REPUBLIK ÖSTERREICH

Bericht Cyber Sicherheit 2018

BUNDESKANZLERAMT ÖSTERREICH

BM.I REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR INNERES

BMLV BUNDESMINISTERIUM FÜR LANDESVERTEIDIGUNG

EUROPA INTEGRATION ÄUSSERES BUNDESMINISTERIUM REPUBLIK ÖSTERREICH

Bericht
Cyber Sicherheit
2018

Wien, 2018

Impressum

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

Wien, im April 2018

Inhalt

Einleitung

Die Österreichische Strategie für Cyber Sicherheit (ÖSCS) legt fest, dass durch die Cyber Sicherheit Steuerungsgruppe ein jährlicher Bericht zur Cyber Sicherheit in Österreich erstellt wird. Der letzte Bericht wurde im Mai 2017 vorgelegt.

Der aktuelle Bericht Cyber Sicherheit 2018 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 2017, einzelne aktuelle Entwicklungen im Jahr 2018 haben Eingang gefunden.

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

1 Cyber Lage / Bedrohungsanalyse

Die heutige Gesellschaft ist fortgesetzt von technischen Errungenschaften und in weiterer Folge von der Verfügbarkeit, Vertraulichkeit und Integrität von Information abhängig. Staaten, Gruppierungen, aber auch kriminelle Akteure nutzen die Werkzeuge der IKT zu ihrem Vorteil; kriminelle Aktivitäten über das Internet nehmen stetig zu. Sowohl die Akteure als auch die angewandten Methoden, die benötigten Ressourcen und die Effektivität der Angriffe variieren dabei in einem sehr breiten Rahmen.

1.1 Lage Cyber Sicherheit – operative Ebene

Die ÖSCS sieht vor, dass auf der operativen Ebene sowohl periodische, als auch anlassbezogene Lagebilder für Cyber Sicherheit zu erstellen sind. Im Jahr 2016 nahm der Innere Kreis der operativen Koordinierungsstrukturen (IKDOK), ein Koordinierungsgremium auf der operativen Ebene, nach umfassenden Vorarbeiten den Regelbetrieb auf. Seit diesem Zeitpunkt wurde im Gremium intensiv daran gearbeitet, eine regelmäßige, umfassende Lagedarstellung zur Cyber Sicherheit in Österreich zu erstellen und an Stakeholder zu kommunizieren. Im Folgenden ist eine Auswahl von wesentlichen Vorfällen aus diesen Lagebildern zusammengefasst; die Zusammenstellung erfolgt in der Reihenfolge des Auftretens dieser Vorfälle.

1.1.1 WannaCry (05 / 2017)

Am 12.05.2017 war unter großem Medieninteresse europaweit eine signifikante Cyber Angriffswelle der Verschlüsselungssoftware (Ransomware) »WannaCry« zu beobachten. Die Schadsoftware nutzte eine zu diesem Zeitpunkt bereits seit Monaten bekannte Sicherheitslücke, um Zielsysteme zu infizieren und deren Festplatteninhalt zu verschlüsseln. Den Infizierten wurde versprochen, dass ihnen gegen Zahlung eines Lösegeldes ein Schlüssel zur Wiederherstellung der Daten übermittelt würde. Während die Auswirkungen in Österreich sehr gering ausfielen, waren europaweit zahlreiche kritische Infrastrukturen in mehreren Staaten betroffen, wie beispielsweise das National Health Service (UK), die Deutsche Bahn (DE) oder das Telekommunikationsunternehmen Telefonica (ES).

1.1.2 NotPetya (07 / 2017)

Während europaweit die Schäden der Schadsoftware »WannaCry« noch nicht vollständig behoben waren, ereignete sich ab 27.06.2017 mit der Verschlüsselungssoftware (Ransomware) »NotPetya« eine neuerliche Welle von Cyber Angriffen. Die Schadsoftware wurde in diesem Fall über kompromittierte Software-Updates einer legitimen Software, die für das Verfassen von ukrainischen Steuererklärungen zu verwenden ist, verbreitet. Zwar waren europa- und weltweit wiederum zahlreiche Unternehmen von der Infektion betroffen, doch zeigte sich bald, dass nur jene Unternehmen infiziert wurden, die geschäftliche Verbindungen zur Ukraine unterhielten. Der Aufbau und die Funktion der Schadsoftware deuten in diesem Fall weniger auf eine Bereicherungsabsicht der Täter, als auf eine gezielte Sabotage der Infrastruktur eines Landes (Ukraine) hin. Wie schon bei »WannaCry« waren auch hier die Mehrzahl der Angriffsvektoren bereits seit Monaten bekannt; fehlendes Patchmanagement und mangelndes Update-Bewusstsein ermöglichten trotzdem eine enorme Anzahl von Infektionen.

Für Österreich markiert das Auftreten von NotPetya eine Zäsur bei der staatlichen Reaktion auf solche Schadsoftwarewellen. So wurde diese Welle von ihrem ersten Auftreten bis zur letztendlichen Bewältigung vollständig vom IKDOK koordiniert. Dabei zeigte sich, dass zur Erkennung und Bewältigung derartiger Bedrohungslagen ein zentrales staatliches Gremium essentiell ist. Während einzelne Unternehmen oder branchenspezifische Gremien lediglich einen Ausschnitt der Situation beobachten können, war es dem Cyber Security Center, gemeinsam mit dem IKDOK möglich, die Lage gesamthaft zu erfassen und außergewöhnlich schnell entsprechende Schritte zu setzen (erster Hinweis um 15:16 Uhr, detailliertes Warnschreiben mit Lageeinschätzung und Handlungsempfehlungen um 18:05 Uhr).

1.1.3 Nationalistische Hackergruppen

Bereits beginnend mit Anfang September 2016 wurden österreichische Einrichtungen der kritischen Infrastrukturen Ziele von politisch motivierten DDoS-Angriffen durch ausländische nationalistische Hackergruppen. Unter den Zielen befanden sich u. a. die Webseite des Flughafens Wien-Schwechat, der österreichischen Nationalbank sowie die Webseiten verschiedener Ministerien und des Parlaments.

Diese Angriffe setzten sich auch im Jahr 2017, allerdings mit geringerer Intensität, fort. Auswirkungen dieser Angriffe waren nicht zuletzt aufgrund zahlreicher entsprechender Maßnahmen des Cyber Security Centers (Warnschreiben, Broschüre, Expertenrunde), erhöhter Wachsamkeit der staatlichen Einrichtungen sowie verbesserten Anti-DDoS Maßnahmen – wie etwa Geo-Fencing – kaum erkennbar.

1.1.4 Armada Collective (10 – 11 / 2017)

Während die DDoS-Angriffe von ausländischen nationalistischen Hackergruppen politisch motiviert waren und der Kategorie Hacktivism zugeordnet werden können, weisen die technisch vergleichbaren Cyber Angriffe des Armada Collective klar eine Bereicherungsabsicht auf und gehören damit in den Bereich des Cyber Crime. Nach jeweils einem kleineren Demonstrationsangriff sahen sich die betroffenen Unternehmen (unter anderem mehrere Zahlungs-Dienstanbieter in Slowenien und der Slowakei, sowie zahlreiche weitere in den Niederlanden) mit Erpressungen unter Androhung eines wesentlich größeren und andauernden Angriffs konfrontiert. Auch in Österreich war ein Unternehmen von einem entsprechenden Demonstrationsangriff und einer Erpressung betroffen. Die Angreifer, die hier unter dem Namen »Die Panzerknacker« aktiv wurden, ließen allerdings nach Verstreichen der Frist keinen Angriff folgen.

1.1.5 Wahlen im Fokus (09 / 2017)

In Deutschland zeigte der Chaos Computer Club (CCC) auf, dass Hard- und Software, die derzeit zur Übermittlung der Ergebnisse von Wahlen zu den jeweils übergeordneten Wahlbehörden eingesetzt werden, offenbar massive Schwachstellen aufweisen. Demnach bestehe die Möglichkeit, dass Wahlergebnisse bei der Übermittlung zur übergeordneten Wahlbehörde gezielt verfälscht werden. Zwar erscheint eine Manipulation des Wahlergebnisses auf diesem Weg in Österreich grundsätzlich nicht möglich, da parallel entsprechende Papierakte angelegt werden, die im Diskrepanz-Fall Priorität haben. Trotzdem könnte eine Verfälschung der Übermittlung (trotz einer anschließenden Korrektur) das Vertrauen der Wähler in das Wahlsystem beeinträchtigen und somit den demokratischen Prozess untergraben.

Aus diesem Grund ist das Cyber Security Center im Vorfeld sowohl an die Bundeswahlbehörde als auch an die Landeswahlbehörden herangetreten, um die Cyber Sicherheit der Nationalratswahlen sicherzustellen. Dabei wurde festgestellt, dass sich die Schnittstellen des Bundes sowie der analysierten Landesrechenzentren technologisch am Stand der Technik befinden und Sicherheitsmängel analog zur Analyse der deutschen Wahlsysteme in Österreich derzeit nicht bestehen.

1.1.6 Schwachstelle »KRACK« (10 / 2017)

Im Oktober 2017 wurde von den Medien unter dem Namen »KRACK« intensiv über eine neu entdeckte Schwachstelle im Protokoll von WLAN-Verbindungen (WPA/WPA2) berichtet. Dieses Protokoll ist die Grundlage nahezu aller WLAN-Verbindungen im privaten, wie im geschäftlichen Umfeld. Eine sofort eingeleitete, gemeinsame Analyse von CERT.at/GovCERT und dem Bundesministerium für Inneres führte jedoch zu dem Ergebnis, dass das Ausnutzen der Schwachstelle erheblichen technischen Aufwand, sowie eine unmittelbare physische Nähe des Angreifers zum Zielsystem bedingt. Daraus konnte abgeleitet werden, dass eine Nutzung der Schwachstelle für zielgerichtete Angriffe zwar möglich ist, eine breitflächige Ausnutzung hingegen unwahrscheinlich erscheint.

1.2 Lage Cyber Sicherheit – Unternehmen und Sicherheitsdienstleister

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

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

eingeladen, um auf der Basis Ihrer Tätigkeit dieses Wissen zu ergänzen. 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[8].

1.2.1 Unternehmen der kritischen Infrastruktur

Bei den Unternehmen der kritischen Infrastruktur war 2018 hinsichtlich des für IT-Sicherheit zur Verfügung stehenden Budgets ein erfreulicher Trend zu beobachten. Während das Budget im letzten Jahr nur bei etwa der Hälfte der Unternehmen gestiegen und bei der verbleibenden Hälfte der Unternehmen gleichgeblieben war, hat sich in diesem Jahr der Anteil gestiegener Budgets maßgeblich erhöht. Damals wie heute ist der Anteil der Unternehmen, die mit einem gesunkenen Budget auskommen müssen, erfreulicherweise verschwindend gering.

8 Einer namentlichen Nennung im Bericht haben die Unternehmen Grant Thornton Unitreu GmbH, Kapsch BusinessCom AG und PwC Österreich GmbH zugestimmt.

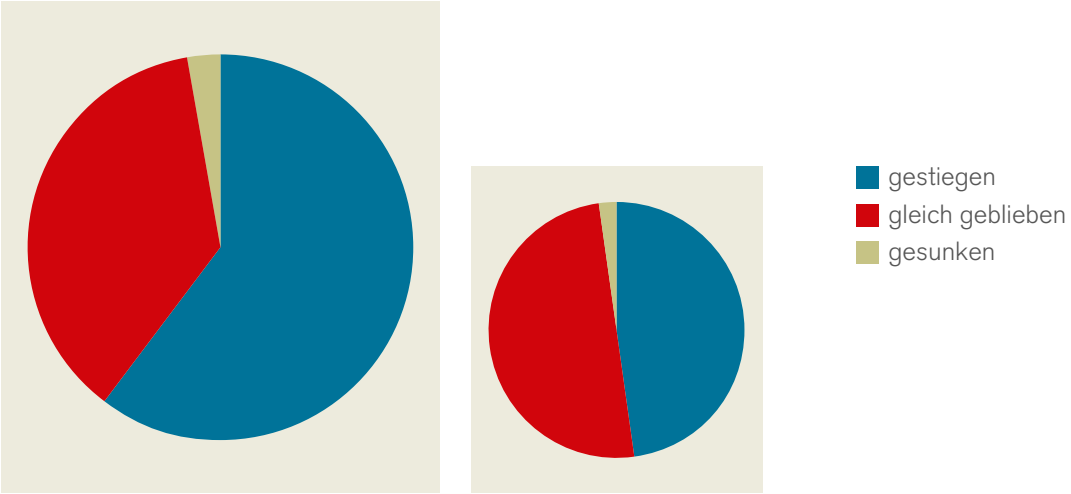


Abbildung 1: IT-Budget 2018
Abbildung 2: Vergleich 2017

Ebenso positiv hervorzuheben ist, dass 2018 bei praktisch allen befragten Unternehmen neue Sicherheitsmaßnahmen implementiert wurden, während dies im Vorjahr nur bei etwa 84 % der Befragten der Fall war. Dies ist insbesondere deshalb von großer Relevanz, da es oftmals erst solche neu eingeführten Maßnahmen ermöglichen, bestimmte IT-Sicherheitsvorfälle überhaupt erst als solche zu erkennen.

Betrachtet man die Art der neu eingeführten Sicherheitsmaßnahmen im Detail, so zeigt sich, dass nach Kategorisierung und gruppenweiser Zusammenfassung der angegebenen Einzelmaßnahmen zwei wesentliche Trends ablesbar sind:

- Zum einen ist festzustellen, dass offenbar ein Paradigmenwechsel eingesetzt hat. Standen im Vorjahr Maßnahmen zur aktiven Abwehr von Angriffen im Zentrum des Interesses, ist im Jahr 2018 ein klarer Trend zu erkennenden bzw. reaktiven Maßnahmen (Monitoring, SIEM[8], IR[9], SOC[10], IDS[11], IPS[12]) zu beobachten. Offenbar geht man zunehmend von der Idee ab, jeden Angriff durch geeignete Maßnahmen verhindern zu können und kommt zu dem Schluss, dass es entscheidender ist, einen Angriff bzw. Vorfall schnell zu erkennen und richtig darauf zu reagieren.
- Der zweite deutliche Trend zeigt, dass die Implementierung weiterer organisatorischer Maßnahmen zur Cyber Sicherheit stark im Steigen begriffen sind. Das unterstreicht die Sichtweise, dass Informationssicherheit kein Zustand, sondern ein Prozess ist, der laufende Evaluierungen, Anpassungen und Überarbeitungen erforderlich macht. Gleichzeitig mag es in diesem Zusammenhang eine Rolle spielen, dass mit dem voraussichtlich im Mai 2018 in Kraft tretenden Netz- und Informationssystemsicherheitsgesetz und der Datenschutzgrundverordnung zwei Normen vor der Tür stehen, die Maßnahmen in diesen Bereichen notwendig machen werden.

Interessant ist jedenfalls festzustellen, dass diese Trends sehr gut mit den ebenso abgefragten Lessons Learned und Trendeinschätzungen der Befragten korrelieren.

8 Security Information and Event-Management
9 Incident Response
10 Security Operations Center
11 Intrusion Detection System
12 Intrusion Prevention System

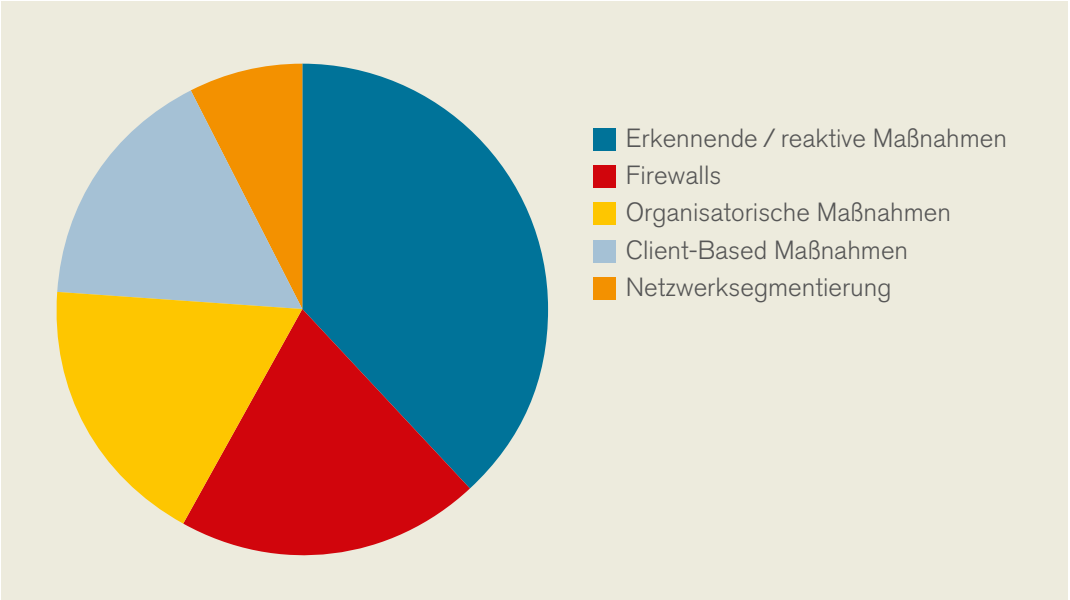
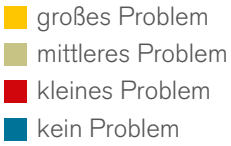


Abbildung 3: TOP5 der neu eingeführten Sicherheits-maßnamen (Verhältnis der Nennungen)

Bei der Einschätzung von Vorfallsursachen zeigt sich 2018 ein im Vergleich zum Vorjahr durchaus vergleichbares Bild. Die entsprechenden Verschiebungen innerhalb der abgefragten Kategorien fielen dabei sehr gering aus.



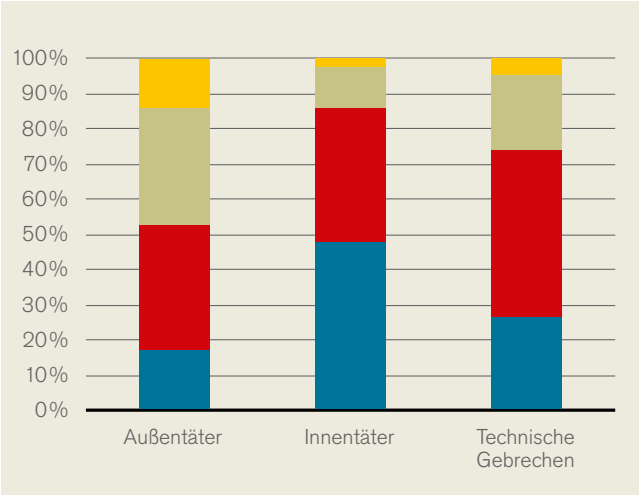


Abbildung 4: Einschätzung von Vorfallsursachen 2018

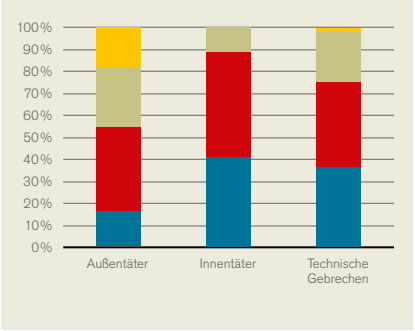
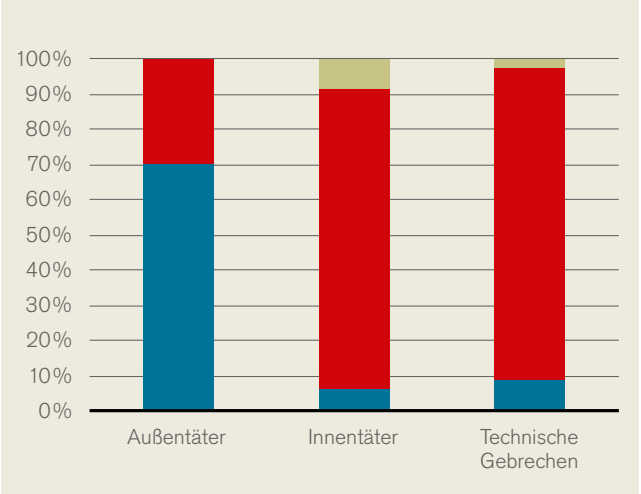
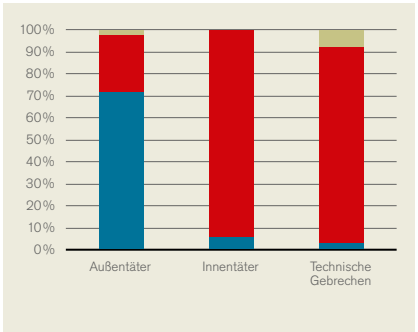


Abbildung 5: Vergleich 2017

Das bedeutet jedoch, dass – obwohl offenbar seit Jahren steigend – Bedrohungen durch Außentäter weiterhin lediglich als gleichbleibendes Problem wahrgenommen werden.





abnehmend
gleichbleibend
steigend

Abbildung 6: Trend bei Vorfallsursachen 2018

Abbildung 7: Vergleich 2017

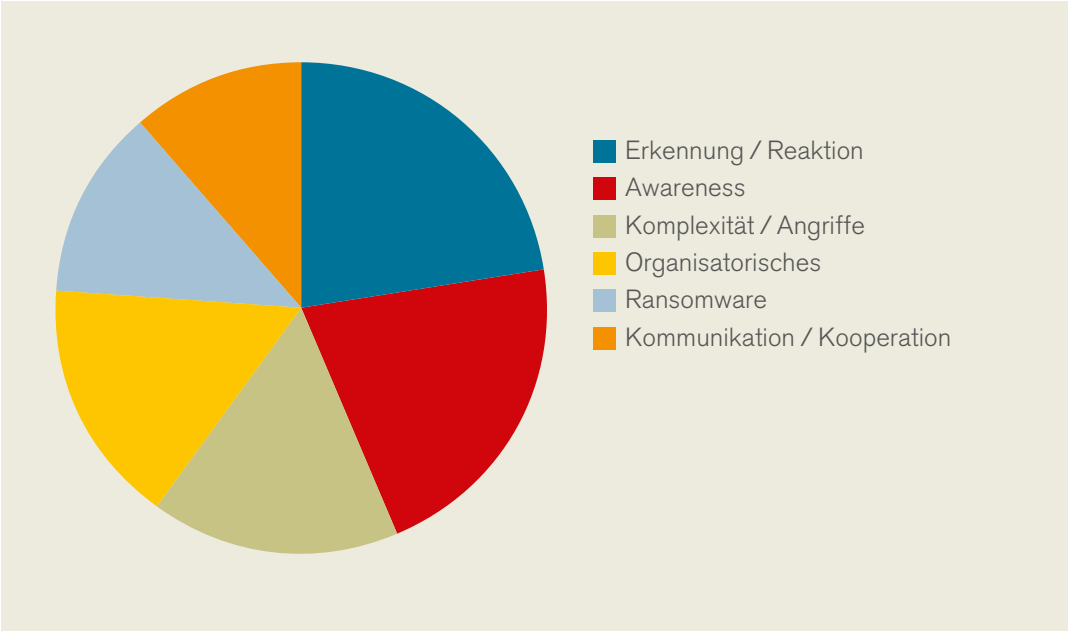
Das bedeutet jedoch, dass – obwohl offenbar seit Jahren steigend – Bedrohungen durch Außentäter weiterhin lediglich als gleichbleibendes Problem wahrgenommen werden.

Betrachtet man die Lessons Learned im Detail, so zeigt sich, dass diese – nach Kategorisierung und gruppenweiser Zusammenfassung – in Teilbereichen erstaunliche Parallelen zu den erkannten Trends und den implementierten Sicherheitsmaßnahmen aufweisen. Dies zeigt eindrücklich, dass die Wahrnehmungen der Verantwortlichen in Unternehmen auch zu entsprechenden Reaktionen und Maßnahmen führen, was sehr positiv bewertet werden kann.

Die TOP 6-Nennungen (Mehrfachnennungen waren möglich) betreffen demnach – in Gruppen zusammengefasst – folgende Erkenntnisse:

- Erkennung/Reaktion: Wichtigkeit von erkennenden bzw. reaktiven Maßnahmen
- Awareness: Awareness der Mitarbeiterinnen und Mitarbeiter ist entscheidend
- Komplexität/Angriffe: Komplexität der IT steigt / Angriffe werden professioneller und häufiger
- Organisatorisches: Wichtigkeit von organisatorischen Maßnahmen (z. B. Risikomanagement)
- Ransomware: Ransomware stellt eine erhebliche Gefahr für das Unternehmen dar
- Kommunikation/Kooperation: Interne und Externe Kommunikation bzw. Kooperation mit CERTs und Behörden ist erforderlich

Abbildung 8: TOP6 der Lessons Learned (Verhältnis der Nennungen)



Bei der Einschätzung der Trends für 2018 zeigt sich ein sehr breites Spektrum an Beobachtungen und Einschätzungen. Nach Kategorisierung und gruppenweiser Zusammenfassung können die meistgenannten Trendeinschätzungen wie folgt zusammengefasst werden:

- Die Gefährdungslage ist im Steigen begriffen. Angriffe werden komplexer und häufiger. Hauptmotivation hinter Angriffen ist in der Monetarisierung zu suchen.
- Cloud Security wird zu einem entscheidenden Thema. Es ist eine zunehmende Abhängigkeit der Unternehmen von den Cloud-Anbietern zu erwarten.
- Netz- und Informationssystemsicherheitsgesetz (NIS-G) und Datenschutzgrundverordnung (DSGV) werden erhebliche Anforderungen an Unternehmen stellen.
- Die Bedeutung organisatorischer Maßnahmen (z. B. Risikomanagement) wird künftig gegenüber rein technischen Maßnahmen zunehmen.
- Man geht davon aus, dass man sich nicht vollständig vor Angriffen schützen kann. Wichtig ist, Angriffe schnell zu erkennen und richtig zu reagieren.
- Die Abhängigkeit der Unternehmen von Hard- und Softwareprodukten stellt eine zunehmende Bedrohung dar.

1.2.2 Führende private Unternehmen aus der Cyber Security Branche

Die Befragung von führenden privaten Unternehmen aus der Cyber Security Branche wies in diesem Jahr eine vergleichsweise geringe Rücklaufquote auf. Das vorhandene Datenmaterial erlaubte es jedoch trotzdem, insbesondere im Hinblick auf die Erkennbarkeit von Trends, valide Aussagen zu treffen.

Die obenstehende Auswertung bestätigt die zuvor getroffene Einschätzung, dass die Vorfallszahlen vor allem in den Bereichen Ransomware und APT[8] offenbar ansteigend sind, wohingegen der Höhepunkt der DDoS-Wellen der Vorjahre überwunden scheint.

Insbesondere Ransomware scheint sich zunehmend als Mittel der Wahl für Cyber Kriminelle etabliert zu haben. Die geringe Zugangsschwelle (entsprechende Baukastensysteme, die ohne jede Vorkenntnisse auskommen, sind im Deepweb bzw. Darknet verfügbar) und die vergleichsweise leichte und risikoarme Monetarisierung der Angriffe (auf Basis von Krytowährungen) lässt die Vorfallszahlen in diesem Bereich stark ansteigen.

Diese Einschätzung korreliert auch sehr gut mit den Trends im Bereich der Motivationen. Hier ist ein massiver Anstieg bei monetär motivierten Cyber Vorfällen festzustellen, der direkt mit dem entsprechenden Anstieg bei Ransomware in Zusammenhang gebracht werden kann.

	A	B	C	D	E	F
monetär	=	+	=	+	+	–
politisch	=	=	=	=	–	
persönlich	=			=	=	=
staatlich	=	=		+	=	–
technisches Gebrechen	+	=		+	=	+

Abbildung 9: Trends bei bearbeiteten Vorfallsarten

8 Advanced Persistant Threat

Abbildung 10: Trends bei Motivationen

Im Hinblick auf die beiden offenbar am stärksten im Zunehmen begriffenen Vorfallsarten sind auch die entsprechenden Lessons Learned der führenden privaten Unternehmen aus der Cyber Security Branche von großer Relevanz.

In Bezug auf Ransomware kann festgestellt werden, dass

- mittlerweile häufig auch große Unternehmen von Angriffen betroffen sind,
- Sicherheitsmaßnahmen rein am Perimeter nicht ausreichend erscheinen,
- Backup-Konzepte, Business Continuity Management und Desaster Recovery Prozesse essentiell sind, jedoch oftmals gar nicht oder nicht ausreichend getestet vorliegen,
- Patchmanagement viel Schaden hätte verhindern können und
- entsprechende Awareness der Anwenderinnen und Anwender – als zentrale Lessons Learned – dringend aufgebaut werden muss.

In Bezug auf Bedrohungen durch APTs ist festzuhalten, dass

- fast ausschließlich große Unternehmen betroffen sind,
- fehlendes Bedrohungsbewusstsein, ein Ignorieren des Gefahrenpotentials und schlicht fehlendes Know-How weit verbreitet sind,
- Technikeinsatz alleine (ohne ausreichendes, geschultes Personal) das Problem nicht lösen kann,
- genaue Kenntnis der eigenen Infrastruktur, sowie umfassende Monitoringmaßnahmen notwendig sind, um die Gefahr rechtzeitig zu erkennen und
- Maßnahmen zur Verhinderung der Ausbreitung im eigenen Netz unbedingt zu setzen sind.

1.3 Lage Cyber Crime

Im Berichtszeitraum 2017 (Jänner-November) wurde durch das Bundeskriminalamt ein Anstieg von mehr als 52,6 % bei Cyber Crime Delikten im Vergleich zum Jahr 2016 verzeichnet. Das Phänomen Ransomware/Verschlüsselungstrojaner verzeichnet dabei mit mehr als 186 % den größten Anstieg. Gerade bei Ransomware muss darüber hinaus von einem großen Dunkelfeld ausgegangen werden, da viele Betroffene keine Anzeigen erstatten und Unternehmen auf Grund eines befürchteten Reputationsverlustes oftmals ebenso davor zurückschrecken. Versuchte Angriffe werden meist gar nicht zur Anzeige gebracht. Der Angriffsvektor für Verschlüsselungstrojaner ist in der Regel computerbasiertes Social Engineering, wobei auf die Gutgläubigkeit oder Unbedarftheit der Opfer gezählt wird. Ein Klick auf und in ein E-Mail, vermeintliche gesendet von der Hausbank oder von einem Paketlieferservice, ermöglicht dem darin eingebetteten Schadcode seine zerstörerische Wirkung zu entfalten. Die Höhe der Erpressungsforderungen durch die Täter werden oft nach einer Prüfung der jeweiligen »Finanzkraft« individuell festgesetzt.

Kriminelle Geschäftsmodelle unter dem Sammelbegriff »Crime as a Service (CaaS)« bieten schnellen und leichten Zugang zu jedweder Art von bösartiger Software und diversen cyberkriminellen Dienstleistungen für den sonst cyber-unbedarften Bedarfsträger. Diese Dienste, u. a. DDOS-Angriffe, können auf einfache Weise im »digital Underground« angekauft oder gebucht und auf anonyme Weise bezahlt werden (z. B. per Bitcoin).

Diese Art der Kriminalität des cyber-dependent Crime ist jedoch ausschließlich abhängig von der Verfügbarkeit von Computernetzen oder anderer Art von Informations- und Telekommunikations-Technologie (IKT). Cyber-dependent Crime untergräbt die Vertraulichkeit, Integrität und Verfügbarkeit in Netzwerke, Geräte sowie Daten und Services in diesen Netzwerken und somit das Vertrauen in Online-Dienste und in neue Technologien wie dem Internet of Things (IoT).

Dabei trägt das IoT durch die rasante Zunahme mangelhaft geschützter Geräte im Internet selbst dazu bei, neue Angriffsszenarien zu eröffnen. Diese Geräte, die Dinge im Internet, sind prädestiniert für die Eingliederung in sogenannte Bot-Netze, wie Mirai.

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. Im Cyber Raum kann die Zurechenbarkeit von (auch offensiven)

Handlungen leicht verschleiert werden, militärstrategische und strategische Zielsetzungen können somit mit verhältnismäßig geringem Aufwand erreicht werden.

Für das BMLV bedeutet dies, sich im Rahmen der Umfassenden Landesverteidigung bestmöglich auf die militärische Landesverteidigung im Cyber Raum auszurichten und vorzubereiten. Sie umfasst sowohl alle Maßnahmen der Informations- und Kommunikationstechnologie

(IKT) Sicherheit als auch alle Maßnahmen zur Abwehr von souveränitätsgefährdenden Cyber Angriffen auf die Republik Österreich. Souveränitätsgefährdend können Cyber Angriffe z. B. auf die militärischen IKT-Systeme sowie auf kritische Infrastrukturen und/oder verfassungsmäßige Einrichtungen Österreichs sein. Generell können aus den vorliegenden Daten des BMLV folgende Trends abgeleitet werden:

- Weiterer Anstieg an automatisierten Angriffen auf Netzwerkebene
- Nutzung von fortgeschrittener Malware und professionelleres Social Engineering via E-Mail
- Häufigere Ausnutzung von altbekannten Schwachstellen, als die Verwendung von Aktuelleren
- Vermehrt politisch motivierte Aktivitäten

Border Protection

Aus den Daten der Sicherheitssysteme des BMLV lassen sich bisherig bekannte Trends unverändert fortführen. So konnte auf Netzwerkebene in den Sicherheitseinrichtungen weiterhin ein wachsender Anstieg an geblockten Zugriffen beobachtet werden. Diese werden vor allem durch automatisierte Angriffe und Scans verursacht. Dies bedeutet auch, dass es einen Anstieg des Grundrauschens bei den Netzwerkkomponenten gibt, welches die Auswertungen erschwert. Für das kommende Jahr ist mit einem weiteren Anstieg in dieser Form zu rechnen.

Mail

Anders sieht dies beim traditionellen E-Mail-Verkehr aus. Ungeachtet von normalen Spam-Nachrichten konnte festgehalten werden, dass es in dieser Domäne zu einer Verschiebung zu fortgeschrittener Malware kommt. Unter fortgeschrittener Malware wird in diesem Zusammenhang Schadcode verstanden, der nicht von herkömmlichen Virenscannern anhand von Signaturüberprüfungen erkannt wird, sondern erst durch Sandboxanalysen (Anm.: mit diesen wird vorab automatisiert geprüft, welche Auswirkungen das Öffnen eines Anhangs oder eines im Mail enthaltenen Links zu einer externen Seite, auf ein System hätte). Dies bedeutet, dass es in Bezug auf den E-Mail-Verkehr, anders als bisher erwartet, in Summe einen Rückgang an Viren und Trojanern gibt, jedoch der Anteil an fortgeschrittener Malware stark zugenommen hat. Damit steigt die Bedrohung durch Schadcode in Mails weiter an.

Schwachstellen

Bei den Beobachtungen in Bezug auf Schwachstellen, die in diesem Jahr veröffentlicht worden sind konnte festgestellt werden, dass diese kaum bis gar nicht für Angriffe ausgenutzt wurden. Der Fokus liegt hier eher bei bewährten Vektoren, wie bekannten Web-Angriffsmustern, Powershell-Skripten in Verbindung mit Dropper, sowie Verschlüsselungssoftware.

Ausblick

In der Zukunft wird mit einem weiteren Anstieg an automatisierten Angriffen gerechnet, wodurch sich auch das Grundrauschen, aus dem relevante Incident-Hinweise extrahiert werden müssen, weiter erhöhen wird. Vor allem beim Angriffsvektor E-Mail ist ein Trend in Richtung automatisierter Personalisierung anzunehmen. Dies bedeutet, dass die Angreifer sich nicht nur als bekannte Services (Bank, Post, Rechnungen, etc.) ausgegeben, sondern auch deutlicher Bezug auf das Unternehmen bzw. die Personen nehmen werden.

Eine weitere Herausforderung von besonderer Bedeutung für den öffentlichen Bereich sowie der kritischen Infrastruktur stellen die zunehmenden Aktivitäten von politisch motivierten Gruppierungen und Hacktivisten dar. Diese versuchen durch Ausnutzung technischer Mittel Schäden in jeglicher Form zu realisieren, um dadurch mehr Aufmerksamkeit zu erlangen.

2 Internationale Entwicklungen

In den letzten Jahren wurden Fragen der Cyber Sicherheit von zahlreichen internationalen Organisationen und multilateralen Foren aufgenommen und 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

In seiner Rede zur Lage der Union am 13.09.2017 hat der Präsident der Europäischen Kommission seine Vorstellungen für die Zukunft Europas bis zum Jahr 2025 dargelegt. Für den Bereich Cyber Sicherheit sei es das erklärte Ziel der Europäischen Kommission, die Reaktionsfähigkeit der EU auf Cyber Angriffe entscheidend zu verbessern. Um dieses strategische Ziel zu erreichen haben die Europäische Kommission und die Hohe Vertreterin am 13. und 19. September 2017 eine breite Palette an Instrumenten und Maßnahmen zum Aufbau einer soliden Cyber Sicherheitsstruktur unter dem Titel »Paket zur Cyber Sicherheit« vorgeschlagen.

Unter dem Ratsvorsitz Estlands wurden am 20.11.2017 Schlussfolgerungen des Europäischen Rates zur »Abwehrfähigkeit, Abschreckung und Abwehr: die Cyber Sicherheit in der EU wirksam erhöhen« angenommen. Begleitend wurde ein Aktionsplan zur Implementierung aller Maßnahmen aus den Ratsschlussfolgerungen und dem Cyber Sicherheitspaket erstellt und am 20.12.2017 angenommen. Dieser Aktionsplan wird laufend von jeder Präsidentschaft bewertet und aktualisiert.

Als Rechtsakt des Pakets zur Cyber Sicherheit hat die Europäische Kommission einen Verordnungsvorschlag veröffentlicht. Dieser Verordnungsvorschlag umfasst im Wesentlichen zwei Kernbereiche, und zwar die Reformierung der ENISA zur Schaffung einer »EU Cyber Sicherheitsagentur« und die Schaffung eines EU-rechtlichen Rahmens für IKT-Sicherheitszertifizierungssysteme (»European ICT Security Certification Framework«) in der EU.

Die Cyber Diplomacy Toolbox (Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyber Aktivitäten) ist Teil des EU-Ansatzes für Cyber Diplomatie, der zur Konfliktverhütung, zur Eindämmung von Cyber Bedrohungen und zu größerer Stabilität in den internationalen Beziehungen beiträgt. Er soll die Zusammenarbeit fördern, unmittelbare und langfristige Bedrohungen eindämmen und auf lange Sicht Einfluss auf das Verhalten potenzieller Angreifer nehmen. Bei ihrer diplomatischen Reaktion auf böswillige Cyber Aktivitäten wird die EU in vollem Umfang von Maßnahmen der Gemeinsamen Außen- und Sicherheitspolitik und,

falls erforderlich, restriktiven Maßnahmen Gebrauch machen. Eine gemeinsame Reaktion der EU auf böswillige Cyber Aktivitäten würde in einem angemessenen Verhältnis zur Tragweite, Größenordnung, Dauer, Intensität, Komplexität, Raffiniertheit und Wirkung der Cyber Aktivität stehen. Die Arbeiten zur Toolbox wurden unter dem EE-Ratsvorsitz abgeschlossen. In den kommenden Monaten, d.h. jedenfalls während der BG Präsidentschaft, aber voraussichtlich auch über die Dauer des österreichischen Vorsitzes, richtet der EAD ein eigenständiges Diskussions-/Workshop-Format zu diesem Thema ein.

Am 5.7.2016 wurde die Mitteilung der EK zur »Stärkung der Abwehrfähigkeit Europas im Bereich der Cyber Sicherheit und Förderung einer wettbewerbsfähigen und innovativen Cyber Sicherheitsbranche« angenommen. Entsprechend dieser EK-Mitteilung wurde eine vertragliche öffentlich-private Partnerschaft (cPPP) für Cyber Sicherheit zwischen der Europäischen Kommission und Akteuren des Cyber Sicherheitsmarkts, die von der ECSO (European Cyber Security Organisation) vertreten werden, eingerichtet. In dieser cPPP wirken neben Vertretern der Industrie auch Vertreter nationaler, regionaler und lokaler öffentlicher Verwaltungen, Forschungszentren und Hochschulen mit. Die NAPAC Gruppe (National Public Authority Representatives Committee) ist innerhalb der ECSO das Gremium, über welches jene öffentlichen Verwaltungen, die Mitglieder in der ECSO sind, in einem gesonderten Format die Aktivitäten der ECSO gestalten. Aktuell sind 15 öffentliche Verwaltungen als Mitglieder in der ECSO registriert und damit auch Teilnehmer in der NAPAC. Österreich ist grundsätzlich durch je einen Vertreter des BKA (Untergruppe GAG (Governmental Advisory Group)) und des BMVIT (Untergruppe R&I-Group) vertreten.

Die Trio-Ratspräsidentschaft aus Estland, Bulgarien und Österreich legte erstmals ein gemeinsames Arbeitsprogramm für den Bereich »Cyber« vor. Darin sind die Zielsetzungen und Hauptaktivitäten für den Zeitraum von Juli 2017 bis Dezember 2018 dargelegt, auf die sich die Trio-Partner im Vorfeld geeinigt hatten, um Kontinuität in diesem dynamischen Bereich zu gewährleisten. Die Erfüllung des Trioprogramms erfolgt in laufender Abstimmung der drei Präsidentschaften. Im Dezember 2017 wurde unter den Trio-Präsidentschaften, auf Initiative von Österreich, ein entsprechender Aktionsplan erstellt.

Am 06.07.2016 wurde die Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-RL) beschlossen. Ziel dieser Richtlinie ist es, das Cyber Sicherheitsniveau in allen Mitgliedsstaaten zu heben, was insbesondere durch folgende Instrumente/Vorgaben erreicht werden soll:

- Annahme einer nationalen NIS-Strategie, sowie die Aufstellung einer oder mehrerer NIS-Behörden und Computer Notfallteams.
- Verpflichtendes Risikomanagement, Mindest-Sicherheitsvorkehrungen sowie eine Meldeverpflichtung bei erheblichen Sicherheitsvorfällen für Betreiber wesentlicher Dienste und Anbieter digitaler Dienste.
- Schaffung einer Kooperationsgruppe bestehend aus den Mitgliedstaaten, der EK und ENISA für strategische Aufgaben und eines CSIRT-Netzwerks für operationelle Aufgaben. Aufbau eines EU-weiten NIS-Kooperationsnetzwerks zum Austausch von Vorfällen und damit zusammenhängender, aufklärungsrelevanter Informationen.

Die Umsetzung der Richtlinie hat gemäß Artikel 25 durch die Mitgliedstaaten zu erfolgen. In Österreich wird diese durch das Cyber Sicherheitsgesetz gewährleistet, welches im Rahmen der interministeriellen legistischen Arbeitsgruppe im Bundeskanzleramt erarbeitet wird.

Angelegenheiten rund um den Themenbereich »Cyber« in seiner Gesamtheit (d. h. Cyber Sicherheit, Cyber Kriminalität, etc.) werden im Rat in einer ständigen Arbeitsgruppe, der sogenannten Horizontalen Gruppe »Fragen des Cyber Raums« (HWP on Cyber Issues) behandelt. Diese Gruppe stellt die strategische und horizontale Koordinierung der grenzüberschreitenden und multidisziplinären Querschnittsmaterie Cyber im Rat sicher und kann auch Legislativvorhaben behandeln. Die HWP on Cyber Issues wird federführend vom BKA im Sinne der gesamtstaatlichen Koordination betreut.

2.2 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. Die Expertengruppe konnte sich diesmal aber auf keinen Konsensbericht einigen; zu groß waren die Differenzen vor allem zu Fragen des Völkerrechts und dessen Anwendbarkeit im Cyber Space. Über die Fortführung der Arbeit der Expertengruppe besteht derzeit keine Einigkeit.

Bereits zur Jahrtausendwende rief die Generalversammlung der Vereinten Nationen (VN-GV) den »World Summit on the Information Society (WSIS)« ins Leben. Der primäre Fokus des WSIS Forums 2017 lag auf der Agenda 2030, wobei die Wirkung von IKTs auf fast allen nachhaltigen Entwicklungsziele (SDGs) hervorgehoben wurde. Cyber Sicherheit und Vertrauen im Internet sind unerlässlich für das weitere erfolgreiche Wachstum des Internets und in der Vertrauensbildung kommt Staaten eine Schlüsselrolle zu. Das Multistakeholder Internet Governance Forum thematisierte Cyber Sicherheit sowohl in den Hauptsitzungen als auch in den Workshops, dabei blieb unbestritten, dass Cyber Angriffe weiterhin eine der größten Sorgen für Staaten, Industrie sowie Endverbraucher sind.

Darüber hinaus beschäftigen sich auch mehrere Komitees der VN-GV 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 Dritten Komitee und im VN-Menschenrechtsrat (MRR) von besonderer Bedeutung. Die von Österreich als einer 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.

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[8] dar und konzentriert sich dabei in seiner Hilfeleistung für betroffene Mitgliedstaaten auf folgende drei Schwerpunkte:

- Verbesserung der Ermittlung, Strafverfolgung, und Beurteilung von Cyber Kriminalität, v. a. im Bereich sexuelle Ausbeutung und Kindermissbrauch 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;
- Stärkung der nationalen und internationalen Kooperation und Informationsaustauschmechanismen zwischen Regierungen, Strafverfolgungsbehörden und der Privatwirtschaft, sowie Stärkung des öffentlichen Bewusstseins.

Die 2010 im Bereich Cyber Crime eingerichtete intergouvernementale Expertengruppe (IEG) trat, nach Sitzungen im Jahr 2011 und 2013, vom 10. bis 13.04.2017 zum dritten 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.[9]

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.

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 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.

Im Kontext der Vereinten Nationen in Genf werden die Aufrufe der Zivilgesellschaft und der Hightech Industrie für eine Cyber Konvention immer lauter. Microsoft Präsident Brad Smith schlägt mit der Digital Geneva Convention ein neues Abkommen vor, um die Zivilbevölkerung im Cyber Space auch in Friedenszeiten zu schützen und ein verantwortungsbewusstes Handeln von Staaten im Cyber Space zu fordern. Dieser Vorschlag hat eine Diskussion in sowohl intergouvernementalen (ITU, CSTD) als auch Multistakeholder Foren (WSIS, IGF) im Internetbereich in Genf ausgelöst, doch wie die Verhandlungen eines solchen Abkommens gegebenenfalls aussehen könnten, bleibt bisher unklar.

8 http://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf
9 CCPCJ Res 26/4 (https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_26/CCCPJ_Res_Dec/CCPCJ-RES-26-4.pdf)

2.3 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. 2017 fanden einerseits formelle und informelle politische Konsultationen zwischen den fünf westeuropäischen Partnern (WEP-5: Schweiz, Irland, Finnland, Schweden, Österreich) und der NATO zu Cyber Themen statt. 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. Auch im Rahmen der regelmäßigen »Staff Talks« mit dem für Partnerschaften zuständigen Assistant Secretary General der NATO, Alejandro Alvargonzález, letztmalig im Jänner 2017 in Wien, wurden Fragen der Cyber Sicherheit thematisiert.

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.

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.

2.4 OSZE

Seit 2012 legt die Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) ein besonderes Augenmerk auf das Thema Cyber Sicherheit. Ziel der Bemühungen ist es, mit vertrauensbildenden Maßnahmen zur Verminderung der Konfliktrisiken beizutragen, die mit dem Gebrauch moderner Informations- und Kommunikationstechnologie verbunden sind. Eine informelle Arbeitsgruppe erarbeitete 2013 einen ersten Katalog von elf vertrauensbildenden Maßnahmen, um durch Transparenz und Zusammenarbeit effizienter auf solche Bedrohungen reagieren zu können.

2014 begannen die 57 Teilnehmerstaaten, 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 tauschen Informationen über die nationale Organisation von Cyber Sicherheitsplänen, sowohl im staatlichen als auch im privaten Bereich, aus. Im März 2016 konnten fünf weitere vertrauensbildende Maßnahmen beschlossen werden, die die bestehende Zusammenarbeit stärken und vertiefen. Die OSZE ist somit bisher die einzige

regionale Organisation, deren teilnehmende Staaten sich auf vertrauensbildende Maßnahmen im Bereich Cyber Sicherheit einigen konnten.

Anlässlich des OSZE-Ministerrates in Hamburg im Dezember 2016 verabschiedeten die teilnehmenden Staaten einen gemeinsamen Beschluss zur Umsetzung und Weiterentwicklung der vertrauensbildenden Maßnahmen im Rahmen der Organisation.

Cyber Sicherheit war auch ein Schwerpunktthema des österreichischen OSZE-Vorsitzes im Jahr 2017. Am 15.02.2017 fand in der Wiener Hofburg die hochrangige Konferenz »Cyber Sicherheit für kritische Infrastruktur: Stärkung von Vertrauensbildung in der OSZE« statt, welche vom österreichischen Außenminister in seiner Funktion als amtierender Vorsitzender der OSZE, eröffnet wurde. Eine zweite große Konferenz, die »Austrian OSCE Chairmenship Conference on Cyber Security«, veranstaltete der österreichische OSZE-Vorsitz am 03.11.2017 in Wien. Im Mittelpunkt beider Konferenzen standen die Implementierung der bereits bestehenden vertrauensbildenden Maßnahmen, der Schutz kritischer Infrastruktur sowie die Förderung der Menschenrechte online. Namhafte nationale und internationale Experten diskutierten mit Vertretern aus nationalen und internationalen öffentlichen Institutionen sowie Vertretern des Privatsektors über Herausforderungen und Möglichkeiten für gesamtstaatliche Lösungsansätze. Beim OSZE Ministerrat in Wien am 07./08.12.2017 konnte nach langen und komplizierten Verhandlungen ein Ministerratsbeschluss zu Cyber Sicherheit angenommen werden. Der Beschluss bekräftigt vor allem die Arbeit der Informellen Arbeitsgruppe zu Cyber Sicherheit sowie die Geltung der Menschenrechte im Cyber Bereich und ruft die Teilnehmerstaaten zur weiteren Implementierung der bereits bestehenden Vertrauensbildenden Maßnahmen auf. Vor dem Hintergrund der schwierigen Ausgangslage in der OSZE (Russland hatte das Mandat der Informellen Arbeitsgruppe Anfang November für erschöpft erklärt) und auf VN-Ebene (die VN-Expertengruppe zu Cyber Sicherheit hatte 2017 keinen Bericht zustande gebracht) kann in diesem Beschluss ein wichtiges positives Signal für die multilaterale Cyber Diplomatie gesehen werden.

2.5 OECD

Die »Working Party On Security and Privacy in the Digital Economy« ist eine Arbeitsgruppe der OECD (Organisation für wirtschaftliche Zusammenarbeit und Entwicklung), die für Regierungen und nationale Stakeholder zu den Themen Cyber Sicherheit und Datenschutz Analysen und High Level Empfehlungen erstellt. In Österreich nimmt das BKA die inhaltliche Koordination für diese Arbeitsgruppe wahr. Schwerpunktthemen bei der OECD zum Thema Cyber Sicherheit 2017 waren unter anderem Sicherheitsleitlinien zum Schutz der kritischen Informationsinfrastrukturen auch im Hinblick auf notwendige Verbesserungen der internationalen Kooperation sowie die Entwicklung eines Bewertungsrahmens zur Verbesserung und Evaluierung von Richtlinien in klein- und mittelständischen Unternehmen im Bereich des digitalen Sicherheitsrisikomanagements.

2.6 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 Mitglieder angehören.
- Die »Central European Cyber Security Plattform« – eine Kooperationsplattform der Länder (und der CERTs / tlw. 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 am 16. April 2015 gegründet wurde. Österreich, vertreten durch das BKA wurde nach Abschluss eines Schweigeverfahrens am 3. Oktober 2017offiziell als 61. Mitglied bestätigt.
- Ferner nahm Österreich an weiteren hochrangigen und renommierten internationalen Cyber Sicherheitskonferenzen teil, wie etwa an den Annual EU Cyber Security Conferences in Brüssel (zuletzt im November 2017) sowie der Cyber Security Conference in Tallin (September 2017), den jeweiligen EU-Vorsitz-Konferenzen (im ersten Halbjahr 2017 in Valetta, im zweiten Halbjahr in Tallinn), der Cyber Intelligence Europe Conference and Exhibition« in Bukarest (September 2017), der EDA Annual Conference mit SG Cyber in Brüssel (November 2017) sowie an weiteren einschlägigen Tagungen, wie etwa in London (März 2017), Prag (Mai 2017), Tel Aviv (Juni 2017), Krakau (Oktober 2017) und New Delhi (November 2017).
- Schließlich hielt das BMEIA im Berichtszeitraum bilaterale Konsultationen zu Cyber Sicherheitsfragen mit Russland und Israel ab.

2.7 Nationalstaaten

2.7.1 Vereinigte Staaten von Amerika

In Anbetracht der Hackingvorwürfe im Zuge der Präsidentschaftswahlen 2016, welche die Administration bis heute beschäftigen, räumt die Administration von US-Staatspräsident Donald Trump dem Kampf gegen Cyber Bedrohung eine hohe Priorität ein. Der Fokus der Bemühungen konzentriert sich auf vier wesentliche Bereiche: IT-Sicherheit der Bundesbehörden, Schutz der Kritischen Infrastruktur, Entwicklung von Maßnahmen zur Umsetzung einer Politik der Abschreckung sowie Unterbindung der Einflussnahme ausländischer Mächte (v. a. durch Russland) in die nationalen, politischen Prozesse.

Bereits kurz nach dem Amtsantritt von Präsident Trump begann die neue Administration im Jänner 2017 mit der Ausarbeitung der Executive Order (EO) 13.800 »Strengthening the Cyber Security of Federal Networks and Critical Infrastructure«. Die EO macht u. a. die Leiter der Bundesbehörden bzw. Bundesagenturen für die Umsetzung eines effektiven Cyber Risikomanagements verantwortlich. Mit Bezug zur Cyber Sicherheit Kritischer Infrastrukturen soll erarbeitet werden, welche Befugnisse und Fähigkeiten der Bundesbehörden eingesetzt werden können, um die Cyber Sicherheit bzw. das Cyber Risikomanagement von Kritischen Infrastrukturen zu erhöhen. Als Grundlage für das Risikomanagement soll der Rahmenplan für die Verbesserung der Cyber Sicherheit in Kritischen Infrastrukturen, erstellt durch das »National Institute for Standards and Technology« (NIST), herangezogen werden.

Um den Kritischen Infrastrukturen die Möglichkeit zu geben, sich gegen Cyber Angriffe aktiv zu verteidigen, wurde im Oktober 2017 der »Active Cyber Defense Certainty Act« (ACDC) als Vorschlag im US-Repräsentantenhaus eingebracht. Kritische Stimmen meinen, dass das Gesetz den Firmen und Privatpersonen erlauben würde, außerhalb ihrer Netzwerke aktiv zu werden, um sich vor Cyber Angriffen zu schützen bzw. darauf zu reagieren. Derartige »hack-back« durch Privatpersonen oder Institutionen könnten zu einer gefährlichen Eskalation führen. Aufgrund der heftigen Kritik konnte der Vorschlag bis dato nicht vorangebracht werden.

Die im Dezember 2017 vom Weißen Haus veröffentlichte »National Security Strategy« formuliert folgende drei prioritäre Handlungsfelder im Cyber Bereich: Verbesserung der Zuordnungs- und Reaktionsfähigkeit bei Cyber Angriffen, Aufstockung von Cyber Fähigkeiten und Expertise der Regierungsbehörden und Kritischer Infrastruktur sowie Vernetzung und Erhöhung der Flexibilität der Behörden und deren Abläufe, um Cyber Operationen gegen Angreifer zu ermöglichen.

Zur Umsetzung dieser und der Cyber Initiativen seines Vorgängers Präsident Obama (z. B. der »Cyber Nationale Action Plan«, CNAP) wurde im Budgetentwurf der Administration Trump für das Fiskaljahr 2018 eine erneute Budgeterhöhung für Cyber Initiativen vorgeschlagen.

Wie hoch die Bedrohung von russischen Aktivitäten im Cyber Raum durch die USA eingeschätzt wird, zeigen eine Reihe von eingeleiteten Initiativen bzw. Gesetzesentwürfe. So wurde im Budget 2018 ein Fonds über ca. 82 Mio. € (entspricht 100 Mio. $) eigens zur Bekämpfung russischer Einflussnahme eingerichtet. Außerdem wurde in dem im August 2017 veröffentlichten »Intelligence Authorization Act« für das Geschäftsjahr 2018 dem »Senate Intelligence Committee« der US-Regierung untersagt, eine Cyber Partnerschaft mit Russland ohne Einbindung des US-Repräsentantenhauses einzugehen[10]. Zudem muss der Director of National Intelligence (DNI) eine gesamtstaatliche Strategie zur Bekämpfung der russischen Cyber Bedrohung in Bezug auf das US-Wahlsystem vorlegen. Vor zukünftigen Bundeswahlen muss im Vorfeld dieser eine Risikoanalyse der Wahlsysteme durch die Nachrichtendienste erfolgen.

Auf militärischer Ebene wurde im August 2017 das »United States Cyber Command« des US-Verteidigungsministeriums (angesiedelt in der National Security Agency), nach langer Vorbereitung zu einem eigenständigen »Unified Combatant Command« aufgewertet. Weiters verkündete GenLt Paul Nakasone, Kommandant der U.S. Army Cyber Command Ende Oktober 2017, dass alle »Cyber Mission Teams« der U.S. Army die volle Einsatzbereitschaft erreicht haben, und das mehr als ein Jahr vor dem Zeitplan. Bis dato konzentrierte sich die U.S. Army darauf, 41 voll einsatzfähige Teams für die aktiven Einheiten aufzubauen. Dabei wurden sowohl defensive (»Cyber Protection Teams«, CPTs) als auch offensive Cyber Teams aufgestellt. In den nächsten Jahren sollen zusätzliche 21 CPTs innerhalb der Nationalgarde und der Miliz eingerichtet werden.

Auf multi- sowie bilateraler Ebene werden die Bemühungen von den Zielen der »U.S. International Strategy for Cyber Space« (2011) geleitet, die fünf prioritäre Bereiche identifiziert: Digitale Wirtschaft, internationale Sicherheitspolitik, Förderung der Sorgfaltspflicht in Cyber Sicherheit, Kampf gegen Internetkriminalität sowie die Verwaltung und Freiheit des Internets. Im multilateralen Kontext wird derzeit der Ansatz einer »Coalition of the Willing« bei der Abwehr von Cyber Angriffen erwägt.

10 Im Juli 2017 erklärte Präsident Trump die Absicht, eine US-russische Cyber Einheit aufzustellen – ein Vorhaben, von dem er sich aufgrund negativer Reaktionen umgehend distanzierte.

Bei dem im Oktober 2017 abgehaltenen »U.S.-China Law Enforcement and Cyber Security Dialogue« (LECD) wurde die Gültigkeit des bisherigen Konsenses und der Kooperationsdokumente bekräftigt. Im September 2017 fand der erste bilaterale »US-Ukraine Cyber Security Dialog« in Kiew statt, in dessen Rahmen die USA 4 Mio. € (entspricht 5 Mio. $) an »cyber assistance« zur Prävention, Entschärfung von und Reaktion auf Cyber Angriffe zusicherten. Im November 2017 wurde der jährliche EU-US Cyber Dialog in Washington D.C. abgehalten. Ähnliche Foren bestehen u. a. mit Japan, Indien und Australien.

Mit Bezug zu der Erarbeitung von Grundlangen zur Cyber Abschreckung leistete der im Februar 2017 veröffentlichte Bericht des »Defense Science Board« des US-Verteidigungsministeriums einen wesentlichen Beitrag. Der Bericht schlägt drei Maßnahmen zur Verbesserung der US-Politik in diesem Bereich vor: Das Verteidigungsministerium muss gezielte Cyber Abschreckungskampagnen durchführen, die Verbesserung der Cyber Sicherheit von ausgewählten militärischen Systemen gewährleisten, um die Zweitschlagsfähigkeit zu erhalten sowie die Attributionsfähigkeit der Bundesbehörden stärken.

2.7.2 Russische Föderation

Im Dezember 2016 billigte der russische Staatspräsident Putin eine neue Informationssicherheitsdoktrin für die Russische Föderation, welche die vorhergehende Doktrin aus dem Jahr 2000 ersetzt. Der Fokus der Doktrin liegt auf der Prävention gegen mögliche Cyber Angriffe. Die überarbeitete Doktrin beschreibt die Potenziale von unterschiedlichen Cyber Bedrohungen und verweist auf die Notwendigkeit der behördenübergreifenden Kooperation, um derartige Angriffe abzuwehren und die Informationssicherheit Russlands zu gewährleisten.

Das russische Verteidigungsministerium führt die begonnene Entwicklung von Technologien zur Cyber Kriegsführung weiter und stellt dafür auch die erforderlichen Investitionen bereit. Russland geht von einem umfassenden Begriff der Informationssicherheit zum Schutz gegen militärisch-politische, terroristische und kriminelle Bedrohungen aus. Die Vorwürfe russischer Einmischungsversuche in westliche Wahlkämpfe werden als haltlos zurückgewiesen, wohingegen vor einer unzulässigen Gefährdung der Stabilität Russlands durch gezielte Propaganda-Kampagnen aus dem Ausland gewarnt wird.

Im Februar 2017 bestätigte der russische Verteidigungsminister Sergej Schoigu vor der Duma die Existenz von Cyber Truppen, die auch zur Gegen-Propaganda eingesetzt werden. Die Organisation sei potenter und effektiver als ihre Vorgänger. Diese Einheiten sollen primär zur nationalen Verteidigung und zu Gegenmaßnahmen im Informationsbereich eingerichtet worden sein.

Im innerstaatlichen Bereich setzt Russland auf eine Ausweitung der Kontrolle über den nationalen Informationsraum. Bei einer erweiterten Sitzung des russischen Sicherheitsrates Ende Oktober 2017 warnte Putin vor der globalen Tragweite von Cyber Angriffen, zu deren Opfern auch Russland zähle. Es gelte daher, das staatliche System gegen computergestützte Angriffe zu verbessern, den Schutz der Informationssysteme staatlicher Einrichtungen zu erhöhen, die Abhängigkeit von ausländischen Informationstechnologien zu reduzieren und die Sicherheit des russischen Segments des Internets zu stärken.

Bereits in den vergangenen Jahren wurde eine Reihe von restriktiven Gesetzen zur Regulierung des Informationsraums erlassen, die mitunter in einem Spannungsverhältnis zu den einschlägigen Grundrechten stehen. So wurden etwa föderale Gesetze zur Speicherung von Daten in örtlicher und zeitlicher Hinsicht geschaffen, die unter bestimmten Voraussetzungen auch den staatlichen Sicherheitsbehörden zur Verfügung zu stellen sind. Andere gesetzliche Änderungen verschärfen die Verantwortlichkeit von Massenmedien für den Inhalt auf deren Internetseiten.

Im Sommer 2017 wurde vom russischen Parlament ein föderales Gesetz zur Verbesserung der Sicherheit Kritischer Informationsinfrastrukturen verabschiedet, das die Kontrollmöglichkeiten für Sicherheitsbehörden ausweitet. Anfang November 2017 traten gesetzliche Änderungen zur Regulierung Virtueller Privater Netzwerke (VPN) in Kraft, welche die Umgehung der Sperrung blockierter Internetseiten verhindern sollen. Ebenso ist die Einführung gesetzlicher Änderungen zur Regulierung von Instant Messanger Diensten geplant, die gegen die anonyme Nutzung solcher Dienste gerichtet sind.

Auf internationaler Ebene strebt Russland eine Stärkung der Zusammenarbeit auf dem Gebiet der Cyber Sicherheit an. Dabei sucht Russland neben der Intensivierung der Zusammenarbeit mit Regionalorganisationen auch den Austausch mit westlichen Staaten, u. a. im Wege entsprechender Konsultationen auf Expertenebene. So wurden die Möglichkeiten zur Intensivierung der Zusammenarbeit auf dem Gebiet der Cyber Sicherheit beispielsweise beim Treffen von Putin mit Trump am Rande des G20-Gipfels im Juli 2017 in Hamburg ausgelotet. Ziel war dabei die volle Beachtung der internationalen Regeln in diesem Bereich sicherzustellen und die Einmischung in die internen Angelegenheiten anderer Länder zu verhindern. Im Rahmen der OSZE tritt Russland für eine verstärkte Thematisierung der Cyber Sicherheit ein.

Bei seiner Rede vor der Generalversammlung der VN im September 2017 in New York warnte Außenminister Lawrow vor einer Militarisierung des Informationsraumes und plädierte für die Ausarbeitung von internationalen Regeln für den digitalen Bereich unter Berücksichtigung der Sicherheitsinteressen aller Staaten. Er stellte diesbezüglich den von Russland ausgearbeiteten Entwurf für eine universelle Konvention zur Bekämpfung von Cyber Kriminalität zur Diskussion.

2.7.3 Volksrepublik China

Wie in den nationalen Strategien und Plänen vorgesehen, konzentriert sich China im Cyber Raum weiterhin auf die Ausweitung der Kontrolle des Staates, die weitere Modernisierung der Streitkräfte sowie die Fortführung der eingeleiteten Entwicklung zukunftsträchtiger Technologien. Die vorrangigen Ziele bleiben damit weiterhin die Verhinderung von Bedrohungen für die innere Stabilität und die Nutzung des Cyber Raumes für den Ausbau des politischen, wirtschaftlichen und militärischen Einflusses Chinas. Internetzensur wird von der Kommunistischen Partei nach wie vor als wesentlicher Faktor für den langfristigen Machterhalt betrachtet. Daher wird ein striktes Zensur-Regime aufrechterhalten und der Zugriff u. a. auf ausländische Medien, Suchmaschinen und Soziale Medien behindert.

Mit einem neuen »Nationalen Abwehrplan« will China auf die weltweit zunehmenden Cyber Angriffe reagieren. Die chinesische Cyber Sicherheitsbehörde gab im Juni 2017 überarbeitete Richtlinien heraus, mit deren Hilfe zukünftig Gefahren abgewehrt werden sollen. So werden etwa die Provinzen verpflichtet, die Computernetzwerke auf den neuesten Stand zu bringen und entsprechende Experten-Teams aufzubauen. Im September 2017 kündigte das Ministerium für Industrie und Informationstechnologie für Anfang 2018 ein Gesetz zur verstärkten Kooperation von staatlichen Unternehmen und staatlichen Institutionen im Bereich der Cyber Sicherheit an. Im Rahmen dessen soll eine zentrale Vorfallsdatenbank für Informationen zu Cyber Angriffen geschaffen werden.

Aufgrund einer im Mai 2017 durch die Behörde für die Verwaltung des Cyber Raums veröffentlichten und mit Juni 2017 in Kraft getretenen Regulierung werden die Betreiber von Online-Nachrichtenplattformen stärker reguliert. So sollen etwa Anbieter mit ausländischer finanzieller Beteiligung einer Sicherheitsüberprüfung unterzogen sowie die Einhaltung gültiger Gesetze sichergestellt werden.

Zudem kündigte die chinesische Behörde für die Verwaltung des Cyber Raumes im November 2017 die geplante Aufstellung einer Datenbank zur Erfassung von Namen von Journalisten und Online-Plattformen, die gefälschte Meldungen verbreiten, an. In diesem Rahmen soll auch die chinesische Öffentlichkeit die Möglichkeit haben, Falschnachrichten zu melden. Die Streitkräfte starteten eigene Initiativen gegen Falschnachrichten. So wurde im November 2017 eine Webseite vom Militär eröffnet, auf der dazu eingeladen wird, Falschnachrichten und Geheimnisverrat bzw. illegale Aktivitäten von Militärpersonen zu melden.

Auch in internationalen Gremien ist China bestrebt, seinen Ansatz für den Cyber Raum umzusetzen. Die Basis dafür bietet die im März 2017 von der Regierung veröffentlichte »Internationale Strategie für die Kooperation im Cyber Raum«. Im Mittelpunkt der Strategie stehen vier Prinzipien, die das Handeln der internationalen Staatengemeinschaft im Cyber Raum bestimmen sollten: Frieden, Souveränität, geteilte Herrschaft, gemeinsame Vorteile für den internationalen Austausch und Kooperation im Cyber Raum. Zur Umsetzung dieser Strategie soll u. a. die internationale Kooperation sowohl auf bi- als auch auf multilateraler Ebene gestärkt werden. Außerdem sollen die VN wesentlich zur Formulierung von internationalen Regeln für den Cyber Raum beitragen. Diese Strategie spiegelt den bereits langjährig verfolgten Ansatz der chinesischen Regierung wieder, wie der Cyber Raum international zukünftig geregelt werden soll.

Im April 2017 kamen China und Australien im Rahmen hochrangiger diplomatischer Gespräche überein, keine Wirtschaftsspionage gegeneinander durchzuführen und gemeinsame Maßnahmen zur Bekämpfung von Cyber Kriminalität zu schaffen. Das Übereinkommen ähnelt dem bereits 2015 zwischen China und den USA unterzeichneten Abkommen.

Im Rahmen der Streitkräfteentwicklung blieb das chinesische Schlagwort »informatisierte Kriegsführung« auch 2017 der Kernbegriff, um das hochgesteckte Ziel zu erreichen, China durch eine enge Kooperation von Militär, Forschung und Industrie bis 2020 zu einer weltweit führenden Nation im Cyber Bereich zu machen. Dies bedeutet die umfassende Nutzung neuer Technologien und innovativer Mittel auf allen Ebenen der Streitkräfte für Ausbildung und Einsatz. Darunter fallen z. B. Systeme für den Einsatz autonomer Drohnen, Präzisionswaffen, Cyber Waffen, »Cloud-Computing« sowie intelligenter Waffen, der Einsatz von Robotik, Künstlicher Intelligenz oder Schwarm-Intelligenz, aber auch moderne Simulationssysteme für die Ausbildung.

2.7.4 Deutschland

In der Sicherheitsstrategie für Deutschland 2016 stellte die deutsche Bundesregierung fest, dass die Cyber Bedrohungslage in Deutschland von steigender Komplexität und Interdependenz der eingesetzten Technik und sich ständig wandelnden Bedrohungen geprägt ist. Als Konsequenz setzte die Bundesregierung ihren Schwerpunkt auf vier Handlungsfelder: Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung, gemeinsamer Auftrag zur Cyber Sicherheit von Staat und Wirtschaft, leistungsfähige und nachhaltige gesamtstaatliche Cyber Sicherheitsarchitektur sowie die aktive Positionierung Deutschlands in der europäischen und internationalen Cyber Sicherheitspolitik.

Zur Erreichung dieser Zielsetzungen wurden 2017 eine Reihe von Maßnahmen gesetzt. So strebt die Bundesregierung z. B. ein Basis-Zertifizierungsverfahren für sichere IT-Verbraucherprodukte an. Diese technischen Richtlinien sollen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) erarbeitet werden. Zudem soll das Forschungsrahmenprogramm zur IT-Sicherheit »Selbstbestimmt und sicher in der digitalen Welt 2015 – 2020« weiter ausgebaut werden.

Für den militärischen Anwendungsbereich der IT- und Cyber Sicherheit übernimmt diese Aufgabe der »Cyber Cluster« an der Universität der Bundeswehr in München mit dem Forschungsinstitut »Cyber Defence und Smart Data« (CODE). Neben dem Aufbau eines Studienlehrganges »Cyber« soll in München insbesondere in den Bereichen Kryptologie, Quantenforschung, Satelliten-Kommunikation, Künstliche Intelligenz und autonome Systeme geforscht werden.

Die kommerzielle Nutzung und Weiterentwicklung innovativer und neuer Ideen in der IT-Sicherheit in Unternehmen und Startups soll explizites Ziel und Bestreben staatlicher Investitionen sein, um so einen möglichst hohen volkswirtschaftlichen Nutzen zu realisieren. Um die Wettbewerbsfähigkeit der nationalen IT-Sicherheitswirtschaft zu stärken, wird die Bundesregierung das Qualitätsmerkmal »IT-Security Made in Germany« fördern und Außenwirtschaftsinstrumente ausbauen.

Auch das Bundesministerium des Inneren, für Bau und Heimat setzte Initiativen, zur Entwicklung von Cyber Expertisen für die Sicherheitsbehörden im eigenen Geschäftsbereich um. So eröffnete Innenminister de Maiziere im September 2017 die in der Universität der Bundeswehr München angesiedelte Zentralstelle für Informationstechnik im Sicherheitsbereich (ZITiS). Die Geschäftsfelder der ZITiS sind in fünf Bereiche gegliedert: Digitale Forensik, Telekommunikationsüberwachung, Kryptoanalyse (Dekryptierung), Massendatenauswertung (»Big Data«) sowie Malware- und Hacking-Analysen.

Zur Stärkung einer leistungsfähigen und nachhaltigen gesamtstaatlichen Cyber Sicherheitsarchitektur wurde 2017 eine Stärkung des BSI angestrebt. Das BSI ist zudem federführend für die Organisation des »Nationalen Cyber Abwehrzentrums« verantwortlich. Der Betrieb des Zentrums basiert auf Kooperationsvereinbarungen der beteiligten Ministerien. Die aktuellen Überlegungen befassen sich mit einer allfälligen (personellen) Erweiterung des Zentrums und den Möglichkeiten einer verstärkten Zusammenarbeit, einschließlich Datenaustausch sowie eines 24/7 Betriebes.

Ein im April 2017 vom Bundestag verabschiedetes Gesetz, soll es deutschen Behörden ermöglichen, künftig aktiv gegen IT-Angriffe vorzugehen. Laut dem Gesetz sollen von Cyber Angriffen betroffene Behörden und Unternehmen Hilfe von einer staatlichen Eingreiftruppe – sogenannter »Mobiler Incident Response Teams« (MIRTs) – anfordern können. Die Experten des BSI sollen somit vor Ort die Abwehr von Cyber Angriffen unterstützen.

Im April 2017 wurde durch das deutsche Verteidigungsministerium der neue Organisationsbereich Kommando Cyber- und Informationsraum (CIR) in Bonn als militärischer Organisationsbereich unter Führung des Inspekteurs des Cyber- und Informationsraums aufgestellt. Zusätzlich soll im Verteidigungsministerium ein eigenes Cyber Lagezentrum geschaffen werden, das eine Redundanz zum Nationalen Cyber Lagezentrum sein soll und die Erfassung der bundeswehr-spezifischen Aspekte sicherstellen soll.

Zur Sicherstellung des personellen Aufwuchses im Cyber Bereich wurde vom Generalinspekteur mit März 2017 das Konzept zur »Cyber Reserve« in Kraft gesetzt. Durch die Schaffung einer »Cyber Reserve« werden die bisherigen Restriktionen bei der Auswahl des Personals teilweise aufgehoben. Die Integration von geeigneten Spezialisten im Cyber Bereich kann zukünftig auch aus dem Personenkreis der »Nichttauglichen«, aus Quereinsteigern und Ausländern erfolgen. Lediglich die Durchführung einer Sicherheitsüberprüfung ist vorgeschrieben.

Neben den gesetzten Maßnahmen ist die Bundesregierung bestrebt, weitere Rechtsgrundlagen zu schaffen. V. a. sollen die als erforderlich eingestuften Kompetenzen für die Durchführung von

offensiven Maßnahmen (»hack-back«) bei Cyber Angriffen geschaffen werden. Ausgangspunkt ist dabei das Grundgesetz mit den dortigen Richtlinien für eine »Gefahrenabwehr«. Ebenfalls in Diskussion stehen die Regelungen von Verfahren und Kompetenzen im Falle einer Cyber Krise, wie z. B. der Übergang zum Verteidigungs- oder Bündnisfall.

2.7.5 Vereinigtes Königreich

Im Jahre 2017 stand der Ausbau des im Oktober 2016 gegründeten und im Februar 2017 in Betrieb genommenen Nationalen Cyber Sicherheitszentrums (»National Cyber Security Center«, NCSC) im Vordergrund der britischen Cyber Sicherheitsbemühungen. Das NCSC vereinigt Fähigkeiten verschiedener Organisationen für Informationssicherheit, den Schutz Kritischer Infrastruktur, die Beobachtung der Cyber Lage sowie die Cyber Reaktionsfähigkeiten des CERT-UK. Zur Erfüllung seiner Aufgaben kann das NCSC auf eine Vielzahl nationaler Mittel zurückgreifen. So ist es dem NCSC möglich mit verschiedenen Regierungsorganisationen, den Strafverfolgungsbehörden, dem Verteidigungsministerium sowie den Sicherheits- und Geheimdiensten, wie auch ausländischen Partnern zusammenzuarbeiten. Dadurch soll die Bedrohung durch Cyber Angriffe für das Vereinigte Königreich (VK) reduziert und eine zeitnahe Reaktionsfähigkeit gewährleistet werden.

Eine besondere Rolle spielt in diesem Zusammenhang die Idee der Kooperation mit nationalen und internationalen Partnern sowie die Offenheit des NCSC gegenüber der nationalen Wirtschaft. Über das »Industry 100« Projekt versucht das NCSC 100 Personen aus dem privaten Sektor, v. a. den Kritischen Infrastrukturen, als Teil- oder Vollzeitmitarbeiter in das NCSC zu bringen. Das NCSC ist national die einzige Stelle, die Empfehlungen mit Bezug zu Cyber Bedrohungen bzw. -Maßnahmen aussprechen darf, um Widersprüche und damit Verwirrungen zu vermeiden.

Bereits im Mai 2017 unterstützte das NCSC die Bekämpfung der Folgen eines großangelegten mit Cyber Mitteln durchgeführten Erpressungsversuches, bei dem u. a. die Computersysteme von 16 britischen Krankenhäusern mittels des Cryptolockers »WannaCry« lahmgelegt wurden. Angesichts der Öffentlichkeitswirkung der WannaCry-Angriffe wiederholte der britische Verteidigungsminister Michael Fallon die bereits im November 2016 für Cyber Sicherheit angekündigte Bereitstellung von mehr als 2 Mrd. €. Davon sollen mehr als 55 Mio. € für den Schutz der Computersysteme der Nationalen Gesundheitsversorgung (NHS) verwendet werden.

Auch Politiker des Vereinigten Königreiches wurden 2017 mehrmals Ziel von Cyber Angriffen. So erfolgte im Juni 2017 ein Angriff auf die Nutzerkonten des britischen Unterhauses und im August 2017 auf das schottische Parlament. In beiden Fällen wurde in Zusammenarbeit mit dem NCSC Maßnahmen zur Abwehr und Analyse der Angriffe eingeleitet. Aufgrund zahlreicher Cyber Angriffe gegen britische Medienhäuser sowie Einrichtungen des Telekommunikations- und Energiesektors betonten sowohl Premierministerin May als auch Verteidigungsminister Fallon mehrmals, dass man bereit sei, auch mit militärischen Mitteln auf Cyber Angriffe zu reagieren.

2.7.6 Frankreich

Die Bedeutung des Themas Cyber Sicherheit wurde von Frankreich bereits vor Jahren erkannt und in den Weißbüchern von 2008 und 2013 festgeschrieben. Im Rahmen der strategischen Überprüfung der nationalen Verteidigungs- und Sicherheitspolitik 2017 (»Revue stratégique de défense et de sécurité nationale«) wird auf die ansteigenden Bedrohungen im Cyber Raum hingewiesen. Wiederholte Cyber Angriffe haben die Verletzlichkeit von Strukturen, die für Staat und Nationale Sicherheit unverzichtbar sind, aufgezeigt. Frankreich hält es für notwendig, darauf mit der Entwicklung offensiver und defensiver Kapazitäten zu reagieren. Die

direkt dem Präsidentenpalast unterstellte neue Koordinationsstelle für Nachrichtendienste und Terrorismusbekämpfung (»Coordinateur national du renseignement et de la lutte contre le terrorisme«, CNRLT) soll eine rasche Reaktion auf Sicherheitsbedrohungen (inkl. Cyber Raum) gewährleisten.

Den Rahmen für den gesamtstaatlichen Ansatz zu Cyber Sicherheit bildet die »Nationale Strategie für digitale Sicherheit« (2015). Federführend bei der Umsetzung ist die »Nationale Behörde für die Sicherheit von Informationssystemen« (»Agence nationale de la sécurité des systèmes d´information«, ANSSI). Die bereits seit 2009 operativ tätige Behörde ist über das Generalsekretariat für Verteidigung und Nationale Sicherheit (»Secrétariat général de la défense et de la sécurité nationale«, SGDSN) dem Premierminister verantwortlich. Die ANSSI verfügt über 250 Mitarbeiter und rekrutiert derzeit mehrere hundert IT-Spezialisten.

Fünf Ziele werden in der Strategie für digitale Sicherheit definiert: Stärkung des Cyber Schutzes durch Ausweitung von Ressourcen und Kompetenzen der ANSSI; Schutz der Bürger (Stärkung des »digitalen Vertrauens« und Schutz der Privatsphäre im Cyber Raum); Sensibilisierung der Nutzer durch spezialisierte Ausbildung; Schaffung eines günstigen Umfelds für die digitale Wirtschaft sowie europäische und internationale Kooperation. Gemeinsam mit Partnern möchte Frankreich eine »Roadmap für die digitale Souveränität Europas« entwickeln.

Ausländische Hacker-Angriffe auf die EDV-Systeme von politischen Parteien sowie auf Mobiltelefone und Tablets von Parteienvertretern im Wahlkampf 2016/2017 wurden von der ANSSI als Versuche der Destabilisierung der Demokratie gewertet. Die Verbreitung von Falschmeldungen über soziale Medien wird als neues Thema im Bereich Cyber Sicherheit verstärkt bearbeitet. Die ANSSI hat auf diese Entwicklungen u. a. mit präventiven Schulungen und Verhaltensinstruktionen für die im Parlament vertretenen Parteien reagiert.

Im Verteidigungsbereich verfügt Frankreich über ergänzende Instrumente und Strukturen zur Cyber Sicherheit. Dies nicht zuletzt vor dem Hintergrund der spezifischen Bedrohungslage für die militärische Infrastruktur und für Operationen der Streitkräfte. Der Pakt zur Cyber Verteidigung von 2014 sieht einschlägige Maßnahmen für die Streitkräfte vor. Bis 2019 sollen im Sektor Cyber Verteidigung 1.000 neue Stellen geschaffen und zusätzlich 1 Mrd. € investiert werden. Ein dem Generalstabschef unterstelltes Cyber Kommando (»ComCyber«) wurde im Mai 2017 eingerichtet. Es soll sich neben dem Schutz eigener Netze auch auf die Aufklärung, aktive Verteidigung und offensive Operationen konzentrieren. Das neue Kommando soll in der Lage sein, in gegnerische Netzwerke/Systeme einzudringen, um diese temporär oder dauerhaft zu zerstören. Bis Ende 2019 soll auch die Aufstellung mit 2.600 Cyber Experten (»digital soldiers«) abgeschlossen sein, zu denen noch weitere 4.400 Cyber Verteidigungsreservisten hinzukommen.«

3 Nationale Akteure und Strukturen

3.1 Innerer Kreis der Operativen Koordinierungsstrukturen (IKDOK)

Gemäß der Österreichischen Strategie für Cyber Sicherheit (ÖSCS) soll unter anderem eine »Struktur zur Koordination auf der operativen Ebene« geschaffen werden. Diese Struktur umfasst im Wesentlichen die Erstellung von periodischen und anlassbezogenen operativen Lagebildern für Cyber Sicherheit, die Erarbeitung von Maßnahmen im Anlassfall sowie die Unterstützung und Koordinierung gesamtstaatlicher Notfallmaßnahmen im Rahmen des Cyber Krisenmanagements (CKM). Hierfür wurde der Innere Kreis der operativen Koordinationsstrukturen aufgebaut und etabliert, der seit 2016 den Regelbetrieb in vollem Umfang aufgenommen hat.

Der IKDOK bildet im Krisenfall, unterstützt durch den äußeren Kreis der operativen Koordinierungsstruktur, die direkte Schnittstelle zum gesamtstaatlichen Cyber Krisenmanagement (CKM). 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, BM.I) 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 (BM.I), das Heeres-Nachrichtenamt (HNaA/BMLV), das Kommando Führungsunterstützung und Cyber Defence mit seinem MilCERT (KdoFüU&CD/BMLV), das GovCERT (BKA) sowie das BMEIA.

Eine zentrale Herausforderung für die an der operativen Koordinierungsstruktur beteiligten Ressorts ist derzeit, die in Beschlussfassung befindliche EU NIS-Richtlinie auf nationaler Ebene umzusetzen und in den bestehenden Strukturen abzubilden.

3.2 Cyber Security Center

Die ÖSCS sieht zum Schutz des Cyber Raums und der Menschen im virtuellen Raum unter anderem die Schaffung einer Struktur zur Koordination auf der operativen Ebene vor; auch die Strategie »INNEN. SICHER« führt Cyber Sicherheit als eine Schlüsselherausforderung an.

Infolgedessen wurde im Juni 2014 das INNEN. SICHER-Projekt »Cyber Security .BVT« ins Leben gerufen, dessen zentrales Element der Aufbau eines Cyber Security Centers (CSC) im Bundesministerium für Inneres (BMI) darstellt. Dieses Projekt konnte im Dezember 2017 mit der Überführung des CSC in den Regelbetrieb erfolgreich abgeschlossen werden. Die Bedeutung des Projektes wird unter anderem dadurch unterstrichen, dass seitens der europäischen Union beachtliche Fördermittel aus dem Fonds für die innere Sicherheit (ISF) zur Verfügung gestellt wurden.

Die zentralen Aufgabenstellungen für das CSC ruhen auf insgesamt vier Säulen:

- Behörde für Netz- und Informationssicherheit
- Prävention & Schutz Kritischer Infrastrukturen
- Koordination & Cyber Krisenmanagement
- Technische Kompetenz & Ansprechpartner

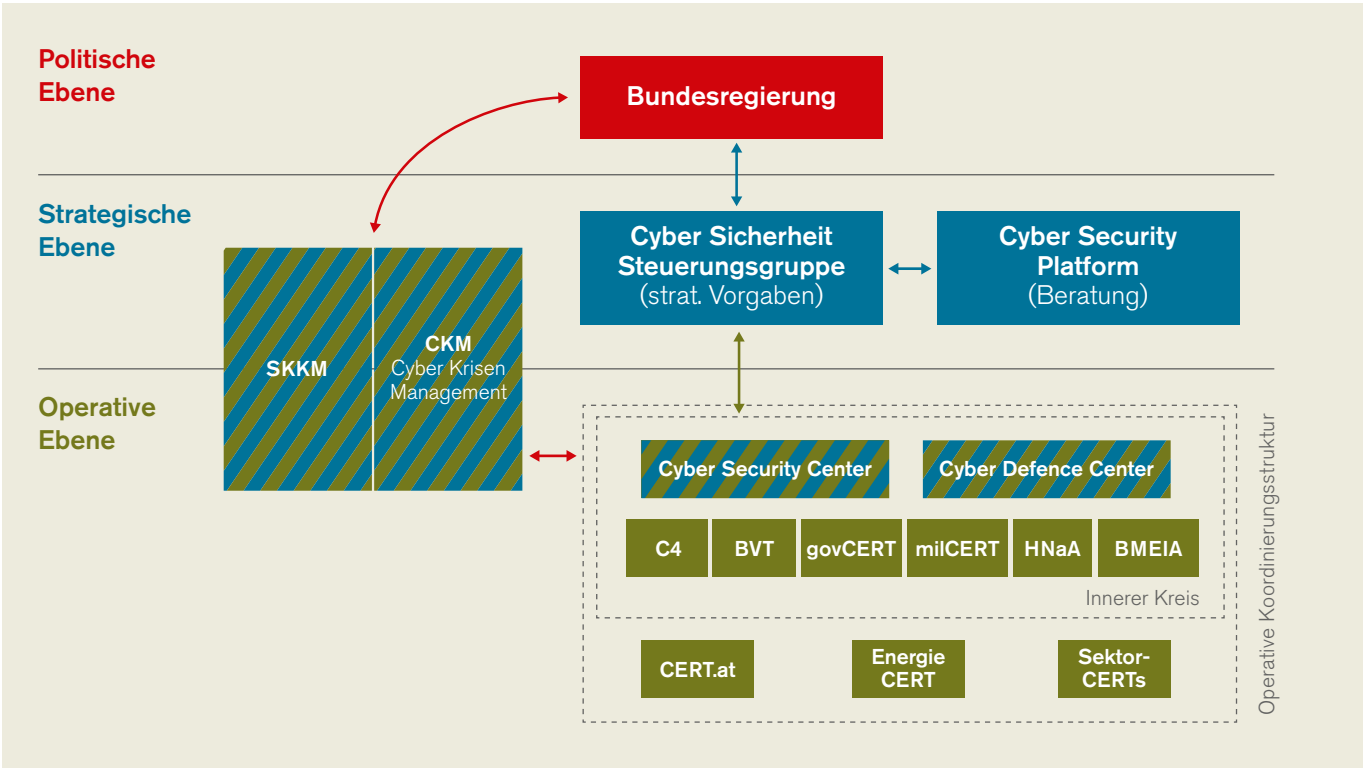
Im Mai 2018 wird das neue Netz- und Informationssystem-Sicherheitsgesetz (NIS-G) in Kraft treten, das für Unternehmen der kritischen Infrastruktur unter anderem die Einführung verbindlicher Mindest-Sicherheitsstandards und eine Meldepflicht für schwere Sicherheitsvorfälle vorsieht. Das CSC wird in diesem Zusammenhang die Aufgaben der operativen NIS-Aufsichtsbehörde wahrnehmen.

Als eine wesentliche zentrale Aufgabe ist die Durchführung umfassender Präventionsarbeit in Form von Awareness-Veranstaltungen und -Vorträgen oder Beratungsgesprächen zu nennen. Besonderer Wert wird dabei auf eine gute Zusammenarbeit mit der Wirtschaft und den bestehenden Strukturen im Bereich der Cyber Sicherheit in Österreich gelegt.

Im Unterschied zu einzelnen Unternehmen oder Sektoren ist das CSC – eingebettet in die Strukturen der operativen Koordinierungsstrukturen (OpKoord) – in der Lage, isolierte IKT-Sicherheitsvorfälle in einen größeren Zusammenhang zu stellen und im Fall einer Krise, welche durch Cyber Probleme ausgelöst wurde, schnellstmöglich mit dem bestehenden staatlichen Krisen- und Katastrophenmanagement zusammenzuarbeiten.

Abbildung 11: Einordnung der »Operativen Koordinierungsstruktur«

Die Erfüllung der gestellten Aufgaben kann durch das CSC nur dann bewältigt werden, wenn eine Bereitschaft zum permanenten Aufbau von technischer Kompetenz besteht. Im Jahr 2017 wurde in diesem Sinne der sukzessive Aufbau eines APT-Kompetenzzentrums forciert.



3.3 Cyber Verteidigungszentrum

Das Abwehramt (AbwA/BMLV) betreibt das Cyber Verteidigungszentrum (CyVZ) des ÖBH und der Republik Österreich. Es bereitet die für die Cyber Verteidigung erforderlichen aktiven Mittel und Fähigkeiten vor. Damit ergänzt es die Cyber Verteidigung des ÖBH durch das Kdo FüU&CD sowie gesamtstaatliche Cyber Verteidigungsanstrengungen. Zu diesem Zwecke stellt das CyVZ ein Lagebild zur Verfügung, in dem gesamtstaatliche und nachrichtendienstliche Informationen aus und über den Cyber Raum zusammengeführt, analysiert und für die Beurteilung von Gegenmaßnahmen herangezogen werden.

Das AbwA trug auch 2017 durch die Organisation der IKT-Sicherheitskonferenz in Villach zur Sensibilisierung im Bereich Cyber Sicherheit bei. Die mittlerweile zum 16. Mal stattgefundene – und im deutschsprachigen Raum größte – Konferenz fand mit mehr als 2.700 Besuchern regen Zuspruch.

3.4 Kommando Führungsunterstützung und Cyber Defence (KdoFüU&CD)

Mit 01.01.2017 wurde das »Kommando Führungsunterstützung und Cyber Defence« (KdoFüU&CD) als Kommando der oberen Führung im Österreichischen Bundesheer etabliert, um den neuen Bedrohungen aus dem Cyber Raum angemessen entgegentreten zu können. Dabei wurden die entsprechenden Fähigkeiten im Bereich der Führungsunterstützung, der IKT-Services, der Elektronischen Kampfführung und im Bereich der operativen Cyber Defence, inklusive der diesbezüglichen Aus-, Fort- und Weiterbildung gebündelt und in notwendigen Bereichen weiterentwickelt. Mit dem neuen »Kommando Führungsunterstützung und Cyber Defence« wurden klare Zuständigkeiten und Verantwortlichkeiten geschaffen. Dort sind die präventiven, operativen und reaktiven Fähigkeiten zur Abwehr von Bedrohungen aus dem Cyber Raum zusammengeführt.

Insbesondere im militärischen Einsatzfall »Militärische Landesverteidigung im Cyber Raum« übernimmt das neue KdoFüU&CD die Operationsführung, unter Einbindung der anderen Kommanden der oberen Führung und in Abstimmung mit dem Abwehramt (AbwA), dem Heeresnachrichtenamt (HNaA) und anderen fachlich relevanten Stellen.

Im Befehlsbereich des KdoFüU&CD sind hinsichtlich des Cyber Bereichs im Wesentlichen folgende Aufgabenträger und Funktionalitäten einrichtet:

- Der Kommandant KdoFüU&CD wurde seit Anfang 2017 gleichzeitig mit der Funktion »Cyber Koordinator BMLV« beauftragt. Damit obliegt ihm die ressortinterne Gesamtkoordination der Cyber Defence Domäne auf militärstrategischer, operativer und taktischer Ebene. Er vertritt das Verteidigungsressort im Bereich Cyber Defence ebenso nach außen. Zur Unterstützung bei der Wahrnehmung dieser Aufgabe wurde unter anderem auf Kommandoebene eine Stabstelle Cyber, Inspektion und Controlling (CIC) eingerichtet.
- Durch die massive Erweiterung der IKT-Sicherheits- und Cyber Verteidigungsaufgaben wurde aus der vormaligen Abteilung IKT-Sicherheit mit deren milCERT das Zentrum IKT- und Cyber Sicherheit (ZIKTCySih) als operationelles Element neu aufgestellt. Damit sind

wesentliche Aufgabenträger für Cyber Defence (CD) nunmehr im KdoFüU&CD konzentriert und abgebildet. Nachrichtendienstliche Aufgaben im Cyber Bereich werden weiterhin im Abwehramt (AbwA) und Heeresnachrichtenamt (HNaA) wahrgenommen.

- In den Organisationseinheiten des KdoFüU&CD (an der Führungsunterstützungsschule, im Führungsunterstützungsbataillon 1 und Führungsunterstützungsbataillon 2) sind so genannte Cyber Schulungszentren (CSZ) für die Aus-, Fort- und Weiterbildung der Cyber Rekruten eingerichtet. Weiters verfügt das Führungsunterstützungsbataillon 1 über ein so genanntes »Cyber Defence Research Centre (CDRC).

3.5 Andere Cyber Defence Research Center des BMLV

Das BMLV betreibt neben dem CDRC beim Führungsunterstützungsbataillon 1 ein weiteres beim Führungsunterstützungsbataillon 2, welches direkt dem Abwehramt zuarbeitet. Die CDRCs werden operativ von den Bedarfsträgern geführt, das sich in der Landesverteidigungsakademie in Wien befindliche zentrale CDRC ist für die Methodenentwicklung und die Bereitstellung zentraler IKT Infrastruktur verantwortlich.

3.6 Zentrum IKT- und Cyber Sicherheit inkl. milCERT

Zur Durchführung der Cyber Verteidigung im nationalen und internationalen Umfeld bedarf es eines grundlegenden Verständnisses über die Struktur des Cyber Raumes. Die hierfür zu entwickelnden Fähigkeiten spiegeln sich auf der technischen Ebene in den zugewiesenen Aufgaben Zentrum IKT- und Cyber Sicherheit im KdoFüU&CD wider (militärischer Eigenschutz im Cyber Raum und Abwehr von Cyber Angriffen). Der Hauptzweck der Cyber Verteidigung ist der Schutz der Souveränität im Cyber Raum, insbesondere der Schutz und die Verteidigung der ÖBH-einsatzrelevanten kritischen Infrastruktur sowie der Schutz von IKT-Systemen und IKT-Services des ÖBH.

Das Zentrum IKT-und Cyber Sicherheit (ZIKTCySih), als Organisationselement des neuen KdoFüU&CD, ist verantwortlich für die Informations- und IKT-Sicherheit aller Systeme des BMLV/ÖBH. Die technischen, taktischen und organisatorischen-prozessualen Fähigkeiten der Cyber Sicherheit und Cyber Verteidigung sind im ZIKTCySih konzentriert. In diesem Rahmen nimmt das ZIKTCySih auch weiterhin die Rolle des militärischen CERTs (milCERT) wahr.

In den letzten Jahrzehnten haben sich Bedrohungen aus dem Cyber Raum im verstärkten Maße in asymmetrische Bedrohungen gewandelt. Durch den Einsatz moderner Technik, die häufig auch zivile Systeme einschließt, entstanden Technologien, die im Rahmen dieser Form der Angriffsszenarien zum Einsatz kommen. Eine verstärkt auftretende Verschränkung des Informationsumfeldes (»Cyber Raum«) mit dem Elektromagnetischen Umfeld (Elektromagnetisches Spektrum) war die direkte Folge. Bei einer (asymmetrischen) Bedrohung ist davon auszugehen, dass Fähigkeiten zur Aufklärung, Überwachung und Störung des nutzbaren elektromagnetischen Spektrums angewandt werden. Daher ist auch der Schutz im elektromagnetischen Spektrum eine immer bedeutendere Komponente im Aktionsradius gegen Bedrohungen aus dem Cyber Raum und ist nun ebenfalls im ZIKT&CySih, in Form des Electronic Warfare Operational Support Center (EWOSC), abgebildet.

Das Zentrum IKT- und Cyber Sicherheit stellt Produkte für die strategischen und operativen Ebenen im BMLV zur Verfügung. Hierzu bedient sich das ZIKTCySih des Cyber Sicherheitsmanagements, eines breiten Spektrums an technischen Filter- und Analysesystemen, sowie Cyber Sicherheitsexperten zur Analyse von und Reaktion auf Bedrohungen und Vorfälle.

Das Zentrum IKT- und Cyber Sicherheit ist in seiner Rolle als milCERT Mitglied im CERT-Verbund und leistet im Rahmen der gesamtstaatlichen operativen Koordinierungsstruktur seinen Beitrag zum gesamtstaatlichen Cyber Krisenmanagement.

3.7 GovCERT, CERT.at und Austrian Energy CERT

GovCERT ist das nationale CERT (Computer Emergency Response Team) der öffentlichen Verwaltung 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 Plattform eng vernetzt. Darüber hinaus nimmt dieses (gemeinsam mit CERT.at) die Österreichische Vertretung im CSIRT-Netzwerk der EU wahr. Im Rahmen der österreichischen EU-Ratspräsidentschaft im 2. Halbjahr 2018 sind hinsichtlich der Unterstützung eines regelmäßigen Informationsaustausches von relevanten Themenbereichen und guten Praktiken Koordinierungstreffen geplant.

Das im Bundeskanzleramt angesiedelte GovCERT arbeitet eng mit dem österreichischen CERT (CERT.at) in Form einer Public-Private-Partnership zusammen. Hierbei übernimmt CERT.at operative Aufgaben des GovCERT und stellt allem voran seine technische Expertise und Know-How zur Verfügung.

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 und Beratung und Unterstützung im Anlassfall auf Anfrage durch. CERT.at versteht sich als Kontaktpunkt für sicherheitsrelevante IKT-Ereignisse in Österreich und dient hier als vertrauenswürdige und anerkannte Informationsdrehscheibe innerhalb österreichischer Organisationen und Unternehmen im Cyber Sicherheitsbereich.

Mit der beabsichtigten Umsetzung der EU NIS-Richtlinie in nationales Recht wird CERT.at auf zusätzliche Aufgabenbereiche erweitert. So sieht diese Umsetzung für Betreiber wesentlicher Dienste sowie Anbieter digitaler Dienste eine Meldeverpflichtung für schwerwiegende Sicherheitsvorfälle vor. Diese verpflichtenden Meldungen werden von den Betroffenen an bestimmte, sektorspezifische Meldestellen (Sektor-CERTs) gesendet und von dort an das CSC weitergeleitet. Auf freiwillige Meldungen trifft dies ebenfalls zu, allerdings werden diese Meldungen vor der Weiterleitung an das CSC von den Sektor-CERTs anonymisiert.

Der Entwurf des NIS-Gesetzes sieht zur Wahrnehmung dieser Meldestellenfunktion die Existenz eines solchen Sektor-CERTs in jedem Sektor kritischer Infrastrukturen vor. Diese CERTs erfüllen neben dieser Meldestellenfunktion eine Vielzahl weiterer CERT-Aufgaben für die Organisationen Ihrer respektiven Sektoren.

Für den Fall, dass ein Sektor kritischer Infrastrukturen noch über kein eigenes Sektor-CERT verfügt, erfüllt CERT.at die Aufgabe einer Meldestelle. Dadurch wird den Unternehmen des betroffenen Sektors die Möglichkeit geboten, ihrer gesetzlichen Meldeverpflichtung nachzukommen. CERT.at bietet in dieser Funktion eines »Ersatz Sektor-CERTs« allerdings im Gegensatz zu einem »echten« Sektor-CERT keine darüber hinausgehenden CERT-Dienstleistungen in der weiteren Bearbeitung verpflichtend gemeldeter Sicherheitsvorfälle an.

Das Austrian Energy CERT (AEC) ist ein brancheneigenes CERT (Computer Emergency Response Team) für die österreichische Elektrizitäts- und Erdgaswirtschaft. Mit dessen Aufbau wurde im November 2016 begonnen. Das AEC ist ein wichtiger Baustein bei der Erhöhung der Resilienz der Energiewirtschaft gegenüber Cyber Attacken. Es erfüllt zugleich die Vorgaben der europäischen Richtlinie für Netz- und Informationssicherheit (NIS) sowie auch die Empfehlungen der Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) für die Erhöhung der IT-Sicherheit kritischer 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 Sicher-heitsmeldungen, 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 Pri-märansprechpartners (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 Behörden innerhalb der Branche gewährleistet.

Durch den Betrieb eines brancheneigenen CERTs und dem damit verbundenen Informationsaustausch sollen Bewusstsein und Prävention im Energiesektor gestärkt werden.

Das Sektor-CERT der Energiebranche (Austrian Energy CERT) hat im November 2017 den Normalbetrieb aufgenommen.

3.8 CERT-Verbund

Zur Erreichung eines wirksamen Sicherheitsniveaus für den Cyber Raum innerhalb der österreichischen Gesellschaft ist ein enges Zusammenspiel zwischen Gesellschaft, Wirtschaft, Wissenschaft und Wirtschaft unumgänglich. Eine wesentliche Rolle wird hierbei den CERTs eingerichtet.

Den CERTs kommt die wesentliche Aufgabe zu, die digitalen Netze und IKT-Systeme 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 an dem CERT-Verbund ist freiwillig und kann jederzeit beendet werden. Jeder einzelne Teilnehmer verpflichtet sich die Ziele – (1) einen regelmäßigen Informations- und Erfahrungsaustausch, (2) ein Identifizieren und Zugänglichmachen von Kernkompetenzen und (3) die Förderung der nationalen CERTs in allen Sektoren – im Sinne eines gemeinschaftlich geführten und auf Kooperation basierenden CERT-Verbundes zu verfolgen.

Seit der Gründung des CERT Verbunds haben sich die aktuell 14 Mitglieder in 29 Sitzungen getroffen und sind auch außerhalb der Treffen über sichere Kommunikationsverteiler miteinander verbunden.

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 2017 wurden die bereits bestehenden CERT-Strukturen (CERT-Verbund, GovCERT) auf nationaler- und Behördenebene weiter gefestigt, ausgebaut und operationalisiert.

Sektorenspezifische CERTs aus dem Bereich der Wirtschaft bestehen bereits, in naher Zukunft sollen solche CERTs weiter etabliert werden und so den äußeren Kreis der OpKoord ergänzen.

3.9 Heeresnachrichtenamt

Das Heeresnachrichtenamt (HNaA) ist umfassend für die Erarbeitung des strategischen Lagebildes vor allem in Bezug auf internationale Akteure und Entwicklungen zuständig. Der Beitrag des HNaA soll in ein gesamtstaatliches Lagebild einfließen und dient als mögliche Entscheidungsgrundlage für die oberste politische und militärische Führung.

Darüber hinaus ist das HNaA für die frühzeitige Erkennung von potentiellen Cyber Bedrohungen aus dem Ausland zuständig und unterstützt im Fall eines großangelegten Cyber Angriffes auf nationale Infrastrukturen mit den zur Verfügung stehenden Methoden eine Identifikation der Angreifer.

3.10 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 Ermittlungen, Forensik und Technik zusammen.

Die Cyber Crime Meldestelle des C4 ist zum einen die Kontaktstelle zur Bevölkerung. Dadurch können dort unter anderem frühzeitig neue Phänomene erkannt werden. Zum anderen ist sie auch Schnittstelle zum CSC und internationale Kontaktstelle in Cyber Crime Angelegenheiten. Eine weitere wichtige Aufgabe ist die Ansprechstelle für alle Polizeidienststellen im Zusammenhang mit Cyber Crime.

Die SOKO Clavis bearbeitet weiterhin erfolgreich das Phänomen Ransomware durch Ermittlungen an zentraler Stelle und koordiniert diesbezüglich die internationale Zusammenarbeit. Sie setzt sich aus erfahrenen Kriminalbeamtinnen und Kriminalbeamte und hochqualifizierten Technikern zusammen.

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

Das neue geschaffene Referat Entwicklung und Innovation, als technisch wissenschaftlicher Dienst, widmet sich technischen Fragestellungen auf dem Gebiet der IT-Kommunikation, insbesondere im Internet, einschließlich der automatischen maschinengestützten Kommunikation (Internet of Things) sowie der Erforschung und Entwicklung von Schutz- und Ermittlungsmöglichkeiten in Hard- und Softwarebereichen.

3.11 Cyber Sicherheit Plattform

Die Cyber Sicherheit Plattform (CSP) stellt die zentrale Austausch- und Kooperationsplattform zwischen Wirtschaft, Wissenschaft und der öffentlichen 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.

Im Jahr 2017 fanden die vierte und fünfte Arbeitstagung der CSP statt. Gegenstand der Sitzungen war v. a. der Umsetzungsstand der NIS-Richtlinie auf nationaler Ebene. Hierbei wurde insbesondere auf die zwei wesentlichen Bereiche Sicherheitsvorkehrungen sowie Regelung der Meldepflicht für Betreiber wesentlicher Dienste (BwD) eingegangen. Des Weiteren wurden konkrete Ergebnisse der innerhalb der CSP eingerichteten Arbeitsgruppe Cyber Security Agenda 2020 präsentiert, die sich zusammengefasst in einem Ergebnisbericht wiederfinden. Der Bericht entspricht dem Ziel der Beitragsleistung für die Weiterentwicklung der ÖSCS 2.0 und verfügt dementsprechend über ein breit aufgestelltes Leitbild für die nächsten fünf Jahre unter Einbeziehung aller wesentlichen Stakeholder. Als wesentliche Themenbereiche wurden untern anderem die bessere Nutzung der vorhandenen Kapazitäten, Ressourcen und Fähigkeiten, die Hebung von Synergien, die Verbesserung der Zusammenarbeit, die Vermeidung von Doppelgleisigkeiten, die Verlinkung mit europäischen Initiativen (ECSO, European cPPP) sowie die Erhöhung der Chancen bei europäischem Funding identifiziert.

3.12 Austrian Trust Circle

Der Austrian Trust Circle ist eine Initiative von CERT.at und dem österreichischen Bundeskanzleramt und besteht aus Security Information Exchanges in den einzelnen Bereichen der strategischen Informationsinfrastruktur. Seit 2016 wird auch die öffentliche Verwaltung als eigener Sektor adressiert.

CERT.at bietet 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 bei der Information über und Behandlung von Sicherheitsvorfällen in den Organisationen
- Operative Experten für das Bundeskanzleramt 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 öffentliche Verwaltung einmal im Jahr im Rahmen einer zweitägigen Veranstaltung gefördert.

Im Jahr 2017 wurden unter anderem die Themen Umsetzung der EU-NIS Richtlinie, Erkennung von Sicherheitsvorfällen und Erfahrungen aus dem Bereich der Krisenkommunikation behandelt.

3.13 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 40 Kooperationspartnern (Bundesministerien, Landesregierungen, Behörden, Universitäten, Fachhochschulen, Forschungsinstitute, Unternehmen, Vereine und Interessensvertretungen) laufend erweitert. Es beinhaltet aktuelle Meldungen und Warnungen, Informatives, Beratung sowie weiterführende Informationen sowohl für Einsteiger als auch für Expertinnen und Experten.

2017 umfassten die Aktivitäten auf dem IKT-Sicherheitsportal insgesamt die Verfassung von 200 Newsartikeln, 30 Publikationseinträgen, 70 Veranstaltungseinträgen und 26 Fachartikeln

zu den neuesten Technologietrends. Im April wurde das Portal einem Relaunch unterzogen, um die Nutzerinnen und Nutzer des Portals noch schneller zu den für sie relevanten Inhalten zu führen. Ein neu eingerichteter Erste-Hilfe-Bereich unterstützt mit Informationen zu Melde- und Beratungsstellen, zur Schadstoffsoftware-Entfernung und Datenrettung. Die Online-Ratgeber zur Wahl geeigneter Sicherheits- und Privatsphäreneinstellungen bei Smartphones und bei Facebook wurden aktualisiert und überarbeitet.

3.14 Büro für strategische Netz- und Informationssystemsicherheit

Im Rahmen einer neuen Geschäftseinteilung wurde mit Wirksamkeit vom 1. November 2017 im Bundeskanzleramt das Büro für strategische Netz- und Informationssystemsicherheit eingerichtet. Der Aufgabenbereich des Büros erstreckt sich von Angelegenheiten im Zusammenhang mit der Vorbereitung und Umsetzung der gesetzlichen Verpflichtung aus der Europäischen NIS-Richtlinie in Österreich (beispielsweise Erarbeitung und Koordination von Standards, Zustellung von Bescheiden etc.), der Mitwirkung und Entwicklung von Strategien für Cyber Sicherheit sowie gesamtstaatlicher Analysen, der Wahrnehmung von Vertretungen von Österreich in – den Gesamtstaat betreffenden – europäischen und internationalen Cyber Sicherheit Gremien bis hin zu einer koordinativen Funktion im Rahmen von nationalen und internationaler Cyber Sicherheit Aktivitäten und öffentlich-privater Kooperationen.

4 Cyber Übungen

Die Österreichische Strategie für Cyber Sicherheit sieht im Handlungsfeld »Strukturen und Prozesse« die regelmäßige Abhaltung von Cyber Übungen zwecks Testung von Abläufen des Cyber Krisenmanagement vor.

4.1 KSÖ Planspiel 2017

Bereits seit dem Jahr 2012 gehören die durch das Kuratorium Sicheres Österreich (KSÖ) organisierten, jährlich oder zweijährlich stattfindenden Planspiele zu einem festen Bestandteil bei der Erprobung und Übung der organisatorischen und technischen Abläufe im Falle eines umfassenden Cyber Angriffes auf Unternehmen der kritischen Infrastruktur. Diese Cyber Übungen leisten dabei einen erheblichen Beitrag zur Steigerung der Resilienz Österreichs und unterstützen damit die Erfüllung der Anforderungen der Österreichischen Strategie für Cyber Sicherheit. Während in den Vorjahren der Fokus eher das staatliche Cyber Krisenmanagement (CKM) gesetzt wurde, standen bei der diesjährigen Übung, die am 6. und 7. November 2017 stattfand, die technische Bewältigung und die Zusammenarbeit mit der operativen Koordinierungsstruktur (OpKoord) im Vordergrund. Dabei wurde zum ersten Mal bei einem KSÖ-Planspiel die Ebene der operativen Koordinierungsstruktur vollständig erprobt und beübt.

Dazu wurde vom KSÖ und dem Austrian Institute of Technology (AIT) ein komplexes Szenario erarbeitet, bei dem es in der Folge von politischen Auseinandersetzungen rund um die Brexit-Verhandlungen letztlich zu gezielten Cyber Angriffen auf Unternehmen der österreichischen Energieversorgung kommt. Die Ziele dieses Übungs-Szenarios lagen dabei auf einer ersten Ebene in der konkreten technischen Bewältigung der Angriffe durch die Verwendung von Werkzeugen an eigens für die Übung generierten Datenbeständen. Auf der nächsthöheren Ebene zielte die Übung darauf ab, dass die Unternehmen die Notwendigkeit der Einbindung koordinierender staatlicher Stellen erkennen und gemäß den Vorgaben des im Mai 2018 in Kraft tretenden Netz- und Informationssystemsicherheitsgesetzes (NIS-G) entsprechende Meldungen an die zuständigen Behörden absetzen. Auf einer dritten Ebene wurden schließlich die Vernetzung, der Austausch und die Diskussionen zwischen den beteiligten Behörden erprobt.

Die Cyber Übung selbst war dabei auf zwei Übungstage ausgelegt. Während am ersten Tag eine Schulung und Übung zur Erkennung von aktuellen Cyber Angriffen und -techniken durch Nutzung von Werkzeugen an einer simulierten technischen kritischen Infrastruktur abgehalten wurde, fand am zweiten Tag eine interaktive Übung zum organisationsübergreifenden Informationsaustausch und zur Kommunikation im Falle von kritischen Störfällen anhand von Beispielen aus der Energieversorgung, sowie der technischen Analyse dieser Störfälle statt.

Das Planspiel kann zusammenfassend als großer Erfolg bezeichnet werden. Insgesamt bearbeiteten mehr als 70 aktive Teilnehmer vor mehr als 100 interessierten Beobachtern unter großem Interesse der Presse die vorbereiteten Übungsannahmen. Die Vorgabe, dass es zu keinem Zeitpunkt zur Ausrufung einer Cyber Krise kommen sollte, ermöglichte es, den Fokus konsequent auf den beteiligten Unternehmen und den staatlichen Partnern auf Ebene der operativen Koordinierung zu belassen. Der Innere Kreis der operativen Koordinierung (IKDOK) koordinierte, unterstützt von mehreren Computer Emergency Response Teams (CERTs bzw.

CSIRTs), die Gegenmaßnahmen vom ersten Eintreffen von entsprechenden Meldungen bis zur letztendlichen Bewältigung der Cyber Angriffe. Dabei konnte er auf ein bereits hervorragend eingespieltes Team an staatlichen Akteuren aus mehreren verschiedenen Ressorts zurückgreifen.

4.2 EU CYBRID 17

Die Übung EU CYBRID 2017 ist eine strategische Table-Top Übung, die erstmalig im September 2017 durch die EU Ratspräsidentschaft im Zuge eines informellen Verteidigungsministertreffens durchgeführt wurde. Die Minister wurden mit einem Szenario von Cyber Attacken in Kombination mit strategischen Fragen mit Mulitple-Choice Antworten konfrontiert. Ein wesentliches Ziel war die unmittelbare Reaktion der Teilnehmer einzufangen, die im Anschluss an die 2-stündige Übung im Rahmen einer Diskussion mit der Hohen Vertreterin der EU für Außen- und Sicherheitspolitik, sowie dem NATO Generalsekretär erörtert wurden. Das Übungsziel, die Steigerung der Aufmerksamkeit für die Notwendigkeit starker Krisenmechanismen, die auch für Vorfälle im Cyber Raum anzuwenden sind, wurde erreicht. Darüber hinaus wurden auch die noch bestehenden Lücken im Bereich der Situational Awareness und eines gemeinsamen Lagebildes verdeutlicht. Der zentrale Aspekt der Attribution wurde durch die EU CYBRID 2017 nicht abgebildet. Dies wurde an die Außenminister für eine Übung im Bereich der Diplomatischen Maßnahmen verwiesen. Auf jeden Fall wurde aber die hohe Relevanz der Übung von strategischen Entscheidungen im Krisenmechanismus durch die Minister und der damit einhergehenden strategischen Kommunikation aufgezeigt.

4.3 EU PACE 17

EU-PACE17 ist eine EU-Krisenmanagement-Übung, die parallel (aber nicht gemeinsam) mit der NATO Anfang Oktober 2017 abgehalten wurde. Das Szenario wurde in verschiedenen EU-Gremien durchgespielt, so z. B. im Politischen und Sicherheitspoltischen Komitee (PSK). Dort wurde eine Woche lang ein ständig eskalierendes Szenario anhand einer fiktiven EU-GSVP Operation durchgespielt, von den Hauptstädten ergingen entsprechende Weisungen. Österreich hat sich aktiv eingebracht und brachte insbesondere vertrauensbildenden Mechanismen der OSZE in die Übung ein.

4.4 Locked Shields 2017 (NATO)

Seit mehreren Jahren nimmt das BMLV an der größten technischen Cyber Verteidigungsübung Locked Shields teil. Während die teilnehmenden Nationen die eigene Infrastruktur in ihren Heimatländern nutzen, findet der Großteil der Übung in Estland statt. Im Rahmen dieser Übung kommen 25 Nationen mit insgesamt 800 Teilnehmern in virtuellen Übungsnetzwerken zusammen, um mit ihren Teams von der Homebase aus die zugewiesenen Netze zu verteidigen. Schwergewicht der Locked Shields 2017 war die Verteidigung der Infrastruktur eines Flughafens. In der zwei Tage dauernden Übung wurden vom international zusammengesetzten

Angreiferteam mehr als 2500 Angriffe gegen die verteidigenden Nationen durchgeführt. Das Team des BMLV konnte 2017 den vierten von 20 Plätzen belegen.

4.5 TRIAL THOR'S HAMMER II 2017

Im Juli 2017 nahmen fünf Soldaten des Kdo FüU&CD gemeinsam mit Teilnehmern aus sieben anderen Nationen für drei Wochen am Trial THOR'S HAMMER II 2017 in Schweden teil. Das Ziel war die Testung von landgestützten Schutzsystemen gegen Bedrohungen im Bereich der Radio Controlled IEDs (Improvised Explosive Devices). Diese Art der Veranstaltung, welche im Abstand von zwei Jahren stattfindet und unter der Schirmherrschaft des NATO Team of Experts on Electronic Countermeasures for Radio Controlled IEDs steht, stellt eine weltweit einzigartige Möglichkeit dar, auf diesem hohen technischen Niveau multinational einsatzrelevante Erfahrungen zu sammeln.

Österreich nahm 2017 das erste Mal teil und es konnten unter realen Bedingungen notwendige Erfahrungswerte für das künftige Schutzsystem des ÖBH erarbeitet werden, um damit einen weiteren Beitrag zum Schutz der Soldaten bei Einsätzen leisten zu können. Diese multinationale Partnerschaft ist beispielsgebend für eine Kooperation im Bereich der Streitkräfte und stellt einen unabdingbaren Mehrwehrt in diesem Spezialbereich dar.

5 Zusammenfassung / Ausblick

Auch im Jahr 2017 hat sich der bereits in den Jahren zuvor beobachtete Trend hin zu einer signifikanten Steigerung von sicherheitsrelevanten Aktivitäten/Vorfällen im Cyber Bereich fortgesetzt. Insgesamt ist daher die Bedrohungslage nach wie vor als ansteigend einzustufen. Während die Vorfallszahlen vor allem in den Bereichen Ransomware und Advanced Persistant Threats (APT) deutlich ansteigend sind, scheint der Höhepunkt der DDoS-Wellen der Vorjahre überwunden zu sein. Insbesondere Ransomware scheint sich zunehmend als Mittel der Wahl für Cyber Kriminelle etabliert zu haben, wobei ein massiver Anstieg bei monetär motivierten Cyber Vorfällen festzustellen ist. Es ist eine Zunahme von Cyber Crime Fällen bei gleichzeitigem Rückgang konventioneller Straftaten zu beobachten. Beeinflussung der öffentlichen Meinung (inkl. Wahlen) via Internet ist evident.

Unternehmen der kritischen Infrastruktur sowie der Cyber Sicherheit Branche reagieren auf die unverändert steigende Bedrohung entsprechend. Es ist sowohl ein Trend zu steigenden Budgets für Maßnahmen zur Erhöhung der Cyber Sicherheit als auch eine laufende Implementierung neuer Sicherheitsmaßnahmen zu beobachten. Angesichts allgegenwärtiger Bedrohungen und kaum zu verhindernder Angriffe aus dem Cyber Raum zielen diese Maßnahmen vermehrt auf die Erkennung und Reaktion auf erkannte Angriffe ab. Rasche Erkennung und richtige Reaktion stehen im Vordergrund von Sicherheits- und Ausbildungsmaßnahmen. Darüber hinaus ist ein Inhousing von IKT-Leistungen (Datensicherheit & Datenhoheit) als Trend erkennbar.

Internationale Entwicklungen lassen klar eine weiterhin steigende Bedeutung des Bereiches Cyber Sicherheit und zunehmende Sensibilisierung im Hinblick auf Cyber Bedrohungen erkennen. Cyber Bedrohungen werden mittlerweile durchgängig als wesentliche Bedrohung für die nationale Sicherheit eingestuft. Nationale Cyber Sicherheit Strategien und gesetzliche Grundlagen werden laufend angepasst, die finanziellen Aufwendungen für die Etablierung von notwendigen Strukturen sind als signifikant zu beurteilen. Der vermehrten Einbindung des privaten Sektors in Cyber Sicherheitsangelegenheiten wird besondere Bedeutung beigemessen. Cyber Sicherheit Maßnahmen sind nur im Verbund zweckmäßig und effizient. Nur Kooperation und Zusammenarbeit statt Insellösungen können zum Erfolg führen. Es bedarf der engen Zusammenarbeit öffentlicher Stellen und Unternehmen, wie auch der Zusammenarbeit von Militär und Zivil. Nationale wie internationale Zusammenarbeit ist gefordert.

Fragen der Cyber Sicherheit werden weiterhin im Rahmen von EU, VN, OSZE, NATO und OECD sowie in multilateralen Foren unter aktiver Beteiligung von Österreich thematisiert. Auf EU-Ebene liegen mit dem Paket zur Cyber Sicherheit und den Cyber Prioritäten der Trio-Präsidentschaft umfassende Maßnahmen zur Verbesserung der Cyber Sicherheit vor. Mit der ab Mai 2018 fälligen Umsetzung der im Juli 2016 beschlossenen Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-RL) wird das Cyber Sicherheitsniveau in allen EU Mitgliedsstaaten gehoben werden.

Im Bereich nationaler Akteure und Strukturen haben die neu aufgestellten bzw. nach aktuellen Bedürfnissen adaptierten Elemente ihre Funktionsfähigkeit im Regelbetrieb bewiesen. Die Anpassung nationaler Strukturen und Prozesse an die neuen Herausforderungen im Cyber Raum wurde damit fortgesetzt. Insbesondere die operationelle Zusammenarbeit zwischen den unterschiedlichen Stakeholdern im Rahmen des inneren Kreises der operativen Koordinierungsstrukturen hat im Jahr 2017 zufriedenstellend funktioniert und deutlichen Mehrwert generiert.

Die Zusammenarbeit zwischen staatlichen und privaten Strukturen, vor allem auch im Lichte der Umsetzung der EU NIS-RL in nationales Recht, wurde weiterhin deutlich forciert.

Die weitere und laufende Anpassung von Strukturen und Prozessen an aktuelle Herausforderungen wird auch zukünftig im Fokus nationaler Entwicklungen im Bereich der Cyber Sicherheit stehen. Das Inkrafttreten des NIS-Gesetzes und die daran anschließende konkrete Umsetzung gemeinsam mit den Betreibern wesentlicher Dienste wird eines der Schwergewichte im Jahr 2018 darstellen. Zudem ist basierend auf den Vorgaben des aktuellen Regierungsprogrammes eine Neuvorlage der ÖSCS geplant. Sowohl für die Umsetzung des NIS-Gesetzes als auch für die koordinierte Umsetzung der strategischen Vorgaben aus der neuen ÖSCS werden auch weiterhin wesentliche Inputs aus der Zusammenarbeit zwischen dem öffentlichen und dem privaten Bereich, insbesondere im Rahmen der Cyber Sicherheit Plattform, erwartet.