Bericht Cyber Sicherheit 2019

Bericht
Cyber Sicherheit
2019

Wien, 2019

Bundeskanzleramt

Bundesministerium
Inneres

Bundesministerium
Landesverteidigung

Bundesministerium
Europa, Integration
und Äußeres

Impressum

Medieninhaberin, Verlegerin und Herausgeberin:
Cyber Sicherheit Steuerungsgruppe
Ballhausplatz 2, 1010 Wien
Grafische Gestaltung: BKA Design & Grafik

Wien, Mai 2019

Inhalt

Einleitung

Die Österreichische Strategie für Cyber Sicherheit (ÖSCS) legt fest, dass durch die Cyber Sicherheit Steuerungsgruppe (CSS) ein jährlicher Bericht zur Cyber Sicherheit in Österreich erstellt wird. Der letzte Bericht wurde im April 2018 vorgelegt.

Der aktuelle Bericht Cyber Sicherheit 2019 baut auf den Inhalten des letztjährigen Berichtes auf und ergänzt diesen um aktuelle Entwicklungen mit Schwerpunkten in den Bereichen internationale und operationelle Entwicklungen. Beobachtungszeitraum ist das Jahr 2018, einzelne aktuelle Entwicklungen im Jahr 2019 haben Eingang gefunden.

Zielsetzung des Berichtes ist eine zusammenfassende Darstellung der Cyber Bedrohungen und wesentlicher nationaler und internationaler Entwicklungen.

1 Cyber Lage/Bedrohung

1.1 Lage Cyber Sicherheit – operative Ebene

Die Österreichische Strategie für Cyber Sicherheit (ÖSCS) sieht vor, dass auf der operativen Ebene sowohl periodische als auch anlassbezogene Lagebilder für Cyber Sicherheit zu erstellen sind. Auch in diesem Berichtsjahr kamen die bereits seit mehreren Jahren bestens etablierten Gremien OpKoord (Operative Koordinierungsstruktur) und IKDOK (Innerer Kreis der Operativen Koordinierungsstruktur) dieser Aufgabe nach. Die Erstellung einer regelmäßigen, umfassenden Lagedarstellung zur Cyber Sicherheit in Österreich und die Kommunikation dieser Lagebilder an die Stakeholder, stellen zentrale Tagesordnungspunkte in den regelmäßigen Abstimmungstreffen dar. Im Folgenden ist eine Auswahl von wesentlichen Vorfällen aus den IKDOK-Lagebildern zusammengefasst. Die Zusammenstellung erfolgt in der Reihenfolge des Auftretens dieser Vorfälle.

1.1.1 Spectre/Meltdown (01/2018)

Zu Beginn des Jahres erfolgte die medienwirksame Veröffentlichung von Informationen zu einer Hardwareschwachstelle in Intel-Prozessoren. Diese Schwachstelle ermöglichte es einem Computerprogramm auf Daten zuzugreifen, auf die es normalerweise keinen Zugriff haben sollte. Da es sich hierbei nicht um eine Sicherheitslücke in der Software, sondern in der Hardware handelte, wurden Sicherheitsexperten vor verschiedene Hindernisse gestellt, die bei normalen Schwachstellen nicht auftreten.

In enger Zusammenarbeit agierten CERT.at und GovCERT hier als Informationsdrehscheibe und kontinuierlicher, verlässlicher Ansprechpartner für Unternehmen und Behörden, um diese bei der Schadensminderung und -behebung zu unterstützen und die aufkommenden Hürden zu bewältigen.

1.1.2 VPNFilter (05/2018)

Ende Mai veröffentlichten Sicherheitsforscher detaillierte Informationen über ein weltweit agierendes Botnetz, von den Forschern „VPNFilter“ genannt. Die Täter nutzten eine Vielzahl von Schwachstellen, um Netzwerkgeräte verschiedenster Marken und Modelle zu übernehmen und mit Schadsoftware zu infizieren, die nicht nur den Missbrauch der Geräte für weitere Attacken, sondern auch das Manipulieren von Netzwerktraffic erlaubte. Auch Monate später ist das genaue Ausmaß noch nicht bekannt, Schätzungen sprechen aber von mindestens 500.000 weltweit betroffenen Geräten.

Aufgrund der Sorgfältigkeit der Netzbetreiber in Hinblick auf die Sicherheitshygiene ihrer Netze, war die Anzahl der betroffenen Geräte in Österreich stark begrenzt. Die wenigen Infektionen wurden, nach durch CERT.at erfolgter Information der Betreiber, rasch bereinigt.

1.1.3 Advanced Persistent Threats (10/2018)

Advanced Persistent Threats (APT) sind komplexe, zielgerichtete Angriffe auf kritische IT-Infrastrukturen von Unternehmen und Behörden. Im Oktober 2018 wurde Österreich Opfer eines solchen Angriffs, mit dem Ziel, die Sicherheit der IT-Systeme von Behörden und Institutionen zu gefährden und im großen Stil Daten zu entwenden. Über verschiedenste Kanäle wurde durch die Angreifer versucht, die Opfer mit Schadsoftware zu infizieren um Benutzerdaten zu kompromittieren, mit dem ultimativen Ziel, die Computernetzwerke zu infiltrieren und vertrauliche Daten zu stehlen.

Durch Vorkehrungen der angegriffenen Institutionen sowie der guten Zusammenarbeit von GovCERT und Cyber Security Center (CSC) war es möglich, die Angriffe bei allen Betroffenen abzuwehren und den Abfluss von Daten zu verhindern. Dass die Auswirkungen trotz des Aufwands der Angreifer minimalst geblieben sind, ist ein weiteres Zeichen für die Effektivität und Wichtigkeit kontinuierlicher Kooperation aller relevanten Stellen auf nationalstaatlicher Ebene.

1.2 Lage Cyber Sicherheit – Unternehmen und Sicherheitsdienstleister

Die Implementierung der Österreichischen Strategie für Cyber Sicherheit (ÖSCS) ist ein permanenter Prozess, der von der Cyber Sicherheit Steuerungsgruppe (CSS) koordiniert wird. Eine der Aufgaben der CSS ist es, einen jährlichen Bericht zur Cyber Sicherheit in Österreich zu erstellen, der einen Überblick über die Cyber Lage im Beobachtungszeitraum, nationale und internationale Entwicklungen, sowie durchgeführte Cyber Übungen geben soll.

Staatliche Stellen sehen im Rahmen ihrer Tätigkeit jedoch lediglich einen Ausschnitt der in Österreich vorliegenden Situation. Um ein möglichst valides und vollständiges Bild der Cyber Lage in Österreich zu zeichnen, wurden zur Erstellung des vorliegenden Berichts auch in diesem Jahr wieder

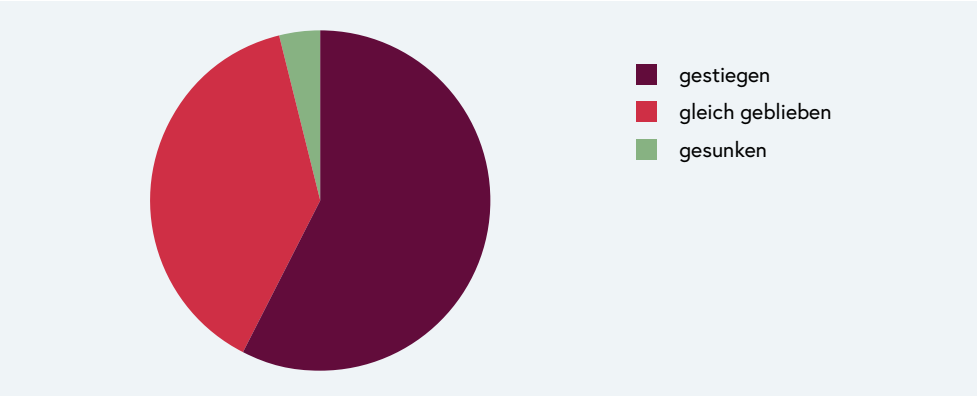
- Unternehmen der kritischen Infrastruktur und verfassungsmäßige Einrichtungen sowie
- führende private Unternehmen aus der Cyber Security-Branche

eingeladen, um auf der Basis ihrer Tätigkeit dieses Wissen zu vervollständigen und die CSS durch ihre Expertise zu unterstützen. Das Hauptaugenmerk ist dabei nicht auf konkrete Einzelfälle, sondern vielmehr auf eine abstrahierte Überblicksdarstellung gerichtet. Wir bedanken uns an dieser Stelle bei allen Unternehmen und Organisationen, die uns ihre Einschätzung zur Verfügung gestellt haben[1].

1.2.1 Unternehmen der kritischen Infrastruktur

Bei den Unternehmen der kritischen Infrastruktur war im Jahr 2017 in Bezug auf die für IT-Sicherheit zur Verfügung stehenden Budgets ein erfreulicher Trend zu beobachten. Der Großteil der befragten Organisationen tätigte Investitionen im Bereich Cyber Sicherheit. Dieser Trend setzte sich im darauffolgenden Jahr unverändert fort. Während nach wie vor die überwiegende Mehrheit an kritischen Infrastrukturen und verfassungsmäßigen Einrichtungen mehr Geld in IT-Sicherheit investierte, blieb der Anteil an Organisationen, die mit einem gesunkenen Budget auskommen müssen, erfreulicherweise verschwindend gering.

Abbildung 1: Entwicklung des zur Verfügung stehenden Budgets



Entsprechend dem gestiegenen Budget für IT-Sicherheit und sogar noch deutlich darüber hinaus wurden auch in den Organisationen neue Sicherheitsmaßnahmen verschiedenster Natur ergriffen: Dies traf bei über 80 % der eingegangenen Rückmeldungen zu. Wesentliche Faktoren hierbei waren wohl die neuen gesetzlichen Auflagen an die IT-Sicherheit, wie die im Mai 2018 in Kraft getretene Datenschutz-Grundverordnung oder das für Betreiber wesentlicher Dienste und Anbieter digitaler Dienste relevante NIS-Gesetz.

1 Einer namentlichen Nennung im Bericht haben die Unternehmen VACE Systemtechnik, FH Joanneum GmbH und Alpha Strike Labs GmbH zugestimmt. Vielen Dank!

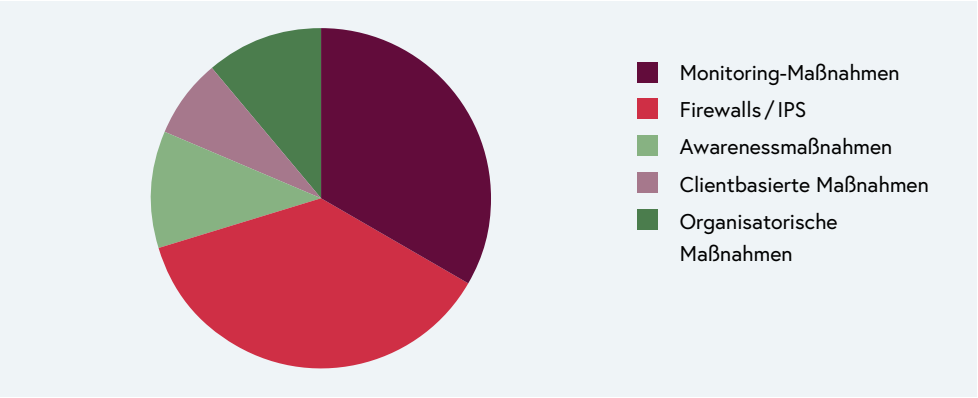


Abbildung 2: Im Jahr 2018 getroffene Maßnahmen

Abbildung 2 gibt einen Überblick über die eingeführten Sicherheitsmaßnahmen. Während der technische Fortschritt in den Bereichen Firewalls/IPS sowie Endpoint Protection (wenn auch in geringerem Ausmaß) zweifellos zu Aufrüstungen der Verteidigungsmaßnahmen geführt hat, setzt sich parallel dazu auch hier der letztjährige Trend fort: Anstatt rein auf Abschottung zu setzen, tendieren immer mehr Organisationen zu Monitoringmaßnahmen zum Aufdecken von Angreifern im eigenen Netz. Hierzu gehört zusätzlich auch die aktive Suche nach aktuellen Bedrohungen für die jeweilige Organisation und in einem zweiten Schritt die gezielte Überprüfung von Systemen nach Infektionen. Begleitend dazu wurden vielerorts vorbereitende Maßnahmen getroffen, um Sicherheitsvorfälle mit forensischen Methoden analysieren zu können.

Awarenessmaßnahmen wurden ebenfalls in mehreren Organisationen neu eingeführt bzw. verstärkt. Diese wurden auch unter der Fragestellung „Lessons Learned" vielfach als effektiv und unverzichtbar zur Prävention von einer Vielzahl von Cyber Angriffen angegeben. Zu solchen Maßnahmen zählten neben Fachvorträgen auch simulierte Phishing- oder Ransomwareattacken. Parallel dazu gaben Unternehmen auch an, dass die in der Vergangenheit getroffenen Maßnahmen im Jahr 2018 Erfolg zeigten und Angriffe dadurch im Vorfeld durch die Benutzerinnen und Benutzer erkannt werden konnten.

Organisatorische Maßnahmen wie z. B. die Einführung von SIEMs, aber auch strengere Policies für Passwörter oder angepasste Unternehmensprozesse waren auch auf der Tagesordnung. Hier ist womöglich ebenfalls ein Zusammenhang mit den unter „Lessons Learned" gegebenen Antworten zu erkennen. Laut diesen beschäftigten sich die befragten Organisationen zunehmend mit neuen regulatorischen Maßnahmen, wie der Datenschutz-Grundverordnung oder der Umsetzung der EU-Richtlinie für Netz- und Informationssicherheit.

In diesem Zusammenhang steigen auch die Anforderungen an Softwarehersteller in Bezug auf Herstellersupport, Wartung, Logging und Adaptierbarkeit. Durch die regulatorischen Maßnahmen mit konkreten Anforderungen sowie die von manchen Kunden wahrgenommene sinkende Qualität von Softwareupdates mehren sich hier die Konflikte.

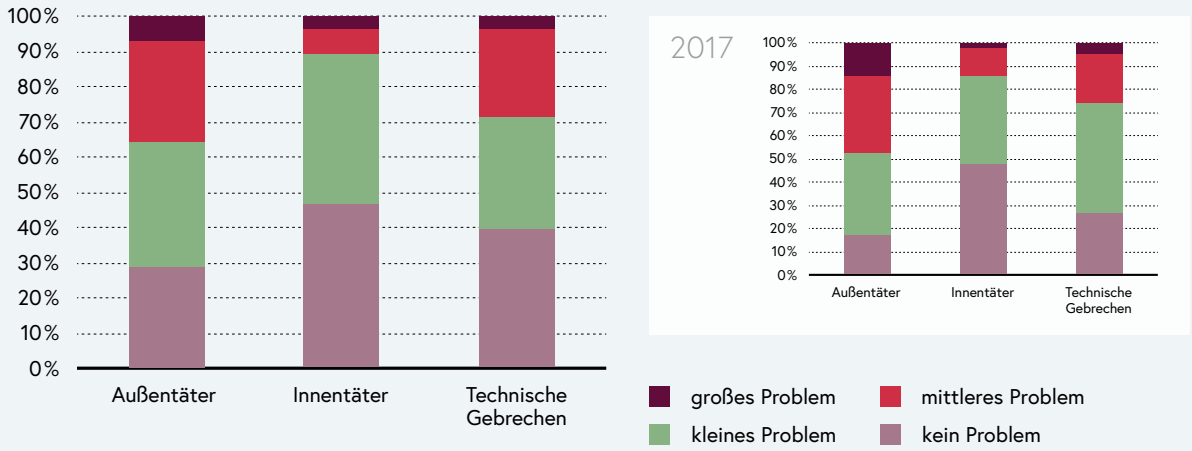


Abbildung 3: Vorfallursachen 2018, vgl. Daten aus 2017

Bei der Einschätzung von Vorfallursachen zeigte sich auch im Jahr 2018 ein im Vergleich zum Vorjahr durchaus vergleichbares Bild. Generell kann eine geringe Verschiebung in Richtung „kein Problem“ festgestellt werden.

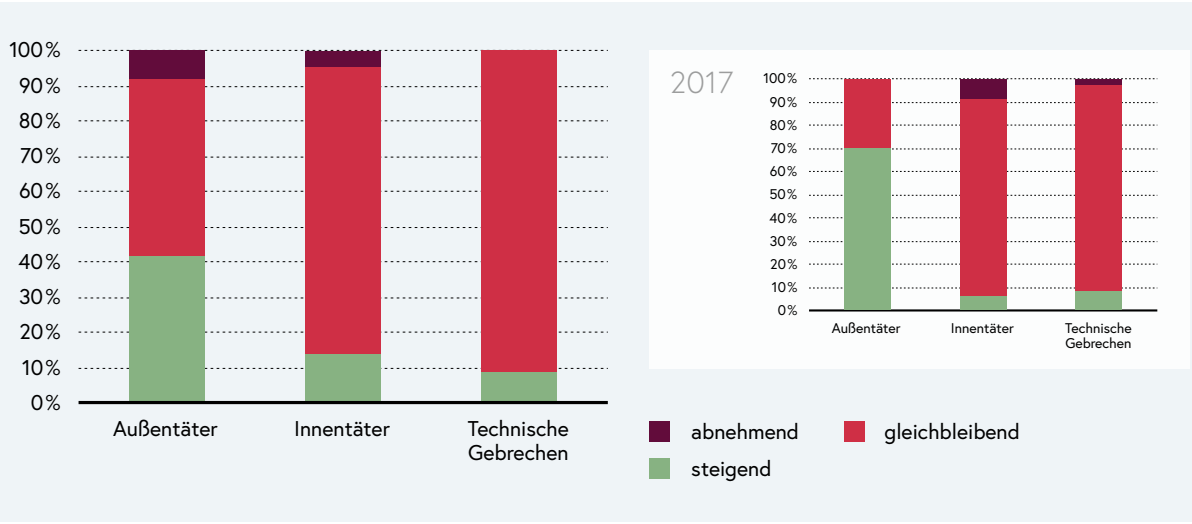


Abbildung 4: Vorfall-ursachen Trends 2018, vgl. Daten aus 2017

Der Trend hingegen wird abgesehen von allen Ursachen eher als steigend angegeben, wenn auch etwas langsamer als im Vorjahr. Dieses Zusammenspiel könnte für Außentäter darauf zurückzuführen sein, dass durch die gesteigerten Abwehrmaßnahmen, insbesondere im Bereich Ransomware und Phishing, das Angriffsvolumen zwar zunimmt, aber immer mehr dieser Angriffe auch im Vorfeld erkannt beziehungsweise abgewehrt werden können.

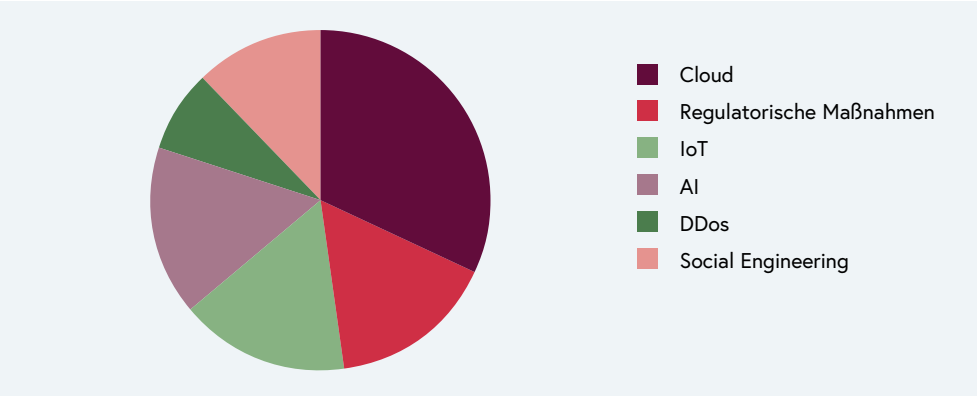


Abbildung 5:
Generelle Trends

Abbildung 5 zeigt generelle Entwicklungen in der IT-Sicherheitsbranche auf. Neben den schon erwähnten, wird Cloud Computing als sehr starker Trend angegeben. Dieser wird jedoch von den befragten Unternehmen durchwegs kritisch betrachtet, sei es bei der gefühlten „verlorenen Hoheit" über seine Daten oder bei der stetigen Abhängigkeit eines externen Anbieters. Allerdings wurde gleichzeitig festgestellt, dass Cloud-Lösungen immer aggressiver zu Lasten von lokalen Anwendungen vertrieben werden, und dass langfristig wohl kein Weg an der Cloud vorbeiführen wird.

1.2.2 Führende private Unternehmen aus der Cyber Security-Branche

Die Befragung von führenden privaten Unternehmen von Sicherheitsdienstleistern wies eine vergleichsweise geringe Rücklaufquote auf; wir danken insbesondere den Firmen VACE Systemtechnik, FH Joanneum GmbH und Alpha Strike Labs GmbH für ihre Antworten. Die folgenden Trends und Erkenntnisse leiten sich aus den eingegangenen Antworten ab.

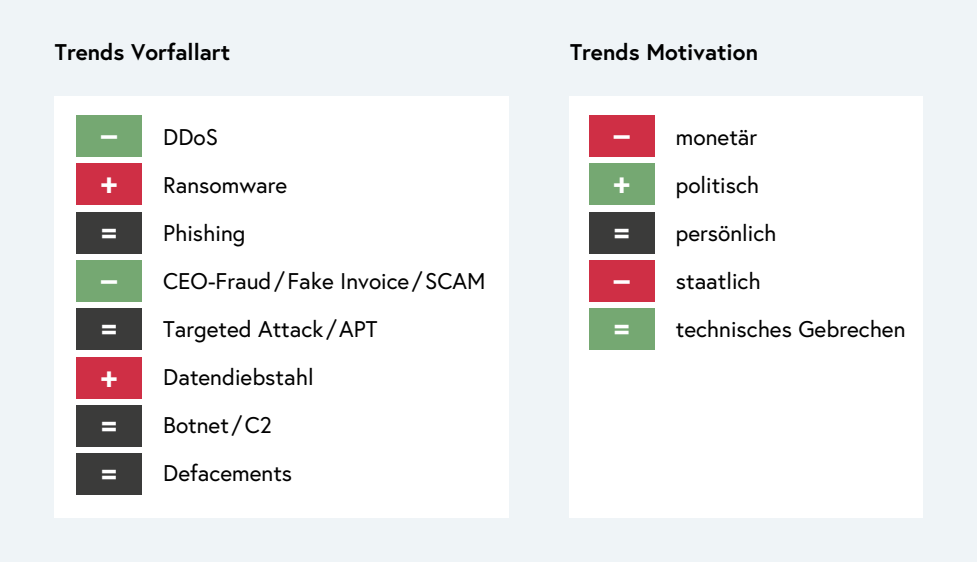


Abbildung 6: Trends bei bearbeiteten Vorfallarten und Motivationen

Während sich im Jahr 2017 ein Abschwächen von DDoS-Vorfällen bereits ankündigte, war die Anzahl im darauffolgendem Jahr tatsächlich rückläufig. Ebenfalls verzeichneten CEO-Frauds und verwandte Betrugsversuche – vermutlich durch eine mittlerweile breite Sensibilisierung des Themas – einen Rückgang. Im Gegensatz zum Jahr 2017 wurden die Sicherheitsdienstleister seltener wegen technischer Gebrechen zu Hilfe gezogen, auf der anderen Seite zeigte sich jedoch ein Anstieg an monetär sowie mutmaßlich staatlich motivierten Cyber Angriffen, was sowohl mit einem weiteren Anstieg an Ransomware-attacken als auch Datendiebstählen in Verbindung gebracht werden kann.

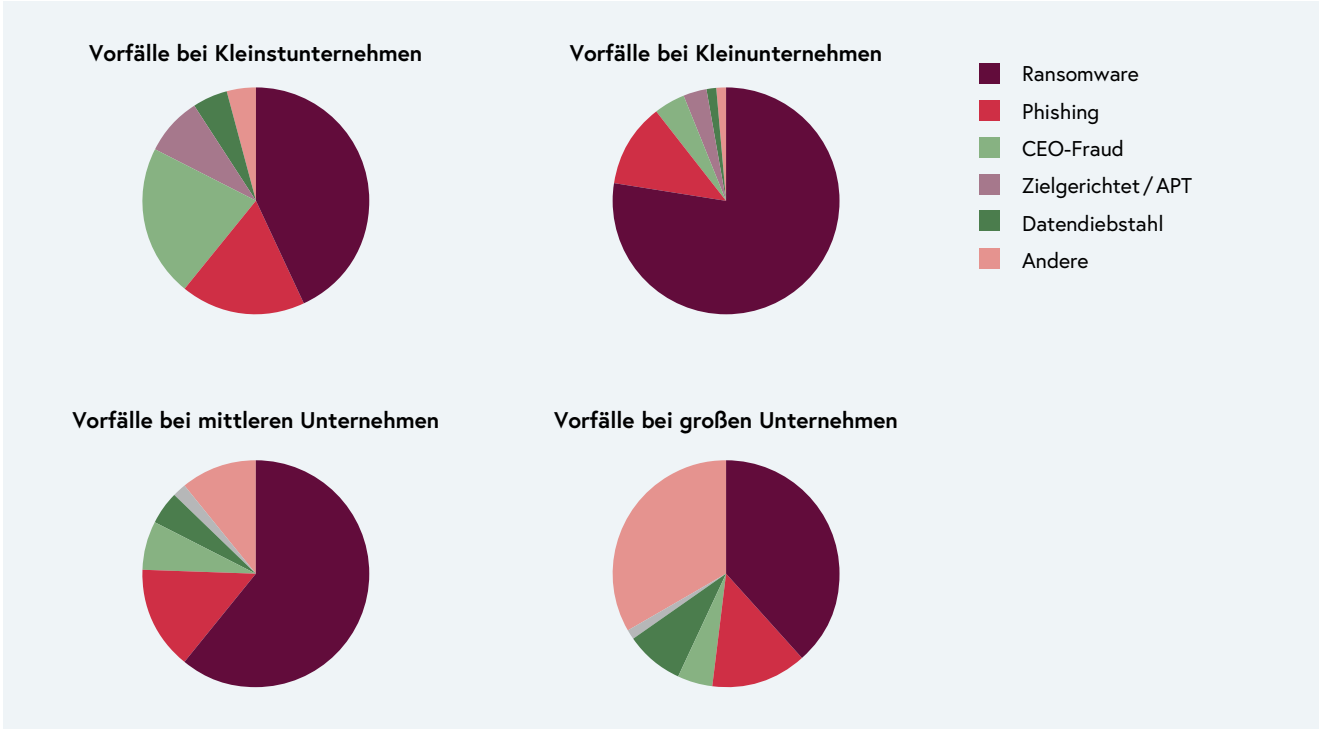


Abbildung 7: Vorfallarten nach Unternehmensgröße

Aufgeschlüsselt nach Unternehmensgröße erkennt man erwartungsgemäß, dass breit gestreute Angriffe wie Ransomware oder Phishing die Mehrheit bilden, insbesondere bei kleinen und mittleren Unternehmen.

Im Hinblick auf die offenbar am stärksten zunehmenden Vorfallarten, sind auch die entsprechenden „Lessons Learned“ und Erkenntnisse der führenden privaten Unternehmen aus der Cyber Security-Branche von großer Relevanz.

Das Ansteigen der erkannten Angriffsversuche durch Ransomware kann auch durch die mittlerweile getroffenen zahlreichen Präventivmaßnahmen erklärt werden, sowohl technischer als auch nicht-technischer Natur. Benutzerschulungen im Bereich Awareness sowie simulierte Phishing-Angriffe oder neue Methoden in der Erkennung von Schadsoftware konnten viele Angriffe im Vorfeld abwehren, wobei hier die großen Unternehmen Vorreiter sind.

Bei Phishing-Angriffen zogen die Sicherheitsdienstleister eine durchwegs positive Bilanz. Obwohl das Angriffsvolumen konstant blieb, waren nur die wenigsten Angriffe erfolgreich. Es zeigte sich, dass Benutzerinnen und Benutzer zunehmend in diese Richtung sensibilisiert sind bzw. Unternehmen Ansprechpartner für mutmaßliche Angriffe stellen.

CEO-Fraud trat wieder zahlreich auf, teilweise im Zusammenhang mit tatsächlichen Hacking-Angriffen im Vorfeld. Die dadurch erbeuteten Informationen wurden dann verwendet, um den „eigentlichen" Betrugsversuch durchzuführen. Da große Unternehmen in diesem Bereich mittlerweile stärker sensibilisiert sind und entsprechende Prozesse eingerichtet wurden, verlagerte sich das Volumen im Vergleich zur Vorperiode in Richtung Klein- und besonders Kleinstunternehmen (weniger als 10 Mitarbeiter). Gerade bei diesen erwies sich der direkte persönliche Kontakt zwischen den handelnden Personen als effektiver Schutz. Weiters ließ sich der Trend beobachten, dass besonders neue Ausgliederungen von Unternehmen angegriffen wurden.

Zielgerichtete Angriffe/APTs mit dem Schwerpunkt Informationsgewinnung konzentrierten sich auf größere Unternehmen und sind wie DDoS-Angriffe im Rückgang. Neben der eigentlichen Abwehr erweist sich hier eine korrekte Zuordnung als großes Problem.

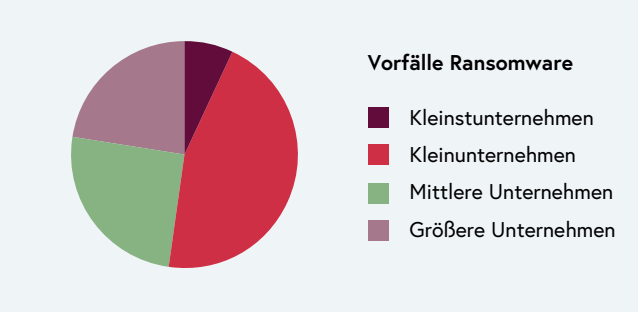


Abbildung 8: Vorfälle Ransomware

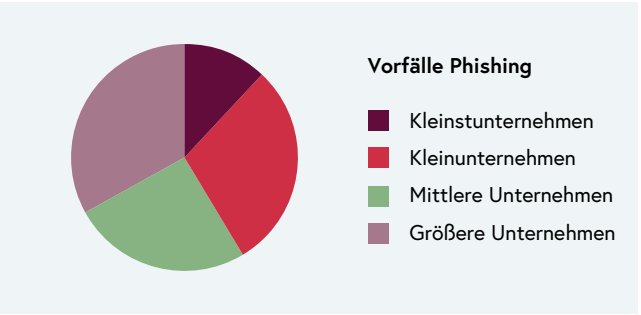


Abbildung 9: Vorfälle Phishing

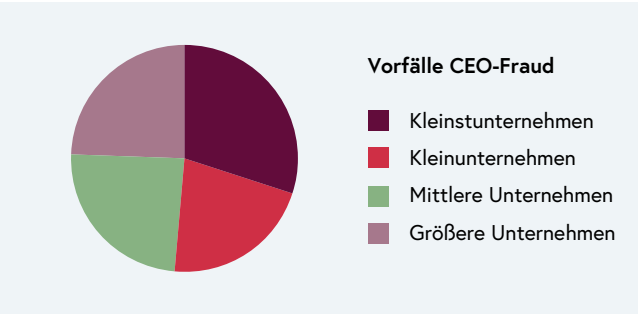


Abbildung 10: Vorfälle CEO-Fraud

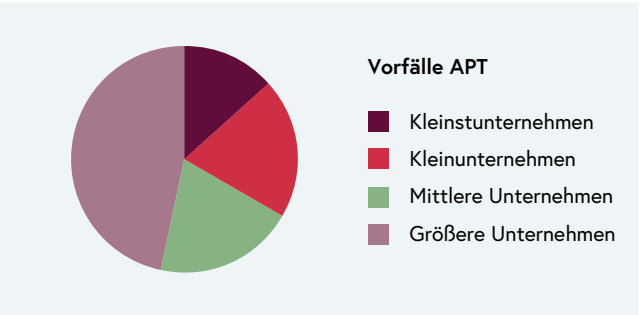


Abbildung 11: Vorfälle APT

Zusammenfassend folgende Grafik:

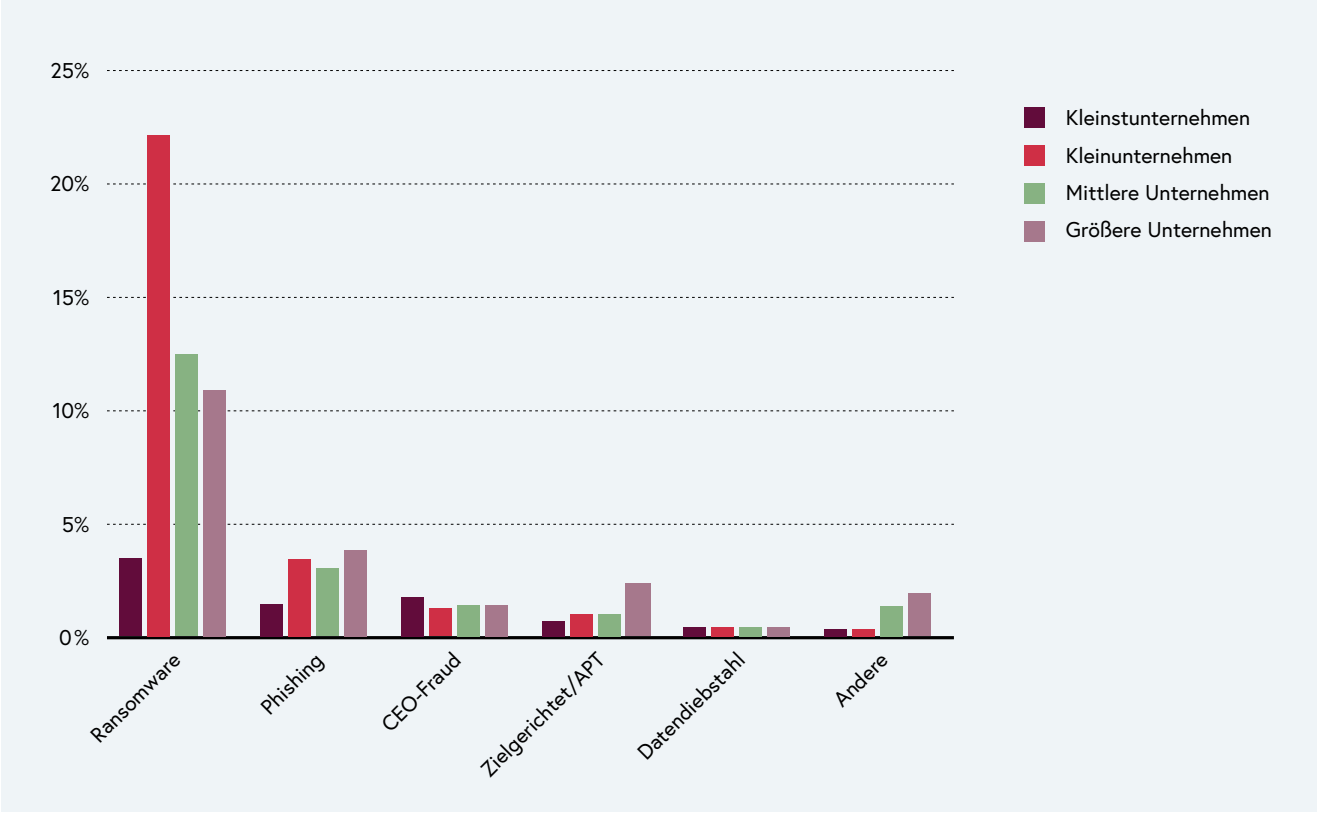


Abbildung 12:
Zusammenfassende Grafik

1.3 Lage Cyber Crime

Die Zahl der Anzeigen von Cyber Crime Delikten im engeren Sinn (Straftaten, die an IT-Systemen oder Daten begangen werden, beispielsweise widerrechtlicher Zugriff auf ein Computersystem oder Datenbeschädigung) war 2018 im Vergleich zum Vorjahr rückläufig. Für diese positive Entwicklung sind vor allem Präventionsmaßnahmen und intensive Ermittlungsarbeit verantwortlich.

Unter anderem konnte im Bundeskriminalamt 2018 die Arbeit der Sonderkommission „SOKO Clavis“ zur zentralen Bekämpfung von Ransomware erfolgreich fortgesetzt werden. Bei Ransomware (auch Verschlüsselungstrojaner genannt) werden die Dateien der Opfer durch eine Schadsoftware verschlüsselt. In weiterer Folge wird von den Tätern für die Entschlüsselung die Bezahlung eines „Lösegelds“ (in der Regel in Form von Bitcoin) zur Entschlüsselung der Daten gefordert. Die „SOKO Clavis“ konnte in diesem Zusammenhang in enger Zusammenarbeit mit Europol (EC3) mehrere Verdächtige ausforschen.

Entschlüsselungstools, die in enger Zusammenarbeit von Europol, internationalen Strafverfolgungsbehörden und privaten IT-Sicherheitsunternehmen entwickelt wurden, werden auf der Seite https://www.nomoreransom.org/ kostenlos zur Verfügung gestellt.

Auch bei Straftaten gemäß § 107c StGB „Fortgesetzte Belästigung im Wege einer Telekommunikation oder eines Computersystems“ - dem sogenannten „Cybermobbing“ – konnte ein Rückgang der Anzeigen verzeichnet werden. Dieser positive Trend kann auf die verstärkte Präventionsarbeit und auf polizeiliche Projekte wie beispielsweise „CyberKids“ beziehungsweise „Click & Check“ zurückgeführt werden.

Bei Internet-Erpressung werden Opfer durch Drohungen, Gewaltdrohungen, bis hin zu Drohungen mit Veröffentlichung von privaten Sex-Videos oder ähnlichem, zu Geldzahlungen genötigt. Teilweise werden nach der Bezahlung die Erpressungen fortgeführt und es werden weitere Zahlungen gefordert. 2018 stieg die Zahl der Anzeigen wegen Erpressung im Internet deutlich an. Dieser Anstieg ist damit erklärbar, dass entsprechende E-Mails mit erpresserischem Inhalt in sehr großer Anzahl (wie bei sogenannten SPAM-Mails) versandt wurden.

Das Bundeskriminalamt rät allen Empfängern dieser E-Mails, diese nicht zu beantworten und auf keinen Fall zu bezahlen oder sonstigen Aufforderungen nachzukommen. *Öffnen Sie keine E-Mail Anhänge von unbekannten Absendern und öffnen Sie keinen Link. Falls Sie einen Bildschirm mit integrierter Kamera haben, verwenden Sie einen Webcamblocker. Sollten Sie bereits Kontakt zu den Absendern aufgenommen haben, so brechen Sie diesen sofort ab. Im Falle einer bereits geleisteten Zahlung erstatten Sie eine Anzeige auf einer Polizeiinspektion. Nehmen Sie dafür alle relevanten Dokumente mit.*

1.4 Cyber Lage Landesverteidigung

Neben den physischen Domänen Land, Luft, Meer und Weltraum hat durch die technologischen Entwicklungen und die globale digitale Vernetzung vor allem der Cyber Raum als immaterielle Domäne im militärischen Bereich massiv an Bedeutung gewonnen.

In keinem militärischen Konflikt der Gegenwart und Zukunft, aber auch im „Graubereich“ zwischen Krieg und Frieden „Hybride Konflikte“, wird auf das Erzielen von Wirkung im Cyber Raum verzichtet. Besonders hervorzuheben ist, dass im Cyber Raum die Attribution von defensiven und offensiven Handlungen verschleiert werden kann. Das kann die (verdeckte) Durchsetzung strategischer und militärstrategischer Zielsetzungen zusätzlich begünstigen.

Für das BMLV bedeutet dies, sich im Sinne der Kernaufgabe des Österreichischen Bundesheeres, festgelegt im § 2 lit.a. Wehrgesetz, bestmöglich auf die militärische Landesverteidigung im Cyber Raum auszurichten und darauf vorzubereiten. Das umfasst sowohl alle Maßnahmen der Informations- und Kommunikationstechnologie-Sicherheit (IKT), als auch alle Maßnahmen zur Abwehr von souveränitätsgefährdenden Cyber Angriffen auf die militärischen IKT-Systeme.

Generell können aus den Erfahrungswerten des vergangenen Jahres folgende Trends abgeleitet werden:

- Gleichbleibende hohe Anzahl an automatisierten Angriffen auf Netzwerkebene,
- Weniger verbreitete Nutzung von fortgeschrittener Malware, dafür professionelleres Social Engineering via E-Mail und großflächigere Angriffe,
- Anstieg an erkannten Schwachstellen auf Hardwareebene,
- Weniger politisch motivierte Aktivitäten.

Border Protection

Aus den Daten der Sicherheitssysteme des BMLV lassen sich bisher bekannte Trends unverändert fortführen. So konnte auf Netzwerkebene in den Sicherheitseinrichtungen weiterhin ein wachsender Anstieg an Zugriffen beobachtet werden, die durch eigene Sicherheitsmaßnahmen geblockt wurden. Diese werden vor allem durch automatisierte Angriffe und Scans verursacht. Wie bereits im Jahr 2018 ist auch für das kommende Jahr mit einem weiteren Anstieg in dieser Form zu rechnen.

Angriffe per E-Mail

Im Vergleich zur vorhergehenden Zeitperiode konnten vergleichsweise weniger Angriffe mit speziell zugeschnittener Malware festgestellt werden. Dafür kam es in dieser Hinsicht zu mehr großflächig angelegten Angriffen über E-Mail-Anhänge wie z. B. mit dem weit verbreiteten Emotet-Schadcode [2].

Schwachstellen

Bei den Beobachtungen in Bezug auf Schwachstellen, die in diesem Jahr veröffentlicht wurden, konnte festgestellt werden, dass es vor allem auf der Hardwareebene zu einem Anstieg an neu erkannten Schwachstellen kam. Probleme bei diesen stellen unter anderem die begrenzten Behebungsmöglichkeiten dar, welche bis zum Austausch der kompletten Hardware reichen können.

Ausblick

In der Zukunft wird mit einem weiteren Anstieg an automatisierten Angriffen gerechnet. Die Trendannahme, vor allem beim Angriffsvektor E-Mail in Richtung automatisierter Personalisierung, hat sich bestätigt und ist auch für das nächste Jahr anzunehmen. Dies bedeutet, dass die Angreifer sich nicht nur als bekannte Services (Bank, Post, Rechnungen, etc.) ausgeben, sondern auch deutlicher Bezug auf das Unternehmen bzw. die Personen selber nehmen bzw. verstärkt nehmen werden.

---

2 Emotet-Schadcode: An die E-Mail ist eine manipulierte Word-Datei angehängt, welche mit dem Öffnen und dem Aktivieren der Makros die eigentliche Schadsoftware unsichtbar im Hintergrund nachlädt und installiert. (Quelle: heise.de)

2 Internationale Entwicklungen

In den letzten Jahren wurden Fragen der Cyber Sicherheit von zahlreichen internationalen Organisationen und multilateralen Foren aufgenommen und teilweise sehr kontroversiell diskutiert. Die relevanten außenpolitischen Maßnahmen werden vom Bundesministerium für Europa, Integration und Äußeres (BMEIA) koordiniert. Im Bereich der Europäischen Union wird das Thema Cyber Sicherheit vom Bundeskanzleramt koordiniert.

Die rasanten Entwicklungen im Cyber Bereich werfen eine Reihe fundamentaler Fragen in Bezug auf Grund- und Menschenrechte auf. Im Allgemeinen setzt sich Österreich auf internationaler Ebene für ein freies Internet ein, wobei die Ausübung aller Menschenrechte auch im virtuellen Raum gewährleistet werden soll. 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

Die Europäische Kommission und die Hohe Vertreterin schlugen letztes Jahr ein breit angelegtes Maßnahmenpaket zur Erhöhung der Cyber Sicherheit in der EU vor. Damit sollten in Europa die richtigen Instrumente zur Verfügung stehen, um die sich ständig verändernde Bedrohung durch Cyber Kriminalität zu bewältigen. Im Jahr 2018 wurden die verschiedenen Teile des Cyber Maßnahmenpakets in den Cyber Sicherheitsgremien intensiv diskutiert und zum Teil bereits verabschiedet. Die wichtigsten Aktivitäten werden in Folge dargestellt.

2.1.1 Umsetzung der NIS-Richtlinie

Der wohl wichtigste Teil des Maßnahmenpakets ist die Umsetzung der Richtlinie zur Netz- und Informationssicherheit (NIS), ein Rechtsakt, der bereits im August 2016 verabschiedet wurde. Abschreckung, Abwehrfähigkeit und Reaktion der EU bei Cyber Angriffen sollen dabei mit einem Ausbau der Cyber Sicherheitskapazitäten, einer verstärkten Zusammenarbeit auf EU-Ebene, Maßnahmen für die Risikoverhütung und ein Umgang mit Cyber Vorfällen verhindert werden.

Die europäische NIS-Richtlinie wurde beginnend mit Mai 2018 durch nationale Legislativen in Kraft gesetzt. Ab diesem Zeitpunkt sind konkrete Umsetzungen in den

Mitgliedstaaten gemäß Vorgaben der NIS-Richtlinie fällig, wie etwa das Einrichten von NIS-Behörden und zentralen Anlaufstellen, das Vorgeben von Sicherheitsmaßnahmen, das Vereinbaren von Meldeverpflichtungen und die Auswahl und Verständigung der Betreiber wesentlicher Dienste.

2.1.2 Ordnungspolitische Vorschläge für Cyber Sicherheit

Neben der NIS-Richtlinie werden zwei weitere Rechtsakte von der Kommission vorgeschlagen, die auf eine Verbesserung der Zusammenarbeit zwischen der Kommission und den Mitgliedstaaten abzielen.

Der Rechtsakt zur Cyber Sicherheit soll einerseits die Agentur der Europäischen Union für Cyber Sicherheit stärken, andererseits einen unionsweiten Zertifizierungsrahmen einrichten, der die Cyber Sicherheit von Produkten und Dienstleistungen innerhalb der EU gewährleisten soll. Das Europäische Parlament, der Rat und die Europäische Kommission haben am 10. Dezember 2018 unter österreichischer Ratspräsidentschaft eine politische Einigung über den Rechtsakt zur Cyber Sicherheit erzielt.

Der zweite Rechtsakt ist eine Verordnung zur Bündelung von Ressourcen und Fachwissen in Forschung und Innovation mit dem Ziel, in Europa eine Führungsrolle in der Cyber Sicherheit der nächsten Generation und bei digitalen Technologien zu übernehmen. Der Vorschlag wurde am 12. September 2018 an die Ratsarbeitsgruppe HWP Cyber und an den ITRE-Ausschuss des Europäischen Parlaments zur Verhandlung übergeben. Zieltermin für eine politische Einigung ist 2019.

2.1.3 EU-Agentur für Cyber Sicherheit

Mit den neuen Vorschriften erhält die EU-Agentur für Cyber Sicherheit (ENISA) ein ständiges Mandat und eine Erweiterung ihres Leistungsspektrums. Dazu zählen neue Aufgaben zur Unterstützung der Mitgliedstaaten, der EU-Institutionen und sonstiger Interessensträger in Fragen der Cyber Sicherheit. Sie wird die EU-Politik zur Cyber Sicherheitszertifizierung unterstützen und eine zentrale Rolle bei der Ausarbeitung der Zertifizierungssysteme spielen. Sie wird die Einführung des neuen Zertifizierungssystems fördern und eine Website mit Informationen über die Zertifikate einrichten. ENISA wird auch weiterhin regelmäßig Cyber Sicherheitsübungen auf EU-Ebene organisieren, einschließlich einer großen umfassenden Übung alle zwei Jahre. Ein Netz nationaler Verbindungsbeamter wird dazu beitragen, den Informationsaustausch zwischen der ENISA und den Mitgliedstaaten zu erleichtern.

2.1.4 Zertifizierungsrahmen für die Cyber Sicherheit

Der EU-weit geltende europäische Zertifizierungsrahmen für die Cyber Sicherheit von IKT-Produkten, Prozessen und Dienstleistungen soll die Sicherheit von vernetzten Produkten, von Geräten des Internets der Dinge und von kritischen Infrastrukturen mithilfe von Zertifikaten erhöhen.

Dank dieses Rahmens werden Sicherheitsmerkmale bereits in der Frühphase der technischen Konzeption und Entwicklung berücksichtigt. Außerdem gibt der Rahmen den Nutzern die Möglichkeit, sich über das Sicherheitsniveau zu vergewissern, und gewährleistet, dass diese Sicherheitsmerkmale von unabhängiger Seite überprüft werden.

2.1.5 Netz nationaler Koordinierungszentren und Europäisches Kompetenzzentrum

Das Netz von nationalen Koordinierungszentren sowie das Europäische Kompetenzzentrum für Cyber Sicherheit in Industrie, Technologie und Forschung unterstützt bereits bestehende EU-Initiativen und baut neue europäische Kapazitäten im Cyber Bereich auf.

Mit einem Europäischen Kompetenzzentrum soll die Verwendung der für Cyber Sicherheit bestimmten Mittel für die Jahre 2021-2027 aus den Programmen „Digitales Europa“ und „Horizont Europa“ koordiniert werden. Das Zentrum wird das Netz nationaler Koordinierungszentren und die Kompetenzgemeinschaft unterstützen und Forschung und Innovation im Bereich Cyber Sicherheit vorantreiben. Ferner wird es gemeinsame Investitionen der EU, der Mitgliedstaaten und der Industrie organisieren.

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

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

2.1.6 Koordinierte Reaktion auf große Cyber Sicherheitsvorfälle und -krisen (Blueprint)

Ziel von Blueprint ist es, durch Festlegung von geeigneten Prozessen in der EU, eine schnelle und koordinierte Reaktion auf großangelegte Cyber Angriffe sicherzustellen.

2018 wurden diesbezüglich mehrere Workshops und Veranstaltungen durchgeführt, um Prozesse und Abläufe festzulegen. Im CSIRTs-Netzwerk und bei Europol werden 2019 neue Krisenmanagementprozesse verabschiedet und die integrierten Maßnahmen der EU für Krisenreaktionen überarbeitet. Bei der Cyber Sicherheitskonferenz in Sofia ist Blueprint das Hauptthema. Die bulgarische Ratspräsidentschaft verabschiedet Ratschlussfolgerungen zu Blueprint und in der NIS-Kooperationsgruppe wird ein gemeinsames Taxonomiesystem für Cyber Angriffe erarbeitet, um die unterschiedlichen Mechanismen der Krisenprozesssteuerungen in Blueprint zusammenzubringen.

Die Abläufe von Blueprint sind Gegenstand von speziellen Übungen und werden in Zukunft bei allen weiteren europaweiten Krisenübungen eine wichtige Rolle spielen.

2.1.7 Cyber Diplomatie

Bei der Cyber Diplomacy-Toolbox (Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyber Aktivitäten, siehe letzten Cyber Bericht) wurden 2018 wichtige Erweiterungen zur praktischen Umsetzung vorgenommen. So wurde im Oktober 2018 mit der Erarbeitung von Parametern für ein Cyber Sanktionenregime begonnen. Da man im Bereich Cyber Sicherheit nicht, wie zu anderen Themen, auf internationale Verträge oder Organisationen aufbauen kann, war hier wichtige Grundlagenarbeit zu leisten, die 2019 fortgesetzt wird. Weitere Diskussionen umfassten das Thema der Zurechnung von Cyber Angriffen und einer koordinierten europäischen Vorgangsweise dazu bei schweren Vorfällen auf Grundlage der Cyber Diplomacy Toolbox. Zurechnung/Attribuierung ist grundsätzlich eine souveräne, politische Entscheidung jedes Mitgliedstaates. Eine Zurechnung ist nicht für alle in der Cyber Diplomacy Toolbox enthaltenen Maßnahmen eine Voraussetzung.

Ein wichtiger Teil der Cyber Diplomatie auf EU-Ebene umfasst die Erarbeitung gemeinsamer Positionen und Strategien zu Cyber Themen auf internationaler Ebene, vor allem bei den Vereinten Nationen, wo 2018 wichtige Weichenstellungen im Normensetzungsbereich getroffen wurden (siehe VN-Kapitel).

2.1.8 Cyber Sicherheit bei den Europäischen Parlamentswahlen

Die Vorbereitung der im Jahr 2019 stattfindenden Europäischen Parlamentswahlen wurden schon 2018 aus dem Blickwinkel der Cyber Sicherheit begonnen. Damit begegnet man der Gefahr von Störungen und Manipulationen, die noch nie so groß waren wie heute. Wahlvorschriften sollen an das digitale Zeitalter angepasst werden, um die Demokratie in Europa zu schützen.

Die Behörden der EU-Mitgliedstaaten sollen technische und organisatorische Maßnahmen treffen, um sich gegen Gefahren für die Sicherheit von Netz- und Informationssystemen

zu wappnen, die für die Organisation von Wahlen zum Europäischen Parlament genutzt werden. Ein in der Kooperationsgruppe erarbeitetes Kompendium für Netz- und Informationssicherheit stellt solche Leitlinien zum Schutz vor Cyber Bedrohungen im Umfeld von Wahlen zu Verfügung. Die darin enthaltenen Sicherheitsvorkehrungen sollen national implementiert werden, um die Wahlsysteme widerstandsfähiger zu machen. Eine Übung für alle Mitgliedstaaten kurz vor den Wahlen soll Umsetzungen nochmals testen.

2.1.9 ECSO-cPPP

Die Europäische Kommission und Akteure des Cyber Sicherheitsmarkts, die von der Europäischen Cyber Sicherheitsorganisation (ECSO) vertreten werden, gründeten 2016 eine vertragliche öffentlich-private Partnerschaft (cPPP) für Cyber Sicherheit.

Der Vertrag zwischen der Europäischen Union und ECSO wurde am 5. Juli 2016 unterzeichnet. ECSO ist sowohl eine Implementierungsmaßnahme der Cyber Sicherheitsstrategie für die Europäische Union von 2013, als auch eine Umsetzungsinitiative der EU-Strategie für einen digitalen Binnenmarkt.

Die ECSO ist eine „Vereinigung ohne Gewinnerzielungsabsicht", die sich vollständig selbst finanziert. Zu den Mitgliedern zählen europäische Großunternehmen, KMUs, Forschungszentren, Hochschulen, sowie lokale, regionale und nationale Verwaltungen aus der EU und dem Europäischen Wirtschaftsraum (EWR), der Europäischen Freihandelsassoziation (EFTA) und den mit dem Programm Horizont 2020 assoziierten Ländern.

Mehrere österreichische Organisationen und Forschungseinrichtungen sind Mitglieder und nehmen an den verschiedenen Gremien und Arbeitsgruppen der ECSO teil. Das Bundeskanzleramt trat am 22. März 2017 der ECSO bei und nahm fortan an den ECSO-Treffen der öffentlichen Verwaltung, der sogenannten ECSO-NAPAC-Group (National Public Authority Representatives Commitee), teil. Im Rahmen der Ratspräsidentschaft wurde in der zweiten Hälfte 2018 der Vorsitz in dieser Gruppe übernommen.

Aus den sehr vielen Aktivitäten 2018 anbei einige Themen und Highlights: Netzwerk europäischer Sektor ISACs, Teilnahme und Rolle der ECSO in der zukünftigen NCCC, Cyber Zertifizierung in Europa, Prioritäten für EU-Standards im Bereich Cyber Sicherheit, Zusammenarbeit mit Standardorganisationen, Marktradar zum Aufsetzen gezielter Initiativen im Bereich Cyber Sicherheit, Synergien mit Staaten der Dritten Welt, Berichte verschiedener Sektoren (Industrie 4.0, Gesundheit, Smart-Cities, Energie), Zugang zu Märkten und Finanzen, Entwicklungspläne für regionale Märkte, Cyber Ranges, Analyse von Lücken in der Aus/Weiterbildung und im professionellen Training, Förderung der Rolle der Frau im Bereich Cyber Sicherheit, Prioritäten für künftige Forschungsprogramme, technische Papiere zu künstlicher Intelligenz, Internet der Dinge, Blockchain, Synergien zwischen Cyber Sicherheit und Cyber Verteidigung.

2.1.10 Programm „Digitales Europa“ 2021–2027

Im Sommer 2018 schlug die Europäische Kommission eine Verordnung für das Programm „Digitales Europa“ zur Maximierung der Vorteile des digitalen Wandels für alle europäischen Bürger, öffentlichen Verwaltungen und Unternehmen vor.

Das Programm „Digitales Europa“ ist ein umfangreiches Investitionsprogramm für die Strategie des digitalen Binnenmarkts und gehört zu dem mehrjährigen Finanzrahmen der EU für den Zeitraum 2021–2027. Es ist auf die operativen Erfordernisse des Kapazitätsaufbaus in den Bereichen Hochleistungsrechnen, künstliche Intelligenz, Cyber Sicherheit und fortgeschrittene digitale Kompetenzen sowie deren breite Nutzung in der gesamten Wirtschaft und Gesellschaft zugeschnitten.

Für den Bereich Cyber Sicherheit sind alleine 2 Milliarden Euro vorgesehen. Damit soll die Kapazität für Cyber Sicherheit in der EU gestärkt, die Bürger vor Cyber Bedrohungen geschützt, neueste Cyber Sicherheitslösungen gefördert und Kompetenzen zusammengeführt werden, um eine ausreichende Kapazität und Exzellenz in der EU zu erreichen.

2.1.11 Kampf terroristischer Inhalte im Internet

Die anhaltende Präsenz terroristischer Inhalte im Internet stellt eine ernste Gefahr für die Bürger und die gesamte Gesellschaft dar. Der Schaden, der durch sie entstehen kann, wird dadurch verschlimmert, dass sie sich rasch über Plattformen hinweg verbreiten.

Die Kommission schlug 2018 ein neues Konzept mit klaren und transparenten Regeln vor, um sicherzustellen, dass wie folgt gehandelt wird, wenn terroristische Inhalte ermittelt werden:

- Inhalte werden so rasch wie möglich entfernt,
- Online-Plattformen treffen Maßnahmen, um sicherzustellen, dass ihre Dienstleistungen nicht missbraucht und entfernte Inhalte nicht anderweitig wieder hochgeladen werden können,
- Grundrechte auf Meinungs- und Informationsfreiheit werden umfassend geschützt.

Dazu gibt es verschiedene Maßnahmen für die Anbieter von Hosting-Diensten, für die Mitgliedstaaten und für Europol.

2.1.12 Aktionsplan gegen Desinformation

Das Recht auf freie Meinungsäußerung ist ein zentraler Wert der EU. Für offene demokratische Gesellschaften ist es entscheidend, dass Bürger Zugang zu einer Vielzahl überprüfbarer Informationen haben und sich somit zu verschiedenen politischen Themen eine Meinung bilden können. Dies erlaubt es den Bürgern, in Kenntnis der Sachlage an

öffentlichen Debatten teilzunehmen und ihren Willen in freien und fairen politischen Prozessen zum Ausdruck zu bringen. Die bewusste, umfassende und systematische Verbreitung von Desinformation kann zu Bedrohungen für die demokratischen Prozesse sowie für öffentliche Güter wie Volksgesundheit, Umwelt und Sicherheit führen.

Im Vorfeld der Wahlen zum Europäischen Parlament wird mit einer Zunahme ständiger gezielter Desinformationskampagnen gegen die EU, ihre Organe und ihre Politik gerechnet. Die schnelle Veränderung der eingesetzten Instrumente und Techniken macht eine ebenso schnelle Weiterentwicklung der Reaktion darauf erforderlich. Insgesamt setzen staatliche Akteure zunehmend Desinformationsstrategien ein, um gesellschaftliche Debatten zu beeinflussen, Spaltungen herbeizuführen und in die demokratische Entscheidungsfindung einzugreifen.

Aus diesem Grund nahm das EK-Kollegium im Dezember 2018 einen Aktionsplan gegen Desinformation an. Der Europäische Rat forderte auf, den Aktionsplan umgehend umzusetzen.

Der Aktionsplan sieht verschiedene Maßnahmen in vier Bereichen vor. Dazu gehören (1) der Ausbau der Fähigkeiten der Organe der Union Desinformation zu erkennen, zu untersuchen und zu enthüllen, (2) koordinierte und gemeinsame Maßnahmen gegen Desinformation, (3) die Mobilisierung des Privatsektors bei der Bekämpfung von Desinformation und (4) die Sensibilisierung der Gesellschaft und Ausbau ihrer Widerstandsfähigkeit. Jeder der Bereiche besteht aus mehreren Maßnahmen.

Der Aktionsplan wird 2019 in den zuständigen Ratsarbeitsgruppen diskutiert und soll bereits mithelfen, die Wahlen zum Europäischen Parlament sicher zu machen.

2.2 Österreichische Ratspräsidentschaft Cyber Sicherheit

Österreich hatte sich für die Ratspräsidentschaft im Hinblick auf Cyber Sicherheit viel vorgenommen. Ein ambitioniertes gemeinsames Arbeitsprogramm (Trio Presidency Cyber Security Arbeitsprogramm) mit den beiden anderen Trio-Präsidenten Estland und Bulgarien wurde auf Betreiben von Österreich aufgesetzt. Dieses Programm diente als Leitfaden während eineinhalb spannender Jahre einer gemeinsamen Trio-Ratspräsidentschaft und der österreichischen Verantwortung in der 2. Jahreshälfte 2018. In dieser Zeit hatte Österreich den Vorsitz in den wichtigsten Cyber Sicherheitsgruppen in der Europäischen Union übernommen. Die österreichische Bilanz ist äußerst positiv, was viele Mitgliedsländer bestätigt haben.

Österreich ist es gelungen, alle Prioritäten aus dem Trio-Arbeitsprogramm sowie die Aktivitäten aus den Arbeitsprogrammen der Vorsitzgremien/-gruppen vollumfänglich und vollinhaltlich umzusetzen.

Als Beispiel für die österreichischen Ergebnisse während der Ratspräsidentschaft seien die Cyber Sicherheitskonferenzen und ausgewählte europäische Cyber Sicherheitsgruppen dargestellt:

2.2.1 Cyber Sicherheitskonferenzen

Insgesamt wurden drei Konferenzen durch den österreichischen Vorsitz im Rat der Europäischen Union organisiert:

- Im Rahmen des österreichischen Vorsitzes im Rat der Europäischen Union 2018 und als Abschluss des Trio-Ratsvorsitzes Estland-Bulgarien-Österreich organisierte und veranstaltete das Bundeskanzleramt eine Cyber Sicherheitskonferenz in Österreich. Diese fand am 3. und 4. Dezember 2018 im Austria Center Vienna in Wien statt. Das Ziel der Konferenz war, eine Bestandsaufnahme zu den Entwicklungen der letzten 18 Monate im Bereich Cyber Sicherheit durchzuführen, und damit das Bewusstsein für Cyber Resilienz in Europa, sowohl auf technischer als auch operativer Ebene, zu stärken.
- Die österreichische Vertretung in Brüssel organisierte ergänzend zwei Sektorenkonferenzen zum Thema Cyber Sicherheit. „Finanzen 5.0 – eine Herausforderung für Cyber Sicherheit?“ (gemeinsam mit der Österreichischen Nationalbank) am 16. Juli 2018 und „Cyber Sicherheit im Energiebereich“ (gemeinsam mit der Europäischen Kommission und dem Institut der deutschen Wirtschaft) am 11. Oktober 2018. Beide fanden in Brüssel statt.

2.2.2 Horizontal Working Party on Cyber Issues

Um die Bedeutung von Cyber Sicherheit in der digitalen und vernetzten Welt des 21. Jahrhunderts zu unterstreichen, wurde 2012 die Gruppe „Friends of Presidency on Cyber Issues“ eingeführt und 2016 in eine Ratsarbeitsgruppe mit ständigem Charakter umgewandelt (Horizontal Working Party on Cyber Issues – HWPCI oder HWP Cyber). Die HWP Cyber ist für alle Angelegenheiten der Cyber Politik zuständig, sie koordiniert strategisch und horizontal die grenzüberschreitende und multidisziplinäre Querschnittsmaterie „Cyber Sicherheit“. Seitdem sie den Status einer Ratsarbeitsgruppe hat, behandelt sie auch Legislativvorhaben.

In der Ratsarbeitsgruppe HWP Cyber kann der österreichische Vorsitz in seiner Präsidentschaft unter anderem Folgendes festhalten:

- Der Rat unter österreichischem Vorsitz, das Europäische Parlament und die Europäische Kommission haben am 10. Dezember 2018 eine politische Einigung über den Rechtsakt zur Cyber Sicherheit (Cybersecurityact) erzielt, mit dem das Mandat der EU-Cyber Sicherheitsagentur gestärkt und ein EU-Rahmen für die Cyber Sicherheitszertifizierung geschaffen wird.
- Der VO-Vorschlag NCCC (Einrichtung des Europäischen Kompetenzzentrums für Cyber Sicherheit in Industrie, Technologie und Forschung und des Netzes nationaler Koordinierungszentren) wurde nach Vorlage am 12. September 2018 in der Ratsarbeitsgruppe HWP Cyber verhandelt. Unter österreichischem Vorsitz konnte bereits ein großer Fortschritt erzielt werden.
- Das Projekt zur Erstellung einer „EU-Institutional Cyber Map“, eine Darstellung aller EU-Institutionen und Gremien, die mit Cyber Sicherheit zu tun haben, wurde mit Unterstützung der ENISA umgesetzt. Die offizielle Vorstellung der Cyber Map erfolgte im Rahmen der Cyber Sicherheitskonferenz in Wien.
- Auch das Projekt „Cyber Resilience“ wurde mit Unterstützung der ENISA umgesetzt. Die Vorarbeiten haben in der NIS-Kooperationsgruppe in Form einer Umfrage begonnen. Das erstellte Referenzdokument diente als Grundlage für die Erstellung von Ratsschlussfolgerungen.
- Im Bereich der Cyber Diplomatie stand die Weiterentwicklung der gemeinsamen diplomatischen Reaktion der EU auf böswillige Cyber Aktivitäten “Cyber Diplomacy Toolbox” im Vordergrund. Hierzu fand Ende November eine Table-Top-Exercise „CYBER-DIPLO-ATTX-18“ statt. Auch das Erreichen einer gemeinsamen EU-Position hinsichtlich internationaler Entwicklungen von Cyber Sicherheit wie beispielsweise im VN-Kontext oder hinsichtlich eines möglichen Cyber Sanktionenregimes bzw. Diskussionen zur Attribuierung standen im Fokus. Die Abhaltung eines technischen Workshops für Delegierte konnte unter österreichischem Vorsitz ebenfalls organisiert werden.

2.2.3 NIS-Kooperationsgruppe

Mit Verabschiedung der EU-Richtlinie 2016/1148 (NIS-Richtlinie), wurde eine NIS-Kooperationsgruppe eingesetzt. Diese dient der Unterstützung und Erleichterung der strategischen Zusammenarbeit sowie des Informationsaustausches zwischen den Mitgliedstaaten. Die Kooperationsgruppe setzt sich aus Vertretern der Mitgliedstaaten, der Kommission und der ENISA zusammen. Die Kooperationsgruppe nimmt ihre Aufgaben auf der Grundlage von zweijährigen Arbeitsprogrammen wahr. Den Vorsitz hat die jeweilige Ratspräsidentschaft.

In der „NIS-Kooperationsgruppe“ (KG) kann der österreichische Vorsitz unter anderem Folgendes festhalten:

- Beim Thema Cyber Resilience aus dem „Trio Presidency Cyber Security Arbeitsprogramm“ wurde eine der größten Umfragen bezüglich Cyber Sicherheit in der EU durchgeführt. Die aufbereiteten Ergebnisse dienen einerseits als Basis für Schlussfolgerungen zum Thema Cyber Robustheit in der EU, andererseits als Best Practice Hilfestellung für die Mitgliedstaaten, eigene Umsetzungen zu optimieren.
- Etliche Referenzdokumente aus der NIS-Kooperationsgruppe wurden verabschiedet und veröffentlicht. Dazu gehören unter anderem die Identifizierung von Betreibern wesentlicher Dienste, grenzübergreifende Konsultationsprozesse, Sicherheitsmaßnahmen, Meldepflicht von Vorfällen, verpflichtender Informationsaustausch zwischen den Mitgliedstaaten, grenzüberschreitende Abhängigkeiten und wie man diese managen kann, Cyber Sicherheit der Wahltechnologie. Die Ergebnisse kann man auf der KG-Webseite abrufen.
- Neue Arbeitsgruppen wurden unter österreichischer Führung gestartet: Die Arbeitsgruppe „Sektorspezifische Aspekte mit dem Schwerpunkt Energie“ soll nationale und europäische Erfahrungen im Sektor Energie zusammenbringen. Die Arbeitsgruppe „Cyber Sicherheit Kapazitäten in der EU“ hat ein Referenzdokument über Cyber Kapazitäten in der EU zum Ziel. Die Arbeitsgruppe „Große Cyber Vorfälle und Krisen“ wurde im Hinblick auf die künftigen Rollen der nationalen Anlaufstellen im europäischen Krisenfall neu aufgesetzt.
- Sehr wichtig war die Herausgabe eines Berichts der NIS-Kooperationsgruppe. Er brachte ein erstes Feedback über die Qualität der Arbeit in der Kooperationsgruppe. Das Umgehen mit den Erkenntnissen aus dem Bericht war ein Schwerpunktthema der österreichischen Präsidentschaft, erste Umsetzungsaktivitäten wurden bereits gestartet.
- Der österreichische Vorsitz hat die strategisch orientierte Kooperationsgruppe und das operativ tätige CSIRTs-Netzwerk zu einem Back to Back-Meeting nach Wien eingeladen. In einer gemeinsamen Sitzung wurden die wichtigsten Themen dieser Gruppen diskutiert. Ein regelmäßiger funktioneller Austausch wurde in die Wege geleitet. Diese gemeinsamen Meetings werden auch in Zukunft stattfinden.

- Der Schwerpunkt der NIS-Kooperationsgruppe liegt auf Aktivitäten im Zusammenhang mit der Umsetzung der europäischen NIS-Richtlinie. Dieses Thema steht im Mittelpunkt jedes Treffens. Hier hat der österreichische Vorsitz Wert darauf gelegt wichtige Themen rechtzeitig zu adressieren. Unsere Aktivität hat mitgeholfen, dass nahezu alle EU-Mitgliedstaaten die NIS-Richtlinie bereits in nationales Recht umgesetzt haben. Damit gibt es ab 2019 erstmals eine harmonisierte Rechtsgrundlage für Cyber Sicherheit in der gesamten EU.
- Eines der Ziele der Trio-Präsidentschaft war das Näherzusammenrücken aller europäischen Gruppen, die sich mit Cyber Sicherheit befassen, um Synergien zu nutzen. Unter österreichischem Vorsitz wurde konsequent in allen Gruppen ein regelmäßiger Informationsaustausch eingerichtet und gegengleich über Aktivitäten berichtet. Alle diese Gruppen werden in Zukunft komplementär wirken, um Doppelgleisigkeiten zu vermeiden.

2.2.4 CSIRTs-Netzwerk

Die EU-Richtlinie 2016/1148 (NIS-Richtlinie) hat das CSIRTs-Netzwerk (CNW) als Kooperationsplattform bestehend aus Vertretern der CSIRTs der Mitgliedstaaten und des CERT-EU ins Leben gerufen.

Die initialen Vorbereitungsschritte für das Netzwerk wurden durch die niederländische Ratspräsidentschaft gesetzt. Der offizielle Start des CNW erfolgte dann 2017 während der Ratspräsidentschaft von Malta. Ebenso wurde durch Malta die initiale Geschäftsordnung des CNW beschlossen, die den Vorsitz des CNW analog zum Vorsitzland der EU-Ratspräsidentschaft vergab.

Den österreichischen CSIRTs, die am Netzwerk teilnehmen, kam daher während der Ratspräsidentschaft von Österreich eine besondere Rolle zu. Folgende Aktivitäten wurden gesetzt:

- Intensive Mitarbeit in den verschiedenen Arbeitsgruppen des CSIRTs-Netzwerks. In den Arbeitsgruppen ging es um Themen wie Werkzeuge (z. B. Software für CSIRTs) für das Netzwerk oder die Prozesse zur Zusammenarbeit zwischen CSIRTs der Mitgliedstaaten.
- Als Teil des Trios (Estland-Bulgarien-Österreich) wurde schon vor der offiziellen Übernahme des Vorsitzes des CNW durch Österreich an der Agenda des Netzwerkes mitgearbeitet.
- In der Rolle des österreichischen Vorsitzes des CNW wurde:
  - der Arbeitsplan des CNW aktualisiert,
  - der in der NIS-Richtlinie vorgeschriebene Bericht des CNW an die NIS-Kooperationsgruppe erstellt, inhaltlich abgestimmt und übergeben,

  - nach einem langen und intensiven Prozess wurde die initiale Geschäftsordnung des CNW grundlegend überarbeitet und durch die Mitglieder des CNW verabschiedet.
- Im November 2018 wurde in Wien zum ersten Mal eine gemeinsame Session des CNW und der NIS-Kooperationsgruppe, während überlappender Arbeitssitzungen der beiden Gruppen, erfolgreich abgehalten. Dieses Format hat die Zusammenarbeit zwischen der NIS-Kooperationsgruppe, welche sich um strategische Agenden der NIS-Implementierung kümmert und den operativ-technischen CNW auf eine neue Ebene gehoben.
- Es ist auch gelungen, erstmals CSIRTs aus der Schweiz und aus Norwegen als Gäste zu den Treffen des CNW einzuladen.

Die Teilnehmer Österreichs im CSIRTs-Network sind CERT.at, das GovCERT Austria und das CERT der Energiewirtschaft Austrian Energy (AEC).

2.3 Vereinte Nationen

Die Frage der Informationssicherheit steht seit 1998 auf der Agenda der Vereinten Nationen, als erstmalig eine Resolution im 1. Komitee (Abrüstung und internationale Sicherheit) der Generalversammlung (VN-GV) verabschiedet wurde. In diesem Zusammenhang wurden seit 2004 “Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security” (GGE) eingerichtet. Die fünfte dieser Expertengruppen widmete sich 2016/17 den existierenden und potentiellen Bedrohungen der internationalen Sicherheit im Bereich Informationssicherheit und Maßnahmen, diesen zu begegnen, inklusive Normen, Regeln und Prinzipien über das verantwortungsvolle Verhalten von Staaten, vertrauensbildende Maßnahmen und Fähigkeitenentwicklung. Diese Expertengruppe konnte sich aufgrund großer Differenzen vor allem zu Fragen des Völkerrechts und dessen Anwendbarkeit im Cyber Space auf keinen Konsensbericht einigen. Nachdem auch die Frage der Fortführung der Arbeit der Expertengruppe 2017 vertagt wurde, kam es 2018 im 1. Komitee zu einer Spaltung, als die Russische Föderation (RU) und die Vereinigten Staaten (US) konkurrierende Resolutionsentwürfe zum weiteren Vorgehen vorlegten. Während der US-Entwurf größtenteils dem – bislang von RU präsentierten – letzten GGE-Mandat mit 25 Experten entsprach, schlug RU die Einrichtung einer offenen Arbeitsgruppe „Open-Ended-Working-Group“ unter Teilnahme aller VN-Mitgliedstaaten, allerdings mit schwierigen inhaltlichen Vorentscheidungen vor. Letztlich wurden beide Resolutionen von der VN-Generalversammlung angenommen, womit nun zwei parallele Prozesse ab der 2. Jahreshälfte 2019 tagen werden. Die EU-Mitgliedstaaten, die sich gegen den RU-Ansatz aussprachen, werden sich dennoch aktiv an der Arbeit der „Open-Ended-Working-Group“ beteiligen. Österreich brachte gemeinsam mit den EU-Partnern die US-Resolution mit ein. Zudem veranstaltete Österreich gemeinsam mit Estland und dem EAD eine Veranstaltung zur Geltung des Völkerrechts im Cyber Raum.

Darüber hinaus beschäftigten sich auch andere VN-Gremien mit Cyber Themen. Aus österreichischer Sicht sind vor allem die seit 2013 laufenden Bemühungen einer Gruppe gleichgesinnter Staaten unter der Führung von Brasilien und Deutschland im 3. Komitee und im VN-Menschenrechtsrat (MRR) von besonderer Bedeutung. Die von Österreich als einem der Hauptsponsoren eingebrachte Resolution zum Recht auf Privatsphäre im digitalen Zeitalter konnte vom MRR im Konsens angenommen werden. Die Initiative wurde zuletzt im März 2017 (Res A/34/7) erfolgreich vorangetrieben und enthält neuerlich ambitionierte Elemente, damit Eingriffe in die Privatsphäre nur im Einklang mit menschenrechtlichen Prinzipien erfolgen. Seit Juli 2015 übt Joseph Cannataci das vom MRR geschaffene Mandat des VN-Sonderberichterstatters zum Thema aus. Im 3. Komitee der VN-GV brachte die Russische Föderation erstmalig eine Resolution zu Informations- und Kommunikationstechnologien (ICT/Cyber Kriminalität) ein, die nach einer Abstimmung angenommen wurde. Die Resolution beauftragt den Generalsekretär der Vereinten Nationen (VN-GS) in der 74. Generalversammlung der Vereinten Nationen (VN-GV) einen Bericht zum Vorgehen gegen den kriminellen Missbrauch von Informations- und Kommunikationstechnologien anzufertigen und beschließt die Schaffung eines neuen Tagesordnungspunktes anlässlich der 74. VN-GV "Countering the use of information and communications technologies for criminal purposes". Damit schafft die Resolution den Ausgangspunkt für eine formelle und substanzielle Behandlung dieser Fragen in der VN-GV, was bestehende Rechtsinstrumente (insbesondere die Budapest-Konvention) und die in Wien angesiedelten Prozesse ernsthaft herausfordern könnte. Die EU-Mitgliedstaaten stimmten daher geschlossen gegen die Resolution.

Cyber Kriminalität 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 Cyber Kriminalität im Sinne der 2013 veröffentlichten umfassenden Studie [3] dar und konzentriert sich dabei in seiner Hilfeleistung für betroffene Mitgliedstaaten auf folgende drei Schwerpunkte:

- Verbesserung der Ermittlung, Strafverfolgung und Beurteilung von Cyber Kriminalität, vor allem im Bereich sexueller Ausbeutung und Kindesmissbrauch im Internet, unter Einhaltung und Förderung der Menschenrechte,
- Förderung eines integrierten und regierungsweiten Ansatzes, einschließlich nationaler Koordinierung, Datenerhebung und wirksamer rechtlicher Rahmenbedingungen, zur nachhaltigen Bekämpfung und effektiven Abschreckung von Cyber Kriminalität,

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

- Stärkung der nationalen und internationalen Kooperation und Informationsaustauschmechanismen zwischen Regierungen, Strafverfolgungsbehörden und der Privatwirtschaft, sowie Stärkung des öffentlichen Bewusstseins.

Die 2010 im Bereich Cyber Kriminalität eingerichtete Intergouvernementale Expertengruppe (IEG) trat, nach Sitzungen im Jahr 2011, 2013 und 2017, von 3. bis 5. April 2018 zum vierten Mal zusammen.

Die Streitfrage, ob eine neue Cyber Konvention ausgehandelt oder die Budapest-Konvention ausgeweitet/umgesetzt werden soll, konnte nicht gelöst werden, die IEG einigte sich aber, die Diskussion darüber fortzuführen. Beschlossen wurde außerdem weiterhin, regelmäßige Sitzungen der IEG abzuhalten, um über grundlegende Themen und Entwicklungen betreffend Cyber Verbrechen zu diskutieren und sich über nationale Gesetzgebung, Best Practice Beispiele, technische Hilfe und internationale Zusammenarbeit im Hinblick auf eine Stärkung der internationalen Maßnahmen gegen Cyber Verbrechen auszutauschen. UNODC wird indes die Informationssammlung über neue Entwicklungen, Fortschritte und Best Practice Beispiele fortführen.

In diesem Zusammenhang fand in Wien im September 2018 auf Initiative einiger interessierter Staaten außerhalb des IEG-Rahmens eine internationale Konferenz zu Cyber Kriminalität statt. Aufgrund der fehlenden breiten Unterstützung für eine VN-Cyber Konvention im Rahmen der IEG, lancierte RU das Thema Cyber Kriminalität auch in der VN-Generalversammlung (siehe oben). Cyber Kriminalität war auch das Hauptthema der 27. Sitzung der Kommission für Verbrechensverhütung und Strafrechtspflege (CCPCJ) 3 im Mai 2018. Trotz dieses thematischen Schwerpunkts konzentrierten sich die Resolutionsentwürfe dieser Sitzung vor allem auf Menschenhandel, wobei der Bezug zur Cyber Kriminalität insbesondere in Res. 27/2 „Preventing and combating trafficking in persons facilitated by the criminal misuse of information and communications technologies“ und in Res. 27/3 „Improving the protection of children against trafficking in persons, including by addressing the criminal misuse of information and communications technologies“ gegeben ist.

Auf operativer Ebene setzt die UNODC Cyber Crime Abteilung neue Initiativen im Bereich der Schul- und Universitätsbildung im Rahmen des neuen Education for Justice Programm (E4J) um. In diesem Zusammenhang zeigt UNODC auch besonderes Interesse an dem von Internet Service Providers Austria (ISPA) erstellten Comic-Buch „der Online-Zoo“, das im Schulunterricht eingesetzt wird, um Kinder über die Gefahren des Internets aufzuklären und deren Online-Kompetenz zu steigern. Zu diesem Buch veranstaltete Österreich im Rahmen der 27. CCPCJ zusammen mit der UNODC-Initiative „Education for Justice“ (E4J) und El Salvador die sehr gut besuchte Nebenveranstaltung „Helping Children Stay Safe Online: Education, Initiatives and Tools“.

Was den Verkauf von illegalen Substanzen im Darknet und die Verwendung von Kryptowährungen als Zahlungsmittel im Drogenhandel angeht, machen diese Phänomene aktuell nur einen relativ geringen Prozentsatz der einschlägigen Gesamttransaktionen aus. Auch bei UNODC nimmt man aber an, dass sich dieses „Segment" des illegalen Drogenhandels in Zukunft sehr dynamisch entwickeln wird und die Bekämpfung dieser Praktiken daher von großer Bedeutung ist.

Die Internationale Atomenergiebehörde (IAEO) widmete dem Thema Cyber Sicherheit in nuklearen Einrichtungen im Jahr 2018 eine eigene Publikation mit dem Titel „Computer Security of Instrumentation and Control Systems at Nuclear Facilities", die relevanten Stellen Handlungsempfehlungen gibt, wie mit der stetig wachsenden Bedrohung umgegangen und wie Schwachstellen in den eigenen Systemen behoben werden können. Für das koordinierte Forschungsprojekt der IAEO mit 10 Mitgliedstaaten mit dem Titel „Enhancing Computer Security Incident Analysis at Nuclear Facilities", das noch bis Mitte 2019 umgesetzt wird, errichtete das Austrian Institute of Technology (AIT) eine spezielle virtuelle IT-Trainings- und Simulationsplattform, die auf hochsensible industrielle Steuerungssysteme ausgelegt ist. Mit dieser Plattform können neue Technologien, Werkzeuge und Prozesse zur Abwehr von Cyber Bedrohungen in Atomanlagen realitätsnah simuliert, getestet und trainiert werden. Im Oktober 2018 lancierte die IAEO außerdem einen „International Training Course on Protecting Nuclear Facilities from Cyber Attacks", der 37 Teilnehmerinnen und Teilnehmern aus 13 Ländern eine zweiwöchige Intensivausbildung im Bereich der „Best Practices" der Computersicherheit bot.

2.4 NATO

Als politisches Bündnis mit einem starken Fokus auf gemeinsame Verteidigung befasst sich die NATO spätestens seit der Verabschiedung ihres neuen strategischen Konzepts von 2010 und der Anerkennung des virtuellen Raumes als eine Domäne 2016 mit den Verteidigungsaspekten von Cyber Sicherheit. Österreich kooperiert hier als Partnerland eng mit der NATO. Andererseits beteiligte sich Österreich auf technischer Ebene an zahlreichen Sitzungen des NATO-C3 Boards und jenen im Zusammenhang mit einschlägigen Smart Defence-Projekten.

Österreich wurde im Februar 2015 als erster Nicht-NATO-Staat zu einer Sitzung des NATO-Cyber Defence Committee (CDC) im Format 28+1 eingeladen. Österreich hat im Rahmen der NATO-Partnership for Peace (NATO / PfP) das Partnerschaftsziel „Cyber Defence" angenommen. Die diesbezüglichen Vereinbarungen für 2015-2017 konnten von österreichischer Seite allesamt erfüllt werden. Derzeit läuft die Bearbeitung des nächsten Partnership for Peace Planning and Review Process (PARP) Zyklus.

Zusätzlich verstärkte sich die Zusammenarbeit mit der NATO seit Oktober 2013 (Technical Arrangement bis 2022) im Bereich der militärischen Landesverteidigung im Cyber Raum durch die dauerhafte Beschickung und Mitarbeit eines Offiziers des BMLV im „Cooperative Cyber Defence Center of Excellence“ (CCD COE) in Tallinn / Estland. 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.

2.5 OSZE

Die OSZE ist bisher die einzige regionale internationale Organisation, deren teilnehmende Staaten sich auf vertrauensbildende Maßnahmen im Bereich Cyber Sicherheit einigen konnten: Eine informelle Arbeitsgruppe erarbeitete 2013 einen ersten Katalog von elf Maßnahmen, um durch Transparenz und Zusammenarbeit effizienter auf Cyber Bedrohungen reagieren zu können. Im März 2016 konnten fünf weitere vertrauensbildende Maßnahmen beschlossen werden.

2014 begannen die 57 Teilnehmerstaaten zudem, sich durch einen strukturierten Austausch von Informationen gegenseitig über Entwicklungen und Probleme im Bereich der Sicherheit von Informations- und Kommunikationstechnologie auf dem Laufenden zu halten. Sie richteten Kontaktstellen für den Dialog ein und tauschten Informationen über die nationale Organisation von Cyber Sicherheitsplänen aus.

Cyber Sicherheit war auch ein Schwerpunktthema des italienischen OSZE-Vorsitzes im Jahr 2018. Am 27. und 28. September richtete Italien die OSZE Cyber Security Conference in Rom aus, die sich sowohl den internationalen Entwicklungen, insbesondere der Cyber Diplomacy, als auch der Zusammenarbeit zwischen Staat und Privaten widmete. Erstmals fand vor der Konferenz eine „scenario based discussion“ statt, bei der die Delegationen ihre Ansätze bei einer fiktiven Cyber Attacke schematisch darlegten. Die Arbeiten der Informellen Arbeitsgruppe zu Cyber Sicherheit konzentrierten sich auf die Umsetzung der beschlossenen vertrauensbildenden Maßnahmen. Vor dem Hintergrund der schwierigen internationalen Ausgangslage und insbesondere der anhaltenden Kritik Russlands an der Arbeit der Informellen Arbeitsgruppe - IWG (diese habe kaum mehr erkennbaren Mehrwert gegenüber der Arbeit in den VN) konnten jedoch keine wesentlichen Fortschritte gemacht werden.

2.6 OECD

Die „Working Party On Security and Privacy in the Digital Economy“ (SPDE) ist eine Arbeitsgruppe der OECD, die für Regierungen und nationale Stakeholder zu den The-

men Cyber Sicherheit und Privatsphäre Analysen und High-Level-Empfehlungen erstellt. Dabei wird auf die Expertise aus OECD-Ländern und Partnerregierungen, Wirtschaft, Zivilgesellschaft und der technischen Internet-Community gesetzt, um Ansätze für die Zukunft zu erarbeiten.

Die SPDE behandelt Cyber Sicherheit und Privatsphäre als komplementäre Themen, die für die Nachhaltigkeit der Internetwirtschaft als Plattform für Wohlstand unerlässlich sind. Politischen Entscheidungsträgern soll ermöglicht werden, Trends zu beobachten, Erfahrungen auszutauschen und die Auswirkungen von Technologien zu analysieren. Die SPDE trifft sich zweimal im Jahr in Paris und organisiert Workshops und Konferenzen. In Österreich nimmt das BKA die inhaltliche Koordination für diese Arbeitsgruppe wahr.

In den beiden Meetings 2018 wurden unter anderem die folgenden Themen behandelt:

- Empfehlungen für kritische Informationsinfrastruktursysteme,
- Vergleichbarkeit von Verstößen gegen den Datenschutz,
- Messung digitaler Risikomanagementpraktiken in Unternehmen,
- Internet der Dinge und künstliche Intelligenz,
- OECD-Datenschutzstrategien.

2.7 Europarat

Den Kern der Aktivitäten des Europarates im Bereich Cyber Sicherheit bildet die Konvention zu Cyber Kriminalität (Budapest-Konvention) aus 2001, die mit aktuell 62 Ratifikationen (darunter im Jahr 2018 Argentinien, Costa Rica, Kap Verde, Marokko, Paraguay und die Philippinen) eine Bedeutung weit über Europa hinaus erlangt hat. Hauptzweck ist die Verfolgung einer gemeinsamen Strafrechtpolitik zum Schutz der Gesellschaft vor Cyber Kriminalität, insbesondere durch entsprechende gesetzliche Regelungen und die Förderung internationaler Zusammenarbeit.

Die Umsetzung der Konvention wird über kapazitätsbildende Projekte unterstützt, die durch ein Cyber Crime Programmbüro des Europarates in Bukarest (C-PROC) koordiniert werden. Unter den vor allem durch außerbudgetäre Beiträge finanzierten Projekten zu erwähnen sind: Beratung bei einschlägigen Legislativmaßnahmen, Hilfe bei der Ausbildung von Richtern und Staatsanwälten, ferner das „iProceeds“ in Südosteuropa mit Fokus auf Erträgen aus Cyber Kriminalität, das „Cyber South“ in Nordafrika sowie das weltweit agierende und in Zusammenarbeit mit Interpol durchgeführte Projekt „GLACY+“. Unter Letzterem fand von 16. bis 18. Oktober 2018 das „First African Forum on Cyber Crime“ in Addis Abeba statt, an dem 50 afrikanische Staaten teilnahmen und dessen Abhaltung als eine neue Qualitätsstufe in der Zusammenarbeit gewertet wird.

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 Europäischen Union, mit Hinblick auf dort derzeit in Entwicklung befindliche relevante Dokumente, ist vorgesehen.

Des Weiteren befindet sich ein Leitfaden („Guidance Notes“) zur Thematik „election interference“ in Ausarbeitung, der für Juli 2019 erwartet wird. Derartige Leitfäden, von denen bislang neun zu verschiedenen Themen veröffentlicht wurden, haben das Ziel, die effektive Anwendung und die Umsetzung der Konvention zu erleichtern.

Zu den weiteren Entwicklungen im Bereich des Europarates im Jahr 2018 zählt die Modernisierung der Datenschutzkonvention des Europarates (ETS 108), die die ursprüngliche Konvention aus dem Jahr 1981 mit neuer Relevanz für die aktuellen Herausforderungen gerade im Online-Bereich ausstattet. Die Lanzarote-Konvention zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch leistet weiterhin einen wesentlichen Beitrag zum Online-Schutz von Kindern. So genannte „Octopus-Konferenzen” befassen sich halbjährlich mit einschlägigen Themen, im Jahr 2018 mit Attacken auf demokratische Prozesse, vor allem Wahlbeeinflussung und -manipulation über das Internet. Als Organisation mit Fokus auf Menschenrechte, Rechtstaatlichkeit und Demokratie bringt sich der Europarat auch aktiv in verschiedene internationale Diskussionen zur Internet Governance ein, vor allem im Bereich der Vereinten Nationen.

2.8 Österreich in anderen Cyber relevanten internationalen Foren

Neben den bereits genannten Foren beteiligt sich Österreich an einer Reihe weiterer internationaler Zusammenarbeitsgremien im Bereich der Cyber Sicherheit. Zu diesen zählen:

- Die „Freedom Online Coalition“ – eine von den Niederlanden im Dezember 2011 gegründete Koalition, die sich weltweit für die effektive Umsetzung der Menschenrechte online in unterschiedlichen Foren einsetzt und der derzeit 30 Mitgliedstaaten angehören.
- Die „Central European Cyber Security Platform“ – eine Kooperationsplattform der Länder (und der CERTs / teilweise milCERTs) der Visegrad-Staaten (Ungarn, Tschechien, Slowakei und Polen) und Österreich, welche im Jahr 2013 auf Initiative von Tschechien und Österreich ins Leben gerufen wurde.
- Das Global Forum on Cyber Expertise (GFCE) ist eine globale Plattform, die 2015 gegründet wurde. Österreich ist seit 2017 Mitglied.
- Das Internet Governance Forum (IGF), das aus dem Weltgipfel zur Informationsgesellschaft (WSIS) hervorging, fand diesmal in Paris statt. Bei diesem Treffen, das

stark auf Zivilgesellschaft und Privatsektor ausgerichtet ist, gibt es bisher keine konkreten Abschlussdokumente.

- Im Rahmen des IGF Paris lancierte der französische Präsident Macron am 12. November 2018 daher den „Pariser Appell zu Vertrauen und Sicherheit im Cyber Space“. Der Appell ist als politische Plattform zur Zusammenarbeit zwischen Staaten, Unternehmen und Zivilgesellschaft konzipiert und soll dazu dienen, dass alle Beteiligten ihr Bekenntnis zu Prinzipien, wie Einhaltung der internationalen Rechtslage im Cyber Raum, bekräftigen und ihre Stimmen in die bevorstehenden New Yorker Normensetzungsprozesse einbringen. Alle EU-Mitgliedstaaten unterstützen diese Initiative.

3 Nationale Akteure und Strukturen

Für die nationalen Akteure und Strukturen stellt die wiederholte Bewältigung von Cyber Angriffen verschiedenster Ausprägung gegen Unternehmen der kritischen Infrastruktur und verfassungsmäßige Einrichtungen eine erhebliche Herausforderung dar. Die Bandbreite der Angriffsmuster ist dabei vielfaltig und umspannt ein Spektrum von einfachen DDoS-Angriffen bis hin zu komplexen Fällen von versuchter Cyber Spionage. Was sich in diesem Zusammenhang immer wieder zeigt, ist, dass eine erfolgreiche Bewältigung solcher Angriffe eine umfassende, vertrauensvolle Zusammenarbeit aller beteiligten, staatlichen wie nichtstaatlichen, Akteure erfordert. Während die Kooperation der staatlichen Stellen in den Gremien OpKoord (Operative Koordinierungsstruktur) und IKDOK (Innerer Kreis der Operativen Koordinierungsstruktur) bereits seit mehreren Jahren etabliert ist und auch die Kommunikation mit den betroffenen Unternehmen auf einer soliden Basis steht, stellt in diesem Berichtsjahr die Implementierung von sogenannten Sektor-CERTs einen weiteren Meilenstein in der Zusammenarbeit dar.

3.1 Innerer Kreis der Operativen Koordinierungsstrukturen (IKDOK)

Das am 31. Dezember 2018 in Kraft getretene Netz- und Informationssystemsicherheitsgesetz (NIS-Gesetz) sieht unter anderem die Schaffung einer Struktur zur Koordination auf der operativen Ebene („Operative Koordinierungsstruktur - OpKoord“), sowie einer interministeriellen Struktur zur Koordination auf der operativen Ebene im Bereich der Sicherheit von Netz- und Informationssystemen („Innerer Kreis der Operativen Koordinierungsstruktur - IKDOK“) vor. Während die OpKoord im Wesentlichen zur Erörterung eines gesamtheitlichen Lagebildes, das auch die freiwilligen Meldungen enthält, eingerichtet wurde, liegen die Hauptaufgaben des IKDOK in der Erörterung und Aktualisierung des Lagebildes über Risiken, Vorfälle und Sicherheitsvorfälle und in der Unterstützung des Koordinationsausschusses im Cyber Krisenmanagement.

Konkret bedeutet dies, dass der IKDOK, unterstützt durch die OpKoord, im Krisenfall die direkte Schnittstelle zum gesamtstaatlichen Cyber Krisenmanagement (CKM) bildet. Hinsichtlich der anzuwendenden Mechanismen und Prozesse orientiert sich das CKM stark an den bereits bewährten und erprobten Abläufen des staatlichen Krisen- und Katastrophenschutzmanagements (SKKM). Regelmäßige Cyber Übungen sollen das Cyber Krisenmanagement sowie die Krisenmanagement- und Kontinuitätspläne testen.

Der IKDOK umfasst das Cyber Security Center (Bundesministerium für Inneres, BMI) und das Cyber Verteidigungszentrum (Bundesministerium für Landesverteidigung, BMLV), die beide den Vorsitz der IKDOK innehaben, sowie weitere staatliche Akteure / Einrichtungen. Im Konkreten zählen hierzu das Cyber Crime Competence Center (BMI), das Heeresnachrichtenamt (HNaA / BMLV), das Zentrum IKT- & Cyber-Sicherheit (ZIKT&CySih / BMLV) mit unter anderem dem Militärischen Cyber Sicherheitszentrum und dem milCERT, das GovCERT (BKA) sowie das BMEIA.

3.2 Cyber Security Center

Das Cyber Security Center (CSC) im Bundesamt für Verfassungsschutz und Terrorismusbekämpfung sah sich in diesem Berichtsjahr sowohl organisatorisch als auch inhaltlich mit erheblichen Herausforderungen konfrontiert. So erfuhr das CSC auf der einen Seite mit der Umwandlung von einem Referat in eine eigenständige Abteilung zwar eine signifikante organisatorische Aufwertung, muss jedoch im Zuge dessen auf der anderen Seite hinkünftig eine Reihe von neuen Aufgabenstellungen erfüllen.

Während nach dem Inkrafttreten des Netz- und Informationssystemsicherheitsgesetzes (NIS-Gesetz) diesbezügliche strategische Aufgaben in den Aufgabenbereich des Bundeskanzleramts fallen, liegt die operative Umsetzung der entsprechenden Regelungen in der Verantwortung des Bundesministeriums für Inneres. Die Rolle der operativen NIS-Behörde wird künftig von der Abteilung Cyber Sicherheit im Bundesamt für Verfassungsschutz und Terrorismusbekämpfung wahrgenommen. Das aktuelle Berichtsjahr war aus diesem Grund von umfangreichen organisatorischen und technischen Vorbereitungsmaßnahmen auf diese neue Aufgabe geprägt.

Gleichzeitig wurde der Bereich der Bewusstseinsbildung und der Cyber Prävention massiv ausgebaut. Neben den laufenden Awareness-Vorträgen und -Veranstaltungen bei Unternehmen der kritischen Infrastruktur und bei verfassungsmäßigen Einrichtungen, werden vom Cyber Security Center regelmäßig vielfältige Schulungsmaßnahmen zu IKT-Sicherheit für das eigene, sowie für andere Ressorts durchgeführt. Abgerundet wird dieser Bereich durch intensives Engagement im Awarenessbereich im Zusammenhang mit der Sicherheit im Rahmen der EU-Ratspräsidentschaft 2018 und der Europawahl 2019.

3.3 Zentrum IKT- und Cyber Sicherheit (ZIKT&CySih)

Im Zuge der Heeresgliederung 2019 wird das ehemalige Kommando Führungsunterstützung und Cyber Defence, welches bis dato in virtueller Form aufgebaut wurde, aufgelöst. Die Kernkompetenzen bleiben weitgehend bestehen und werden in den nachfolgenden Kompetenzbereichen näher beschrieben.

3.3.1 Militärisches Cyber Sicherheitszentrum (MilCySihZ)

Das MilCySihZ als Teil des ZIKT&CySih ist jene Stelle im Österreichischen Bundesheer, die bei der Abwehr von Bedrohungen oder Angriffen aus dem Cyber Raum gegen die eigenen IKT-Systeme und -Netze wirksam wird.

Um diesen Schutz aufrecht zu erhalten, ist es essentiell, eine durchgängige und konsequente Abdeckung aller Aspekte der Cyber Sicherheit aufzuweisen. Dies spiegelt sich im Aufgaben- und Kompetenzbereich des MilCySihZ wider:

- Auswahl, Einführung und Betrieb von IKT-Sicherheitskomponenten (z. B. Firewall, End-Point-Protection – Virenschutz etc.),
- Erstellung eines Cyber Sicherheitslagebild (durch Beobachten und Bewerten von aktuellen Technologien, IKT-Systemen und Komponenten des Österreichischen Bundesheeres),
- Forensik,
- Auditieren[4] der eigenen IKT-Systeme und -Netze,
- Cyber Sicherheitsmanagement,
- Cyber Truppenübungsplatz,
- Elektronische Kampfführung (Eigenschutz und Assistenzleistung).

3.3.2 Eigenschutz

Dem militärischen Cyber Sicherheitszentrum obliegt die Planung und Implementierung der Cyber Sicherheitssysteme und -komponenten für den Eigenschutz und die Verteidigung des Österreichischen Bundesheers gegen Cyber Angriffe. 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 Österreichischen Bundesheeres kann ein vollständiges Lagebild zur Cyber Sicherheit erstellt werden. Um fortlaufend alle IKT-Systeme auf ihre sicherheitstechnische Eignung für den Einsatz im Österreichischen Bundesheer überprüfen zu können, werden mit System- und Komponenten-Audits konzeptionelle und strukturelle Schwächen in Technologien, Produkten, Komponenten und Systemen frühzeitig erkannt.

3.3.3 milCERT (Military Computer Emergency Readiness Team)

Für den Fall eines bevorstehenden oder laufenden Cyber Angriffs müssen ausreichende technische und personelle Kapazitäten zur Erkennung, Eindämmung und Abwehr vorgehalten werden. Unverzichtbarer Bestandteil dafür ist die Fähigkeit zur Erfassung und Darstellung der aktuellen Cyber Lage. Um möglichst genaue und aktuelle Informationen

4 Regelmäßige Überprüfung/Revision, um etwaige Schwachstellen frühzeitig zu erkennen.

zu Cyber Sicherheitsvorfällen und aktuellen Erkenntnissen zu erhalten, steht das milCERT im ständigen Austausch mit nationalen und internationalen Partnerorganisationen. Es koordiniert die Maßnahmen beim Auftreten von IT-Sicherheitsvorfällen und warnt rechtzeitig vor Sicherheitslücken.

3.3.4 Cyber Truppenübungsplatz

Da hochspezialisierte Kräfte nur begrenzt verfügbar sind, ist eine mit den Konzepten und Verfahren akkordierte Ausbildung und entsprechendes Training der Angehörigen der Armee erforderlich. Im Rahmen des Cyber Truppenübungsplatzes (Cyber Range) werden Übungen im Cyber Umfeld koordiniert und Forschungsprojekte zusammen mit wissenschaftlichen Einrichtungen erarbeitet. Dabei werden aktuelle Cyber Sicherheitstrends analysiert und in die Cyber Verteidigungsverfahren des Österreichischen Bundesheeres eingearbeitet.

3.3.5 Informationssicherheit

Zur Ergänzung der technischen und taktischen Fähigkeiten müssen Informationssicherheit, Cyber spezifische Risiken und das Zusammenwirken mit österreichischen und internationalen Partnern gemanagt werden. Das militärische Cyber Sicherheitszentrum betreibt ein umfassendes IKT- und Cyber Risikomanagement, eingebettet in ein Information Security Management System und vertritt das Österreichische Bundesheer in nationalen und internationalen Zulassungsbehörden. Für einen sicheren Informationsaustausch führt das Österreichische Bundesheer Sicherheitszulassungen und -Audits von Systemen auf Basis nationaler und internationaler Sicherheitsvorschriften durch.

3.3.6 Elektronische Kampfführung

Als Teil der Cyber Verteidigung ist das Zentrum 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 Cyber Verteidigungszentrum

Das Abwehramt (AbwA) betreibt das Cyber Verteidigungszentrum (CyVZ) des Österreichischen Bundesheeres (ÖBH). Es bereitet die für die Cyber Verteidigung erforderlichen aktiven Mittel und Fähigkeiten vor. Damit ergänzt es die Cyber Verteidigung des Österreichischen Bundesheeres und auch die gesamtstaatlichen Cyber Verteidigungs-

anstrengungen. Zu diesem Zweck stellt das CyVZ ein Lagebild zur Verfügung, in welchem gesamtstaatliche und auch nachrichtendienstliche Informationen aus und über den Cyber Raum zusammengeführt, analysiert und für die Beurteilung von Gegenmaßnahmen herangezogen werden.

Weiters wird durch das AbwA alljährlich die im deutschsprachigen Raum größte IKT-Sicherheitskonferenz veranstaltet, um das Sicherheitsbewusstsein weiter zu erhöhen.

3.5 Heeresnachrichtenamt

Als strategischer Auslandsnachrichtendienst trägt das Heeresnachrichtenamt (HNaA) vor allem durch Darstellung des strategischen Kontexts bei großangelegten Cyber Vorfällen zum gesamtstaatlichen Cyber Lagebild bei. Neben dem rechtzeitigen Erkennen von Cyber Bedrohungen aus dem Ausland erlauben von ihm beschaffte Informationen über Absichten und Fähigkeiten internationaler Cyber Akteure eine wesentliche Beitragsleistung zur Attribuierung, und damit zur Entscheidungsfindung der obersten politischen und militärischen Führung, unter anderem bezüglich allfälliger Gegenmaßnahmen.

3.6 GovCERT, CERT.at und Austrian Energy CERT

GovCERT ist das Computer-Notfallteam der öffentlichen Verwaltung nach dem NIS-Gesetz und Teil des bereits genannten IKDOK. Das GovCERT stellt den CERT Point of Contact für Österreich und ist daher mit internationalen Organisationen und Ansprechpartnern wie der European GovCERT Group oder der Central European Cyber Security Platform eng vernetzt. Darüber hinaus nimmt das GovCERT (gemeinsam mit CERT.at) die österreichische Vertretung im CSIRTs-Netzwerk der EU wahr.

CERT.at ist das österreichische Computer Emergency Response Team (CERT) und wurde 2008 gemeinsam mit GovCERT in Kooperation mit nic.at eingerichtet. Das Team von CERT.at wird in erster Linie bei akuten Sicherheitsbedrohungen und -ereignissen aktiv. Dies geschieht durch Verständigung von betroffenen Stellen oder auf Basis eigener Recherchen.

Darüber hinaus führt CERT.at auch vorbeugende Maßnahmen wie Früherkennung, Öffentlichkeitsarbeit, Beratung und Unterstützung im Anlassfall auf Anfrage durch. 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 Cyber Sicherheitsbereich.

Das im Bundeskanzleramt angesiedelte GovCERT arbeitet eng mit CERT.at in Form einer Public-Private-Partnership zusammen.

Mit der Umsetzung der NIS-Richtlinie in nationales Recht durch das Netz- und Informationssystemsicherheitsgesetz (NIS-Gesetz) wurden die Aufgabenbereiche für das GovCERT festgeschrieben. So sieht diese Umsetzung unter anderem für Betreiber wesentlicher Dienste sowie Anbieter digitaler Dienste eine Meldeverpflichtung für schwerwiegende Sicherheitsvorfälle vor. Diese verpflichtenden Meldungen werden von den Betroffenen an bestimmte, sektorenspezifische Meldestellen (sektorenspezifische Computer-Notfallteams) gesendet und von dort an das 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 nimmt das GovCERT die Entgegennahme und Weiterleitung solcher Meldungen vor, falls die Einrichtung nicht im IKDOK vertreten ist. Zusätzlich kann das GovCERT auch Frühwarnungen, Alarmmeldungen, Handlungsempfehlungen und Bekanntmachungen vornehmen, erste allgemeine technische Unterstützung bei der Reaktion auf einen Sicherheitsvorfall leisten, um Risiken, Vorfälle und Sicherheitsvorfälle zu beobachten, zu analysieren sowie die Lage zu beurteilen.

Das NIS-Gesetz sieht zur Wahrnehmung dieser Meldestellenfunktion die Existenz eines solchen Sektor-CERTs in jedem Sektor vor. Diese CERTs erfüllen neben der Meldestellenfunktion eine Vielzahl weiterer CERT-Aufgaben für die Organisationen ihres Sektors.

Für den Fall, dass ein Sektor noch über kein eigenes Sektor-CERT verfügt, wird die Aufgabe einer Meldestelle durch das noch zu nominierende, nationale Computer-Notfallteam wahrgenommen. Sollte kein nationales Computer-Notfallteam eingerichtet sein, so übernimmt das GovCERT diese Aufgabe. Dadurch wird sichergestellt, dass Unternehmen des betroffenen Sektors ihrer gesetzlichen Meldeverpflichtung nachkommen können.

Das Austrian Energy CERT (AEC) ist ein brancheneigenes CERT (Computer Emergency Response Team) für die österreichische Energieindustrie. Das AEC ist ein wichtiger Baustein bei der Erhöhung der Resilienz der Energiewirtschaft gegenüber Cyber Attacken. Es kommt als Sektor-CERT im Sinne der NIS-Richtlinie und des NIS-Gesetzes in Betracht und erfüllt zugleich die Vorgaben der europäischen Richtlinie für Netz- und Informationssicherheit (NIS) sowie die Empfehlungen der Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) für die Erhöhung der IT-Sicherheit bei kritischen Infrastrukturen.

Die Hauptaufgaben des Austrian Energy CERTs dienen der Stärkung der IT-Sicherheitskompetenz des Energiesektors. Zu diesen Aufgaben gehört das laufende Security Incident Management, also die Bearbeitung von täglich eingehenden Anfragen und Sicherheitsmeldungen, Durchführung von Schulungstätigkeiten, Teilnahme an internationalen Cyber Sicherheitsübungen oder Mitarbeit bei der Erstellung technischer Sicherheitskonzepte für die Elektrizitäts- und Erdgaswirtschaft. Darüber hinaus erfüllt das AEC die Rolle des Primäransprechpartners (Single Point of Contact) bei nationalen und internationalen

Security Incidents im Energiesektor. Somit wird neben der schnellen und effizienten Kommunikation auch die Koordination der IT-Sicherheitsexpertinnen und -experten und Behörden innerhalb der Branche gewährleistet.

Durch den Betrieb eines brancheneigenen CERTs und dem damit verbundenen Informationsaustausch sollen Bewusstsein und Prävention im Energiesektor gestärkt werden. Zusätzlich konnte im Jahr 2018 eine Mitgliedschaft im internationalen Netzwerk der CERTs weltweit (FIRST) erreicht werden sowie der Status eines „accredited members" beim europäischen Verband der CERTs (Trusted Introducer). Im Rahmen dieser vertrauensvollen Gremien ist es möglich, sich mit anderen CERTs über Best Practice Ansätze auszutauschen, um das gesamtheitliche Sicherheitsniveau zu erhöhen.

3.7 CERT-Verbund

Um das Sicherheitsniveau der österreichischen Gesellschaft im Cyber Raum weiterzuentwickeln ist es notwendig, dass das Zusammenspiel zwischen Gesellschaft, Wirtschaft und Wissenschaft weiter gefördert und ausgebaut wird. Eine wesentliche Rolle bei der Weiterentwicklung nehmen dabei die Computer-Notfall-Teams (CERTs) in Österreich ein.

Die inhärente Aufgabe der CERTs ist es, IKT-Systeme und digitale Netze zu schützen. Als erste Anlaufstelle für sämtliche Bereiche der Cyber Sicherheit kommt den Aspekten Prävention, Reaktion und Bewusstseinsbildung höchste Priorität zu. Intensiver Austausch und Vernetzung auf nationaler und internationaler Ebene stellen die Voraussetzungen für den Aufbau notwendiger Expertise dar.

Im Mittelpunkt des Aufgabenbereichs des nationalen CERT-Verbunds (Österreich) stehen die Verbesserung der Zusammenarbeit zwischen den österreichischen CERTs sowie die Förderung der CERT-Aktivitäten in Österreich.

Ein flächendeckendes Netz an CERTs ist das wirksamste Mittel zur Absicherung der vernetzten Informations- und Kommunikationssysteme. Eine Sichtweise, die sich in Österreich in einer stetig wachsenden Anzahl von CERTs bestätigt.

Der CERT-Verbund wurde 2011 als Kooperation aller damals existierenden österreichischen CERTs aus öffentlichen wie auch privaten Sektoren gegründet. Intention war die Bündelung der verfügbaren Kräfte zur optimalen Nutzung des gemeinsamen Know-hows zur Gewährleistung von bestmöglicher IKT-Sicherheit.

Die Teilnahme am CERT-Verbund ist freiwillig. Jeder einzelne Teilnehmer verpflichtet sich zu regelmäßigem Informations- und Erfahrungsaustausch, zur Identifikation und Verfügungstellung von Kernkompetenzen und zur Förderung der CERTs in allen Sek-

toren – im Sinne eines gemeinschaftlich geführten und auf Kooperation basierenden CERT-Verbundes – beizutragen.

Seit der Gründung des CERT-Verbunds haben sich die aktuell 15 Mitglieder in 33 Sitzungen getroffen und sind auch außerhalb der Treffen über sichere Kommunikationsverteiler miteinander im ständigen Austausch.

Wichtigster Inhalt der Sitzungen ist der gegenseitige operative Informations- und Erfahrungsaustausch und der Aufbau von Vertrauen untereinander. Dadurch kann auf Unterstützung und Bereitstellung von zusätzlicher Expertise in einem Cyber Krisenfall zurückgegriffen werden.

Im Jahr 2018 wurden die bereits bestehenden Cyber Sicherheitsstrukturen (OpKoord, IKDOK etc.) durch das Netz- und Informationssystemsicherheitsgesetz (NIS-Gesetz) auf eine gesetzliche Basis gestellt. Ebenso wurde durch das NIS-Gesetz der Errichtung von sektorenspezifischen Computer-Notfallteams der Weg geebnet und deren Teilnahme an der OpKoord gesetzlich verankert. Aus Sicht des CERT-Verbund sind diese Entwicklungen zu begrüßen.

3.8 Cyber Crime Competence Center (C4)

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

Die Cyber Crime Meldestelle des C4 fungiert in Cyber Crime Angelegenheiten als internationaler Kontaktpunkt und Schnittstelle zum CSC, sowie als Kontaktstelle zur Bevölkerung. Dies ermöglicht die frühzeitige Erkennung von neuen Phänomenen. Darüber hinaus nimmt die Cyber Crime Meldestelle als Ansprechstelle für alle Polizeidienststellen im Zusammenhang mit Cyber Crime eine weitere wichtige Aufgabe wahr.

Die „SOKO Clavis“ bearbeitet weiterhin erfolgreich zentral und operativ sämtliche Ransomwaredelikte im gesamten Bundesgebiet und koordiniert gemeinsam mit anderen Ländern die internationale Zusammenarbeit.

Mobile Forensik, Multimedia Forensik und KFZ-Forensik ergänzen und erweitern die Kompetenzen des C4 im Bereich der digitalen Beweissicherung.

Das Referat Entwicklung und Innovation, als technisch wissenschaftlicher Dienst, widmet sich unter anderem der Forschung auf speziellen Cyber relevanten Gebieten, der Er-

forschung und Bewertung von Phänomenen im Bereich der IT-Kommunikation sowie der Erforschung und Entwicklung von Schutz- und Ermittlungsmöglichkeiten in Hard- und Softwarebereichen.

Die ursprünglich auf das C4 zugeschnittene technische Infrastruktur hat sich bewährt und wird daher bereits in einzelnen Fällen anderen Abteilungen des Bundeskriminalamtes sowie der Landeskriminalämter zur Verfügung gestellt.

3.9 Cyber Sicherheit Plattform (CSP)

Die Cyber Sicherheit Plattform (CSP) stellt die zentrale Austausch- und Kooperationsplattform zwischen Wirtschaft, Wissenschaft und öffentlicher Verwaltung dar. Sie dient dem Erfahrungs- und Informationsaustausch im Bereich Cyber Sicherheit mit besonderem Fokus auf kritische Infrastrukturen. Darüber hinaus berät und unterstützt die CSP die Cyber Sicherheit Steuerungsgruppe (CSS) in strategischen Fragen der Cyber Sicherheit.

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 Cyber Sicherheit dar. Die Ergebnisse der Arbeiten der Plattform haben hohen Stellenwert in der Gestaltung der nationalen Cyber Sicherheitspolitik.

Im Jahr 2018 fanden die sechste und siebente Arbeitstagung der CSP statt. Gegenstand der Sitzungen waren einerseits die wesentlichen Schwerpunkte des Regierungsprogramms 2017–2022 in Bezug auf die Thematik Cyber Sicherheit sowie die mit dem neuen Bundesministeriengesetz geänderten Zuständigkeiten und Verantwortlichkeiten in diesem Bereich.

Andererseits wurde ausführlich über den jeweils aktuellen Stand der Umsetzung der NIS-Richtlinie durch das NIS-Gesetz sowie die begleitenden Verordnungen beraten. Zahlreiche Inputs, insbesondere von potentiell Betroffenen, die in der CSP vertreten sind, wurden aufgenommen und in den Bearbeitungen des NIS-Gesetzes berücksichtigt.

Einen weiteren Themenschwerpunkt bildeten Fortschrittsberichte über die im Rahmen der CSP etablierten Arbeitsgruppen zu den Bereichen „Rechtliches und Regulatorisches“, „Technologien, Prozesse, Ausbildung, Forschung und Entwicklung“ sowie „betriebliches Krisenmanagement“.

Darüber hinaus wurden Vorgaben, Grundannahmen und Arbeitsweisen zur Erstellung einer aktualisierten Österreichischen Strategie für Cyber Sicherheit (ÖSCS 2.0) vorgestellt und diskutiert.

Bei der im Rahmen der siebenten Arbeitstagung im Herbst 2018 durchgeführten Neuwahl des Vorsitzes der CSP (gemäß Geschäftsordnung werden die Vorsitzenden für eine dreijährige Funktionsperiode bestellt) wurden Dr. Thomas Stubbings und Dr. Wolfgang Schwabl als Vorsitzende für eine weitere Funktionsperiode wiederbestellt.

3.10 Austrian Trust Circle (ATC)

Der Austrian Trust Circle ist eine Initiative von CERT.at, Austrian Energy CERT und dem österreichischen Bundeskanzleramt und besteht aus Security Information Exchanges in den einzelnen Bereichen der strategischen Informationsinfrastruktur.

Der Austrian Trust Circle der öffentlichen Verwaltung besteht seit 2016.

CERT.at und Austrian Energy CERT bieten hier in Kooperation mit GovCERT Austria und dem Bundeskanzleramt einen formellen Rahmen für praxisnahen Informationsaustausch und gemeinsame Projekte im Sicherheitsbereich.

Wesentliche Zielsetzungen des Austrian Trust Circles sind:

- Unterstützung der Selbsthilfe in den Sektoren im Bereich Sicherheit,
- Operative Kontakte für CERT.at / Austrian Energy CERT / GovCERT Austria bei der Information über und Behandlung von Sicherheitsvorfällen in den Organisationen,
- Bereitstellung von operativen Experten für die öffentliche Verwaltung im Krisenfall,
- Das Schaffen einer Vertrauensbasis, um im Ernstfall gemeinsam agieren zu können,
- Vernetzung und Informationsaustausch in und zwischen den Sektoren der strategischen Infrastruktur.

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

Im Jahr 2018 wurden unter anderem die Themen Umsetzung der NIS-Richtlinie, sichere Softwareentwicklung, Präventionsmaßnahmen gegen Distributed Denial of Service-Attacken (DDoS) sowie der Austausch über Erfahrungen im Umgang mit Sicherheitsvorfällen behandelt.

3.11 IKT-Sicherheitsportal

Das IKT-Sicherheitsportal onlinesicherheit.gv.at ist eine interministerielle Initiative in Kooperation mit der österreichischen Wirtschaft und fungiert als zentrales Internetportal für Themen rund um die Sicherheit in der digitalen Welt.

Die Initiative verfolgt als strategische Maßnahme der nationalen IKT-Sicherheitsstrategie und der Österreichischen Strategie für Cyber Sicherheit das Ziel, durch Sensibilisierung und Bewusstseinsbildung der betroffenen Zielgruppen sowie durch Bereitstellung zielgruppenspezifischer Handlungsempfehlungen, die IKT- und Cyber Sicherheitskultur in Österreich zu fördern und nachhaltig zu stärken.

Das Informations- und Serviceangebot wird im Rahmen regelmäßiger Redaktionssitzungen mit den 39 Kooperationspartnern (Bundesministerien, Landesregierungen, Behörden, Universitäten, Fachhochschulen, Forschungsinstitute, Unternehmen, Vereinen und Interessensvertretungen) laufend erweitert. Es beinhaltet aktuelle Meldungen und Warnungen, Beratungen sowie weiterführende Informationen sowohl für Einsteigerinnen und Einsteiger als auch für Expertinnen und Experten.

2018 umfassten die Aktivitäten auf dem IKT-Sicherheitsportal insgesamt die Verfassung von 150 Newsartikeln, 50 Publikationseinträgen und 70 Veranstaltungseinträgen. In jedem Monat wurde ein Schwerpunktthema zu aktuellen Trends festgelegt, wozu insgesamt 34 Fachbeiträge veröffentlicht wurden. Schwerpunkte waren beispielsweise zu Beginn des Jahres die Datenschutz-Grundverordnung und in der Vorweihnachtszeit Sicherheitsmaßnahmen beim Online-Shopping. Im Oktober wurde zu den österreichischen Aktivitäten im Zuge des „European Cyber Security Month“ (ECSM) berichtet.

3.12 Büro für strategische Netz- und Informationssystemsicherheit

Das Büro für strategische Netz- und Informationssystemsicherheit ist im Bundeskanzleramt als Teil der Abteilung I/8 für Angelegenheiten im Zusammenhang mit der Umsetzung der gesetzlichen Verpflichtung aus der EU-Richtlinie 2016/1148 in Österreich und dem Bundesgesetz für Netz- und Informationssystemsicherheit (NIS-Gesetz) zuständig.

Es nimmt die Aufgaben einer strategischen NIS-Behörde in Österreich wahr und ist für die Regelung von Kriterien und Grenzwerten von Betreibern wesentlicher Dienste, Anbieter digitaler Dienste und CSIRT-Meldestellen zuständig.

Die Adressaten des NIS-Gesetzes werden durch das NIS-Büro im Bundeskanzleramt über Zuständigkeiten und Verpflichtungen informiert. Das NIS-Büro betreibt eine Servicestelle für alle Angelegenheiten der strategischen Umsetzung.

Zu den Umsetzungsverantwortungen aus der Richtlinie gehören des Weiteren die Teilnahme an der europäischen NIS-Kooperationsgruppe und anderen EU-weiten und internationalen Cyber Sicherheitsgremien mit strategischer Ausrichtung, Strategien für Cyber Sicherheit und die öffentlich-private-Kooperation.

Das NIS-Büro hatte im Jahr 2018 zwei Schwerpunkte. Zum einen wurde die Verabschiedung des NIS-Gesetzes vorangetrieben und die Umsetzung der Richtlinie in Österreich vorbereitet. Zum anderen war das NIS-Büro in der österreichischen Ratspräsidentschaft zum Thema Europäische Cyber Sicherheit federführend involviert.

Zur Richtlinie und deren Umsetzung:

- Das Netz- und Informationssystemsicherheitsgesetz wurde nach Annahme durch den Nationalrat am 11. Dezember 2018 und durch den Bundesrat am 19. Dezember 2018 im BGBl. I Nr. 111/2018 kundgemacht und ist somit mit 28. Dezember 2018 in Kraft getreten. Das NIS-Gesetz setzt somit die EU-Richtlinie 2016/1148 in Österreich um.
- Dem Inkrafttreten vorangegangen ist eine umfangreiche nationale Vorbereitung, um die Vorgaben der europäischen NIS-Richtlinie bestmöglich in die österreichische Umgebung abzubilden, inklusive der Berücksichtigung von bereits vorhandenen nationalen Cyber Sicherheitsprozessen und -strukturen. Das Einbinden der Bereiche Staat, Wirtschaft, Bildung, Forschung und Gesellschaft war von Anfang an ein wichtiges Ziel.
- Auf europäischer Ebene war das NIS-Büro in allen Sitzungen hinsichtlich der Umsetzung der NIS-Richtlinie aktiv. Das umfasste
  - die Teilnahme an den Plenarsitzungen der europäischen NIS-Kooperationsgruppe und
  - das aktive Einbringen in allen europäischen Arbeitsgruppen, die konkrete Vorschläge für die Umsetzung der NIS-Richtlinie ausarbeiten.
- National startete das NIS-Büro 2018 die Vorbereitung zur Gesetzwerdung des NIS-Gesetzes. Dies geschah in mehreren Runden von Gesprächen mit Vertretern der relevanten Sektoren. Inhaltlich umfasste das unter anderem die Festlegung der wesentlichen Dienste in Österreich, die Auswahl der Betreiber der wesentlichen Dienste, die Festlegung der Kriterien und Parameter für Cyber Vorfälle, das Vorbereiten der Prozesse der Meldeverpflichtungen und das Ausarbeiten von Sicherheitsmaßnahmen.

- Alle Themen werden mit den zuständigen operativen Expertinnen und Experten im BMI eng abgestimmt. Mit Fact Sheets werden Adressaten des NIS-Gesetzes jeweils über den Status Quo informiert.
- Mit einer gemeinsamen NIS-Webseite (erreichbar unter nis.gv.at) mit dem BMI und einer eigenen Kontaktstelle (erreichbar unter nis@bka.gv.at) wird das NIS-Büro die Umsetzung der Maßnahmen des NIS-Gesetzes bestmöglich unterstützen.

Zur Österreichischen Ratspräsidentschaft:

- Das NIS-Büro hatte während der Österreichischen Ratspräsidentschaft den Vorsitz in den europäischen Cyber Sicherheitsgruppen „Horizontal Working Party on Cyber Issues“ und „NIS-Kooperationsgruppe“ und war an der inhaltlichen und organisatorischen Gestaltung der Wiener Konferenz im Dezember 2018 federführend beteiligt.
- Siehe dazu: Kapitel „Österreichische Ratspräsidentschaft Cyber Sicherheit“.

4 Cyber Übungen

Auch in diesem Berichtsjahr leisteten Cyber Übungen einen wesentlichen Beitrag zur Erprobung festgelegter Prozesse, zur Überprüfung gesetzter Maßnahmen, sowie zur Beübung innerstaatlicher Zusammenarbeit im Cyber Bereich.

Der Erkenntnisgewinn aus der Teilnahme an Planspielen „Lessons Learned" ist ein ganz entscheidender Faktor bei der Erhöhung der gesamtstaatlichen Resilienz. Durch die aktive Teilnahme an gleich einer Reihe von unterschiedlichen Übungen konnten in diesem Jahr die staatlichen Stakeholder im Bereich Cyber Sicherheit eine ganze Palette von Szenarien abdecken.

4.1 Austrian Strategic Decision Making Exercise (ASDEM) 18

Bei der ASDEM handelt es sich um eine gesamtstaatliche Cyber Sicherheit / Hybrid-Übung. Sie ist ein Planspiel, welches unter maßgeblicher Beteiligung des KdoFüU&CD, insbesondere in der Rolle seines Kommandanten als (ehemaliger) Cyber Koordinator des BMLV, am 20. und 21. Februar 2018 in Wien an der LVAK stattfand.

An dieser Veranstaltung nahmen 118 Teilnehmer aus dem IKDOK (BKA, BMLV, BMI, BMEIA, CERT) sowie aus dem Bereich der kritischen Infrastruktur teil. 70 internationale Beobachter aus 21 Ländern und viele nationale Beobachter von öffentlichen Institutionen und Firmen nahmen ebenfalls an der Übung teil.

Der Zweck der Übung bestand in der lageangepassten Überprüfung der gesamtstaatlichen Abläufe im Rahmen des Cyber Krisenmanagements (CKM) zum Schutz der kritischen Infrastruktur bis hin zur Klärung des Überganges des zivil geleiteten CKM zum militärisch geleiteten Cyber Verteidigungsfall, die Anwendbarkeit auf hybride Anlassfälle und die damit verbundenen politischen, rechtlichen und völkerrechtlichen Problemstellungen.

Der Fokus der Übung lag auf der strategischen (Entscheidungs-)Ebene sowie der Kommunikation innerhalb der Ministerien und der kritischen Infrastruktur. Daher wurden bei dieser Übung technische Problemstellungen nicht behandelt. Die Entwicklung der Übung wurde von Österreich unterstützt, die Ausarbeitung erfolgte von Seiten der Europäischen Verteidigungsagentur (EDA) beauftragten „Estonian Defence League" (EDL), welche in die ASDEM integriert war und die Spielleitung stellte.

4.2 CROSSED SWORDS 2018 (XS18)

Diese technische Cyber Defence Übung fand vom 30. Jänner bis 2. Februar 2018 in Riga, Lettland (LVA) statt. Sie wurde durch die NATO CCD-COE in Zusammenarbeit mit CERT.LV geleitet und es nahmen ca. 80 Soldaten und Zivilisten aus 20 Staaten teil. Das BMLV stellte dabei zwei Teilnehmer vom KdoFüU&CD/ZIKT&CySih.

Der Übungszweck bestand darin, dass Penetrationstester, forensische Experten und Special Operations Forces als gemeinsames Team arbeiteten, um die gesetzten Missionsziele und technischen Herausforderungen in einer virtuellen Cyber Umgebung zu erfüllen. Der Hauptfokus lag bei der Entwicklung von taktischen Fähigkeiten in einem reaktiven Cyber Verteidigungsszenario und der Bereitstellung von angemessenem Situationsbewusstsein der Teilnehmer. Ein weiteres Ziel der Teilnahme war es, die vorhandenen Fähigkeiten im Penetration Testing, welches zur Überprüfung eigener IKT-Systeme benötigt wird, zu verbessern. Ebenso relevant war der Erfahrungsaustausch mit Spezialisten aus anderen Nationen.

4.3 LOCKED SHIELDS 2018 (LS18)

Bei dieser größten technischen „Life-fire" Übung im Cyber Defence Bereich war Defence im Fokus, jedoch wurden auch begleitende Verfahren (Rechtslage „Cyber", Öffentlichkeitsarbeit, Collaboration und Forensic) angewendet. Die Übung fand vom 23. bis 27. April 2018 in Tallin, Estland (EST) statt und wurde durch die NATO CCD-COE geführt. Dabei nahmen mehr als 1000 Soldatinnen und Soldaten und Zivilisten aus 30 Staaten sowie NATO- und EU-Organisationen teil. Österreich stellte dabei sechs Übungsteilnehmerinnen und -teilnehmer direkt vor Ort, sowie 38 Übungsteilnehmerinnen und -teilnehmer in Wien als Blue Team (BT) in den Räumlichkeiten des KdoFüU&CD.

Bei dieser Übung wurden primär die Fähigkeiten, ein wenig bekanntes Netzwerk zu schützen, Angriffe zu identifizieren und darauf geeignet zu reagieren, geübt.

Die teilnehmenden IT-Spezialistinnen und IT-Spezialisten hatten als Teams umfassende Cyber Angriffe zu erkennen, die Auswirkungen zu beschränken und die Vorfälle entsprechend einheitlicher Vorgaben zu bearbeiten (z. B. rechtliche Aspekte, Informationsaustausch, forensische Analysen). Aus den Aktionen der Übungsteilnehmer sollten Lösungsansätze für reale Probleme abgeleitet werden, zur Stärkung der internationalen Zusammenarbeit durch Schaffung von Vertrauen, Verbesserung der Fähigkeit zur Durchführung ähnlicher Übungsvorhaben, Testung von Werkzeugen, dem Ausbau der Fähigkeiten im Bereich Cyber Defence und dem Ausbau der Fähigkeiten im Bereich aktive Cyber Handlungen.

4.4 CYBER PHALANX 2018 (CP18)

Bei der CP18 handelte es sich um eine Table Top Exercise (TTX) vom 4. bis 8. Juni 2018 in der Schwarzenberg Kaserne Salzburg. Die Übung war ein Pilotprojekt der European Defence Agency (EDA) und es nahmen 135 Soldatinnen und Soldaten und Zivilisten aus 16 Staaten teil. Die Übung wurde unter Bildung eines EXCON, einer JOPG, CJOPG und CyCell unter Abstützung auf eine Real Life Support Zelle abgehalten.

Der Zweck der Übung bestand darin, die Führungskräfte und ihre Mitarbeiterinnen und Mitarbeiter auf Themen aus dem Cyber Bereich zu sensibilisieren und darauf vorzubereiten, das volle Spektrum möglicher Cyber Vorfälle zu behandeln, welche während einer Militäroperation auftreten könnten. Der Fokus der Übung lag auf der Führung und man ging daher nicht auf technische Details ein.

In den ersten beiden Tagen wurden im Rahmen eines Cyber Awareness Seminars die Grundlagen zur Bewältigung der daran anschließenden Übung geschaffen.

Der Übungszeitraum wurde in zwei Themenbereiche gegliedert: Die ersten beiden Tage waren für die Durchführung eines Fachseminars anberaumt. Darauf folgte in den nächsten drei Tagen die Durchführung des Übungsanteiles. Die Inhalte des Seminars folgten einer auf die Bedürfnisse der Übungsteilnehmerinnen und -teilnehmer maßgeschneiderten Staffelung, beginnend mit globalen Kontexten der Mechanismen zur Krisenbewältigung (Zusammenarbeit Planungstätigkeiten EEAS-EUMS, Cyber Governance, Cyber Diplomacy, rechtliche Aspekte), hinführend zu konzentrierter Aufbereitung von Themenbereichen, die unmittelbar die Übungsdurchführung ab STARTEX unterstützten (z. B. Cyber Defence auf Ebene EUMS, Berücksichtigung von Cyber Aspekten in der Planung einer EU-CSDP Operation, Referenzdokumente, Cyber Defence Aspekte, die im Collaborative Planning Cycle zwischen der BXL – einem designiertem OHQ sowie FHQ – zu berücksichtigen sind). Abgerundet wurden alle Vorträge immer mit fach- bzw. sachdienstlichen Hinweisen im konkreten Zusammenhang der anzuspielenden Lage.

4.5 Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise (CWIX18)

Bei der CWIX18 handelte es sich um eine großangelegte Command Post Exercise (CPX) mit besonderem SG auf Interoperabilitätstests sowie V&V von einsatzorientierten IKT-Systemen, Services und Applikationen, die im Zeitraum vom 11. bis 28. Juni 2018 in Polen/BYDGOSZCZ stattfand.

Es nahmen knapp 1300 Soldatinnen und Soldaten und Zivilisten aus 29 Nationen sowie NATO-Organisationen an der Übung teil. Dabei stellte Österreich 25 Teilnehmerinnen

und Teilnehmer. Das Hauptthema der CWIX stellte die wiederkehrende Interoperabilitätsübung mittels abgestimmtem Szenario und der Möglichkeit, parallel dazu zusätzliche Tests, z. B. zum Datenaustausch mit Testpartnern nach vorherigen Absprachen, durchzuführen.

4.6 COMMON ROOF 2018 (CR18)

Die CR18 war eine dreiwöchige Übung, die vom 2. bis 18. Mai 2018, verteilt in den drei Ländern der Deutschland-Österreich-Schweiz-Kooperation, stattfand. Die diesjährige Lead Nation der Übung war Deutschland. An der CR18 nahmen ca. 100 Soldatinnen und Soldaten und Zivilisten aus den drei D-A-CH Nationen teil, wobei Österreich durch 41 Teilnehmerinnen und Teilnehmer vertreten war.

Im Zuge der Übung wurde gemeinsam ein multinationales Mission Network aufgebaut, betrieben und gegen Cyber Bedrohungen geschützt. Im Mittelpunkt standen standardisierte (bzw. teilweise noch zu standardisierende) IKT-Service-Management-Prozesse, IKT-Sicherheitsprozesse und die dabei zum Einsatz kommenden IKT-Services. Die Überwachung und Steuerung der multinationalen Netzwerkanteile übernahm eine multinationale Network Operation Cell (NOC).

4.7 Cyber Europe und Cyber Europe Austria 2018

Alle zwei Jahre organisiert die Europäische Agentur für Netzwerk- und Informationssicherheit (ENISA) die größte pan-europäische IT-Notfall- und Krisenübung „Cyber Europe“. Im Jahr 2018 fand diese Übung bereits zum fünften Mal statt und konzentrierte sich auf ein Cyber Bedrohungsszenario rund um den europäischen Flugsektor. Österreich beteiligt sich unter Federführung des Bundeskanzleramtes schon seit 2010 an der Cyber Europe. Seit 2012 erfolgt dies in Form einer parallel abgehaltenen nationalen Übung, der „Cyber Europe Austria“.

Das vorrangige Ziel der internationalen Cyber Europe ist die Verbesserung der Kooperation auf europäischer Ebene. Im Zuge dessen bot sich 2018 die Möglichkeit, Prozess- und Kooperationsmechanismen, welche sich aus der europäischen NIS-Richtlinie ergeben, unter den teilnehmenden Staaten im Rahmen eines Szenarios, in welchem ein internationaler, groß angelegter Cyber Angriff auf die Fluginfrastruktur Europas abzielt, zu beüben.

Auch auf nationaler Ebene konnten die für so einen Fall relevanten Akteure aus dem staatlichen wie dem privaten Sektor im Rahmen der Cyber Europe Austria ihre koordinierte Reaktion auf den Cyber Ernstfall bei einer großangelegten Attacke auf den österreichischen Flugsektor testen.

Die Cyber Europe Austria ermöglicht es, nationale Strukturen, Kooperations- und Kommunikationsprozesse auf ihre Effektivität und Effizienz zu testen, um so Stärken und mögliche Defizite aufzuzeigen. Die beteiligten Akteure können auf diese Weise die Vorbereitung auf einen Cyber Ernstfall optimieren und damit die Resilienz Österreichs erhöhen.

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

4.8 Cyber SOPEx 2018

Das CSIRTs-Netzwerk, das durch die NIS-Richtline gegründet wurde und das der operativen Zusammenarbeit zwischen den designierten CSIRTs in der EU dient, hat für genau diese Kooperation im Krisenfall Vorgehensweisen (Standard Operating Procedures - SOPs) ausgearbeitet. Diese lehnen sich an das Regelwerk an, das über die Jahre in den Cyber Europe Übungen erarbeitet wurde. Die Cyber SOPEx 2018 wurde am 30. Jänner 2018 durchgeführt und hatte als Ziel, diese Prozeduren der Zusammenarbeit zum ersten Mal im CSIRTs-Netzwerk zu testen. Es ging daher nicht um eine innerstaatliche Eskalationsübung, sondern rein um die Prozesse zwischen den CSIRTs in der ganzen EU.

Als Szenario wurden Angriffe auf Containerhäfen angenommen. Ziel im Spiel war es, die Informationen aus allen betroffenen Staaten zu sammeln, um daraus ein gemeinsames Lagebild und eine abgestimmte Vorgehensweise zu entwickeln. Da Österreich nur am Rande selber betroffen war, hat der Vertreter des österreichischen CERTs die Koordinationsrolle („facilitator“) innerhalb des CSIRTs-Netzwerks übernommen.

Die Übung hat ihr Ziel, die Prozesse zu testen und deren Schwächen und Stärken herauszuarbeiten, erreicht. Die Ergebnisse flossen in die Weiterentwicklung der SOPs ein, die schon bald im größeren Rahmen der Cyber Europe 2018 wieder zum Einsatz kamen.

4.9 Cyber Incident Situational Awareness Planspiel (CISA Planspiel)

Das Cyber Incident Situational Awareness-Planspiel (CISA-Planspiel) hatte eine von den anderen Planspielen abweichende Zielsetzung. In dieser Übung sollte anhand eines Cyber Angriffsszenarios herausgefunden werden, welche Darstellung und Verknüpfung von Daten bei einem laufenden Cyber Angriff für eine zentrale Stelle (Lagezentrum) optimale Handlungsfähigkeit schaffen kann. Im Rahmen der Übung wurden mehrere

solcher Lagezentren von den teilnehmenden Organisationen gebildet, die gleichzeitig mit jeweils denselben Informationen zur Cyber Lage bespielt wurden. Ziel war es, dass diese Lagezentren die zur Verfügung gestellten Informationen individuell erfassen, aufbereiten und geeignet darstellen, um so eine Lageeinschätzung durchführen zu können.

4.10 EU-HEX-ML 18 (PACE)

Vom 5. bis 23. November 2018 fand die Krisenmanagementübung „Hybrid Exercise Multilayer 18“ (HEX-ML 2018 PACE) statt. Diese wurde von der EU ausgerichtet. Auch Österreich beteiligte sich daran.

Ziel der Übung war es, in Zusammenarbeit mit der NATO die Bewältigung hybrider Bedrohungslagen einzuüben, um die Reaktionsfähigkeit der EU auf kommende hybride Krisen zu verbessern.

Das Szenario basiert auf einer fiktiven Intervention der EU in einem Konflikt in einem angrenzenden Staat, der innerstaatlich ein Sicherheitsproblem und mit Opposition und terroristischen Gruppen zu kämpfen hat. Da der Staat ein Stabilitätsanker in der Region ist und ökonomisch, militärisch und politisch in den letzten Jahren zunehmend mit der EU kooperiert hat, hilft die EU diesem Staat.

Die EU-Mitgliedstaaten hatten die Möglichkeit, bei der Übung bevorzugte Bereiche einzubringen: vor allem hybride Bedrohungen, deren militärische Beantwortung trainiert werden soll. Ein wesentlicher Teil der Übung ist das Umgehen mit Fake News, mit Verbreitung von Propagandanachrichten und mit Bewegungen, die sich gegen westliche Interessen einsetzen. Bei der Übung waren terroristische, gesundheitliche und konsularische Krisen zu managen, mit einem Fokus auf die Abwehr von komplexen Cyber Angriffen, Desinformation und Anschlägen innerhalb und außerhalb der EU.

4.11 CYBER DIPLO ATTX18

Im Kontext des Rahmens für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyber Aktivitäten (Cyber Diplomacy Toolbox) hielt die Österreichische Ratspräsidentschaft (Abteilung für Cyber Sicherheit im BKA gemeinsam mit BMEIA) auf Ratsebene am 29. November 2018 in Brüssel eine Tischübung für EU-Mitgliedstaaten ab, um mögliche diplomatische Maßnahmen als Reaktion auf eine Krise zu erproben. Die Übung wurde inhaltlich an die zuvor abgehaltene EU-NATO-Übung HEX-ML 18 angelehnt und wurde mit maßgeblicher Unterstützung des Europäischen Auswärtigen Dienstes und des Generalsekretariats des Rates der EU organisiert. Vertreter verschiedendster relevanter Organisationen (Europäische Kommission, Europol EC3, ENISA, CERT-EU, NIS-Kooperationsgruppe, EDA und EUISS) nahmen als Beobachter teil.

5 Zusammenfassung / Ausblick

Im Jahr 2018 war die Erstellung von umfassenden Lagedarstellungen zur Cyber Sicherheit und die Kommunikation der Lage an die Stakeholder ein gut eingespielter Prozess. Die im Zuge der Umsetzung der Österreichischen Strategie für Cyber Sicherheit eingerichteten operativen Koordinierungsstrukturen IKDOK und OpKoord trafen sich regelmäßig und bereiteten die Lage in einem gemeinsamen Prozess auf.

Die Zusammenarbeit von staatlichen Organisationen funktionierte auf Basis der Koordinierungsstrukturen sehr effizient. Neuen und herausfordernden Bedrohungen konnte gut und schnell begegnet werden. Dies zeigte sich bei den großen Vorfällen des Jahres 2018: Bei den Hardwareschwachstellen Spectre und Meltdown, beim Botnetz VPNFilter oder bei einem großen zielgerichteten Angriff auf kritische Infrastrukturen von Unternehmen und Behörden konnte die Bedrohung rasch analysiert und Hilfe bereitgestellt werden.

Der erfreuliche Trend, in Österreichs Unternehmen ausreichend Budget für die Absicherung ihrer Netz- und Informationssysteme zur Verfügung zu stellen, hielt auch 2018 an. In vielen Unternehmen wurden neue Sicherheitsmaßnahmen eingeführt, um die Cyber Sicherheit zu erhöhen. Dazu gehörten vor allem eine technische Aufrüstung, organisatorische Vorkehrungen und eine Sensibilisierung der Mitarbeiter. Zu beobachten waren vermehrte Aktivitäten in Richtung Aufdecken von Angreifern im eigenen Netz und dem damit verbundenen Einführen von SIEMs und strengeren Unternehmensprozessen. Treiber für Investitionen in Cyber Sicherheit waren, neben dem technischen Fortschritt, die 2018 in Kraft getretene Cyber Sicherheit relevante Legistik – das NIS-Gesetz und die Datenschutz-Grundverordnung.

Eine Steigerung von sicherheitsrelevanten Vorfällen im Cyber Bereich war auch 2018 ein Trend. Monetär motivierte Cyber Angriffe, wie Ransomwareattacken und Datendiebstähle stiegen 2018 besonders an. In die Breite gestreute Angriffe wie Ransomware oder Phishing waren in allen Unternehmensgrößen die am meisten erkannten Angriffsversuche. Im Gegensatz dazu waren DDoS-Vorfälle rückläufig, ein Trend der sich bereits im Vorjahr abzeichnete. Auch zielgerichtete Angriffe mit dem Schwerpunkt Informationsgewinnung waren im Rückgang.

Durch gesteigerte Abwehrmaßnahmen der Unternehmen und durch eine gute Sensibilisierung von Mitarbeiterinnen und Mitarbeitern konnten Angriffe oftmals bereits im Vorfeld erkannt und abgewehrt werden. Dies war besonders signifikant im Bereich Ransomware

und Phishing. Weiters ließ sich 2018 ein Trend beobachten, dass neue Ausgliederungen von Unternehmen besonders gerne angegriffen wurden.

Anzeigen wegen Cyber Crime-Delikten und Cyber Mobbing waren 2018 in Österreich rückläufig, auch hier griffen Präventionsmaßnahmen und intensive Ermittlungsarbeit. Gegen den Trend stieg die Zahl der Internet-Erpressungen allerdings deutlich an.

Die österreichische Landesverteidigung beobachtete 2018 neben den bereits oben genannten Themen eine weniger verbreitete Nutzung von fortgeschrittener Malware, dafür ein professionelleres Social Engineering via E-Mail und großflächigere Angriffe. Eine interessante Beobachtung in diesem Jahr war ein Rückgang von politisch motivierten Aktivitäten.

Cyber Bedrohungen wurden 2018 generell als Bedrohung für die nationale Sicherheit eingestuft. Nationale Cyber Sicherheit Strategien und gesetzliche Grundlagen mussten laufend angepasst werden, um mit der Entwicklung Schritt zu halten. Die Bedeutung des Bereichs Cyber Sicherheit spiegelte sich in den vielfältigen Aktivitäten in internationalen Organisationen wider. Fragen der Cyber Sicherheit wurden – für Österreich wichtig – in der EU, VN, OSZE, NATO, OECD, Europarat sowie in multilateralen Foren unter aktiver Beteiligung von Österreich thematisiert.

Thematisch stand in der EU die Umsetzung der Richtlinie zur Netz- und Informationssicherheit im Fokus. Die Richtlinie wurde 2018 unionsweit durch nationale Gesetze in Kraft gesetzt. Alle EU-Mitgliedstaaten starteten 2018 mit den Umsetzungen. Weitere ordnungspolitische Vorschläge – der Rechtsakt für Cyber Sicherheit, der eine starke Cyber Sicherheitsagentur und einen EU-weiten Zertifizierungsrahmen bringen wird und die Verordnung zur Bündelung von Ressourcen und Fachwissen in Forschung und Innovation – wurden 2018 in den Gremien verhandelt.

Für eine koordinierte Reaktion auf Cyber Sicherheitsvorfälle wurden Prozesse und Abläufe in der EU festgelegt, um bei großangelegten Cyber Angriffen schnell reagieren zu können. Der Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Aktivitäten wurde 2018 in Richtung Cyber Sanktionenregime erweitert. Besonderes Interesse galt dabei dem Thema Zurechnung von Cyber Angriffen und koordinierte europäische Vorgangsweise bei schweren Vorfällen.

Weitere große EU-Themen waren ein umfangreiches Investitionsprogramm für Cyber Sicherheit im Rahmen des Programms „Digitales Europa“ 2021-2027, die Vorbereitung der Europäischen Parlamentswahl im Hinblick auf Cyber Sicherheit, der Kampf gegen terroristische Inhalte im Internet und ein Aktionsplan gegen Desinformation, um demokratische Prozesse abzusichern.

Österreich hatte in der zweiten Hälfte 2018 im Rahmen der Ratspräsidentschaft den Vorsitz über die wichtigsten Cyber Sicherheitsgruppen in der EU inne. Ein herausforderndes gemeinsames Trio-Arbeitsprogramm für Cyber Sicherheit wurde auf Betreiben von Österreich aufgesetzt. Die Ziele – Cyber Sicherheit in der EU in ausgewählten Bereichen voranzubringen – waren sehr ambitioniert und konnten vollumfänglich und vollinhaltlich umgesetzt werden. Im Dezember 2018 veranstaltete die Österreichische Ratspräsidentschaft eine Cyber Konferenz in Wien.

In den VN wurden Themen der Cyber Sicherheit und Fragen des Völkerrechts im digitalen Raum in verschiedenen Gremien behandelt. Bei der thematisch wichtigsten Gruppe, den sogenannten Groups of Governmental Experts (GGE) kam es 2018 zu einer Spaltung wegen großer inhaltlicher Differenzen, künftig werden zwei parallele Prozesse weitergeführt. Eine österreichische Resolution „Eingriffe in die Privatsphäre nur im Einklang mit menschenrechtlichen Prinzipien" wurde im VN-Menschenrechtsrat (MRR) behandelt. Im September 2018 fand in Wien im Rahmen der IEG, der für Cyber Kriminalität eingerichteten intergouvernementale Expertengruppe, eine Konferenz zum Thema Cyber Kriminalität statt.

Österreich hat im Rahmen der NATO Partnership for Peace das Partnerschaftsziel „Cyber Defence" angenommen. Die diesbezüglichen Vereinbarungen für 2015 bis 2017 konnten von österreichischer Seite allesamt erfüllt werden. Derzeit läuft die Bearbeitung des nächsten PARP-Zyklus.

Cyber Sicherheit war ein Schwerpunktthema der OSZE im Jahr 2018. Internationale Cyber Diplomatie, die Zusammenarbeit zwischen Staat und Privaten und Lösungsansätze für fiktive Cyber Attacken waren Fokusthemen. Die Arbeiten der Informellen Arbeitsgruppe zu Cyber Sicherheit konzentrierten sich 2018 auf die Umsetzung der beschlossenen vertrauensbildenden Maßnahmen.

Die Wichtigkeit von Cyber Sicherheit in Österreich spiegelte sich in der Anzahl nationaler Strukturen mit einem Fokus auf diese Thematik wider. Nationale Cyber Strukturen haben 2018 ihre Funktionstüchtigkeit im Regelbetrieb bewiesen, sie wurden etabliert, vernetzt und sie werden laufend an aktuelle Herausforderungen angepasst.

Öffentlich-private-Partnerschaften und Plattformen brachten die verschiedenen nationalen Akteure auf strategischer und operativer Ebene zusammen. Es bedarf für die Zukunft einer weiteren engen Zusammenarbeit aller Stakeholder, privat und öffentlich, militärisch und zivil, national und international, um die Widerstandsfähigkeit in Österreich gegen Cyber Bedrohungen weiterzuentwickeln.

Verschiedene ordnungspolitische Instrumente, wie das NIS-Gesetz, die Datenschutz-Grundverordnung, die Österreichische Strategie für Cyber Sicherheit und die ent-

sprechenden Stellen des Regierungsprogramms bildeten den Rahmen für ein nationales Cyber Ökosystem. Mit dem Inkrafttreten des NIS-Gesetzes 2018 wird die europäische NIS-Richtlinie umgesetzt. Diese wird Cyber Sicherheit in Österreich auf ein der Bedrohungslage angemessenes Niveau heben.

Die Funktionstüchtigkeit nationaler Strukturen wurde 2018 in etlichen nationalen und internationalen Cyber Übungen unter Beweis gestellt.