÖBH ausgewirkt hat. Das BMLV/ÖBH konnte neben der logistischen und personellen Unterstützung der Test- und Impfstraßen diesen auch technische Unterstützung – durch Hard- und Software sowie durch technische Expertinnen und Experten – anbieten.

Da während der Pandemie verstärkt Homeoffice eingesetzt wurde, mussten die eigenen Lösungen für den sicheren Homeoffice-Zugang erweitert werden. Dies zeigte, dass das BMLV/ÖBH auch in Krisensituationen in der Lage ist, sich aktuellen Herausforderungen anzupassen.

Ein weiterer gefährlicher Trend, der vor allem 2020 immer präsenter wurde, ist die gezielte Beeinflussung der Öffentlichkeit durch Desinformationskampagnen. Diesen Trend konnte man im Vorfeld von Präsidentschaftswahlen oder öffentlichkeitswirksamen nationalen und internationalen Verhandlungen beobachten, aber auch im Zusammenhang mit nahezu jedem medienwirksamen Thema wie COVID-19. Das BMLV/ÖBH führt intensive nationale und internationale Medienbeobachtungen durch, um Spannungen in der Gesellschaft zu erkennen und in das nationale Lagebild einfließen zu lassen.

Auch wenn die Pandemie viele Neuerungen gebracht hat, blieben die Trends der Angriffe auf die IKT-Infrastruktur des BMLV im Großen und Ganzen im Vergleich zu den Vorjahren gleich. Auch heuer konnte wieder ein wachsender Anstieg an versuchten unauthorisierten Zugriffen beobachtet werden, welche aber durch die etablierten Sicherheitsmaßnahmen präventiv blockiert wurden. Zusätzlich zum üblichen „Grundrauschen“ aus automatisierten Angriffen und Scans, wurden auch zunehmend manuelle oder kombinierte Angriffe festgestellt. Neben einer Vielzahl an versuchten DDoS- und Bruteforce-Angriffen konnten durch die BMLV/ÖBH-Cyberexperten auch wieder gehäuft gezielte Phishing-Angriffe gegen Mitarbeiterinnen und Mitarbeiter des BMLV/ÖBH entdeckt und verhindert werden. Eine stetig wachsende Gefahr stellt auch die sogenannte Ransomware dar, bei welcher Daten auf Computern verschlüsselt werden. Sollte der Lösegeldforderung nicht nachgekommen werden, wird mit Veröffentlichung sensibler Inhalte gedroht. Diese Be-

obachtungen sind jedoch nicht nur auf das BMLV/ÖBH beschränkt. Diverse Studien und Untersuchungen zur Entwicklung des möglichen Schadens von Cyberangriffen zeigen, dass diese weltweit weiterhin stetig steigen und ein immer größeres Risiko darstellen. Die monetären Auswirkungen unterscheiden sich je nach Studie und nehmen Schadensausmaße im Höhe von Billionen von US-Dollar an.

Was nahezu alle Studien verbindet ist die Aussage, dass Cybercrime und Spionage deutlichen Zuwachs erhalten. Daher ist es für das BMLV/ÖBH unumgänglich, die nötigen Kompetenzen zur Abwehr dieser Gefahren auf die ressorteigenen Systeme zu vertiefen und zu erweitern. International haben in den letzten Jahren viele Länder damit begonnen, staatliche, militärische und zivile Cybersicherheitskompetenzen aufzubauen. So hat beispielsweise Großbritannien bekanntgegeben, dass für den Bereich der Cyberdomäne ein 250 Personen starkes Cyberregiment, mit dem Ziel der Cyber- und Informationskriegsführung, aufgestellt wird.

Des Weiteren ist international auch ein starker Trend zur KI zu beobachten, wodurch sich immer mehr Nationen im (sowohl defensiven als auch offensiven) Cybersicherheitsbereich sowie in der hybriden Kriegsführung weiterentwickeln. Diese Fähigkeiten wurden auch gegen andere Nationen oder Unternehmen bereits mehrfach eingesetzt. Ein Beispiel hierfür ist der andauernde Konflikt zwischen Israel und dem Iran, welcher sich auch immer mehr im Cyberraum auswirkt. So versuchten vermeintlich iranische Hacker im Frühjahr 2020 Teile der israelischen Wasserversorgung zu manipulieren, woraufhin wiederum vermeintliche israelische Angreifer einen iranischen Hafen für Tage lahmlegten. Keiner der Akteure bestätigte die Handlungen, jedoch zeigt dieses Beispiel anschaulich, welche Ausmaße gezielte staatliche Cyberangriffe annehmen können. Das BMLV/ÖBH ist daher bemüht, die gesamtstaatliche Sicherheit zu erhöhen und zu unterstützen.

2 Internationale Entwicklungen

Im Allgemeinen setzt sich Österreich auf internationaler Ebene für ein freies, offenes und sicheres Internet ein, wobei die Ausübung aller Menschenrechte auch im virtuellen Raum gewährleistet werden muss. Dabei muss auf ein angemessenes Gleichgewicht zwischen den Interessen der Strafverfolgung und der Achtung grundlegender Menschenrechte, wie dem Recht auf freie Meinungsäußerung und Informationsfreiheit sowie dem Recht auf Privatleben und Privatsphäre geachtet werden.

2.1 Europäische Union (EU)

Die zunehmende Bedeutung der Cybersicherheit zeigte sich auch im Jahr 2020 in der Behandlung dieses Themas in zahlreichen internationalen Organisationen und multilateralen Foren, wo es teilweise sehr kontroversiell diskutiert wurde.

Außen- und sicherheitspolitische Maßnahmen werden vom BMEIA koordiniert, dem BKA obliegt die Koordination der Cybersicherheit im Zusammenhang mit der EU.

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 Cyberraum, 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.

Schwerpunkte der HWP Cyber waren das Europäische Kompetenzzentrum für Cybersicherheit und die Schlussfolgerungen des Rates zur Cybersicherheit vernetzter Geräte

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.

Die HWP Cyber fand im Jahr 2020 zu insgesamt 40 Sitzungen zusammen. Der Schwerpunkt der Arbeit lag, wie schon im Jahr 2019, auf den Verhandlungen zum EU-Verordnungsvorschlag zur Einrichtung des Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung und des Netzes nationaler Koordinierungszentren. Der kroatischen Präsidentschaft gelang es dabei im Juni 2020 ein neues Mandat zu erreichen, in dessen Folge die Trilogverhandlungen mit dem Europäischen Parlament (EP) wiederaufgenommen werden konnten. Unter dem deutschen Vorsitz wurde im

Dezember 2020 schlussendlich eine informelle Vereinbarung mit dem EP erreicht. Zum näheren Inhalt des Verordnungsvorschlags siehe Kapitel 2.1.9.

Der Schwerpunkt der Arbeit im Bereich der Cyberdiplomatie war 2020 die strukturierte Umsetzung der Cyber Diplomacy Toolbox (Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten). So fand 2020 das Cybersanktionenregime mit Kontoeinfrierungen und Reisebeschränkungen erstmalig Anwendung (siehe Kapitel 2.1.8).

Die HWP Cyber bereitete die „Schlussfolgerungen des Rates zur Cybersicherheit vernetzter Geräte" vor, welche vom Rat am 2. Dezember 2020 gebilligt wurden. Durch das „Internet of Things (IoT)", also die Vernetzung verschiedenster Konsumgüter als auch industrieller Geräte mit dem Internet, entstehen neue Risiken für die Privatsphäre sowie die Informations- und Cybersicherheit. Die Schlussfolgerungen zielen darauf ab, durch höchste Standards bei Abwehrfähigkeit und Sicherheit, nicht nur das Schutzniveau, sondern auch die Wettbewerbsfähigkeit der europäischen IoT-Industrie zu erhöhen. Es ist zu erwarten, dass in weiterer Folge hierzu horizontale Rechtsvorschriften entwickelt werden.

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 Vertretern der Mitgliedstaaten, der EK und der ENISA zusammen. Der Vorsitz wird von der jeweiligen Ratspräsidentschaft gehalten.

Die NIS-Kooperationsgruppe nimmt ihre Aktivitäten auf der Grundlage von zweijährigen Arbeitsprogrammen wahr. Während das erste Arbeitsprogramm für den Zeitraum 2018 bis 2020 ein erster Schritt war, um die Arbeitsmethoden der NIS-Kooperationsgruppe zu gestalten, Vertrauen zwischen den Mitgliedstaaten aufzubauen und die dringendsten

Ergebnisse im Zusammenhang mit der Umsetzung der NIS-Richtlinie zu erarbeiten, hat sich die NIS-Kooperationsgruppe in der Zwischenzeit als wichtiges Forum und Bezugspunkt für die Diskussion über Cybersicherheitspolicies innerhalb der EU etabliert. Das neue Arbeitsprogramm für den Zeitraum 2020 bis 2022 beauftragt eine Bestandsaufnahme der bisher erbrachten Leistungen, eine Bewertung, deren Auswirkungen und die Identifikation von Verbesserungspotentialen. Ziel ist es, der NIS-Kooperationsgruppe die Umsetzung der NIS-Richtlinie weiterhin zu erleichtern, den Informationsaustausch weiter zu operationalisieren sowie eine strategische Diskussion über wichtige politische Dokumente für die Cybersicherheit in der EU, wie zum Beispiel in Bezug auf 5G, KI oder IoT, zu ermöglichen.

Die NIS-Kooperationsgruppe traf sich im Jahr 2020 zu fünf Plenarsitzungen und 33 Sitzungen im Rahmen ihrer Arbeitsbereiche („Work Stream Meetings“).

Auch im Jahr 2020 wurden neue Referenzdokumente von der NIS-Kooperationsgruppe erarbeitet und veröffentlicht. Einen Schwerpunkt bildete die Arbeit zum Thema der Cybersicherheit von 5G-Netzen. Bei den veröffentlichten Referenzdokumenten handelt es sich konkret um:

- CG Publication 01/2020 – Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures;
- CG Publication 02/2020 – Report on Member States' progress in implementing the EU Toolbox on 5G Cybersecurity;
- CG Publication 03/2020 – Annual Report NIS Directive Incidents 2019;
- CG Publication 04/2020 – Synergies in Cybersecurity Incident Reporting.

2.1.3 Horizontal Working Party on Enhancing Resilience and Countering HybridThreats

Die Horizontale Arbeitsgruppe zur Stärkung der Resilienz und zur Abwehr hybrider Bedrohungen (HWP ERCHT) ist im Jahr 2019 aus der „Friends of Presidency Group" entstanden. Ihr Ziel ist es, einen Überblick über Fragen im Zusammenhang mit hybriden Bedrohungen zu bieten, um die Kohärenz und die Zusammenarbeit zwischen der EU und ihren Mitgliedstaaten zu unterstützen. Der Fokus der Arbeit liegt auf der Abwehr von hybriden Bedrohungen, der Stärkung der Resilienz von Staaten und der Gesellschaft gegenüber solchen Bedrohungen, der Verbesserung der strategischen Kommunikation und der Bekämpfung von Desinformation.

Am 15. Dezember 2020 nahm der Rat die „Schlussfolgerungen zur Stärkung der Resilienz und zur Abwehr hybrider Bedrohungen, einschließlich der Desinformation, im Zusammenhang mit der COVID-19-Pandemie", an. In diesen, von der HWP ERCHT vorbereiteten, Schlussfolgerungen stellt der Rat fest, dass böswillige Cyberaktivitäten häufig ein Schlüsselelement hybrider Bedrohungen darstellen. Er erkennt an, dass die kontinuierliche Anwendung des Instrumentariums der EU für die Cyberdiplomatie ein wichtiger Schritt ist, um böswilligen Cyberaktivitäten vorzubeugen, sie zu verhindern, von ihnen abzuschrecken und auf sie zu reagieren. Dies trifft gleichermaßen auf hybride Kampagnen zu.

Neues Cybersicherheitspaket soll die Cybersicherheitsstrategie 2013 ablösen

2.1.4 Cybersicherheitsstrategie der EU für die digitale Dekade

Am 16. Dezember 2020 stellte die EK ein neues Cybersicherheitspaket vor, zu dessen Inhalt unter anderem eine neue EU-Cybersicherheitsstrategie zählt. Diese wurde in Form einer gemeinsamen Mitteilung der EK und des Hohen Vertreters der EU veröffentlicht und soll die Cybersicherheitsstrategie 2013 mit einem neuen strategischen Referenzrahmen für Cybersicherheit auf EU-Ebene ablösen.[1]

1 JOIN(2020) 18 final.

Die gemeinsame Mitteilung zielt darauf ab, das digitale Leben der Menschen in Europa sicher zu gestalten. Sichere und vertrauenswürdige digitale Instrumente sind für Wirtschaft, Demokratie und Gesellschaft gleichermaßen wichtig. Daher wurden folgende Vorschläge erarbeitet:

- Steigerung der Resilienz von kritischer Infrastruktur und vernetzten Dingen;
- Aus- und Aufbau von operativen Kapazitäten zur Vorbeugung, Abschreckung und Reaktion auf Cyberangriffe;
- Zusammenarbeit mit internationalen Partnern für einen globalen, offenen, stabilen und sicheren Cyberraum, in welchem Völkerrecht, Menschenrechte, Grundfreiheiten und demokratische Werte gelten.

Folgende in diesem Zusammenhang stehende Initiativen wurden im Jahr 2020 insbesondere verfolgt:

- NIS: Beginn der Überarbeitung der NIS-Richtlinie auf Grundlage des Vorschlages der EK vom 16. Dezember 2020. Die neue NIS-Richtlinie (NIS 2) hat das Ziel, ein hohes gemeinsames Niveau von Cybersicherheit in der EU zu erreichen. Zum näheren Inhalt siehe Kapitel 2.1.5.
- IoT: Aufbauend auf den Ratschlussfolgerungen zur Cybersicherheit von vernetzen Geräten vom 2. Dezember 2020 stellt die EK die Vorlage eines Rechtsaktes Ende 2021 in Aussicht. Damit soll ein verbindliches Mindestniveau an IT-Sicherheit für Geräte, die mit dem Internet verbunden sind, erzielt werden.
- 5G: Die Finalisierung der Umsetzung der 5G-Toolbox soll bis zum 2. Quartal 2021 erreicht werden. Im Anhang der gemeinsamen Mitteilung sind darüber hinaus noch Maßnahmen und Ziele angeführt, wie insbesondere die Sicherstellung konvergenter nationaler Ansätze zur effektiven Risikominderung in der EU, die Unterstützung des kontinuierlichen Wissensaustauschs und Kapazitätsaufbaus sowie die Förderung der Widerstandsfähigkeit der Lieferkette und anderer strategischer Sicherheitsziele der EU.

- Cybersicherheit der EU-Institutionen: Erarbeitung der Vorlage einer Verordnung für Informationssicherheit sowie einer Verordnung für gemeinsame Cybersicherheitsregeln für Institutionen, Einrichtungen und Agenturen der EU.

Die EK und der Hohe Vertreter sind entschlossen, die neue Cybersicherheitsstrategie in den kommenden Monaten des Jahres 2021 umzusetzen. Es obliegt nun dem EP und dem Rat, die vorgeschlagene NIS-2-Richtlinie sowie die ebenfalls am 16. Dezember 2020 im Rahmen des neuen Cybersicherheitspakets vorgeschlagene Richtlinie über die Widerstandsfähigkeit kritischer Einrichtungen zu prüfen und anzunehmen. Sobald die Vorschläge angenommen und verabschiedet sind, müssen die Mitgliedstaaten sie innerhalb von 18 Monaten nach ihrem Inkrafttreten umsetzen.

2.1.5 NIS-2-Richtlinie

NIS 2 soll das Cybersicherheitsniveau in der EU weiter erhöhen

Am 16. Dezember 2020 wurde das Cybersicherheitspaket durch die EK vorgestellt. Neben einer neuen EU-Cybersicherheitsstrategie beinhaltet dieses unter anderem auch den Vorschlag einer neuen Richtlinie über Maßnahmen für ein hohes gemeinsames Maß an Cybersicherheit in der gesamten Union (NIS-2-Richtlinie, kurz „NIS 2“). NIS 2 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:

- 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): NIS 2 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.

NIS 2 wird im EP im Ausschuss für Industrie, Forschung und Energie (ITRE) sowie im Rat der EU in der Horizontal Working Party on Cyber Issues (s. Kapitel 2.1.1) behandelt. Es ist vorgesehen, dass sie innerhalb von 18 Monaten nach dem Tag ihres Inkrafttretens in nationales Recht umzusetzen ist.

2.1.6 EU-Zertifizierungsrahmen für die Cybersicherheit (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. Anbieter und Hersteller 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 eine 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“ (englisch European Cybersecurity Certification Group [ECCG]) wurde durch den Cybersecurity Act eingesetzt und nahm ihre Arbeit im Jahr 2019 auf. Die ECCG setzt sich aus Vertreterinnen und Vertretern der nationalen Behörden für die Cybersicherheitszertifizierung oder Vertreterinnen und Vertretern anderer einschlägiger nationaler Behörden zusammen. Österreich wird in der ECCG durch den CIO des Bundes (Bundesministerium für Digitalisierung und Wirtschaftsstandort [BMDW]) und das strategische NIS-Büro (BKA) vertreten. Die ECCG traf sich im Jahr 2020 zu sechs Plenarsitzungen und mindestens vier weiteren Sitzungen von Untergruppen.

Im Jahr 2020 konnte nunmehr auch die Gruppe der Interessensträger für die Cybersicherheitszertifizierung (Stakeholders Cybersecurity Certification Group [SCCG]) eingesetzt werden. Diese unter dem gemeinsamen Vorsitz der EK und der ENISA stehende Gruppe setzt sich aus Vertreterinnen und Vertretern aus akademischen Einrichtungen, Verbraucherschutzorganisationen, Konformitätsbewertungsstellen, Organisationen, die Normen entwickeln, Unternehmen, Handelsverbänden und anderen zusammen. Die SCCG soll in strategischen Fragen der Cybersicherheitszertifizierung beraten.

EUCC soll die Sicherheit von Cloud-Diensten regeln

Bereits im Jahr 2019 beautragte die EK die ENISA mit der Ausarbeitung eines ersten möglichen Schemas für die Cybersicherheitszertifizierung. Dieses trägt den Namen European Union Common Criteria Scheme (EUCC) und soll der Nachfolger des bestehenden SOG-IS (Senior Officials Group Information Systems Security) und MRA (Mutual Recognition Agreement) werden. Unter dem EUCC wird eine Zertifizierung der Cybersicherheit von IKT-Produkten vorgesehen. Das EUCC basiert auf Common Criteria, Common Methodology for Information Technology Security Evaluation und den entsprechenden Normen ISO/IEC 15408 und ISO/IEC 18045. Ein wichtiger Meilenstein in der Entwicklung des europäischen Cybersicherheitszertifizierungsrahmens konnte mit der öffentlichen Konsultierung des Entwurfs für das EUCC, die im Juli 2020 stattgefunden hat, erreicht werden.

Nach dem EUCC wurde die ENISA von der EK am 21. November 2019 zur Vorbereitung eines weiteren Schemas für die Cybersicherheitszertifizierung beauftragt. Dieses trägt den Namen European Union Cybersecurity Certification Scheme on Cloud Services (EUCS) und soll die Sicherheit von Cloud-Diensten regeln. Ziel ist es, die Sicherheit von Cloud-Diensten mit EU-Vorschriften, internationalen Standards, bewährten Praktiken der Industrie sowie mit bestehenden Zertifizierungen in EU-Mitgliedstaaten zu harmonisieren und das Vertrauen in Cloud-Dienste zu stärken. Auch hier konnte ein Meilenstein erzielt werden, als der Entwurf für das EUCS im Dezember 2020 zur öffentlichen Begutachtung gestellt wurde. Dieser sieht ein horizontales und technologisches Programm vor, das die Cybersicherheit in der gesamten Cloud-Lieferkette gewährleisten und eine solide

Grundlage für sektorale Programme bilden soll. Es soll auf alle Arten von Cloud-Diensten (von Infrastruktur bis Anwendungen) anwendbar sein und Transparenzanforderungen, wie den Ort der Datenverarbeitung und -speicherung, beinhalten.

2.1.7 Cybersicherheit von 5G-Netzen

Die Sicherheit der 5G-Technologie, auch „fünfte Generation des Mobilfunknetzes“ (5G) genannt, stand auch in diesem Jahr im Fokus der Aufmerksamkeit von Cybersicherheitsbehörden.

Nach den Vorarbeiten im Jahr 2019 (Erstellung einer nationalen Risikoanalyse, Überprüfung der national gesetzten Maßnahmen bis hin zur EU-weit koordinierten Risikoanalyse) wurden die Arbeiten an und rund um das Thema Cybersicherheit von 5G-Netzen gleich zu Beginn 2020 fortgeführt.

So wurde am 29. Jänner 2020 die „Cybersecurity of 5G networks EU Toolbox of risk mitigating measures“, im Folgenden „Toolbox“, vorgestellt. Diese definiert und schlägt „risks“ (wurden 2019 mit der EU-weiten Risikoanalyse identifiziert), „mitigating measures“ (diese unterteilt in „strategic measures“ und „technical measures“) und „supporting actions“ vor, die den Mitgliedstaaten zur Verfügung stehen, um ihre Netze sicherer zu gestalten.

Zusätzlich wurde den Mitgliedstaaten bis zum 15. Mai 2020 eingeräumt, die Vorschläge aus der Toolbox nationalstaatlich umzusetzen.

Die entsprechende Verordnung der Rundfunk und Telekom Regulierungs-GmbH (RTR), nämlich die „Telekom-Netzsicherheitsverordnung 2020 (TK-NSiV 2020)“, trat nach einer Begutachtungsfrist am 4. Juli 2020 in Kraft. Mit dieser Verordnung werden sämtliche technischen Maßnahmen der Toolbox umgesetzt.

Am 24. Juli 2020 erschien der „Report on Member States' progress in implementing the EU Toolbox on 5G Cybersecurity", eine Bestandsaufnahme, wie weit die Mitgliedstaaten bei der Umsetzung der 5G-Toolbox sind und welche Problemfelder sichtbar wurden. In diesem Report finden sich vier österreichische Umsetzungsbeispiele aus der oben angeführten TK-NSiV der RTR.

Aus dem Work Stream der NIS-Kooperationsgruppe „on the 5G Cyber Security Recommandation" bildete sich 2020 ein Sub-Work-Stream. Die Vorbereitungen dafür starteten zwar schon 2019, das erste Treffen fand aber erst am 25. Mai 2020 statt. Die Sub-Arbeitsgruppe „SubGroup on 5G standardisation and certification policy" arbeitete zu Beginn daran, die bestehenden Standards zu sammeln und zu kategorisieren, um dann in weiterer Folge ein Zertifizierungsschema nach dem Cyber Security Act zu erarbeiten. In dieser Arbeitsgruppe gab es 2020 vier virtuelle Treffen.

Umsetzungen der 5G-Toolbox bis zum zweiten Quartal 2021

Abgesehen von den Tätigkeiten im Rahmen der NIS-Kooperationsgruppe fand am 23. und 24. September 2020 die zweite „Prague 5G Security Conference" virtuell statt. Dort wurde das „Prague Repository" vorgestellt, eine Datenbank, in der nationale „Best Practices" und die netzsicherheitsspezifische Legislatur der teilnehmenden Staaten gesammelt wird.

Ende November wurden die diesjährigen Arbeiten zur Aktualisierung der nationalen Risikoanalyse des Telekomsektors abgeschlossen. Die Aktualisierung erfolgte im PPP-Rahmen in mehreren, durch die RTR vorrangig virtuell veranstalteten, Sitzungen.

Wie oben angeführt, stellt 5G auch in der „Cybersicherheitsstrategie der EU für die digitale Dekade", die am 16. Dezember 2020 vorgestellt wurde, ein Arbeits- und Vorhabensprojekt dar. Unter anderem sollen die nationalen Umsetzungen der 5G-Toolbox bis zum zweiten Quartal 2021 abgeschlossen werden. Weiters wurden zusätzliche Ziele und Maßnahmen angeführt, deren Erreichung oder Umsetzung die Mitgliedstaaten 2021 nachhaltig beschäftigen werden.

2.1.8 Cyberdiplomatie

Bei der Cyber Diplomacy Toolbox (Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten) wurden im Jahr 2020 wichtige Umsetzungsschritte unternommen. Im Mai 2019 hatte der Rat ein Cybersanktionenregime angenommen, mit dem gegen Einzelpersonen und Entitäten (nicht Staaten) mit Kontoeinfrierungen und Reisebeschränkungen vorgegangen werden kann. Im Jahr 2020 erfolgte erstmalig eine konkrete Listung von acht Personen und vier Entitäten. Eine konkrete Attribution ist nicht für alle in der Cyber Diplomacy Toolbox enthaltenen Maßnahmen Voraussetzung. Ein Teil der Maßnahmen, mit denen die EU auf Cyberangriffe reagieren kann, ist öffentlich, z. B. Ratsschlussfolgerungen oder Erklärungen. So wurden im Februar 2020 eine EU-Erklärung zu schwerwiegenden Cyberangriffen auf wichtige Infrastruktur in Georgien veröffentlicht und im April 2020 zu Cyberangriffen, welche die COVID-19-Pandemie ausnützen.

Cyber Diplomacy Toolbox – wichtige Umsetzungsschritte im Jahr 2020

Ein wichtiger Teil der Cyberdiplomatie auf EU-Ebene umfasst die Erarbeitung gemeinsamer Positionen und Strategien zu Cyberthemen auf internationaler Ebene. Hier vor allem in Zusammenarbeit mit den Vereinten Nationen (VN), wo seit 2019 zwei Normensetzungsprozesse im Bereich internationale Sicherheit laufen und 2020 die Vorbereitungen zu einer VN-Cybercrime-Konvention begonnen haben (siehe Kapitel 2.2 zu den Vereinten Nationen). Die neue EU-Cybersicherheitsstrategie vom 16. Dezember 2020 steht ganz im Zeichen der digitalen Souveränität, welche auch als Ziel im EK-Arbeitsprogramm verankert ist. Mit der geopolitischen Ausrichtung von EK und EAD wird erstmals der Cyberdiplomatie eine Schlüsselrolle zugeschrieben, denn Normensetzung im Cyberraum und für neue Technologien sind längst geopolitische Konfliktzonen. Die 2020 exponentiell angestiegenen Angriffe auf europäische Einrichtungen durch staatlich gelenkte Akteure verstärken diese Polarisierung. Mit dem Anspruch einer EU-Führungsrolle auf internationaler und regionaler Ebene soll die EU-Vision für das globale und offene Internet verankert und dabei sichergestellt werden, dass neue Technologien auf Menschen und den Schutz ihrer Privatsphäre fokussieren und ihr Einsatz rechtmäßig und ethisch erfolgt.

2.1.9 Netz nationaler Koordinierungszentren und Europäisches Kompetenzzentrum

Die EK legte am 12. September 2018 den Entwurf für eine Verordnung zur Einrichtung eines Europäischen Kompetenzzentrums für Cybersicherheit, die Errichtung eines Netzes nationaler Koordinierungszentren sowie der Einrichtung einer Kompetenzgemeinschaft für Cybersicherheit[2] vor. Der Vorschlag erging als eine konkrete Maßnahme zur Umsetzung der gemeinsamen Mitteilung der EK und der Hohen Vertreterin vom September 2017 über „Maßnahmen zur Erhöhung der Abwehrfähigkeit, der Abschreckung und der Abwehr gegen Cyberattacken und zur wirksamen Erhöhung der Cybersicherheit in der EU".

Das Netz nationaler Koordinierungszentren sowie das Europäische Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung unterstützen bereits bestehende EU-Initiativen und sollen neue europäische Kapazitäten im Cyberbereich aufbauen.

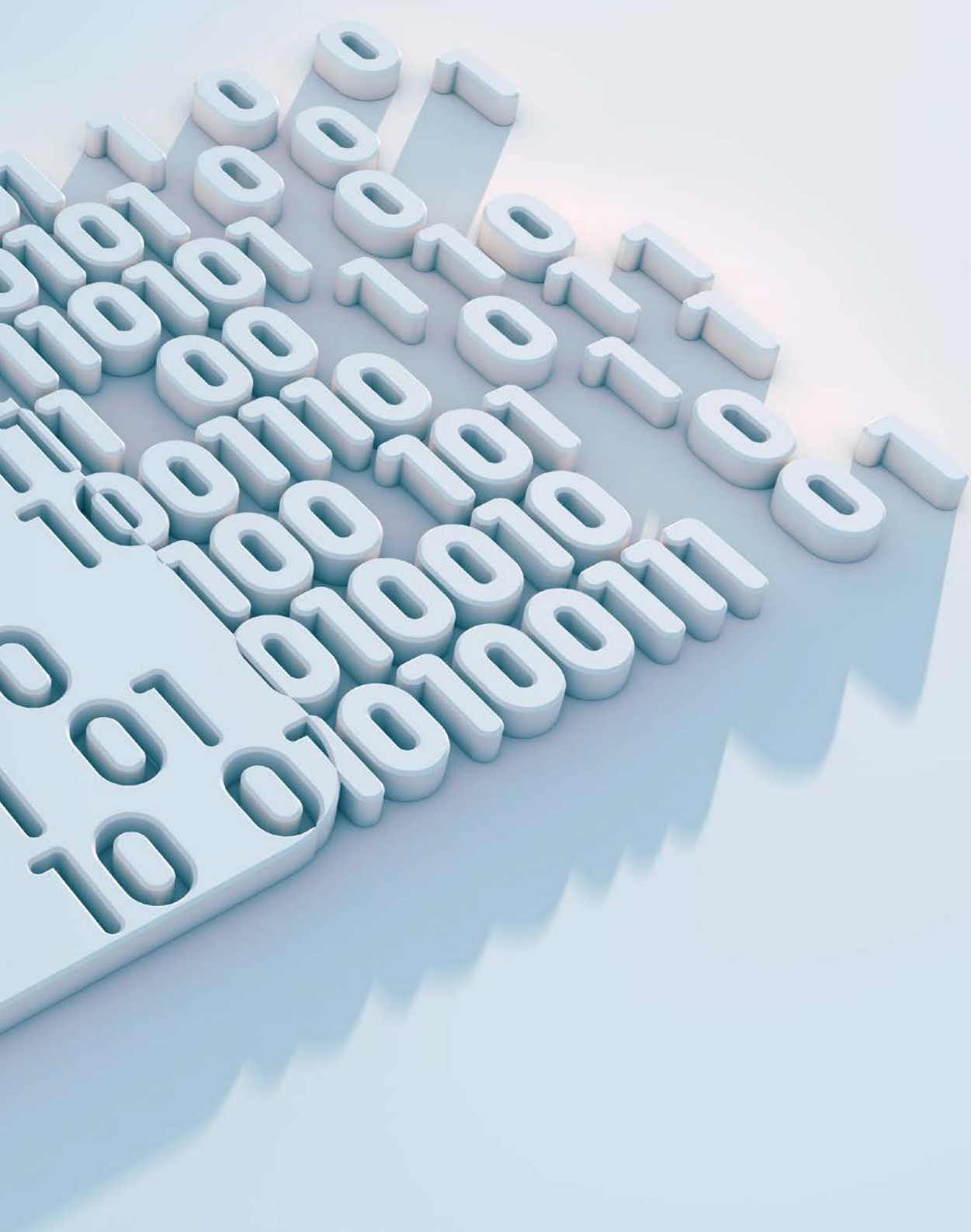
Mit einem Europäischen Kompetenzzentrum soll die Verwendung der Mittel, die für Cybersicherheit für die Jahre 2021–2027 bestimmt wurden, aus den Programmen „Digitales Europa" und „Horizont Europa" koordiniert werden. Das Zentrum wird das Netz nationaler Koordinierungszentren und die Kompetenzgemeinschaft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

2 COM (2018) 630

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

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

Zum Verhandlungsstand siehe Kapitel 2.1.1.



2.2 Vereinte Nationen (VN)

Cybersicherheit wurde im Zuge des 1. Komitees (Abrüstung und internationale Sicherheit) der Generalversammlung der Vereinten Nationen (VN-GV) 1998 erstmalig behandelt. Seitdem 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 Stabilität zu minimieren. Im Zuge der Verhandlungen gelang es, vier prioritäre Handlungsbereiche zu identifizieren, die für die Etablierung und Durchsetzung eines internationalen Normengerüstes für den Cyberraum besondere Relevanz besitzen:

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

Die 2018 durch GV-Resolutionen initiierten und parallel, aber nominell unabhängig voneinander agierenden, Prozesse zur Cybersicherheit – die allen Staaten offenstehende Open-Ended Working Group (OEWG) sowie die Group of Governmental Experts (GGE), der Expertinnen und Experten aus 25 Mitgliedstaaten angehören – setzten ihre Beratungen 2020 fort. Aufgrund der COVID-19-Pandemie kam es jedoch zu zeitlichen Verschiebungen. Österreich brachte sich aktiv in die Diskussionen im Rahmen der OEWG ein. Die Beratungen der GGE, der Österreich nicht angehört, wurden passiv mitverfolgt.

Der für 2020 anvisierte Abschluss der OEWG musste covidbedingt auf 2021 verschoben werden. Das dadurch entstandene Zeitfenster wurde durch eine Reihe von informellen Konsultationen genützt, die die Grundlage für die Verhandlung und mögliche Annahme eines Abschlussberichts im März 2021 bieten.

Während im Rahmen der OEWG im Herbst noch die mandatierten Diskussionen über die weitere institutionelle Verankerung der Cybersicherheit in den VN liefen, lancierten Russland und China – unterstützt durch einige andere Staaten in der VN-GV – ein Resolutionsvorhaben, mit dem als Nachfolgeprozess eine neue OEWG eingerichtet werden soll. Trotz der geschlossenen Ablehnung dieses Vorhabens seitens Österreichs, der EU-Mitgliedstaaten und gleichgesinnter Staaten fand es eine Mehrheit – die neue OEWG wird ihre Arbeit 2021 nach Abschluss der derzeit laufenden (das Mandat erstreckt sich noch bis 2025) beginnen. Es bleibt offen, wie sich die neue OEWG zu der von 50 Mitgliedstaaten, darunter Österreich, propagierten Einrichtung eines handlungsorientierten Aktionsplans (Programme of Action) zu Cybersicherheit verhalten wird.

Während sich inhaltlich in Bereichen wie Kapazitätsaufbau und der Bedeutung von vertrauensbildenden Maßnahmen in einigen Punkten eine Übereinstimmung ergab, bestehen insbesondere im Bereich der genauen Anwendbarkeit des Völkerrechts nach wie vor teils große Auffassungsunterschiede innerhalb der Staatengemeinschaft.

UNIDIR-Konferenz zur Zukunft der VN-Prozesse im Bereich Cybersicherheit

Der Bereich der internationalen Cybersicherheit findet sich ebenso in der 2018 lancierten Abrüstungsagenda des Generalsekretärs der VN 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. 2020 wurden die dahingehenden Implementierungsmaßnahmen durch die Staaten fortgesetzt.

Unterstützt wird die Umsetzung der Abrüstungsagenda sowie die Arbeit der GGE und der OEWG durch das Büro der VN für Abrüstungsfragen (United Nations Office for Disarmament Affairs [UNODA]). Das Institut der VN für Abrüstungsforschung (United Nations Institute for Disarmament Research [UNIDIR]) trägt mit der Veröffentlichung wissenschaftlicher Publikationen zu den internationalen Cybersicherheitsdiskussionen bei. Darüber hinaus veranstaltet UNIDIR jährlich eine Konferenz zur Cyberstabilität. Die Konferenz 2020 beschäftigte sich mit Fragen zur Zukunft der VN-Prozesse im Bereich der Cybersicherheit.

Im VN-Sicherheitsrat wurde das Thema Cybersicherheit insbesondere unter dem Vorsitz Estlands im Mai 2020 im Rahmen mehrerer Veranstaltungen erstmals detailliert thematisiert.

Das High-level Panel on Digital Cooperation (HLPDC) ist ein Gremium für digitale Zusammenarbeit, welches im Jahr 2018 einberufen wurde, um Empfehlungen zur Stärkung der Zusammenarbeit zwischen Regierungen, dem Privatsektor, der Zivilgesellschaft, internationalen Organisationen, der Wissenschaft, der technischen Gemeinschaft und anderen relevanten Stakeholdern im digitalen Raum vorzulegen. Im vergangenen Jahr legte es erstmals einen Bericht vor. VN-Generalsekretär Guterres lancierte 2020 zur institutionellen Unterstützung des Themas einen Auswahlprozess zur Ernennung eines Sondergesandten für Technologie („Tech Envoy") – für 2021 bleibt abzuwarten, welche Impulse dieser setzen wird und wie seine Prioritäten im VN-System verankert werden können.

Auch während des 15. Internet Governance Forums (IGF) im November 2020 wurde Cybersicherheit thematisiert. Hier insbesondere im Hinblick auf die Notwendigkeit eines sicheren Zugangs zum Internet während der COVID-19-Pandemie. Als besonders kritisch wurde das mangelnde Vertrauen von Regierungen, dem privaten Sektor und des Einzelnen den Technologien und ihren Anbietern gegenüber, festgestellt. Daraus leitete sich die Forderung ab, dass Digitalpolitik an die Nichtgegebenheiten des Internets anzupassen sei.

Im Kontext der VN in Genf arbeitet die Internationale Fernmeldeunion (ITU) an Richtlinien für die Nutzung ihrer „Global Cybersecurity Agenda" (GCA). Diese zielt darauf ab, das Vertrauen und die Sicherheit in der Informationsgesellschaft zu stärken. Die GCA wird von westlichen Staaten teilweise sehr kritisch gesehen. Die sich im Entwurf der Richtlinien befindliche Empfehlung, rechtliche Regelungen zur Bewältigung globaler Cybersicherheitsfragen in der ITU zu entwickeln, war und wird wahrscheinlich auch in Zukunft im Mittelpunkt der Diskussionen zwischen den Mitgliedstaaten stehen.

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. Hilfestellung für betroffene Mitgliedstaaten basiert auf einer 2013 veröffentlichten umfassenden Studie[3] und konzentriert sich auf folgende drei Schwerpunkte:

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

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

Die 2010 im Bereich Cyberkriminalität eingerichtete „Intergouvernementale Expertengruppe“ (IEG) trat im März 2020 zum insgesamt sechsten Mal und hierbei erstmals virtuell zusammen. Die Streitfrage, ob eine neue Cyber-Konvention ausgehandelt oder die Budapest-Konvention ausgeweitet werden soll, konnte nicht gelöst werden. Final wurde der Beschluss gefasst, die Diskussionen der IEG über grundlegende Themen

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

und Entwicklungen betreffend Cyberverbrechen fortzuführen und sich über nationale Gesetzgebung, Best Practice-Beispiele, technische Hilfe und internationale Zusammenarbeit auszutauschen.[4]

Cyberkriminalität war auch zentrales Thema der 29. Tagung der Kommission für Verbrechensverhütung und Strafrechtspflege (CCPCJ) im Frühjar 2020. Österreich legte dabei gemeinsam mit Kanada und Kolumbien eine Resolution mit dem Schwerpunkt Cybercrime vor, die konsensual angenommen wurde.

Zusätzlich zu den Diskussionen rund um Cybersicherheit im 1. Komitee der VN-GV brachte Russland den Aspekt der Bekämpfung der Cyberkriminalität 2018 das erste Mal in die VN-GV ein. Auf Basis der VN-GV Resolution A/RES/73/187 sollte ein Bericht des VN-GS zur Situation von Cyberkriminalität entstehen. Österreich – ebenso wie die restlichen EU-Mitgliedstaaten und gleichgesinnte westliche Staaten – lehnte diese Resolution ab und verwies auf die Behandlung von Cyberkriminalität bei den VN im Rahmen der Intergouvernementalen Expertengruppe (IEG). Russland beharrte darauf, die Diskussionen zu Cyberkriminalität in die VN-GV zu verlagern und Verhandlungen über eine VN-Konvention zur Bekämpfung von Cyberkriminalität zu beginnen. Verhandlungen eines solchen völkerrechtlichen Instruments ohne grundlegende Vorbereitungen, ohne Einbeziehung bereits bestehender Instrumente (wie der Budapest-Konvention) und ohne internationalen Konsens, sind aus Sicht der EU-Mitgliedstaaten problematisch.

Im Rahmen der 74. Sitzung der VN-GV wurde die Resolution A/RES/74/247, die die Errichtung eines Ad-hoc-Komitees zur Erarbeitung der Konvention (Ad hoc Committee – AHC) vorsah, mittels Abstimmung angenommen. Auch hier stimmten die EU und gleichgesinnte Staaten dagegen und verwiesen auf die Duplizierung von VN-Prozessen (IEG Cybercrime). Österreich führte für die EU die Verhandlungen zur Resolution A/RES/74/247. Im Zentrum

---

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

stand und steht das außenpolitische Ziel der Verwurzelung des neuen Verhandlungsprozesses in Wien (Stärkung des Amtssitzes zu Cyberkriminalität), der Festlegung der konsensuellen Verhandlungsführung sowie die Mandatierung eines transparenten und inklusiven Verhandlungsprozesses (unter Einbindung von Nichtregierungsorganisationen).

Im Rahmen der 41. Tagung des VN-Menschenrechtsrats (VN-MRR) im Juni 2019 brachte Österreich als einer der Hauptsponsoren (neben Südkorea, Brasilien, Dänemark, Marokko und Singapur) erstmals eine Resolution zum Thema „Neue und aufkommende Technologien und Menschenrechte“ ein (A/HRC/Res/41/11). Diese wurde im Konsens angenommen. Der beratende Ausschuss des Menschenrechtsrats wurde mit der Ausarbeitung einer Studie zum Thema beauftragt – dies mit dem Ziel, im VN-MRR einen breiten Diskurs über menschenrechtliche Herausforderungen und Potentiale im Zusammenhang mit der rasanten Entwicklung digitaler Technologien (insbesondere im Bereich der KI) anzustoßen. Der Bericht wurde im Jänner 2021 veröffentlicht, im Juni 2021 planen die Hauptsponsoren, dem VM-MRR die nächste Resolution vorzulegen.

Die im September 2020 während der 45. Tagung des VN-MRR erneut von Österreich eingebrachte Resolution zur Sicherheit von Journalisten (A/HRC/RES/45/18) 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 NATO seit der Verabschiedung ihres geltenden strategischen Konzepts von 2010 und der Anerkennung des virtuellen Raums als eine Domäne im Jahr 2016 sowie des Weltraums als eine weitere Domäne im Jahr 2019 mit den Verteidigungsaspekten von Cybersicherheit. Österreich kooperiert hier als Partnerland eng mit der NATO und beteiligt sich auf technischer Ebene an Sitzungen des NATO-C3 (Consultation, Command and Control) Boards sowie jenen im Zusammenhang mit einschlägigen Smart Defence-Projekten. Ein Themenschwerpunkt lag 2020 besonders in der Verhinderung von Cyberangriffen und der Warnung vor Desinformation im Zusammenhang mit COVID-19.

Seit 2013 stellt das 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 stellt Österreich auch einen Mitarbeiter des BMLV für das „European Centre of Excellence for Countering Hybrid Threats“ in Helsinki, an dem sich auch die NATO beteiligt, ab.

2.4 Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE)

Als größte 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 konzentrierte sich darüber hinaus auf die Wahrung und Stärkung der Menschenrechte im Cyberraum.

Für die Weiterentwicklung und Implementierung der VBM vorrangig zuständig ist die Informelle Arbeitsgruppe zu Cyber (Cyber-IWG). Das der OSZE zugrundeliegende Sicherheitsverständnis leitet auch die Arbeit der Cyber-IWG: Die Thematik wird unter Berücksichtigung politisch-militärischer, wirtschaftlicher und menschenrechtlicher Aspekte behandelt. 2020 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 hat sich gemeinsam mit Belgien und Estland vorgenommen, die Umsetzung der CBM 14 zu Public-Private-Partnerships voranzutreiben.

Neben der institutionalisierten Behandlung der Thematik durch die Cyber-IWG setzen seit einigen Jahren die jeweiligen Vorsitzstaaten der OSZE die Cybersicherheit auf ihre Vorsitzagenda. So hat es sich etabliert, dass regelmäßig Cybersicherheitskonferenzen durch den jeweiligen OSZE-Vorsitz abgehalten werden. 2020 fand diese aufgrund der Pandemie rein virtuell statt. Die Konferenz thematisierte die Zusammenarbeit aller wesentlichen Akteure von Staaten, Internationalen Organisationen und Privaten zur Sicherung eines stabilen Cyberumfelds. Auch bot sie Gelegenheit zum Austausch über die Rolle von privaten Akteuren sowie Gender Equality im Cyberbereich.

2.5 Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD)

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

2020 lag der Themenschwerpunkt auf der Verbesserung der Sicherheit von intelligenten Produkten und der Behandlung von Schwachstellen. Aufbauend auf Fallstudien und einer umfassenden Analyse der Wertschöpfungskette und des Lebenszyklus intelligenter Produkte wurden übergeordnete Prinzipien und Handlungsempfehlungen für politische Entscheidungsträger und Interessenvertreterinnen und -vertreter skizziert. Der zweite Bericht zielt darauf ab, das Bewusstsein der Politik für die Bedeutung eines verantwortungsvollen „Umgangs mit Schwachstellen“ zu schärfen, das heißt für die Entdeckung, das Management und den Umgang sowie die koordinierte Offenlegung von digitalen Sicherheitslücken in Produkten und Informationssystemen. Beide Arbeitsstränge dienen als wichtige Basis für die geplante Überarbeitung der OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity aus dem Jahr 2015.

2.6 Europarat

Den Kern der Aktivitäten des Europarates im Bereich Cybersicherheit bildet die „Budapest-Konvention“ aus 2001, die mit aktuell 65 Ratifikationen (2020 Kolumbien) 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 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 sowie das weltweit agierende und in Zusammenarbeit mit Interpol durchgeführte „GLACY+“ unterstützt. Das jüngste Projekt „Cyber East“ zielt auf die Verbesserung der Partnerschaftsstrukturen mit östlichen Staaten ab und wird durch das Europäische Nachbarschaftsinstrument finanziert.

Derzeit laufen die Verhandlungen für ein Zweites Zusatzprotokoll zur Budapest-Konvention, das sich mit internationaler Rechtshilfe und dem damit verbundenen grenzüberschreitenden Zugang zu Daten befassen wird. Eine enge Zusammenarbeit mit der EU im Hinblick auf dort derzeit in Entwicklung befindlicher relevanter Dokumente ist vorgesehen.

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

Die sogenannten „Oktopus-Konferenzen“ dienen Expertinnen und Experten sowie Organisationen als wichtige Plattform im Bereich Cyberkriminalität. Die letzte Konferenz im Jahr 2019 befasste sich mit Beweismitteln im Cyberspace und der Arbeit am Zweiten Zusatzprotokoll zur Budapest-Konvention.

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 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 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.

Das erste Treffen 2020 fand noch wie geplant im Februar in Stockholm statt, die weiteren beiden (vorgesehen waren Zagreb und Bonn) fanden aufgrund der Corona-Pandemie als Videokonferenzen statt. Auch die für Juni 2020 geplante europäische Notfallübung „Cyber Europe 2020" musste abgesagt werden, weil der als Zielgruppe geplante Gesundheitssektor keine Kapazitäten stellen konnte. Stattdessen wurde parallel zum letzten CNW-Treffen ein „Capture the Flag" Event veranstaltet, welcher technische Rätsel mit einem Quiz zu den Prozessen der Zusammenarbeit im CNW verband.

Mit dem weltweiten Ausbruch der COVID-19-Pandemie im März 2020 wurden im CNW am 19. März 2020 der „Alert Cooperation Mode" ausgerufen und wöchentlich Zusammenfassungen der Cybersecurity Lage in der EU mit Bezug auf die Pandemie erstellt. Es stellte sich heraus, dass die Netze mit der Umstellung auf Heimarbeit und Fernunterricht wenig Probleme hatten, es kaum relevante Angriffe auf den Gesundheitssektor gab und Berichte rund um Betrugsversuche mit COVID-Bezug nicht für eine Bearbeitung durch das Netzwerk geeignet sind. Das CNW ging daher am 6. Mai 2020 wieder in den Normalbetrieb über.

Im Rahmen des MeliCERT-2-Projekts der EK wurde im Sommer 2020 unter Leitung von CERT.at der Bedarf für die Toolbox des CNW neu erhoben. Am 5. März 2020 wurde der von der NIS-Richtlinie geforderte offizielle Bericht des CSIRTs-Netzwerks an die Kooperationsgruppe zum zweiten Mal übermittelt.

2.8 Andere Gremien und Foren

WTO eCommerce

Auf der Grundlage der Joint Statement Initiative zu eCommerce wurden die Verhandlungen zu eCommerce, die unter anderem handelsbezogene Cybersicherheitsthemen berühren, im Rahmen der Welthandelsorganisation (WTO) fortgesetzt.

Freedom Online Coalition

Die „Freedom Online Coalition“ ist eine informelle Vereinigung von Staaten, die sich für die effektive Umsetzung weltweiter Online-Menschenrechte einsetzt. Auch Österreich gehört dieser Initiative an, die im Dezember 2011 von den Niederlanden gegründet wurde. Bei der 8. Freedom Online Konferenz vom 5. bis zum 7. Februar 2020 in Accra, Ghana, wurde eine Erklärung zu „Human Rights Impact of Cybersecurity Laws, Practices and Policies“ verabschiedet.

3
Nationale Akteure

3.1 Cyber Security Center (CSC)

Das im BVT angesiedelte CSC konnte sich trotz anhaltender Herausforderungen in organisatorischer und inhaltlicher Hinsicht auch in diesem Berichtsjahr weiter etablieren und erfolgreich den Personalstand vergrößern.

Seit Inkrafttreten des NISG liegt die operative Umsetzung des Gesetzes im Verantwortungsbereich des BMI (strategische Aufgaben verbleiben im BKA). Aus diesem Grund war das Berichtsjahr von weiteren Maßahmen zur Umsetzung organisatorischer und technischer Notwendigkeiten in Bezug auf die zusätzliche neue Aufgabe sowie von operativer Tätigkeit als Behörde im Rahmen des NISG und der zugehörigen Verordnung geprägt.

Im Bereich der Cyberprävention wurden zahlreiche Maßnahmen in Form von Awareness-Vorträgen und Veranstaltungen, der Bewusstseinsbildung bei Unternehmen der kritischen Infrastruktur und bei verfassungsmäßigen Einrichtungen, gesetzt.

Darüber hinaus führte das CSC regelmäßig vielfältige Schulungsmaßnahmen zu IKT-Sicherheit für das eigene sowie für andere Ressorts durch.

3.2 Cyber Crime Competence Center (C4)

3.2.1 Zuständige Ermittlungsbehörden

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

3.2.2 Tätigkeiten

Internationale Kooperation im Bereich Cybercrime:

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

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

3.3 IKT und Cybersicherheitszentrum (IKT&CySihZ)

Das IKT&CySihZ als Teil des Kommando Streitkräftebasis (KdoSKB) ist das Kompetenzzentrum des ÖBH für Informations- und Kommunikationstechnologie, Cyberverteidigung und MilGeoWesen. Das IKT&CySihZ verfügt über zwölf Dienststellen in insgesamt sieben Bundesländern, in welchen es die Bereiche der Informations- und Kommunikationstechnik, Cyberverteidigung, Elektronische Kampfführung sowie das Militärische GeoWesen im Einsatz-, Übungs- und Friedensbetrieb abdeckt.

Eine der Kernaufgaben ist die Zurverfügungstellung von interoperablen, sicheren und innovativen Leistungen und IKT-Services für den Einsatz im In- und Ausland sowie für den wirkungsorientierten Verwaltungsbetrieb. Dabei ist das IKT&CySihZ 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. Dadurch stellt das IKT&CySihZ die Führungsfähigkeit und die Informationsüberlegenheit für das ÖBH in der Cyberdomäne sicher.

3.3.1 Militärisches Cyberzentrum (MilCyZ)

Das MilCyZ als Teil des IKT&CySihZ ist jene Stelle im ÖBH, die bei der Abwehr von Bedrohungen oder Angriffen aus dem Cyberraum gegen die eigenen IKT-Systeme und -Netze wirksam wird. Dem MilCyZ obliegt die Planung und Implementierung der Cybersicherheitssysteme und -komponenten für den Eigenschutz sowie die Verteidigung des ÖBH bei Cyberangriffen. Diese Systeme werden laufend weiterentwickelt und an die aktuelle Bedrohungslage angepasst. In Kombination mit Beobachtungen, Bewertungen und Maßnahmen über Schwachstellen bei aktuellen Technologien, IKT-Systemen und Komponenten des ÖBH kann ein vollständiges Lagebild zur Cybersicherheit erstellt werden. Um fortlaufend alle IKT-Systeme auf ihre sicherheitstechnische Eignung für den Einsatz im ÖBH überprüfen zu können, werden durch System- und Komponenten-Audits konzeptionelle und strukturelle Schwächen in Technologien, Produkten, Komponenten und Systemen frühzeitig erkannt.

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

- Auswahl, Einführung und Betrieb von IKT-Sicherheitskomponenten (z. B. Firewall, End-Point-Protection – Virenschutz, etc.);
- Erstellung eines militärischen Cyberlagebildes sowie die ebengerechte Anpassung und Kommunikation des Lagebildes an die Bedarfsträger;
- Forensik und Schadsoftwareanalyse;
- Auditieren der eigenen IKT-Systeme und -Netze;
- Informations- und Cyberrisikomanagement;
- Schutz der Informationen und militärischen IKT-Systeme durch ein zentrales Security Operations Center (SOC);
- Bereitstellung von Rapid Response Teams zum Eigenschutz der militärischen Infrastruktur.

3.3.2 Military Computer Emergency Readiness Team (milCERT)

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

3.3.3 Elektronische Kampfführung

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

3.4 Abwehramt (AbwA)

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 NISG das Computer-Notfallteam der öffentlichen Verwaltung und Mitglied des IKDOK. 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

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.

AUSTRIAN ENERGY CERT

Das Austrian Energy CERT (AEC) ist ein brancheneigenes Computer Emergency Response Team für die österreichische Energie Industrie. Es wurde 2020 als sektorenspezifisches Computer-Notfallteam gemäß NISG für den Sektor „Energie“ akkreditiert. Die Hauptaufgaben des AEC dienen der Stärkung der IT-Sicherheitskompetenz des Energiesektors und erhöht die Resilienz des Sektors gegenüber Cyberattacken. Zu den Aufgaben gehört neben dem Security Incident Management die Bearbeitung von täglich eingehenden Anfragen und Sicherheitsmeldungen, die Durchführung von Schulungstätigkeiten, die Teilnahme an internationalen Cybersicherheitsübungen oder die Mitarbeit bei der Erstellung technischer Sicherheitskonzepte für die Elektrizitäts- und Erdgaswirtschaft. Darüber hinaus erfüllt das AEC die Rolle des primären Ansprechpartners (Single Point of Contact) bei nationalen und internationalen Security Incidents im Energiesektor. Damit wird neben der schnellen und effizienten Kommunikation auch die Koordination der IT-Sicherheitsexpertinnen und -experten und Behörden innerhalb der Branche gewährleistet.

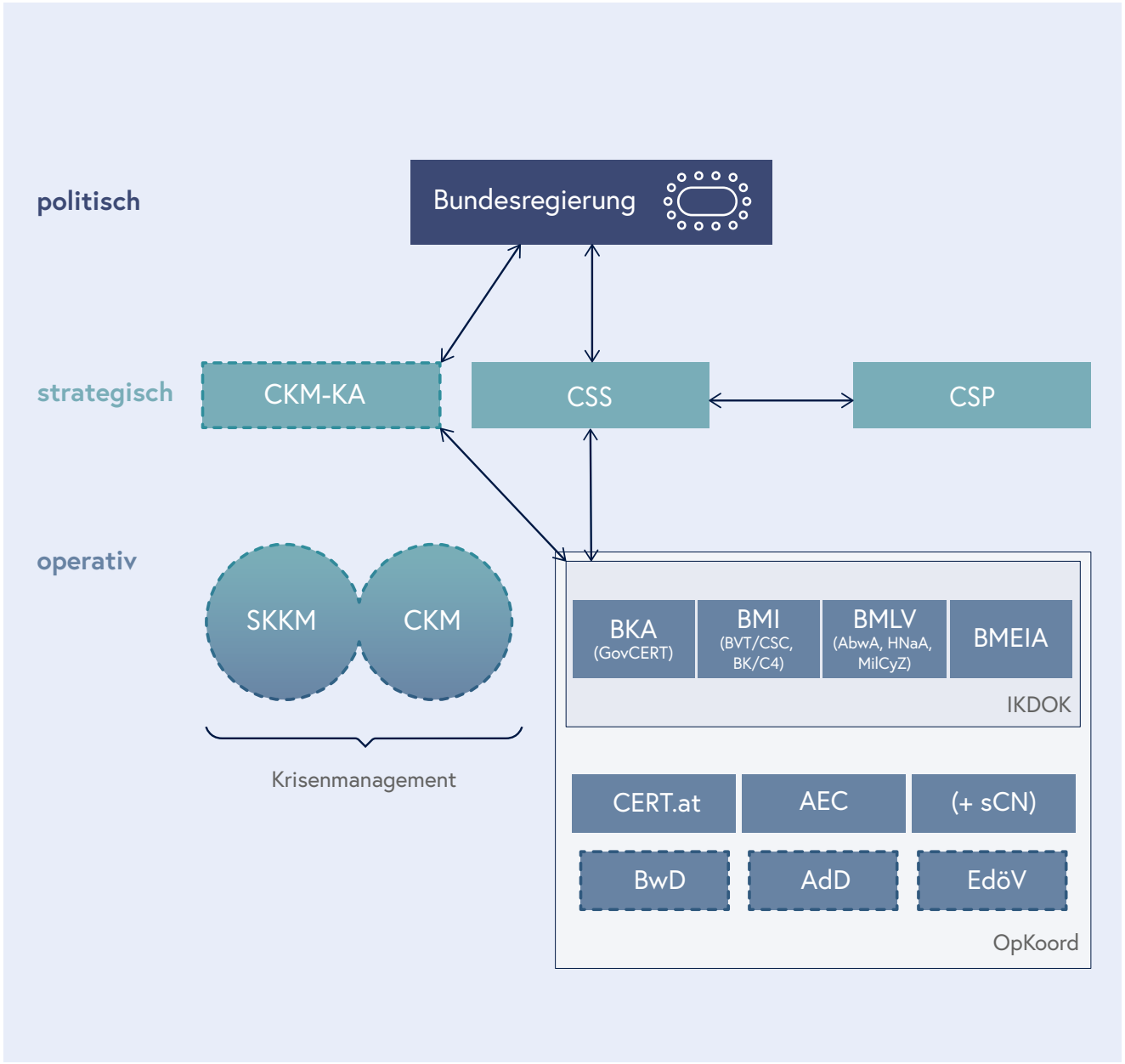
Gemeinsam erfüllen die drei CERTs die Aufgaben gemäß §14 NISG und decken damit Vorgaben der europäischen Richtlinie für Netz- und Informationssicherheit sowie die Empfehlungen der Agentur ENISA für die Erhöhung der IT-Sicherheit bei kritischen Infrastrukturen ab. Sie stellen auch die österreichischen 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 auch vorbeugende Maßnahmen wie Früherkennung, Öffentlichkeitsarbeit, Beratung und Unterstützung im Anlassfall sowie auf Anfrage durch. Mit der Umsetzung der NIS-Richtlinie in nationales Recht (NISG) wurden die Aufgabenbereiche für die CERTs festgeschrieben. So sieht das Gesetz in der Umsetzung unter anderem für Betreiber wesentlicher 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 BMI bzw. das im BVT angesiedelte CSC weitergeleitet. Auf freiwillige Meldungen trifft dies ebenfalls zu, allerdings können diese Meldungen vor der Weiterleitung an das CSC von den Sektor-CERTs anonymisiert werden. Für die Einrichtungen der öffentlichen Verwaltung, mit Ausnahme jener im IKDOK vertretenen, nimmt GovCERT Austria die Entgegennahme und Weiterleitung solcher Meldungen vor. Zusätzlich kann GovCERT Austria auch Frühwarnungen, Alarmmeldungen, Handlungsempfehlungen und Bekanntmachungen vornehmen, erste allgemeine technische Unterstützung bei der Reaktion auf einen Sicherheitsvorfall leisten, Risiken, Vorfälle und Sicherheitsvorfälle beobachten und analysieren sowie die Lage beurteilen. Das NISG sieht zur Wahrnehmung dieser Meldestellenfunktion die Etablierung eines Branchen- oder Sektoren-CERTs in jedem Sektor vor. Wurde in einem Bereich noch kein eigenes CERT etabliert, werden die Aufgaben des Computer-Notfallteams und die der Meldestelle durch CERT.at wahrgenommen.

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 2020 – trotz der schwierigen Umstände angesichts der COVID-19-Pandemie – erfolgreich fort. So wurde beispielsweise mit der bescheidmäßigen Feststellung der Eignung und Ermächtigung des AEC als erstes sektorenspezifisches Computer-Notfallteam im Sinne des NISG ein wichtiger Schritt gesetzt. Auch konnten bei den Ermittlungen der Betreiber wesentlicher Dienste auf Grundlage der NIS-Verordnung substantielle Fortschritte erzielt 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. Das NIS-Büro arbeitete unter anderem intensiv mit den betroffenen Behörden und Regulatoren am Thema der Cybersicherheit von 5G-Netzen. Des Weiteren konnten im Jahr 2020 im Bereich der Informationstätigkeit weitere Aktivitäten gesetzt werden. Hervorzuheben sind hier die englischen Übersetzungen des NISG und der NIS-Verordnung, die auf der NIS-Website (nis.gv.at) abgerufen werden können. Gemeinsam mit dem BMI wurden auf der NIS-Website darüber hinaus der NIS Fact Sheet 8/2018 („Mapping-Tabelle von IKT-Sicherheitsstandards und Cyber Security Best Practices“) bereits in der 3. Version sowie der NIS Fact Sheet 7/2019 („Qualifizierte Stellen“) in der 2. Version veröffentlicht.

Legende

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


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

4 Nationale Strukturen

4.1 Innerer Kreis der Operativen Koordinierungsstruktur (IKDOK)

Mit 29. Dezember 2018 trat das NISG in Kraft. Dieses bildet neben der Umsetzung der europäischen Richtlinie 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). Am Beginn dieses Berichtszeitraums wurde der IKDOK und das CKM einer ersten harten Bewährungsprobe unterzogen, wobei in weiterer Folge ein Cyberangriff auf eine verfassungsmäßige Einrichtung (siehe Punkt 1.1.1) ohne bleibende Schäden abgewehrt und eine Bereinigung des betroffenen Netzwerks erfolgreich koordiniert und durchgeführt werden konnte.

Der IKDOK setzt sich aus Vertreterinnen und Vertretern von BMI (CSC, C4), BMLV (AbwA, HNaA, IKT&CySihZ), BKA (GovCERT) und BMEIA zusammen. Das CSC und das Cyber Verteidigungszentrum führen den Vorsitz im IKDOK. 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. 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.

Im Mittelpunkt des Aufgabenbereichs des CERT-Verbundes Austria stehen die Verbesserung der Zusammenarbeit zwischen den österreichischen CERTs sowie die Förderung der CERT-Aktivitäten in Österreich. Hintergrund ist, dass ein flächendeckendes Netz an CERTs als eines der wirksamsten Mittel zur Absicherung der vernetzten Informations- und Kommunikationssysteme verstanden wird. Die stetig wachsende Anzahl an CERTs, CSIRTs, Security Operations Centers (SOC) und Cyber Defence Teams in den österreichischen Unternehmen sowie deren gelebte enge Partnerschaft bestätigen dies.

Die 2019 eingeführte Geschäftsordnung hat sich in ihrer Anwendung im Corona-Jahr 2020 grundsätzlich bewährt und bedurfte lediglich kleiner Anpassungen. Beim ersten Treffen des Jahres 2020 konnten die Mitglieder noch persönlich teilnehmen, alle weiteren geplanten Treffen wurden online abgehalten.

Seit der Gründung des CERT-Verbundes Austria haben sich die aktuell 16 mitwirkenden Teams in 44 Sitzungen getroffen und sind auch außerhalb der regelmäßigen Treffen über sichere Kommunikationskanäle im ständigen Austausch miteinander.

4.3 Cyber Sicherheit Plattform (CSP)

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

Im Jahr 2020 fand die 10. Arbeitstagung der CSP statt. Inhaltliche Schwerpunkte waren die Umsetzung des NISG, europäische Entwicklungen (insbesondere Review der NIS-Richtlinie), Cyberdiplomatie sowie Berichte zum aktuellen Cyberlagebild.

4.4 Austrian Trust Circle (ATC)

Der ATC ist eine nationale Initiative für den fachlichen Informationsaustausch in Bezug auf Cybersicherheit und in diesem Zusammenhang stehender Vorfälle. Zielgruppe sind alle Sektoren der strategischen Infrastruktur sowie die öffentliche Verwaltung in Österreich. Der ATC wurde im Jahr 2011 gegründet und ist eine Initiative des nationalen CERT.at mit Unterstützung des BKA. Der ATC besteht aus sektorenspezifischen Security Information Exchanges und adressiert Unternehmen und Organisationen der kritischen Infrastruktur und Behörden in Österreich. CERT.at und das AEC bieten hier in Kooperation mit GovCERT Austria bzw. dem BKA einen formellen Rahmen für praxisnahen Informationsaustausch und gemeinsame Projekte im Sicherheitsbereich.

Die wesentlichen Ziele des ATC sind:

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

Neben regelmäßigen Treffen innerhalb der einzelnen Sektoren, die aufgrund der Corona-Situation 2020 nur vereinzelt stattfinden konnten, wird der Austausch zwischen den Sektoren inklusive der öffentlichen Verwaltung einmal im Jahr im Rahmen einer zweitägigen Veranstaltung gefördert. Im Jahr 2020 gab es, bedingt durch die Corona-Pandemie, nur sehr eingeschränkte ATC-Aktivitäten.

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.

2020 umfassten die Aktivitäten auf dem IKT-Sicherheitsportal insgesamt die Erstellung von 133 Newsartikeln, 43 Publikationseinträgen und 70 Veranstaltungseinträgen. Jedes Monat wurde ein Schwerpunktthema zu aktuellen Trends festgelegt, wozu insgesamt 44 Fachbeiträge veröffentlicht wurden. Dies waren beispielsweise im April die IT-Sicherheit im privaten WLAN und im Oktober die österreichischen Aktivitäten, die im Zuge des „European Cyber Security Month“ (ECSM) veranstaltet wurden. Zusätzlich wird – situationsbedingt – langfristig ein Schwerpunkt für Inhalte mit thematischem Bezug zur Corona-Pandemie gepflegt. Diese reichen von Ratschlägen für adäquate IT-Sicherheit im Homeoffice bis hin zu Hinweisen auf aktuelle Betrugsversuche.

Als erste Fach-Website präsentiert sich das restrukturierte IKT-Sicherheitsportal seit Oktober 2020 im neuen Corporate Design des Bundes, wodurch die Nutzungsfreundlichkeit deutlich verbessert wurde.

Besucherstatistiken zum IKT-Sicherheitsportal für die Jahre 2019/2020
(Stand: 31.12.2020):

Besuche 2019

~249.000

(+20 % gegenüber 2018)

Besuche pro Tag (Spitzen MO–DO)

Ø 900 / Tag

Besuche 2020

~323.000

(+30 % gegenüber 2019)

Besuche pro Tag während des "Corona-Hochs" von Mitte März bis Mitte Mai

Ø 1.300 / Tag

5 Cyberübungen

Um die Gesundheit der Teilnehmerinnen und Teilnehmer nicht zu gefährden, wurden aufgrund der COVID-19-Pandemie nahezu alle nationalen und internationalen Vorhaben abgesagt. Das BMLV/ÖBH nahm daher dieses Jahr nur an zwei Übungen teil.

Crossed Swords 2020

Die Crossed Swords 2020 wurde, wie jedes Jahr, durch das NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE) organisiert und durchgeführt.

Der Übungszweck bestand darin, Penetration Tester, forensische Expertinnen und Experten und Special Operations Forces als gemeinsames Team zum Zusammenwirken zu bringen, um die gesetzten Missionsziele und technischen Herausforderungen in einer virtuellen Cyberumgebung zu erfüllen. Das ÖBH konnte auch dieses Jahr wieder Teilnehmerinnen und Teilnehmer stellen, um die vorhandenen Fähigkeiten im Penetration Testing, welches zur Überprüfung eigener IKT-Systeme benötigt wird, zu verbessern. Besondere Bedeutung kam auch dem Erfahrungsaustausch mit Spezialistinnen und Spezialisten aus anderen Nationen zu.

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

5.1 Common Roof

Im Zuge der Übung wurde auch dieses Jahr wieder ein gemeinsames, multinationales Mission Network zwischen Österreich, Schweiz und Deutschland aufgebaut, betrieben und gegen Cyberbedrohungen geschützt. Im Mittelpunkt standen neben den standardisierten (beziehungsweise teilweise noch zu standardisierenden) IKT-Service-Management-Prozessen auch IKT-Sicherheitsprozesse und die dabei zum Einsatz kommenden IKT-Services. Die Überwachung und Steuerung der multinationalen Netzwerkanteile übernahm eine multinationale Network Operation Cell (NOC). Die Vernetzung mit Deutschland und der Schweiz konnte weiter ausgebaut werden und die Einsatzsysteme wurden erfolgreich beübt.

6 Zusammenfassung / Ausblick

6.1 Der BMEIA-Vorfall und seine gesamtstaatlichen Konsequenzen

Der Angriff auf das Netzwerk des Bundesministeriums für europäische und internationale Angelegenheiten zu Beginn des Jahres 2020 stellte den bisher größten und umfangreichsten Cybervorfall auf ein Ministerium in Österreich dar und führte erstmalig zur Aktivierung der im Netz- und Informationssystemsicherheitsgesetz vorgesehenen gesamtstaatlichen Krisenmechanismen (siehe hierzu auch Kapitel 1.1.3). Alle Gremien und Einsatzstrukturen arbeiteten hochprofessionell und effizient und konnten somit die Situation rasch unter Kontrolle bringen. Gleichzeitig haben sich die Prozesse gemäß Netz- und Informationssystemsicherheitsgesetz und der Österreichischen Strategie für Cybersicherheit in großen Teilen als zielgerichtet und effizient erwiesen.

Im Zuge der Nachbearbeitung des Cybervorfalles wurde unter Koordination des Bundeskanzleramtes ein strategisches „Lessons Identified"-Dokument mit dem wesentlichen Ziel erstellt, durch Maßnahmen einerseits das Cybersicherheitsniveau insbesondere der Bundesverwaltung zu erhöhen beziehungsweise insgesamt zu stärken und andererseits die österreichische Verwaltung als Ganzes resilienter gegenüber Cyberangriffen zu machen. Mittels eines gemeinsamen Beschlusses der Generalsekretärinnen und Generalsekretäre der Ministerien wurde die sukzessive Umsetzung dieser Maßnahmen beauftragt. Diese fungieren auch als Basis für die Festlegung und Umsetzung von Mindeststandards.

In einem ersten unmittelbaren Schritt wurde das Government Computer Emergency Response Team Austria durch einen neuen, verbesserten Vertrag nachhaltig gestärkt und eine 24/7/365-Verfügbarkeit sichergestellt. Ebenso wurde die Etablierung von Chief Information Security Officers in den Ministerien und der öffentlichen Verwaltung auf den Weg gebracht, um im Falle von Cyberkrisen ressortübergreifend auf standardisierte Strukturen zugreifen zu können.

Cybersicherheit wird in der ministeriellen Landschaft als ein fortlaufender Prozess verstanden. Die Erfahrungen, die im Zuge der Vorfallsbehandlung gemacht wurden, dienen dazu, im risikobasierten Ansatz kontinuierlich Anpassungen an den Sicherheitsstrukturen und Prozessen vorzunehmen und somit die Bundesverwaltung Schritt für Schritt sicherer zu machen.