REPUBLIK ÖSTERREICH

Bericht Cyber Sicherheit 2017

BUNDESKANZLERAMT ÖSTERREICH

BM.I REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR INNERES

Bundesministerium für Landesverteidigung und Sport bmlvs.gv.at

EUROPA INTEGRATION ÄUSSERES BUNDESMINISTERIUM REPUBLIK ÖSTERREICH

Bericht
Cyber Sicherheit
2017

Wien, Mai 2017

Impressum

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

Wien, im Mai 2017

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 2016 vorgelegt.

Der aktuelle Bericht Cyber Sicherheit 2017 baut auf den Inhalten des letztjährigen Berichtes auf und ergänzt diesen um aktuelle Entwicklungen mit einem Schwergewicht im operationellen Bereich.

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

1 Cyber Lage / Bedrohungsanalyse

Die heutige Gesellschaft ist immer mehr von den 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 immer häufiger 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 Phänomenologie

1.1.1 Denial of Service / Distributed Denial of Service-Attacken

DoS (Denial of Service) und DDoS (Distributed Denial of Service) Attacken zählen derzeit zu den häufigsten und wirksamsten Cyber Attacken.

DDoS-Attacken legen Webserver oder ganze Netzwerke lahm. Im Gegensatz zu einer einfachen DoS-Attacke haben DDoS-Angriffe eine wesentlich höhere Schlagkraft. Mehrere Computer greifen dabei gleichzeitig und im Verbund (beispielsweise über ein Botnetz) eine Webseite oder eine ganze Netzinfrastruktur an. Das angegriffene System wird mit (teils sinnlosen) Anfragen überflutet, die mit den dort zur Verfügung stehenden Ressourcen nicht mehr schnell genug abgearbeitet werden können. Typische DDoS-Angriffe zielen dabei regelmäßig auf die Überlastung der Internetanbindung, der Ressourcen der Netzwerkkomponenten sowie der Web- und Datenbankserver ab.

DDoS-as-a-Service

Gegenwärtig ist in immer stärkerem Ausmaß die Entwicklung zu beobachten, dass DDoS-Angriffe im Internet als Dienstleistung »eingekauft« werden. So bieten im »Darknet« (einem für normale Internetbenutzer nur über technische Umwege zugänglichen Bereich des Internets, der aufgrund seines eingeschränkten Zugangs und der Möglichkeit, Aktivitäten von Benutzern unnachvollziehbar zu verschleiern, verstärkt für kriminelle Zwecke mißbraucht wird) zahlreiche Anbieter gegen vergleichsweise geringes Entgelt die Möglichkeit, Angriffe nach Dauer und Volumen preislich gestaffelt zu »bestellen«. Die Bezahlung erfolgt in den meisten Fällen auf Basis der Cryptowährung Bitcoin.

So funktioniert ein DoS / DDoS-Angriff im Detail

Bei DoS-Angriffen werden häufig Schwächen in Anwendungen, Betriebssystemen oder Webprotokollen ausgenutzt. Die Attacken können in verschiedenen Varianten durchgeführt werden:

- **Syn Flooding**
  Soll eine TCP-Verbindung – etwa zum Abruf einer Webseite – aufgebaut werden, führt dies zu einem Austausch von SYN- und ACK-Datenpaketen zwischen Client und Server (Handshake). Im Falle eines Syn Flooding-Angriffs werden von den Angreifern viele SYN-Pakete losgeschickt die jeweils eine gefälschte Absender-IP-Adresse enthalten. Das Zielsystem antwortet auf diese mit entsprechenden SYN-ACK-Paketen, nur gehen diese Antworten natürlich an die gefälschten IP-Adressen. Dabei wird jeweils etwas Rechenleistung und für eine gewisse Zeit Speicherkapazität in Anspruch genommen. Je höher

die Rate der empfangenen SYN-Pakete ist, umso mehr erfolglose Antwortanfragen werden losgeschickt und Ressourcen gebunden. Sind die Verbindungskapazitäten (TCP State Table) ausgeschöpft, kann das System keine weiteren Verbindungen mehr annehmen und ist damit auch für legitime Anfragen nicht mehr erreichbar. Für effektive SYN Flooding Angriffe reichen oft schon Bandbreiten im Bereich von wenigen Mbit pro Sekunde. Mittels SYN Cookies, welche die Bindung von Ressourcen auf einen späteren Zeitpunkt im Handshake verschieben, lassen sich diese Angriffe allerdings gut abwehren.

- **Reflected-DoS-Angriff**
  Diese Angriffsvariante zielt auf die Überlastung von Leitungskapazitäten und nutzt legitime, aber schlecht konfigurierte UDP-basierte Server im Internet als Reflektoren/Verstärker von Paketen. Der Angreifer schickt dabei viele (kleine) Anfragen an diese Server, wobei er aber die IP-Adresse des Opfers als Absenderadresse einträgt (IP-Spoofing). Die Server halten diese Anfragen für legitim und beantworten sie mit großen oder mehreren Antwortpaketen. Diese werden aufgrund des IP-Spoofing jedoch an das Opfer dieser Attacke anstelle den eigentlichen Sender zugestellt.

  Dadurch hat der Angreifer folgende Vorteile:
  - Seine Angriffsbandbreite wird durch die Reflektoren verstärkt.
  - Nutzt er viele verschiedene Server als Reflektoren, so sieht das Opfer breit verteilte Angreifer, die sich nicht einfach mit einer Filterliste ausblenden lassen.
  - Der Standort des Angreifers, bzw. die Quelle der gefälschten Pakete ist schwer auszuforschen.

- **Angriffe auf den Applikationslayer**
  Sowohl gegen Webserver, als auch gegen Nameserver wurden in der letzten Zeit spezifische Angriffsmuster beobachtet.

  Webserver können durch viele parallele Anfragen überlastet werden. Bei Webseiten, die verschlüsselt übertragen werden (https) ist der Verbindungsaufbau deutlich aufwändiger, da hier ein kryptographischer Schlüsselaustausch ausgeführt werden muss. Auch ist eine DDoS-Mitigation durch den ISP hier deutlich schwieriger, da dieser durch die Verschlüsselung weniger Möglichkeiten hat, »gute« von böswilligen Anfragen zu unterscheiden.

  Ähnlich wie Reflection-Attacks funktionieren Angriffe auf Basis der Wordpress-Pingback Funktion. Dies funktioniert folgendermaßen: Blogs verweisen auf Artikel anderer Blogger, was gerne mit einem Retour-Link (»Folgende Blogs zitieren diesen Artikel«) beantwortet wird. Im Hintergrund notifiziert der zitierende Blog die Quelle, das dortige Wordpress verifiziert das und setzt erst dann den Pingback Link. Dieses Verifizieren ist jedoch ein Problem: Wenn ein Angreifer tausenden von Wordpress-Installationen mitteilt, dass die Webseite des Opfers gerade einen Link gesetzt hat, dann versuchen sie alle, das zu verifizieren und lösen so eine Überlastung beim Opfer aus.

  Angriffe auf das Domain Name System werden ebenfalls regelmäßig registriert. Aktuell beobachtet man »Random Subdomain Requests« als größte Bedrohung: Hierbei werden aus einem Botnet heraus sehr viele Anfragen zu zufällig gewählten Subdomains des Opfers an beliebige Nameserver gestellt. Diese Randomisierung hebt den Effekt von Caches auf, wodurch eine Flut von Anfragen die Nameserver des Opfers erreicht.

  Abbildung 1 zeigt, welche IP-Adressen in den jeweiligen Netzen für eine DDoS Angriffsverstärkung verwendet werden können.

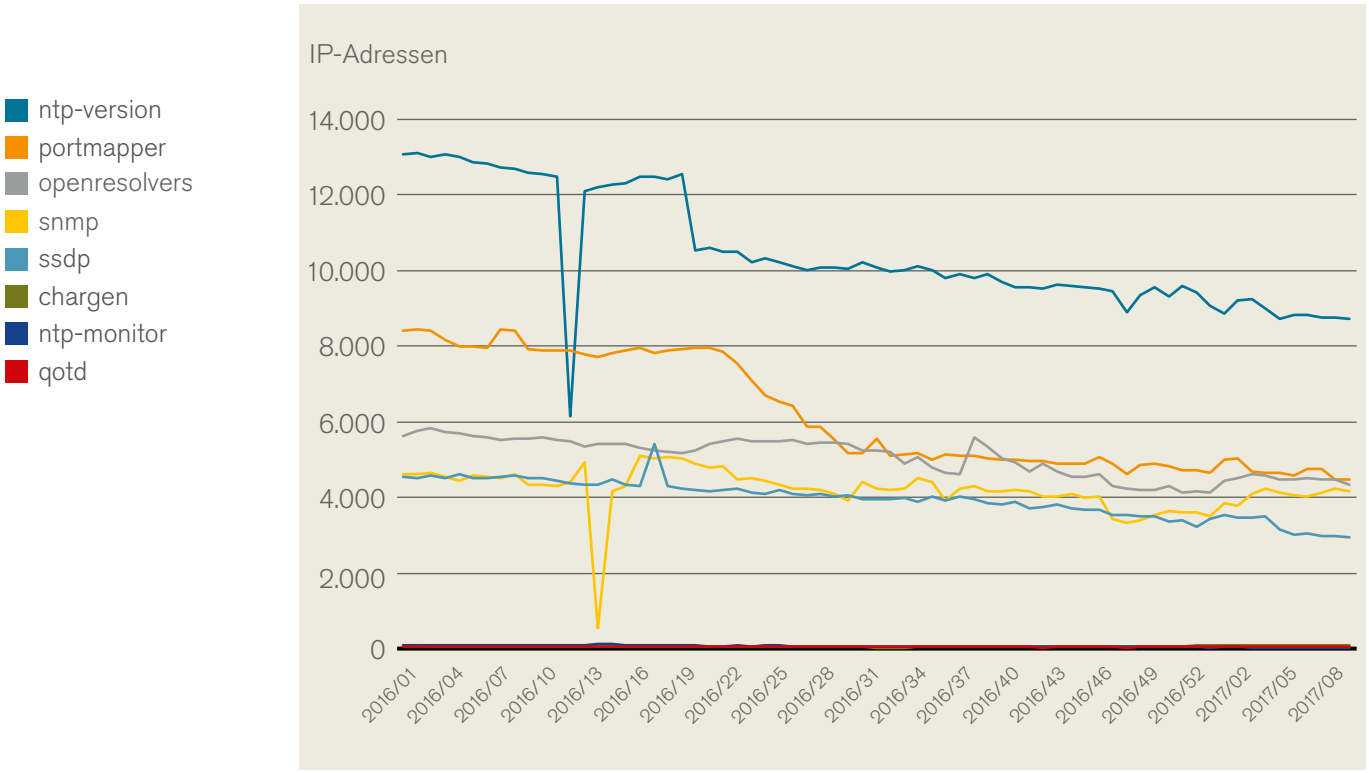

Abbildung 1: Zahl der IP-Adressen als potentielle Angriffsverstärker nach den jeweiligen Netzen im Zeitverlauf, Quelle: CERT.at

Österreichische Unternehmen als Opfer von DDoS-Attacken

In den letzten zwei Jahren hat sich der Kreis der DDoS-Opfer auch in Österreich stark erweitert, vor allem durch das Aufkommen von damit einhergehenden Erpressungsversuchen. So gerieten zuletzt etwa auch österreichische Firmen ins Blickfeld der Hacker-Gruppe DD4BC (DDoS for Bitcoins). Initial richteten DD4BC ihre Attacken auf Bitcoin-Webseiten, dann auf Finanzdienstleister, E-Commerce Webseiten und Internet Service Provider. Im Dezember 2015 konnten im Zuge einer Aktion von Europol – unter Federführung des österreichischen Cyber Crime-Competence-Centers (C4) im Bundeskriminalamt – die Angreifer gefasst werden.

Auch 2016 gab es Attacken auf österreichische Unternehmen und Organisationen. Prominente Opfer: A1, das Außenministerium, das Bundesheer, die OeNB und der Flughafen Wien. Bei A1 war das Motiv Geld. In einem Erpresserschreiben wurden 100.000 Euro in Bitcoins verlangt, im Gegenzug wurde von den Erpressern, wie in solchen Fällen üblich, ein Abbruch der bereits angelaufenden Attacke versprochen. Erst als die Erpresser erkannten, dass die Techniker von A1 imstande waren, den Angriff abzuwehren, gaben sie auf. Die Suche nach den Angreifern gestaltete sich jedoch schwierig, da diese aus mehreren Ländern operierten, unter anderem aus Osteuropa und dem asiatischen Raum. In anderen Fällen waren die Angriffe politisch/nationalistisch motiviert.

Lange galt eine Attacke, die 2013 von einem damals 16-jährigen Briten durchgeführt wurde, als größter DDoS-Angriff. Er brachte es ExpertInnen zufolge auf etwa 300 Gigabit pro Sekunde. Im September 2016 wurde eine Attacke bekannt, die diesen Wert deutlich übertraf. Das Opfer war der französische Hoster OVH, der mit bis zu 1,1 Terabit pro Sekunde angegriffen wurde.

Vorkommnisse 2016 mit Mirai und die Verbindung zu Botnets

Mirai ist eine Schadsoftware für Internet of Things (IoT)-Geräte (welche unter speziellen Linux-Varianten laufen), mit deren Hilfe Botnetze aufgebaut werden können. Damit lassen sich beispielsweise gezielte Angriffe durch absichtliche Überlastungen von Netzen durch DoS- oder DDoS-Attacken organisieren. Mirai befällt IoT-Systeme und schaltet dann die infizierten Geräte mit anderen zu einem Botnet zusammen.

Gerade im letzten Quartal 2016 haben sich die Angriffe in Verbindung mit Mirai-Botnets stark gehäuft:

- Der Internet-Dienstleister Dyn ist Mitte Oktober das Opfer einer Attacke mit zig-Millionen involvierten IP-Adressen geworden. Durch den Angriff auf Dyn waren Zugänge zu Diensten wie Twitter, Spotify, Paypal, Netflix, Airbnb oder Amazon für viele NutzerInnen in den USA, Europa, Japan und Australien mehrere Stunden lang nicht zu erreichen. Die Angreifer haben für die Attacke zu einem großen Teil mit dem Internet der Dinge (IoT) verbundene Geräte wie Webcams, Router, Drucker, TV-Festplatten-Receiver oder sogar Babyphones genutzt.

- Ende November versuchte Mirai auch, über eine Sicherheitslücke der Wartungsprotolle TR-069 und TR-064 in Modems von DSL und Kabelkunden einzudringen. Im Falle der Deutschen Telekom führte das dazu, dass knapp eine Million Menschen ohne Internet waren, weil deren Modems von diesen Anfragen in ihrer Funktion gestört wurden.

- Abbildung 2 gibt einen Überblick über die Infektionen in Verbindung mit Mirai-Botnets in Österreich seit Oktober 2016.

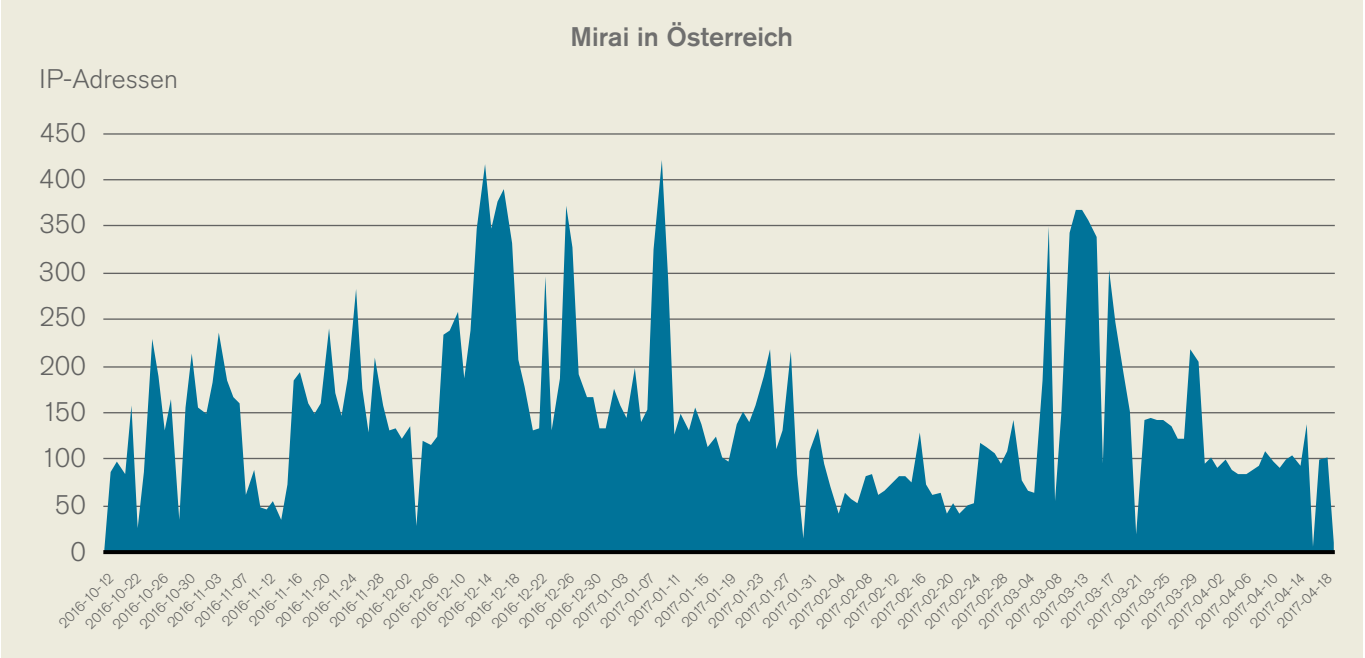

Abbildung 2: Vorfälle in Verbindung mit Mirai seit Oktober 2016 (pro Tag) in Österreich. Quelle: CERT.at

1.1.2 Politisch motivierte DDoS-Angriffe

Im Juni 2016 waren Vorzeichen für ein erneutes Ansteigen der Gefahr von DDoS-Angriffen in Österreich zu erkennen. Beginnend mit Anfang September wurden österreichische Einrichtungen der kritischen Infrastrukturen sektorübergreifend von einer bisher beispiellosen Reihe von politisch motivierten DDoS-Angriffen heimgesucht. In mehreren Wellen wurden, teils auch mehrfach, der Flughafen Wien-Schwechat, die österreichische Nationalbank, die Website eines prominenten österreichischen Politikers, das Bundesministerium für Landesverteidigung und Sport, das Bundesministerium für Europa, Integration und Äußeres, sowie das österreichische Parlament angegriffen.

Nach dem bisherigen Erkenntnisstand ist die türkische Hackergruppe »Aslan Neferler Tim« für diese Vorfälle verantwortlich. Sie reagierte damit nach eigenem Bekunden auf – aus ihrer Sicht – türkeifeindliche Aktionen, die durch die betroffenen Unternehmen und Einrichtungen gesetzt wurden. In sozialen Medien beschreibt die Gruppe die Motivation für ihre Angriffe wie folgt:

> »Solange politische Einstellung wider der Türkei anhält, werden Angriffe fortgesetzt.«

> »Der das Wort Türkei in den Mund nimmt, soll genau überlegen, sonst wird seine Stimme zum Schweigen gebracht.«

Bisher sind jedoch keine Belege evident, die auf eine aktive Beteiligung des türkischen Staates an diesen Angriffen hindeuten würden.

Anlässlich der letzten Welle dieser Angriffe veranstaltete das Cyber Security Center im Dezember 2016 eine diesbezügliche »Expertenrunde«. In einer Serie von hochkarätigen Vorträgen (Heeres-Nachrichtenamt, Cyber Security Center, next layer, A1 Telekom Austria und GovCERT) wurde das Thema vor mehr als hundert Vertretern der kritischen Infrastruktur aus allen relevanten Blickwinkeln beleuchtet.

Die Angriffsserie zeigte auch einige positive Aspekte im Bereich der Cyber Sicherheit in Österreich auf. Zum einen war es den operativen Koordinierungsstrukturen aufgrund der mittlerweile eingespielten Zusammenarbeit möglich, einzelne Angriffe bereits zwei Stunden vor ihrem Eintreten konkret vorherzusagen und entsprechende Vorkehrungen zu treffen bzw. Warnungen auszusprechen. Zum anderen ist anzumerken, dass die Angriffsopfer offenbar gut auf eine derartige Situation vorbereitet waren. Jedenfalls kam es im Zuge der Angriffe lediglich zu vergleichsweise unbedeutenden Ausfällen von Systemen; in keinem einzigen Fall war ein Ausfall eines unternehmens- oder sicherheitskritischen Systems zu verzeichnen. Dies belegt eindrucksvoll den hohen Resilienzgrad österreichischer Unternehmen der kritischen Infrastrukturen gegenüber Bedrohungen aus dem Cyber Raum.

1.1.3 Ransomware

Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern. Eine Freigabe dieser Ressourcen erfolgt nur gegen Zahlung eines geforderten Lösegeldes (engl. ransom). Es handelt sich dabei um einen Angriff auf die Verfügbarkeit von Daten und Computern und verwirklicht den Straftatbestand der Erpressung bei Forderung von Lösegeld.

Bereits seit 2010/2011 wird Ransomware verbreitet für Cyber Angriffe eingesetzt. Auch davor gab es bereits erste Varianten dieses Schadprogramm-Typs.

Im Laufe der Zeit wurden vermehrt Ransomware-Varianten entwickelt, die Daten verschlüsseln. Dadurch stehen diese dann dauerhaft, trotz Bezahlung des Lösegelds, nicht mehr zur Verfügung (z. B. Cryptolocker). Für die Verschlüsselung werden meist hochwertige Algorithmen eingesetzt, was eine Entschlüsselung praktisch unmöglich macht. Zusätzlich zu den Daten des infizierten Clients können auch Daten auf zugänglichen Netzlaufwerken (Netzwerk-Shares), angesteckten USB-Geräten oder eingebundenen Cloud-Diensten verschlüsselt werden. Mittlerweile gibt es nicht nur Ransomware für Windowssysteme sondern auch für Apple Mac, Linux und Smartphones.

Die Verteilung dieser Schadsoftware erfolgt hauptsächlich durch Verwendung von Social Engineering Techniken (beispielsweise per kompromittierten E-Mail-Anhang). Aber auch sogenannte Drive-by-Downloads bei infizierten Webseiten können diesen Schadcode an die – somit zufällig »vorbeischauenden« – Computersysteme ausliefern.

Derzeit werden ca. 700 Ransomware-Fälle (Tendenz stark steigend) mit verschiedensten Varianten in der Sonderkommission »CLAVIS« (diese wurde 2016 in Reaktion auf das Phänomen Ransomware ins Leben gerufen) bearbeitet. Diese Varianten gliedern sich derzeit in folgende Ransomware Familien: AES256, AiraCrop, Al-Namrood 2.0, Apocalypse, CERBER, Crypt0l0cker, CryptoWall, Dharma, DMA Locker, DXXD/Mobdef/Yakes, Globe, Goldeneye, Hakuna Matata, Jigsaw, LinuxEncoder, LOCKY in verschiedenen Unterarten, Microsoft Decrypter, MISCHA/PETYA, Mongo_DB, Paycrypt/CrySIS, Philadelphia, Teslacrypt, Ultracrypter, Zeta und ZEPTO. Als am meisten verbreitete Ransomware Arten können Crypt0l0cker, CERBER und MISCHA/PETYA angeführt werden.

Es lässt sich ein Trend weg von den großen Ransomware Familien hin zu kleineren Ransomware Arten feststellen. Viele dieser kleineren Arten werden als sogenannte Ransomware Kits im Internet angeboten. Bei diesen Ransomware Kits ist von den Täterschaften kein technisches Know-How notwendig, sie können von nahezu jedermann verbreitet werden.

Von einer hohen Dunkelziffer nicht angezeigter Fälle ist auszugehen. Dies begründet sich darin, dass viele betroffene Privatanwender keine Anzeigen erstatten, viele Unternehmen auf Grund eines vermuteten Reputationsverlustes ebenso keine Anzeigen erstatten bzw. notwendige Vorkehrungen (Backup der betroffenen Dateien) vorhanden sind, welche eine rasche Systemwiederherstellung möglich machen. Darüber hinaus gelangen versuchte Attacken in Form von Phishing Mails ohnehin nicht zur Anzeige.

Das Internet of Things wird sich für Ransomware-Anwender und -Entwickler in ein besonderes Betätigungsfeld entwickeln. Da diese Geräte typischerweise wenig bis gar keine Sicherheitsmerkmale eingebaut haben und auch nicht dafür vorgesehen sind, entsprechende Software-Updates zu erhalten, bleiben sie so lange für Angriffe anfällig bis sie letztendlich aus dem Netz entfernt werden.

1.1.4 CEO-Fraud

CEO-Fraud bedient sich einer »internen« Variante des Rechnungsbetruges. Hier geben sich Angreifer als Teil des Unternehmens – z. B. als Geschäftsführer oder Finanzvorstand – aus und fordern von MitarbeiterInnen, oft unter Hinweis auf die notwendige Geheimhaltung, eine dringende Überweisung, beispielsweise durch eine gefälschte E-Mail an die Buchhaltung.

Auch hier wurde in der Regel im Vorfeld bereits die firmeninterne Struktur zum Zwecke des Angriffs ausspioniert, sodass durch die Vorgabe umfangreicher Kenntnisse über das Unternehmen der Betrugsverdacht beim Opfer minimiert wird. Mit dem Hinweis auf die geheime und

dringende Überweisung werden die MitarbeiterInnen zum Durchführen einer Überweisung auf ein falsches Konto gebracht.

1.1.5 Verstärkte Nutzung des Cyber Raumes für Informations- und Desinformationskampagnen

2016 erreichte die Nutzung des Cyber Raumes zur gezielten Einflussnahme auf Politik und Gesellschaft durch staatliche und nichtstaatliche Akteure international einen neuen Höhepunkt. Die mögliche Bandbreite der Einflussnahme reicht von der gezielten Verbreitung politisch-ideologischer Positionen – oft unter Einsatz verfälschter oder falscher Nachrichten – bis hin zur Veröffentlichung von durch Hacking-Aktivitäten entwendeter Information zur Deskreditierung von Personen oder Organisationen. Informations- und Desinformationskampagnen stellen zwar per se keine Cyber Bedrohung dar, können aber durch den Verlust und die Veröffentlichung vertraulicher Daten – sogenannten »Leaks« nach Hacking-Angriffen – ausgelöst werden.

Informationen, die mit Hacking-Methoden gewonnen wurden, können durch ihre Exklusivität sowie bei brisanten Inhalten eine hohe Verbreitung erreichen und sind somit geeignet, die öffentliche Meinung zu beeinflussen. Hierbei werden sowohl authentische wie auch gefälschte Daten zur Durchführung von Informations- bzw. Desinformations-Kampagnen genutzt. 2016 wurden weltweit rund 3.000 Daten-Leaks bekannt, bei denen etwa 2,2 Mrd. Datensätze veröffentlicht wurden.

Der wohl markanteste Fall war die als »DNC-Hack« bekannt gewordene Veröffentlichung von gehackten E-Mails der US-Demokraten im Zuge des Präsidentschaftswahlkampfes durch die Enthüllungsplattform Wikileaks im Juli 2016. Der »DNC-Hack« fügte der Wahlkampagne von Präsidentschaftskandidatin Hillary Clinton massiven Schaden zu und führte zum Rücktritt einiger hoher Funktionäre der US-Demokraten. Auch nach den Wahlen beschäftigen und beeinflussen die Auswirkungen des »DNC-Hack« die US-Politik.

Im Oktober 2016 veröffentlichte die ukrainische Hacker-Gruppe »CyberHunta« mehr als ein Gigabyte an E-Mails und Dokumenten, die vermeintlich von E-Mail-Konten zweier Assistenten des bedeutenden russischen Kreml-Mitarbeiters und Präsidentenberaters Wladislaw Surkow stammen sollen. Mit den veröffentlichten Daten sollte die Einmischung Russlands zur Destabilisierung der Ukraine bewiesen werden. Im Daten-Leak befanden sich aber nicht nur authentische E-Mails, sondern auch gefälschte Daten, wie etwa ein Plan zur Unterminierung der ukrainischen Regierung und zur Auslösung vorgezogener Wahlen.

1.2 Cyber Lage

1.2.1 Lage Cyber Sicherheit

Die Implementierung der Österreichischen Strategie für Cyber Sicherheit ist ein permanenter Prozess, der von einer eigenen Cyber Sicherheit Steuerungsgruppe (CSS) koordiniert wird. Die CSS wurde in diesem Zusammenhang mit der Schaffung einer gesamtstaatlichen Struktur zur Koordination auf operativer Ebene beauftragt. Seit 2014 wird von der CSS der jährliche Bericht zur Cyber Sicherheit erstellt, der einen Überblick über die Cyber Lage (Bedrohungsanalyse), nationale und internationale Entwicklungen, sowie die durchgeführten Cyber Übungen gibt.

Staatliche Stellen sehen im Rahmen ihrer Tätigkeit lediglich einen Ausschnitt der in Österreich vorliegenden Situation. Um in diesem Bereich jedoch ein möglichst valides und vollständiges

Bild der Situation in Österreich zu zeichnen, wurden aus diesem Grund zur Erstellung des vorliegenden Berichtes sowohl

- Unternehmen der kritischen Infrastruktur, als auch
- führende private Unternehmen aus der Cyber Security-Branche

eingeladen, auf der Basis ihrer Tätigkeit dieses Wissen zu vervollständigen. Das Interesse galt dabei nicht konkreten Einzelfällen, sondern vielmehr einer abstrahierten Überblicksdarstellung.

Unternehmen der kritischen Infrastruktur

Im Jahr 2016 ist bei den befragten Unternehmen der kritischen Infrastruktur das für IT-Security zur Verfügung stehende Budget gegenüber dem Jahr 2015 bei einer stark überwiegenden Anzahl entweder gestiegen oder zumindest gleich geblieben (Abbildung 3).

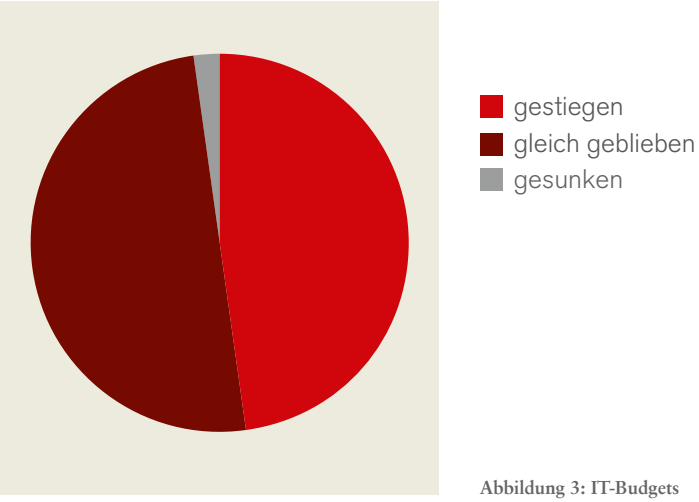

Abbildung 3: IT-Budgets

Gleichzeitig wurden bei einem Großteil der Unternehmen (84 %) im Jahr 2016 neue Sicherheitsmaßnahmen implementiert. Viele dieser Maßnahmen ermöglichen es den Unternehmen, IKT-Sicherheitsvorfälle überhaupt erst als solche zu erkennen. Das kann möglicherweise auch erklären, warum die meisten Unternehmen einen steigenden Trend bei, insbesondere von Außentätern ausgehenden, Angriffen erkennen (Abbildung 4).

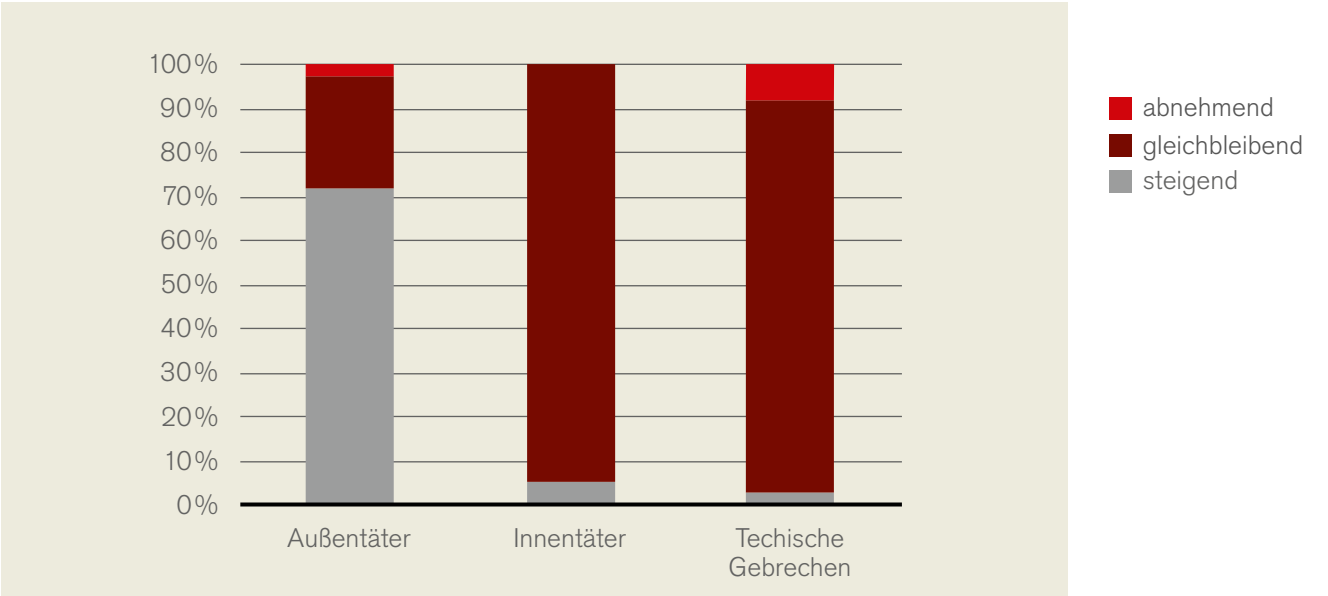

Abbildung 4: Trends Cyber Vorfälle 2016

Allerdings stellen diese Bedrohungen im Cyber Bereich – unabhängig von den Trends – für die betreffenden Unternehmen nach eigener Einschätzung noch immer meist nur ein kleines bis gar kein Problem dar (Abbildung 5).

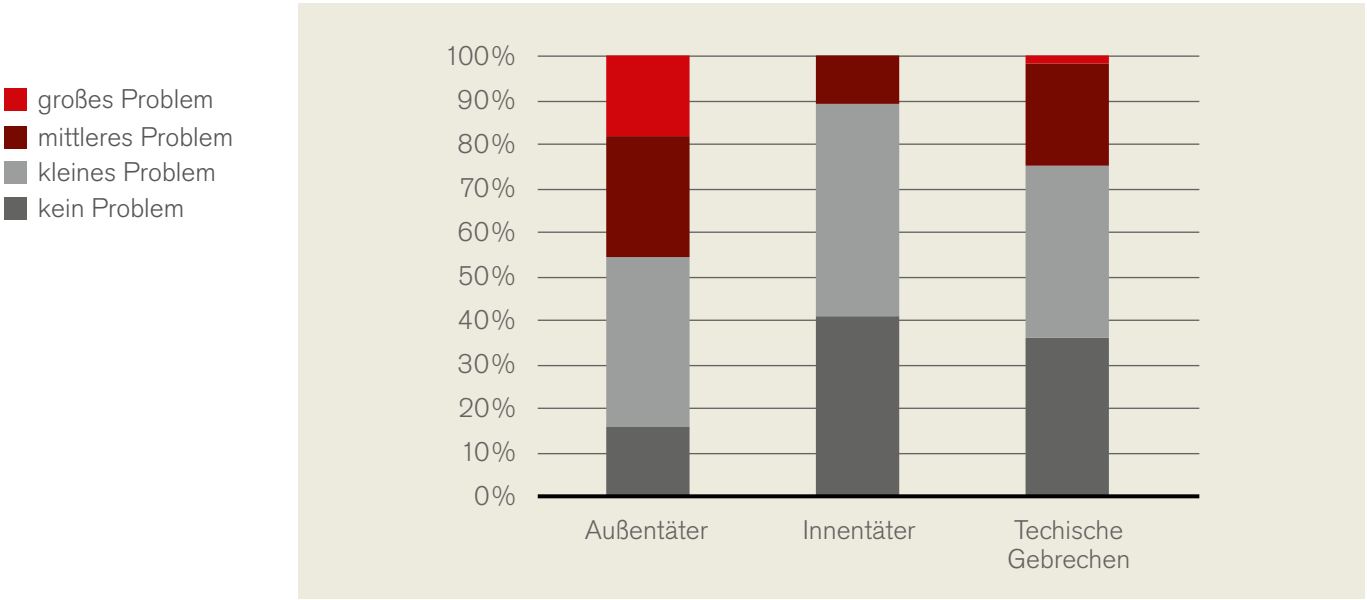

Abbildung 5: Beurteilung von Vorfallsursachen 2016

Aus der Befragung von mehr als 40 kritischen Infrastrukturen und staatlichen Organisationen geht hervor, dass in erster Linie zwar die Schnittstellen zur Peripherie gehärtet wurden (zum Beispiel durch fortschrittlichere Firewall-Lösungen mit Deep-Packet-Inspection oder Sandboxing zur Analyse potentieller Malware), aber generell gesprochen »Sicherheit« nun als holistisches Konzept wahrgenommen wird.

So führte das verstärkte Aufkommen von Ransomware, wie Crypto-Trojanern oder auch zunehmend professionalisierte Online-Betrugsversuche (CEO-Fraud) dazu, dass die Awareness der Endbenutzer als zentraler Faktor in der Unternehmenssicherheit erkannt wurde. Dementsprechend finden nun in vielen (vor allem größeren) Organisationen verstärkt Awareness-Veranstaltungen statt. Diese werden für Unternehmen der kritischen Infrastruktur auch verstärkt durch das Cyber Security Center angeboten.

Weiters wurde ein reines Überwachen an der Peripherie als unzulänglich erkannt; kritische Infrastrukturen setzten 2016 neue Maßnahmen zum systematischen Monitoring der internen Datenströme, als auch Härtung und Reporting an den einzelnen Arbeitsplatz-Rechnern.

Je nach Größe der Organisation wurden diese Maßnahmen mit Hilfe von externen Sicherheitsdienstleistern bewerkstelligt; insbesondere die größeren Infrastrukturen gaben an, lieber die eigene IT-Abteilung dementsprechend aufzustocken und sich hier nicht in Abhängigkeit von Dritten zu begeben. Lediglich bei der Abwehr der 2016 ebenfalls stark angestiegenen Anzahl an DDoS-Angriffen herrscht Einigkeit, dass dafür externe Hilfe unbedingt nötig ist. Für unternehmensinterne Sicherheitsmaßnahmen spielten DDoS-Angriffe aber nur eine untergeordnete Rolle.

Befragung führender privater Unternehmen aus der Cyber Security-Branche

Die Befragung von führenden privaten Unternehmen aus der Cyber Security-Branche war in diesem Jahr von einer geringen Rücklaufquote gekennzeichnet. Das vorhandene Datenmaterial erlaubt keine validen Aussagen über die Verteilung der Vorfallsarten (im Bezug zur Gesamtanzahl an IKT-Sicherheitsvorfällen). Ein grober Überblick ergibt jedoch, dass bei den Rückmeldungen nach wie vor Ransomware, CEO Fraud und Phishing-Angriffe in Österreich für die meisten (an IT-Dienstleister gemeldeten) Vorfälle verantwortlich zeichnen.

Ein klareres Bild ist bei den Trends erkenntlich. Bemerkenswert ist hier vor allem, dass bei keinem IT-Sicherheitsdienstleister für eine Vorfallsart eine sinkende Tendenz beobachtet wurde.

Im Vergleich zum Vorjahr blieb die Anzahl der Phishing-Vorfälle konstant, während sich bei Ransomware, neben steigenden Vorfallszahlen, auch eine zunehmende Professionalisierung abzeichnet. So stieg die Anzahl an Ransomware durch »Geschäftsmodelle« wie Ransomware-as-a-Service sprunghaft an. Auch Versuche von CEO Frauds wurden zunehmen aufwändiger und vermehrt auf die jeweiligen Opfer maßgeschneidet.

Ein eindeutiges Bild zeigt die »Motivation« bei den IKT-Sicherheitsvorfällen, zu deren Bewältigung ein IT-Sicherheitsdienstleister herangezogen wurde. Etwa 80 % dieser Vorfälle haben demnach einen monetären/kriminellen Hintergrund (Abbildung 6).

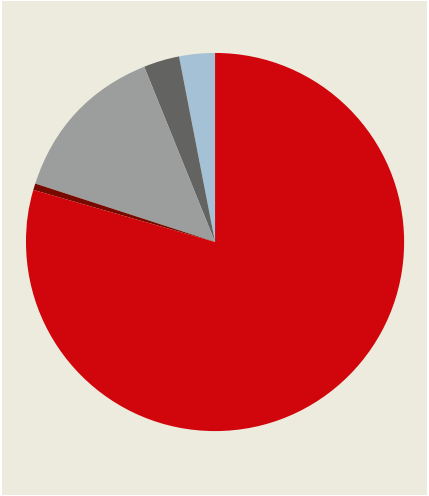

Abbildung 6: Motivationen

1.2.2 Lage Cyber Crime

Im Berichtszeitraum 2016 wurde durch das Bundeskriminalamt ein Anstieg von mehr als 55 %[1] bei Cyber Crimedelikten im Vergleich zum Jahr 2015 verzeichnet. Besonders kristallisierten sich die Phänomene Ransomware und (distributed) Denial of Service Angriffe (DDOS) sowie das kriminelle Geschäftsmodell Crime as a Service (CaaS) heraus. CaaS bietet schnellen und leichten Zugang zu jedweder Art von bösartiger Software und cyberkriminellen Dienstleistungen für den sonst cyber-unbedarften Bedarfsträger. Diese Dienste, u. a. DDOS-Angriffe, können auf einfache Weise im »digital Underground« (Darknet) angekauft oder gebucht und anonym 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). untergräbt die Vertrauenswürdigkeit, Integrität und Verfügbarkeit von Netzwerken, Geräten sowie Daten und Services in diesen Netzwerken und somit das Vertrauen in Online-Dienste und in neue Technologien wie das Internet of Things.

Mit einem Anteil von über 38 % aller bei der Polizei im Jahr 2016 angezeigten Fälle liegt das Phänomen Ransomware bei den Delikten des Cyber Crime im engeren Sinn an der Spitze. Es muss jedoch von einem großen Dunkelfeld ausgegangen werden, da viele betroffene Privatanwender keine Anzeigen erstatten und viele Unternehmen auf Grund eines vermuteten Reputationsverlustes ebenso davor zurück schrecken. Versuchte Angriffe werden meist gar

[1] Polizeiliche Kriminalstatistik Österreich, BMI, Bundeskriminalamt – Büro 4.3

nicht zur Anzeige gebracht. Dies deckt sich mit internationalen Erfahrungen. Angriffsvektor für diese Verschlüsselungstrojaner ist meist computer-based Social Engineering. Hier wird oft das mangelnde Bewusstsein über Bedrohungen aus »dem Internet« den Opfern zum Verhängnis.

1.2.3 Lage Landesverteidigung ÖBH/BMLVS

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. Für das BMLVS bedeutet dies, sich bestmöglich auf die militärische Landesverteidigung im Cyber Raum auszurichten und vorzubereiten. Gegnerische militärische Aufklärungsmaßnahmen gegen den Staat oder gegen zivile und militärische Einrichtungen, derzeit wahrscheinlich in erster Linie um Schwachstellen aufzuklären bzw. möglicherweise auch Schadsoftware einzubringen, können nicht ausgeschlossen werden.

Im Berichtszeitraum konnten zahlreiche Angriffe gegen Teile der IKT-Infrastruktur des ÖBH/BMLVS festgestellt werden. Der Großteil wurde durch die Abwehrsysteme erkannt und abgewehrt.

Im Durchschnitt sind pro Tag 60.000 Events zu verzeichnen, im vergangenen Jahr wurden davon ca. 300 als konkrete Angriffe erkannt. Vielfach handelt es sich um breit gestreute Massenangriffe, nichts destotrotz sind auch hier teilweise Merkmale zu finden, die darauf schließen lassen, dass es sich um Angriffe im Rahmen von international angesetzten Cyber Spionagekampagnen handelt.[2]

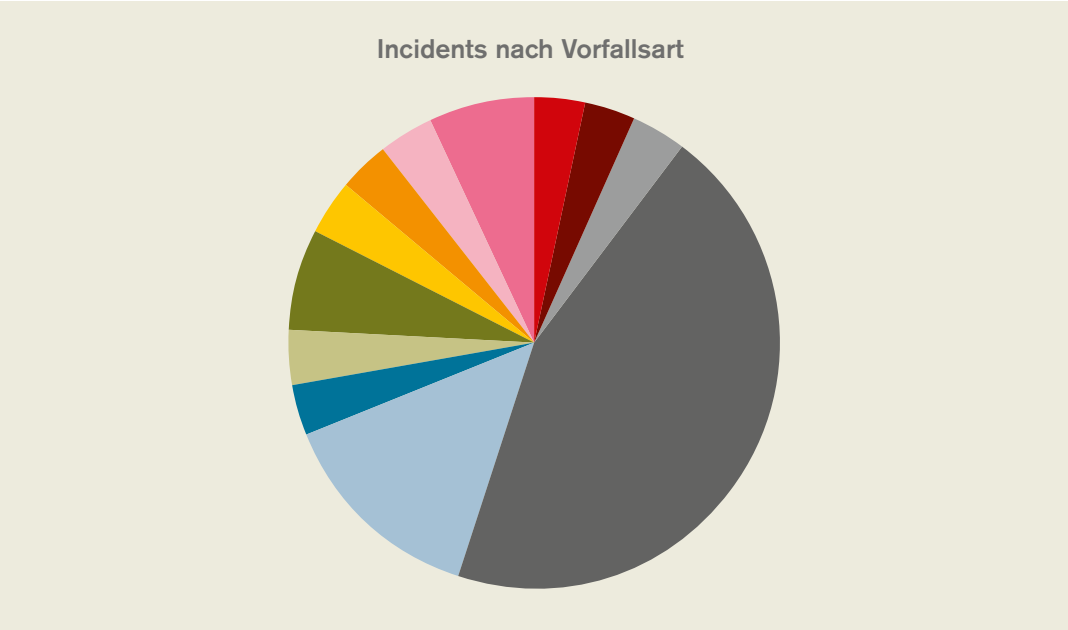

Abbildung 7: Anteile der zu behandelnden Vorfälle

[2] Immer wieder gibt es vor allem im Rahmen international erkannter Vorfälle Hinweise, dass Vermischungen von glaublich für monetäre Zwecke durchgeführten Cyber Angriffe mit Cyber Spionageangriffen gezielt eingesetzt werden, um einer Verfolgung durch zuständige Behörden zu entgehen (dies kann bspw. durch die Nutzung der gleichen Angriffs-Infrastruktur erfolgen wie auch durch die Verwendung eines ähnlichen modus operandi)

Wie Abbildung 7[3] zeigt, bestand der Großteil der zu behandelnden Vorfälle aus Phishing-Mails. Diese zielen vorrangig auf die Bekanntgabe von Zugangsdaten oder ähnlichem ab. Bereits an zweiter Stelle finden sich gezielte Phishing-Angriffe, die aufgrund der Inhalte bzw. der Angriffsziele erkennen lassen, dass es hier um die Erlangung anderer Informationen als Zugangsdaten handelt. Oftmals lassen sich derart gezielte Phishing-Mails nur schwer einer APT[4]-Kampagne zuordnen, werden aber in diese Richtung beobachtet.

Ein großer Teil der erkannten Angriffe im Bereich Phishing oder auch Spear-Phishing[5] werden aufgrund verschiedenster Merkmale der Gruppierung APT28 aka SOFACY[6] zugeordnet. Wie bereits in den vergangenen Jahren tritt diese Gruppierung somit weiterhin am aktivsten in Erscheinung und es wird auch in Zukunft verstärkt mit Angriffen bzw. Angriffsversuchen im Rahmen von Cyber Spionageaktionen (aber nicht nur seitens APT 28) gegen ÖBH/BMLVS-Infrastruktur zu rechnen sein.

Aufgrund politischer Spannungen kam es auch zu DDoS-Angriffen gegen die Infrastruktur des ÖBH (konkret den Webauftritt). Insgesamt drei Mal (1 Angriff im November 2016, 2 Angriffe im Dezember) war aufgrund durchgeführter DDoS-Attacken durch eine türkisch-patriotische Hackergruppierung die Verfügbarkeit der Homepage des ÖBH beeinträchtigt. Es kam zu keinen Datenverlusten oder schwerwiegenden Auswirkungen bzw. Schäden. Da sich die politischen Spannungen bis dato nicht gelegt haben, muss mit weiteren Angriffen gegen die Infrastruktur des ÖBH aber auch gegen die anderer österreichischer Institutionen/Behörden gerechnet werden.

---

3 Abbildung: eigene Aufbereitung

4 APT – Advanced Persistent Threat

5 gezieltes Phishing

6 Bei diesem vermutlich bereits seit 2005 operierenden Akteur wird ein staatlicher/nachrichtendienstlicher russischer Hintergrund vermutet. SOFACY weist einen sehr hohen Professionalisierungsgrad auf. Der Gruppierung, die zahlreiche weitere Namen hat (bspw APT28 oder SEDNIT,) werden die Angriffe auf den deutschen Bundestag 2015 wie auch die Angriffe im Rahmen der US-Präsidentschaftswahl 2016 zugeschrieben. Konkrete Beweise gibt es weder für die russische Steuerung noch für die Verantwortlichkeit der genannten Angriffe.

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

2.1 Europäische Union

Die Europäische Union (EU) beschäftigt sich vor allem im Rahmen ihrer 2010 beschlossenen Digitalen Agenda für Europa mit Fragen der Cyber Sicherheit. Anfang 2013 legte die Hohe Vertreterin zusammen mit der Europäischen Kommission (EK) die EU-Cyber Sicherheitsstrategie sowie den Vorschlag für eine Richtlinie zur Netz- und Informationssicherheit (NIS-RL) vor. Am 18.11.2014 wurde durch den Rat der EU ein EU-Cyber Defence Policy Framework angenommen, das die vorrangigen Aufgaben für die Gemeinsame Sicherheits- und Verteidigungspolitik (GSVP) im Cyber Bereich identifiziert und eine verbesserte Kooperation der EU mit dem privaten Sektor wie auch der Nordatlantischen Vertragsorganisation (NATO) gewährleisten soll. Der Rat nahm weiters am 10.02.2015 Schlussfolgerungen zur Cyber Diplomatie an, die einen gemeinsamen, umfassenden und kohärenten Ansatz zur Bewältigung der sich kontinuierlich verändernden Herausforderungen für die EU-Außenpolitik im Cyber Raum vorsehen. Mit der neuen globalen Strategie der EU (EUGS), die beim Europäischen Rat am 28./29.06.2016 begrüßt wurde, wurde auch dem Bereich Cyber ein entsprechendes Gewicht im außen- und sicherheitspolitischen Handeln der EU eingeräumt. Derzeit wird an der Umsetzung der EUGS, auch im Bereich Cyber, gearbeitet. In diesem Zusammenhang wurde u. a. im militärischen Bereich am 22.11.2016 das EU-Konzept »Cyber Defence for EU-led military Operations and Missions« angenommen. Am 5.7.2016 wurde ferner die Mitteilung der EK zur »Stärkung der Abwehrfähigkeit Europas im Bereich der Cyber Sicherheit und Förderung einer wettbewerbsfähigen und innovativen Cyber Sicherheitsbranche« angenommen. Auf Ratsebene (Rat Allgemeine Angelegenheiten) wurden dazu am 15./16.11.2016 Ratsschlussfolgerungen angenommen. Diese wurden in der Formation »Friends of Presidency on Cyber Issues« diskutiert. Die Ratsschlussfolgerungen anerkennen die bis dato erfolgte Arbeit auf dem Bereich der Cyber Sicherheit und der Verwirklichung des Digitalen Binnenmarktes und begrüßen die Schlüsselelemente der EK-Mitteilung. Weiters unterstreichen die Ratsschlussfolgerungen die Wichtigkeit der Implementierung der NIS-RL und die Kooperation unter den MS und mit den EU-Einrichtungen. Die RSF enthalten Aufforderungen an die EK, konkrete Schritte in Bezug auf die Stärkung der Cyber Resilienz vorzulegen, und an die MS, ihre Kooperation untereinander und mit der EK weiterhin zu pflegen und zu vertiefen, sowie laden die Stakeholder zur aktiven

Mitarbeit ein. Die EK-Mitteilung sieht u. a. die Einrichtung einer öffentlich-private Partnerschaft (cPPP) für Cyber Sicherheit vor, mit der eine europäische Forschungs- und Innovationsagenda zur Steigerung Wettbewerbsfähigkeit vorangebracht werden soll.

2.1.1 ENISA und NIS-Richtlinie

Unterstützt werden die EU-Aktivitäten von der European Network and Information Security Agency (ENISA), deren Aufgabe es ist, gemeinsam mit den Mitgliedsstaaten und anderen EU-Institutionen die Netzwerk- und Informationssicherheit zu verbessern. Das Bundeskanzleramt (BKA) stellt den nationalen Liaison Officer zur ENISA.

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 RL ist es, das Cyber Sicherheitsniveau in allen MS 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-Sicherheitsanforderungen, 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.

Gem. Art. 25 der RL ist diese bis 09.05.2018 durch die Mitgliedsstaaten umzusetzen; in Österreich wird dies durch das Cyber Sicherheitsgesetz erfolgen, das im Rahmen einer interministeriellen Arbeitsgruppe im Bundeskanzleramt erarbeitet wird.

2.1.2 Kooperationen

Am 10.02.2016 unterzeichneten das EU-CERT und dessen NATO-Pendant ein Technical Arrangement, um den Austausch von technischen Informationen zur Erkennung, Abwehr von und Reaktion auf Cyber Angriffe zu gewährleisten.

Die Gruppe »Friends of Presidency Initiative on Cyber Issues« wurde 2013 vorrangig zur Unterstützung der Implementierung der EU-Cyber Security Strategy gegründet. Heute ist es die primäre Aufgabe der Gruppe alle Cyber Themen in der EU horizontal zu koordinieren. Damit soll die Effektivität von bestehenden Aktivitäten und Beratungsfunktionen zu Cyber Thematiken verbessert werden. Die Gruppe, in der Österreich durch das BKA vertreten ist, wurde nach drei Jahren Bestehens zum zentralen Gremium des Informationsaustausches innerhalb der EU hinsichtlich Cyber Sicherheit.

Am 8. Juli 2016 wurde beim NATO-Gipfel in Warschau durch den NATO GS und den Präsidenten des Europäischen Rates sowie den EU-Kommissionspräsidenten eine gemeinsame Deklaration zur Stärkung der EU-NATO Kooperation unterzeichnet. Zur Umsetzung dieser Deklaration wurde bis November 2016 eine Liste mit über 40 konkreten Umsetzungsmaßnahmen, darunter mehrere im Bereich Cyber, erarbeitet und beim Rat am 6. Dezember 2016 angenommen.

2.1.3 European Cyber Security Month

Der »European Cyber Security Month (ECSM)« ist eine von der ENISA alljährlich organisierte Kampagne zur Bewusstseinsbildung zum Thema Cyber Sicherheit in den EU-Mitgliedsstaaten. Dabei bietet sich Organisationen einerseits die Gelegenheit, eigene Aktivitäten zum Thema Cyber Sicherheit öffentlichkeitswirksam zu präsentieren, andererseits wird damit das Thema Cyber Sicherheit in der allgemeinen Wahrnehmung stärker verankert. Die Federführung bei der Österreichischen Beteiligung an dieser Kampagne liegt dabei im Bundeskanzleramt.

Österreich beteiligte sich 2016 bereits zum vierten Mal am ECSM und konnte dabei im internationalen Vergleich stets mit zahlreichen, von Organisationen eingemeldeten Veranstaltungen aufwarten. 2016 konnten in Österreich 24 eingemeldete Aktivitäten von Organisationen aus den Bereichen der öffentlichen Verwaltung, der Privatwirtschaft, Banken, Sicherheitsinitiativen, Interessensvertretungen und Forschung verzeichnet werden. Die Bandbreite dieser Aktivitäten umfasste dabei Awareness-Kampagnen, Trainings, Konferenzen, Workshops, Vorträge, Forschungsveranstaltungen, Hacking-Wettbewerbe und vieles mehr.

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. Seitdem berichtet der Generalsekretär jährlich der VN-GV über die Positionen der einzelnen Mitgliedsstaaten.

In diesem Zusammenhang wurden seit 2014 »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 den potentiellen Bedrohungen der internationalen Sicherheit bei der Anwendung von Informationstechnologie. Deren Analysen beschäftigen sich mit dem internationalen Recht, der Erweiterung bzw. Klärung von Rechtsnormen sowie den Erwartungen gegenüber einem verantwortungsvollen Verhalten der Staaten im Cyber Space. Diese Gruppe soll im September 2017 der 72. VN-GV über ihre Ergebnisse berichten.

Bereits zur Jahrtausendwende rief die Generalversammlung der Vereinten Nationen (VN-GV) den »World Summit on the Information Society (WSIS)« ins Leben. Das WSIS Forum 2016 bot erstmals nach Verabschiedung der nachhaltigen Entwicklungsziele (SDGs) im September 2015 die Gelegenheit, die WSIS Action Lines im Lichte der SDGs zu diskutieren. Im Rahmen des Kapazitätsaufbaus, den die Umsetzung der IKT-bezogenen SDGs verlangt, wurde u. a. Cyber Sicherheit als eine von acht digitalen Kernkompetenzen eingestuft.

Es beschäftigen sich auch mehrere Komitees der VN-GV mit Cyber Themen. Aus österreichischer Sicht ist vor allem die Arbeit im Dritten Komitee und im VN-Menschenrechtsrat (MRR) von Interesse. Die von Österreich als einer der Hauptsponsoren eingebrachte Resolution zum Recht auf Privatsphäre im digitalen Zeitalter konnte vom MRR im Konsens angenommen werden. Mit der Schaffung eines Mandats für einen eigenen VN-Sonderberichterstatter zum Thema durch den VN-Menschenrechtsrat und der Annahme einer weiteren Resolution zum Schutz der Privatsphäre im digitalen Zeitalter (A/71/199), die viele ambitionierte Elemente enthält, konnten die seit 2013 laufenden Bemühungen einer Gruppe gleichgesinnter Staaten unter der Führung von Brasilien und Deutschland erfolgreich vorangetrieben werden.

Cyber Kriminalität hat sich rasch zu einer globalen und äußerst profitablen Verbrechenssparte entwickelt. Das VN-Büro für Drogen- und Verbrechensbekämpfung in Wien stellt weiterhin einen unverzichtbaren Bestandteil in der effektiven weltweiten Bekämpfung von Cyber Kriminalität im Sinne der 2013 veröffentlichten umfassenden Studie[7] dar und konzentriert sich dabei in seiner Hilfeleistung für betroffene Mitgliedstaaten auf folgende drei Schwerpunkte:

- Verbesserung des Verständnisses verschiedenster Varianten von Cyber Kriminalität.
- Wissenserweiterung im Sinne von richtiger Erkennung und Verhinderung von Cyber Kriminalität.
- Stärkung regionaler Kooperationen und Informationsaustauschmechanismen bei der Bekämpfung von Cyber Kriminalität.

Die 2010 im Bereich Cybercrime eingerichtete intergouvernmentale Expertengruppe trat, nach Sitzungen im Jahr 2011 und 2013, vom 10. bis 13.04.2017 zum dritten Mal zusammen. Behandelt werden Themen, zu denen international unterschiedliche Ansichten herrschen, insbesondere was Beschränkung des Internets (Meinungs- und Ausdrucksfreiheit etc.) betrifft; Streitthema ist zudem die Frage, ob eine neue Cyber Konvention ausgehandelt oder die Budapest Konvention ausgeweitet/umgesetzt werden soll.

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 (hauptsächlich Unterrichtsmaterialien zur Aufklärung über die Gefahren im Internet) um.

Hinsichtlich Friedensoperationen der Vereinten Nationen fanden auch 2016 Veranstaltungen im Rahmen der Initiative »Partnership for Technology in Peacekeeping« unter Federführung der »Information and Communications Technology Division (ICTD)« des »UN Departement of Field Support« statt. Österreich war beim dritten Fachsymposium im November 2016 in Seoul durch einen BMLVS-Experten vertreten.

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 mit den Verteidigungsaspekten von Cyber Sicherheit. Österreich kooperiert hier als Partnerland eng mit der NATO. 2015 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 zur Cyber Zusammenarbeit.

Darüber hinaus führt Österreich (unter Federführung des BMEIA und Beteiligung von BMLVS und BKA) regelmäßig sog. »cyber-staff-talks« mit dem für die »Emerging Security Challenges« zuständigen Assistant Secretary-General der NATO über Themen der Cyber Sicherheit und Cyber Verteidigung, zuletzt im Juli 2016. Im Zuge dieser Konsultationen mit der NATO wurde Österreich im Februar 2015 als erster Nicht-NATO-Staat zu einer Sitzung des NATO-Cyber

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

Defence-Committee (CDC) im Format 28+1 eingeladen. Überdies werden Fragen der Cyber Sicherheit mit weiteren bilateralen Formaten mit der NATO thematisiert, u. a. im Rahmen der regelmäßigen »Staff Talks« mit dem für Partnerschaften zuständigen Assistant Secretary-General der NATO Alejandro Alvargonzález im Jänner 2017.

Österreich hat im Rahmen der NATO Partnership for Peace (NATO/PfP) das Partnerschaftsziel »Cyber Defence« angenommen. Die diesbezüglichen Vereinbarungen für 2016 konnten allesamt erfüllt werden. Dieses Partnerschaftsziel ist auch Thema bei den regelmäßig im Frühjahr statfindenden PARP-Verhandlungen.

Zusätzlich verstärkte sich die Zusammenarbeit mit der NATO seit Oktober 2013 im Bereich der militärischen Landesverteidigung im Cyber Raum durch die dauerhafte Beschickung und Mitarbeit eines Offiziers des BMLVS im »Cooperative Cyber Defence Center of Excellence« in Tallinn/Estland.

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

Anlässlich des OSZE-Ministerrates in Hamburg bekräftigen im Dezember 2016 die teilnehmenden Staaten ihren Willen zur Umsetzung und Weiterentwicklung der vertrauensbildenden Maßnahmen im Rahmen der Organisation.

Die 57 Teilnehmerstaaten haben damit zum ersten Mal einen multilateralen, politisch-verbindlichen Mechanismus geschaffen, der sich auf die Umsetzung von praktischen Maßnahmen zur Verbesserung der zwischenstaatlichen Zusammenarbeit mit mehr Transparenz, Vorhersehbarkeit und Stabilität konzentriert. Risiken, die sich aus Missverständnissen durch den Gebrauch von IKT-Netzwerken ergeben und zu Spannungen oder Konflikten führen könnten, sollen damit reduziert werden. Ein strukturierter und transparenter Austausch von Informationen über laufende Entwicklungen und Herausforderungen im Bereich der Sicherheit von Informations- und Kommunikationstechnologie (IKT) kann zum verstärkten Schutz gegen Angriffe auf diesem Gebiet beitragen.

Durch die Schaffung vermehrter Transparenz sowie durch die Vernetzung und Zusammenarbeit nationaler Expertinnen und Experten soll das Vertrauen der teilnehmenden Staaten auch in Krisenfällen untereinander gestärkt werden. Für Österreich stehen dabei die Sicherheit und die Freiheit des Internets, der freien Meinungsäußerung aber auch der vor Überwachung geschützten Privatsphäre im Vordergrund.

Cyber Sicherheit ist ein Schwerpunktthema des österreichischen OSZE-Vorsitzes im Jahr 2017 mit Fokus auf dem Aspekt »Schutz kritischer Infrastrukturen«. Am 15.02.2017 fand in der Wiener Hofburg die Konferenz »Cybersicherheit für kritische Infrastruktur: Stärkung von Vertrauensbildung in der OSZE« statt, welche von Außenminister Sebastian Kurz, dem amtierenden Vorsitzenden der OSZE, eröffnet wurde. Im Mittelpunkt der Konferenz stand die Implementierung der vertrauensbildenden Maßnahmen sowie der Schutz kritischer Infrastruktur. Namhafte nationale und internationale Experten diskutierten mit Vertretern aus nationalen und internationalen Institutionen bzw. dem Privatsektor über Herausforderungen und Möglichkeiten für gesamtheitliche Lösungsansätze. Österreich unterstrich damit auch seine Bedeutung als Sitzstaat für internationale Organisationen und wichtige Drehscheibe für zukünftige essentielle weiterführende dimensionsübergreifende Zusammenarbeit im Bereich der Cyber Sicherheit.

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 koordinative Tätigkeit für diese Gruppe wahr. Schwerpunktthemen bei der OECD zum Thema Cyber Sicherheit 2016 waren vor allem der Schutz von Kindern im Internet, der Schutz kritischer Informationsinfrastrukturen, der Schutz von persönlichen Daten im digitalen Gesundheitsbereich, die Chancen und Herausforderungen des Internet der Dinge, Empfehlungen zum Thema Kryptografie und die Rolle des Staates bei Versicherungen für den Bereich Cyber Sicherheit.

2.6 Österreich in anderen cyberrelevanten 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.

- Die »Global Conference on Cyberspace« – die wichtigste Konferenz im Bereich Cyber

Diplomatie, welche zuletzt vom 15.–17. April 2015 in Den Haag tagte. Die bislang fünfte Auflage dieser Konferenz ist für Ende 2017 in Indien geplant.

- Ferner nahm Österreich an weiteren hochrangigen und renommierten internationalen Cyber Sicherheits-Konferenzen teil, wie etwa an den Annual EU-Cyber Security Conferences in Brüssel (zuletzt im November 2016), den jeweiligen EU-Vorsitz-Konferenzen (im ersten Halbjahr 2016 in Amsterdam, im zweiten Halbjahr in Preßburg), sowie an weiteren einschlägigen Tagungen, wie etwa in Tel Aviv (Juni 2016), Krakau (September 2016) oder London (März 2017).

- Schließlich hielt das BMEIA im Berichtszeitraum eine Reihe von bilateralen Konsultationen mit wichtigen Akteuren zu Cyber Sicherheitsfragen ab, so u. a. mit Russland und mit Israel.

2.7 Nationalstaaten

2.7.1 Vereinigte Staaten von Amerika

Die Vereinigten Staaten von Amerika betrachten Cyber Bedrohung als eine der größten Bedrohungen für die Nationale Sicherheit. Mit der Veröffentlichung der Executive Order (EO) 13694 am 01.04.2015 deklarierte Präsident Obama die zunehmenden hochwertigen Cyber Angriffe auf US-Entitäten als Gefahr für die nationale Sicherheit, die US-Außenpolitik sowie die US-Wirtschaft und erklärte diese zum nationalen Notfall. Im Fiskaljahr 2016 wurden dem U.S. Computer Emergency Readiness Team des Department of State 30.899 Cyber Security Vorfälle in Behörden gemeldet.

In der Vergangenheit wurde mit (umstrittenen) Maßnahmen wie dem »Cybersecurity Information Sharing Act« (CISA) 2015, gültig für 10 Jahre, der Austausch von cyber-sicherheitsrelevanten Informationen zwischen der Wirtschaft und den Behörden vereinfacht. Am 09.02.2016 veröffentlichte das Weiße Haus den »Cybersecurity National Action Plan« (CNAP). Dieser dient als Rahmenplan sowohl für kurz- und mittelfristige Maßnahmen als auch langfristige strategische Ausrichtungen der US Bundesregierung im Cyber Sicherheitsbereich. Ziel des CNAP ist die Erhöhung der Cyber Sicherheit in der gesamten Bundesregierung bzw. den Bundesbehörden, Bewusstseinsbildung für Cyber Sicherheit in der US-Bevölkerung, Schutz der Privatsphäre, Aufrechterhaltung der öffentlichen, wirtschaftlichen und nationalen Sicherheit sowie der verbesserte Schutz kritischer Infrastruktur.

Zur Umsetzung des Plans wurden von Präsident Obama ca. 17 Mrd. € (19 Mrd. $) an Budgetmittel für 2017 veranschlagt, ein Plus von ca. 35 % im Vergleich zu 2016. Ebenso wurden in einem ersten Budgetentwurf der Administration Trump in diesem Bereich Erhöhungen vorgeschlagen. So soll beispielsweise dem Department of Homeland Security 1,4 Mrd. € (1,5 Mrd. $) zusätzlich für den Schutz kritischer Cyber Infrastruktur zugeteilt werden.

Ebenfalls im CNAP wurde die geplante Veröffentlichung einer eigenen Richtlinie angekündigt, welche die Koordination bei Cyber Vorfällen regelt und einen Kriterienkatalog zur Bestimmung der Schwere von Cyber Vorfällen beinhaltet. Diese Richtlinie wurde im Juli 2016 als Präsidialdekret PPD-41 »United States Cyber Incident Coordination« herausgegeben. Das Dekret gibt klare Vorgaben für die Vorgehensweisen und Zuständigkeiten der einzelnen Behörden der Bundesregierung bei einem signifikanten Cyber Vorfall. Die Bearbeitung von Cyber Vorfällen wird in drei Bereiche gegliedert: Reaktion auf die Bedrohung; Unterstützung für die betrof-

fenen Entitäten und nachrichtendienstliche Unterstützung für ein gemeinsames Lagebild. Bei der Reaktion auf Bedrohungen hat das Justizministerium mit der National Cyber Investigative Joint Task Force des FBI die Federführung. Das National Cybersecurity and Communications Integration Center des Heimatschutzministeriums (DHS) wirkt federführend bei der Unterstützung der betroffenen Einrichtungen. Dem Cyber Threat Intelligence Integration Center des Office of the Director of National Intelligence obliegt die nachrichtendienstliche Unterstützung. Bei einem schwerwiegenden Cyber Vorfall ist eine Cyber Unified Coordination Group vorgesehen, um die Aktivitäten unterschiedlicher Behörden zu koordinieren und bei Bedarf die Zusammenarbeit mit dem Privatsektor sicherzustellen. Das PDD-41 wies auch das DHS an, innerhalb von 180 Tagen eine umfassende Überprüfung und Aktualisierung des National Cyber Incident Response Plans durchzuführen. Ein überarbeiteter Plan wurde Mitte Jänner 2017 durch das DHS veröffentlicht.

Im Februar 2016 reichte das US-Verteidigungsministerium (DoD) einen Budgetantrag ein, in dem gegenüber 2016 eine Anhebung von 15 % für Cyber Operationen vorgesehen ist. Diese Anhebung würde die zweite in Folge darstellen. Hauptziele des Budgets 2017 sind: die Organisation der 133 Teams der Cyber Mission Forces, die Ende 2018 volle Einsatzbereitschaft erreichen sollen; die Ausstattung für das Joint Operations Center des U.S. Cyber Command, das 2018 bezogen werden soll; Aufbau einer virtuellen Testumgebung für Übungszwecke; Schutz der DoD Netzwerke sowie Unterstützung für die Kommandanten der Kampftruppen und offensive Operationen.

Auf multi- sowie bilateraler Ebene werden die Bemühungen von den Zielen der U.S. International Strategy for Cyberspace (2011) geleitet, welche fünf prioritäre Bereiche identifiziert: digitale Wirtschaft, internationale Sicherheitspolitik, Förderung der Sorgfaltspflicht in Cyber Sicherheit, Kampf gegen Internetkriminalität sowie die Verwaltung und Freiheit des Internets.

Auf bilateraler Ebene fand im Dezember 2015 der erste »USA-China Cyber Dialogue« statt, bei dem sich die Präsidenten beider Staaten auf eine Reihe von Schwerpunkten in der Cyber Kooperation einigten. Dieses bilaterale Forum wurde am 15.06.2016 mit einem zweiten »USA-China Cybercrime and Related Issues High Level Joint Dialogue« auf hochrangiger Beamtenebene mit Fokus auf der Umsetzung des erreichten Konsens von 2015 fortgesetzt. Bereits im Dezember 2016 wurde ein weiteres Treffen abgehalten und ein nunmehr jährlicher Tagungsrhythmus vereinbart.

Am 16.12.2016 fand der dritte »USA-EU-Cyber Dialogue« statt, im Rahmen dessen die Zusammenarbeit in den Bereichen Aufbau von Cyber Fähigkeiten, Anwendbarkeit bestehender internationaler Gesetze im Cyber Raum, Cyber Resilience und Kooperation im Kampf gegen Cyber Kriminalität bekräftigt wurden. Ähnliche Foren bestehen u. a. mit Japan, Indien und Australien.

Auch unter der Administration von Präsident Trump bleibt der Kampf gegen diese Bedrohung eine Priorität. Die EO »Strengthening U.S. Cyber Security and Capabilities« befand sich bereits kurz nach Amtsantritt im Januar und Februar 2017 in Ausarbeitung, wurde bis dato allerdings noch nicht unterschrieben. Auch soll eine neue Nationale Verteidigungsstrategie künftig die Vormachtstellung der USA im Cyber Space festigen.

Die Vorwürfe der Einflussnahme auf das Wahlergebnis der US-Präsidentschaftswahl durch Russische Hacker erhöht die Aufmerksamkeit in dieser Hinsicht weiter. In der Legislative beschäftigen sich derzeit verschiedene Ausschüsse mit diesem und engverwandten Cyber Security Themen, u. a. wird auch angedacht diese Kapazitäten in einem Senate Select Committee on Cyber Security zu bündeln.

2.7.2 Russische Föderation

Am 05.12.2016 unterzeichnete Präsident Wladimir Putin die neue Informationssicherheitsdoktrin der Russischen Föderation (RF). Diese ersetzt die Doktrin aus dem Jahr 2000. Laut Angaben der Präsidialverwaltung stellt die Doktrin ein System von offiziellen Perspektiven zum Schutz der Informationssicherheit Russlands auf Grundlage der Verfassung, der Prinzipien und Normen des Völkerrechts, der föderalen Gesetzgebung sowie der Rechtsakte des Präsidenten und der Regierung dar. Der Fokus der Doktrin liegt auf der Prävention gegen mögliche Cyber Angriffe. Die neue 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. Die Doktrin hat keinen Gesetzescharakter, gibt aber den Rahmen zur Weiterentwicklung des einschlägigen Regelwerks zur Informationssicherheit vor.

Somit stellt die neue Doktrin ein strategisches Planungsdokument dar. Inhaltlich sowie rhetorisch ähnelt das Dokument der im Dezember 2015 veröffentlichten Nationalen Sicherheitsstrategie. Im Vergleich zur Vorgängerdoktrin von 2000 wird der Informationsraum breiter definiert und nimmt erstmals technologische Entwicklung als Motor für soziale Veränderungen wahr. Neben Bedrohungen wie z. B. ansteigende Cyber Angriffsfähigkeiten ausländischer Staaten und Cyber Spionageaktivitäten gegen russische staatliche Einrichtungen, v. a. im Bereich der Forschung und im Verteidigungssektor, wird auch die versuchte Einflussnahme im »informationspsychologischen« Bereich als Gefahr dargestellt. Darunter wird die Einflussnahme auf die Bevölkerung durch gezielte Informationskampagnen von Regimekritikern im In- und Ausland verstanden. Auch die aus russischer Sicht stattfindende Diskriminierung und Einschränkung russischer Medien im Ausland wird als Bedrohung für die Souveränität der Russischen Föderation im Informationsraum dargestellt. Nach gegenwärtiger Ansicht der russischen Führung befindet sich Russland in einem Informationskrieg. Somit vertritt die Russische Föderation den Standpunkt, dass eine starke Kontrolle über die nationalen IKT-Infrastrukturen sowie eine internationale Regulierung des Internets erforderlich sind.

Neben der neuen Informationssicherheitsdoktrin strebte Russland 2016 den Ausbau der Kontrolle über den nationalen Informationsraum an. Im Sommer 2016 wurden z. B. eine Reihe von Bundesgesetzen (z. B.: Jarowaja-Gesetz) im Bereich Anti-Terrorismus und öffentliche Sicherheit verabschiedet. Diese Gesetze beinhalten u. a. neue Regelungen zur Speicherungen von Benutzerdaten durch Internet Service Provider. So müssen alle Metadaten zu Telefonaten und Textnachrichten für sechs Monate bis drei Jahre gespeichert werden. Außerdem müssen ISP und Message Service Provider Hintertüren in ihre Systeme einbauen und diese den Sicherheitsbehörden zur Verfügung stellen, um u. a. den Sicherheitsbehörden zu ermöglichen, Verschlüsselungstechnologien zu umgehen. Weitere Verschärfungen der Cyber Gesetzgebung stehen in Diskussion.

Auf internationaler Ebene strebt Russland weiterhin einen Auf- bzw. Ausbau der Kooperationsabkommen an. Dazu wurden im Jahr 2016 beispielsweise bilaterale Vereinbarungen mit Japan (über internationale Informationssicherheit) und mit Indien (bilaterale Kooperation) getroffen. Am 13.01.2016 fand ein Delegationstreffen zwischen Deutschland und Russland in Moskau statt. Dabei wurde über die geplante Regierungsexpertengruppe für internationale Cyber Sicherheit bei den VN, vertrauensbildende Maßnahmen in der OSZE im Rahmen des deutschen Vorsitzes sowie über die bilaterale Zusammenarbeit gegen die terroristische Nutzung von Informations- und Kommunikationstechnologie und zum Schutz staatlicher IKT-Ressourcen beraten. Weiters fand im April 2016, basierend auf dem Abkommen mit China vom Mai 2015, erstmals ein russisch-chinesisches Cyber Forum in Moskau statt. In der internationalen Kooperation sucht die Russische Föderation die bilaterale Zusammenarbeit vor allem auch mit

westlichen Staaten, unter anderem im Wege entsprechender Konsultationen auf Expertenebene. Diesbezüglich fanden am Rande der OSZE-Cyber Sicherheitskonferenz am 15.02.2017 informelle Gespräche mit einer hochrangigen russischen Delegation in Wien statt.

Das russische Verteidigungsministerium führt die begonnene Entwicklung von Technologien zur Cyber Kriegsführung weiter und stellt dafür auch die erforderlichen Investitionen bereit. Das Verteidigungsministerium hat 2016 weitere Maßnahmen zur Härtung eigener Systeme gegen Cyber Angriffe angeordnet und deren Umsetzung bis Jahresende vorangetrieben.

2.7.3 Volksrepublik China

Die chinesische Führung legitimiert mit dem Schlagwort »Internetsouveränität« sowohl intensive Internet-Zensur im Land als auch ihre außenpolitischen Bestrebungen, Informationsüberlegenheit im Cyber Raum zu schaffen, und die öffentliche Meinung zu zensurieren und zu steuern.

Zur verstärkten Kontrolle über den chinesischen Cyber Raum wurde am 07.11.2016 das Mitte 2015 präsentierte Cyber Sicherheitsgesetz beschlossen. Dieses wird am 01.07.2017 in Kraft treten und regelt den Schutz und die Kontrolle von Daten sowie den Schutz Kritischer Infrastruktur. Dazu zählen Telekommunikation, Energie, Transport, Wasserversorgung, Finanzwesen, öffentliche Versorgungsanlagen und E-Government-Dienstleistungen sowie Bereiche mit Auswirkungen auf u. a. nationale Sicherheit oder das öffentliche Interesse. Da letzteres nicht klar definiert wird, liegt es im Ermessen der Behörden das Gesetz zur Kontrolle der Bevölkerung einerseits und zur Abschirmung des heimischen IKT-Marktes von ausländischer Konkurrenz andererseits zu nutzen. Das Cyber Sicherheitsgesetz verfolgt das Ziel des (konventionellen) Datenschutzes – auch gegen Hackerangriffe und Sabotage – mit Auswirkungen auf alle Netzwerkbetreiber und Dienstleister. Ab Juli 2017 müssen persönliche Daten und Daten mit Bezug zu Kritischer Infrastruktur innerhalb der Volksrepublik China gespeichert werden. IT-Produkte in Verbindung mit Kritischer Infrastruktur sowie Daten, die in das Ausland transferiert werden sollen, müssen einer staatlichen Prüfung unterzogen werden. Das Gesetz sieht weitreichende Befugnisse für die »Cyberspace Administration of China« (CAC), die in teilweiser Personal- und Verwaltungsunion mit dem Propagandabüro der Kommunistischen Partei steht, vor. Es ist daher mit einer Intensivierung der Kontrollen sowie der Blockade bzw. der Zensur von ausländischen Webseiten und inländischen Social-Media-Accounts zu rechnen. Als führende Internet-Zensurbehörde ist CAC für die Steuerung der öffentlichen Meinung auf Internet-Plattformen verantwortlich, wobei vom Einsatz einer großen Anzahl bezahlter Trolle ausgegangen wird. Die strafrechtliche Verfolgung zahlreicher kritischer BloggerInnen in den letzten Jahren hat zu weit verbreiteter Selbstzensur geführt. An politisch relevanten Jahrestagen (z. B. Tiananmen-Massaker) oder bei Vorfällen in der Tibetischen Autonomen Region oder in Xinjiang wird die Internet-Nutzung regelmäßig weiter eingeschränkt, mitunter regional gänzlich unterbunden.

Auf internationaler Ebene verfolgt China einen ähnlichen Ansatz wie die Russische Föderation. So befürwortet China ebenfalls das weltweite Internet unter Aufsicht einer internationalen Institution wie der International Telecommunications Union (ITU) der VN zu stellen (und diese zu kontrollieren). China unterhält bilaterale und regionale Kooperationen zum Thema, etwa mit der EU und im Rahmen der Shanghai Cooperation Organisation. Österreich ist am »Sino-European Cyber Dialogue« beteiligt, bei dem – auf »track two« (also im halb-formellen Rahmen) – verschiedene Punkte der Zusammenarbeit im Cyber Sicherheitsbereich zwischen Europa/EU und China behandelt werden. Auf Grund der halb-formellen Natur dieser Gespräche, die über den EU-Rahmen hinausgehen, sind nur ausgewählte europäische Staaten an ihnen beteiligt.

Aufgrund des CN-US Abkommens, das im September 2015 durch die beiden Präsidenten unterzeichnet wurde und neben einer engeren Kooperation im Kampf gegen Cyber Krimina-

lität auch die Selbstverpflichtung beider Seiten enthält, sich nicht an der Durchführung oder wissentlichen Unterstützung von Cyber Spionageaktivitäten gegen wirtschaftliche Ziele im jeweiligen Land zu beteiligen, sollen 2016 die Cyber Spionageaktivitäten gegen wirtschaftliche Ziele in den USA durch chinesische Akteure massiv zurückgegangen sein. Chinesische »patriotische« Hackergruppen waren jedoch auch 2016 sehr aktiv. So legten z. B. chinesische Hackergruppen im Juli 2016 ca. 68 nationale und lokale philippinische Regierungswebseiten durch DDoS-Angriffe lahm. Grund für die Angriffe war die Entscheidung des Ständigen Schiedsgerichtshofes in Den Haag in einem von den Philippinen angestrengten Schlichtungsverfahren über chinesische Territorialansprüche im südchinesischen Meer, welches von China als seinen Interessen widersprechend ausgelegt wurde.

Im Bereich der Streitkräfte setzte China 2016 die Modernisierung der Streitkräfte im Cyber Bereich, die bereits im Mai 2015 den Cyber Raum als eine neue Säule der ökonomischen und sozialen Entwicklung definiert und als bedeutender Aspekt für die nationale Sicherheit beschrieben haben, fort. Um die Cyber Verteidigungsfähigkeiten auszubauen, soll u. a. der Ausbau von Cyber Truppen forciert und ein besseres operatives Lagebild gewährleistet werden.

2.7.4 Deutschland

Am 09.11.2016 beschloss die deutsche Bundesregierung die neue »Cyber Sicherheitsstrategie für Deutschland 2016«, derzufolge die deutsche Bundesregierung in ihrer Cyber Sicherheitspolitik in den kommenden Jahren Schwerpunkte in den folgenden vier Handlungsfeldern setzen wird:

1. Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung
2. Gemeinsamer Auftrag Cyber Sicherheit von Staat und Wirtschaft
3. Leistungsfähige und nachhaltige gesamtstaatliche Cyber Sicherheitsarchitektur
4. Aktive Positionierung Deutschlands in der europäischen und internationalen Cyber Sicherheitspolitik

Diese Strategie stellt eine Fortschreibung der Strategie aus 2011 dar. Die Strategie 2016 sieht einen Nationalen Cyber Sicherheitsrat vor, dem die Verantwortung für die politisch-strategische Planung zugeordnet ist. Dieser soll auch die Zusammenarbeit zwischen Staat und Wirtschaft koordinieren. Die Strategie definiert und beschreibt dabei 30 strategische Zielsetzungen und Maßnahmen, einschließlich eines ressortübergreifenden, gesamtstaatlichen Rahmens, der auf den sicherheitspolitischen Aspekten des Weißbuchs 2016 aufbaut und den Ressorts die unterschiedlichen Aufgaben zuweist. Zu dem Bündel an geplanten bzw. zum Teil bereits in Umsetzung befindlichen Maßnahmen zählen etwa ein Basis-Zertifizierungsverfahren für sichere IT-Verbraucherprodukte, dessen Kriterien durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) festgelegt werden. Die Bundesregierung baut hierfür das Forschungsrahmenprogramm zur IT-Sicherheit »Selbstbestimmt und sicher in der digitalen Welt 2015–2020« weiter aus und vernetzt dieses eng mit den anderen Maßnahmen der Cyber Sicherheitsstrategie. In diesem Zusammenhang werden auch die bestehenden Kompetenzzentren für IT-Sicherheitsforschung CRISP (Darmstadt), CISPA (Saarbrücken) und KASTEL (Karlsruhe) weiter gestärkt. 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.

Die Sicherheitsstrategie 2016 beinhaltet aber auch Vorgaben für die operativen Ebenen. So soll das unter dem BSI und unter direkter Beteiligung des Bundesamtes für Verfassungsschutz und des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe befindliche nationale Cyber Abwehrzentrum weiter ausgebaut und zur zentralen Kooperations- und Koordinationsplattform entwickelt werden. Dieses Zentrum wird für die Koordination sowie den Schutz und die

Abwehrmaßnahmen bei Cyber Vorfällen zuständig sein und mit den wesentlichen öffentlichen und privaten Stellen – z. B. den Betreibern Kritischer Infrastrukturen – zusammenarbeiten. Es ist auch vorgesehen, dass das Cyber Abwehrzentrum dem Cyber Sicherheitsrat regelmäßig oder anlassbezogen Empfehlungen abgeben soll. Bei unmittelbaren und absehbaren Krisen soll das Cyber Abwehrzentrum direkt an den Leiter des Krisenstabs, dem Staatssekretär des BM für Inneres, berichten. Haben Cyber Angriffe ihren Ursprung im Ausland, müssen außen- und sicherheitspolitische Aspekte miteinbezogen werden. Bei Cyber Sicherheitsvorfällen, die bundesweit zahlreiche Institutionen betreffen, wächst das Cyber Abwehrzentrum zu einem Krisenreaktionszentrum auf.

Dem Bundesministerium für Verteidigung obliegen die Verteidigungsaspekte der gesamten Cyber Sicherheitsarchitektur. Nach Grundaufstellung der neuen Abteilung Cyber und Informationstechnik (CIT) wurde Hardy Mühleck, ehemaliger ThyssenKrupp-Manager, durch Verteidigungsministerin Ursula von der Leyen am 05.10.2016 als Leiter CIT vorgestellt. Die Aufstellung der Abteilung CIT ist Teil der umfassenden Pläne zur Bündelung der Cyber und IT-Fähigkeiten der Bundeswehr. Dazu wurde ein Aufbaustab für das Kommando Informationsraum (Kdo CIR) mit geplanten 13.500 Dienstposten aufgestellt. Mit April 2017 soll die Herstellung einer grundsätzlichen Einsatzbereitschaft abgeschlossen sein, wobei die volle Einsatzbereitschaft 2021 erreicht werden soll.

2.7.5 Vereinigtes Königreich

Am 01.11.2016 veröffentlichte das Vereinigte Königreich die neue »National Cyber Security Strategy 2016 to 2021«. Darin werden Cyber Angriffe abermals als große Bedrohung für Wirtschaft und Sicherheit bezeichnet. In der Strategie wird das Budget für diese fünf Jahre auf 2,2 Mrd. € (1,9 Mrd. GBP) festgelegt. Ziel und Vorgabe der Strategie ist es, die gesamtstaatliche Kooperation zur Abwehr bzw. Minimierung der Auswirkungen von Cyber Angriffen auf das Vereinigte Königreich sicherzustellen. Außerdem wird das nationale offensive Cyber Programm fortgesetzt, das Kapazitäten für einen Gegenangriff im Cyber Space entwickelt. Dafür soll, in Zusammenarbeit mit Industriepartnern, eine automatisierte Abwehr vor bzw. Verteidigung von Cyber Angriffen entwickelt werden. Die Strategie basiert auf den drei Säulen Verteidigung, Abschreckung und Entwicklung, die sich aus den Faktoren Ziele, Handlungen und Kriterien zusammensetzen. Spezielles Augenmerk hat hier die intensive Kooperation mit privaten Firmen und der Industrie. Zwei neue Innovationszentren und ein mit 10 Mio. GBP dotierter Innovationsfonds werden sich ebenfalls mir Cyber Sicherheit auseinandersetzen. Auch der Kooperation auf internationaler Ebene wird ein hoher Stellenwert eingeräumt.

Um die Kooperation bzw. Koordination der Cyber Sicherheitsangelegenheiten sowohl innerhalb des öffentlichen Sektors als auch mit dem privaten Sektor zu optimieren, wurde am 01.10.2016 das National Cyber Security Center (NCSC) als Teil des zivilen technischen Nachrichtendienstes Government Communications Headquarters (GCHQ) in London aufgestellt. Das NCSC berichtet direkt an die Regierung und führt die Fähigkeiten der Communications-Electronics Security Group (CESG), und des Centre of Cyber Assessment (CCA) des GCHQ sowie das CERT-UK und die Cyber Angelegenheiten des Centre for the Protection of National Infrastructure (CPNI) zusammen.

2.7.6 Frankreich

Die Bedeutung des Themas Cyber Sicherheit wurde bereits vor Jahren erkannt und in den Weißbüchern von 2008 und 2013 festgeschrieben. Auf gesamtstaatlicher Ebene konzentrierte sich die französische Regierung 2016 auf die Umsetzung der im Oktober 2015 veröffentlichten nationalen Strategie für digitale Sicherheit. Federführend bei der Umsetzung war die nationale Behörde für die Sicherheit von Informationssystemen, die Agence nationale de la sécurité des

systèmes d´information (ANSSI). Ab 2017 wurde der Personalstand der ANSSI von 500 auf 600 Personen aufgestockt.

Fünf Ziele werden in der französischen Strategie definiert: 1) Stärkung des Cyber Schutzes durch Ausweitung von Ressourcen und Kompetenzen der ANSSI; 2) Schutz der Bürger (Stärkung des »digitalen Vertrauens« und Schutz der Privatsphäre im Cyber Space); 3) Sensibilisierung der Nutzer durch einen Ausbildungsschwerpunkt im Bereich Cyber Sicherheit; 4) Schaffung eines günstigen Umfelds für die digitale Wirtschaft; 5) europäische und internationale Kooperation. Gemeinsam mit Partnern möchte Frankreich eine »Roadmap für die digitale Souveränität Europas« entwickeln.

Hacker-Angriffe auf die EDV-Systeme von politischen Parteien sowie auf Mobiltelefone und Tablets von Parteienvertretern wurden 2016 von der ANSSI als Bedrohung im Wahlkampf für das Präsidentenamt identifiziert. Die Verbreitung von Falschmeldungen über soziale Medien wird als neues Thema im Bereich Cyber Sicherheit sehr ernst genommen. 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. Der Pakt zur Cyber Verteidigung von 2014 sieht einschlägige Maßnahmen im Rahmen der Streitkräfte vor. In Bruz (Region Bretagne) wurde im selben Jahr ein Kompetenzzentrum für Cyber Verteidigung eröffnet. Bis 2019 sollen im Sektor Cyber Verteidigung 1.000 neue Stellen geschaffen und zusätzlich 1 Mrd. Euro investiert werden. Im Dezember 2016 gab der französische Verteidigungsminister Jean-Yves Le Drian die Aufstellung eines französischen Cyber Kommandos (ComCyber) bekannt. Das dem Generalstab unterstellte ComCyber soll sich neben dem Schutz eigener Netze auch auf die Aufklärung, aktive Verteidigung und offensive Operation konzentrieren. Somit soll das neue ComCyber sowohl offensive als auch defensive Fähigkeiten besitzen. Hierzu wurde ein Budget in der Höhe von 2,1 Mrd. € veranschlagt. Le Drian begründete die Notwendigkeit für das ComCyber damit, dass es eine »Reaktion auf Realitäten neuer Methoden der Kriegsführung« sei. Allein im Jahr 2016 gab es ca. 24.000 Cyber Angriffe auf Institutionen der frz. Streitkräfte und damit doppelt so viele wie 2015. Er betonte weiters, dass ein Cyber Angriff einen kriegerischen Akt darstellen könnte. Das neue Kommando soll in der Lage sein, in gegnerische Netzwerke/Systeme einzudringen, um diese temporär oder dauerhaft zu zerstören. Die Unterstellung des ComCyber unter den Generalstab ermöglicht aus Sicht Frankreichs einerseits, Cyber Angelegenheiten direkt an die strategische Ebene weiterzugeben und andererseits eine angestrebte Integrierung von Cyber Operationen in militärische Operationen sicherzustellen. Die Schulungsmaßnahmen für Soldaten und Mitarbeiter im Bereich Cyber wurden intensiviert. Die private Kommunikation bei Operationen im In- und Ausland ist stark reglementiert. Damit soll das »Social Engineering« (Ausspähen der Familie etc.) verhindert werden.

Angelegenheiten und Unterstellungen der französischen Nachrichtendienste werden mit der Aufstellung des ComCyber nicht verändert. 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

Die Österreichische Strategie für Cyber Sicherheit (ÖSCS) verlangt unter anderem die »Schaffung einer Struktur zur Koordination auf der operativen Ebene«. Diese soll sowohl periodische, als auch anlassbezogene Lagebilder für Cyber Sicherheit erstellen und im Krisenfall auf der operativen Ebene über zu treffende Maßnahmen beraten. Das Jahr 2016 war das Schlüsseljahr für die Etablierung dieser Anforderungen.

Während im Jahr 2015 noch die Institutionalisierung von interministeriellen Abstimmungen im Vordergrund stand, nahm der Innere Kreis der operativen Koordinierungsstrukturen (IKDOK) im Jahr 2016 nach umfassenden Vorarbeiten den Regelbetrieb auf. Der IKDOK bildet im Krisenfall, unterstützt durch den äußeren Kreis der operativen Koordinierungsstruktur, die direkte Schnittstelle zum Cyber Krisenmanagement (CKM). Die Mechanismen des CKM lehnen sich eng an die bereits erprobten Abläufe des staatlichen Krisen- und Katastrophenschutzmanagements (SKKM) an. Dem IKDOK gehören neben den Vorsitz führenden Stellen Cyber Security Center (Bundesministerium für Inneres, BM.I) und Cyber Defense Center (Bundesministerium für Landesverteidigung und Sport, BMLVS) weitere staatliche Akteure an. Dazu zählen das Cyber Crime Competence Center (BM.I), Abwehramt, Heeres-Nachrichtenamt und MilCERT (alle BMLVS), sowie das GovCERT (BKA).

Der IKDOK musste seine erste große Bewährungsprobe im Oktober 2016 bestehen, als im Rahmen der europäischen Cyber Übung Cyber Europe 2016 (CE.AT 2016) ein umfassendes, hochrealistisches Cyber Krisenszenario bearbeitet werden musste. Bei dieser Übung wurde die nationale Krisenbewältigung erstmalig vollständig durch den IKDOK verantwortet. Nach einer intensiven Auswertungsphase durch Veranstalter und Übungsbeobachter konnte die Feststellung getroffen werden, dass der IKDOK unter der Koordination des Cyber Security Centers, die ihm übertragenen Aufgaben sowohl inhaltlich, wie auch organisatorisch einwandfrei umsetzen konnte.

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.

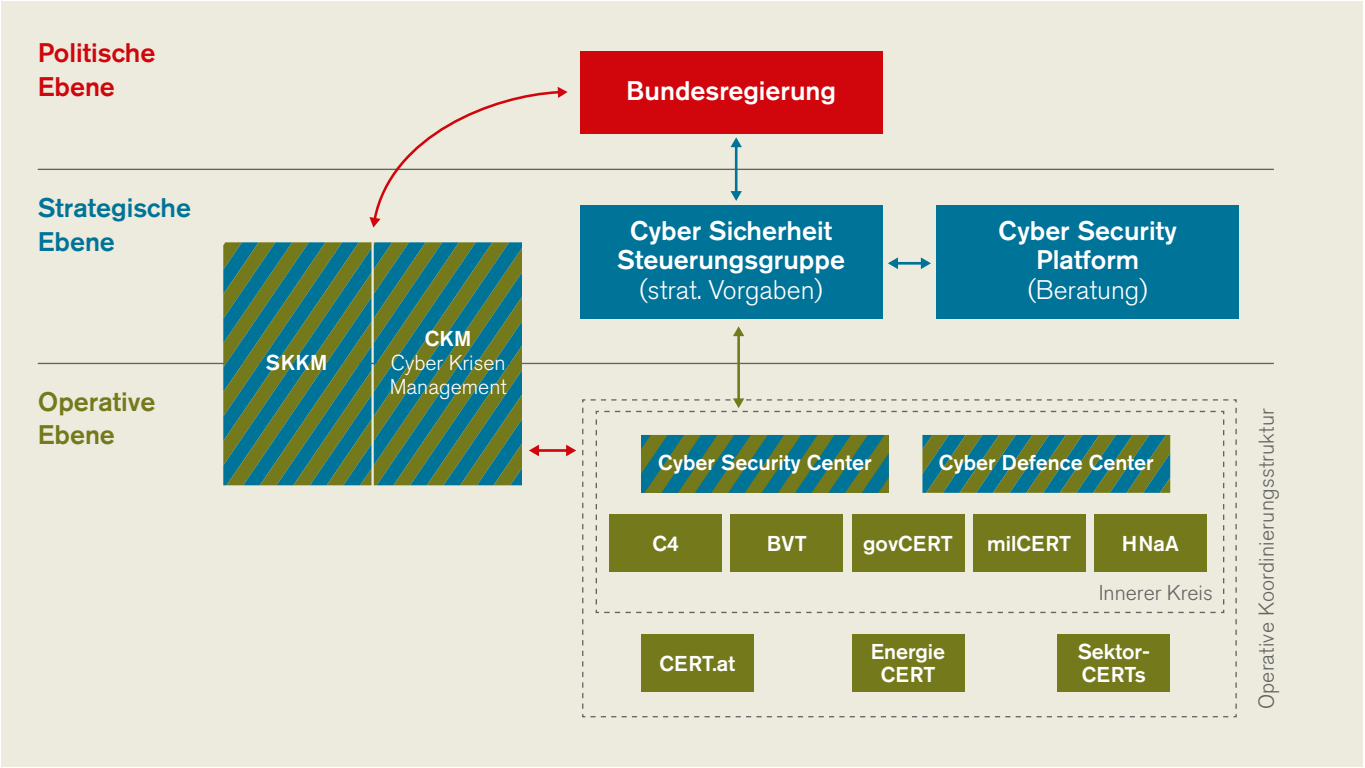

Abbildung 8: Einordnung der »Operativen Koordinierungsstruktur«

3.2 Cyber Security Center

Das Bundesministerium für Inneres (BM.I) hat in einer gemeinsamen Initiative mit der Europäischen Union am 1. Juni 2014 das »INNEN.SICHER«-Projekt Cyber Security Center .BVT ins Leben gerufen. Die Rahmenbedingungen für die Errichtung und den Betrieb des Cyber Security Centers (CSC) im Bundesministerium für Inneres sind in der »Österreichischen Strategie für Cyber Sicherheit« (ÖSCS), im »Arbeitsprogramm der österreichischen Bundesregierung 2013–2018 Erfolgreich. Österreich.«, sowie in der »Cyber Sicherheitsstrategie des Bundesministeriums für Inneres« festgeschrieben.

Ziel des Projekts ist die Schaffung von Strukturen und Prozessen zur Steigerung der Cyber Sicherheit in Österreich. Im Unterschied zu einzelnen Unternehmen, kann das Cyber Security Center isolierte IKT-Sicherheitsvorfälle in einen größeren Zusammenhang stellen und im Fall einer Krise, die durch Cyber Probleme ausgelöst wurde, schnellstmöglich mit dem bestehenden staatlichen Krisen- und Katastrophenmanagement zusammenarbeiten.

Eine weitere zentrale Aufgabe ist die Durchführung umfassender Präventionsarbeit in Form von Awareness-Veranstaltungen und -Vorträgen oder Beratungsgesprächen. Besonderer Wert wird auf eine gute Zusammenarbeit mit der Wirtschaft (Public-Private-Partnership) und den bestehenden Cyber Sicherheits-Inititativen und Strukturen in Österreich, wie etwa dem GovCERT im Bundeskanzleramt oder CERT.at, die über jahrelange Erfahrungen in diesem Bereich verfügen, gelegt. Auch ist es ein explizites Ziel, die Branchen in ihrer Selbstorganisation und in ihrer Vernetzung im Bereich der Cyber Security zu unterstützen.

Das Projekt zum Aufbau des CSC sieht die Aufnahme des operativen Vollbetriebs mit Ende Dezember 2017 vor. Der organisatorische Probebetrieb des CSC läuft bereits seit Oktober 2015. Ein technischer Probebetrieb wurde Mitte 2016 aufgenommen. Für 2017 ist auch der sukzessive Aufbau eines APT-Kompetenzzentrums angedacht. Die Bedeutung des Projektes wird unter anderem dadurch unterstrichen, dass seitens der europäischen Union beachtliche Fördermittel aus den Fonds für die innere Sicherheit (ISF) zur Verfügung gestellt wurden.

3.3 Cyber Defence Center (Cyber Verteidigungszentrum)

Dem Auftrag des aktuellen Regierungsprogramms folgend, sowie den militärischen Erfordernissen einer leistungsfähigen militärischen Landesverteidigung im Cyber Raum entsprechend, wurden die Grundlagen zur Etablierung des »Cyber Verteidigungszentrum« (CVZ) im Abwehramt des BMLVS geschaffen. Während das milCERT primär für BMLVS-interne Aufgabenstellungen vorgesehen ist und maßgeblich dem Schutz der militärischen IKT-Infrastruktur dient, tragen das CVZ und das milCERT gemeinsam zur Erfüllung von gesamtstaatlichen Aufgaben des BMLVS/ÖBH im Sinne des Souveränitätsschutzes im Rahmen der Umfassenden Landesverteidigung und Umfassenden Sicherheitsvorsorge bei.

Zur Steigerung der Sensibilität und des Bedrohungsbewusstseins insbesondere der Führungskräfte, wurde 2016 durch das BMLVS zum 15. Mal die IKT-Sicherheitskonferenz mit mehr als 1.800 Teilnehmern in Sankt Johann/Salzburg durchgeführt. Parallel dazu fand die 3. Arbeitstagung der Cyber Security Plattform unter Federführung des BKA statt.

Weiters wurde zum 5. Mal die Cyber Security Challenge, ein Wettbewerb für die Cyber Talente Österreichs, durchgeführt. Das Finale im europäischen Rahmen (mit Mannschaften aus 10 Ländern) erfolgte in Deutschland. Österreich belegte dabei – nach zwei Siegen in Serie – Platz 4. Beide Veranstaltungen, die IKT-Sicherheitskonferenz und die Cyber Security Challenge, werden auch 2017 fortgesetzt.

3.4 Kommando Führungsunterstützung und Cyber Defence

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 weiter entwickelt. 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 des »Cyber Koordinator BMLVS« 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. Auch zur 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 Verteidigungsfähigkeiten wurde aus der vormaligen Abteilung IKT-Sicherheit mit deren milCERT, das neue 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. Das Zentrum IKT- und Cyber Sicherheit (ZIKTCySih), als Organisationselement des neuen KdoFüU&CD, ist verantwortlich für die Informations-und IKT-Sicherheit aller Systeme des BMLVS/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. Das Zentrum IKT- und Cyber Sicherheit stellt Produkte für die strategischen und operativen Ebenen im BMLVS zur Verfügung. Hierzu bedient sich das ZIKTCySih des Cyber Sicherheitsmanagements, eines breiten Spektrums an technischen Filter- und Analysesystemen, sowie Cyber Sicherheitsexperten zur Analyse von Bedrohungen und Vorfällen. 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.

- In den Organisationseinheiten des KdoFüU&CD (an der Führungsunterstützungsschule und in den Führungsunterstützungsbataillonen 1 und 2) sind sogenannte Cyber Schulungszentren (CSZ) für die Aus-, Fort- und Weiterbildung der Cyber Soldaten eingerichtet. Weiters verfügt das Führungsunterstützungsbataillon 1 über ein sogenanntes Cyber Defence Research Center (CDRC).

3.5 GovCERT und CERT.at

GovCERT ist das nationale CERT (Computer Emergency Response Team) der öffentlichen Verwaltung und Teil des zuvor beschriebenen IKDOK. Als Österreichischer CERT Point-of-Contact ist das GovCERT mit internationalen Organisationen und Ansprechpartnern wie der European GovCERT Group, TF-CSIRT oder der Central European Cyber Security Plattform vernetzt. Auch nimmt GovCERT (gemeinsam mit CERT.at) die Österreichische Vertretung im CSIRT-Netzwerk der EU wahr.

Zur Wahrnehmung seiner Aufgaben arbeitet das im Bundeskanzleramt angesiedelte GovCERT eng mit dem österreichischen CERT (CERT.at) in Form einer Public-Private-Partnership zusammen. CERT.at übernimmt dabei operative Aufgaben des GovCERT und stellt dafür technische Expertise und Know-How zur Verfügung.

Zur Wahrnehmung dieser Aufgaben ist in der ÖSCS eine Erweiterung des GovCERTs vorgesehen. Konkret sollen »… Verantwortung, Befugnisse und Wirkungsbereich, die Verankerung innerhalb der öffentlichen Verwaltung, die Rolle des GovCERTs im Krisenfall und das Zusammenspiel mit der Operativen Koordinationsstruktur … detailliert und neue Anforderungen spezifiziert werden«. Dieser Erweiterung ist derzeit in Planung und ermöglicht es dem GovCERT, künftige Aufgaben, die etwas aus der kürzlich beschlossenen EU-NIS-Richtlinie und dem damit einhergehenden Bundesgesetz für Cyber Sicherheit erwachsen (z. B. der Betrieb eines Sensornetzwerks für die öffentliche Verwaltung), wahrzunehmen.

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 innerhalb der österreichischen Sicherheits-Community sowie unter den österreichischen Organisationen und Unternehmen anerkannte Informationsdrehscheibe.

Die Umsetzung der EU-NIS-Richtlinie in nationales Recht hat auch für CERT.at zusätzliche Aufgaben gebracht. 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.

Das Bundesgesetz für Cyber Sicherheit 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.

GovCERT und CERT.at präsentierten am 20. Jänner 2017 gemeinsam den Jahresbericht Internet-Sicherheit Österreich 2016.

3.6 CERT-Verbund

Um für die österreichische Gesellschaft ein wirksames Sicherheitsniveau für den Cyber Raum auf- und auszubauen ist ein breites Zusammenwirken zwischen Zivilgesellschaft, Wirtschaft, Wissenschaft und Behörden notwendig. Speerspitze dabei sind die CERTs.

CERTs sind dafür da unsere digitalen Netze und IKT Systeme zu schützen. Mit Prävention, Reaktion und Bewusstseinsbildung sind sie erste Anlaufstelle für alle Bereiche der Cyber Sicherheit. Das dafür notwendige Wissen erhalten sie unter anderem aus intensiver nationaler und internationaler Vernetzung. Aus genau diesem Grund gibt es den österreichischen CERT Verbund.

Der nationale CERT-Verbund Österreichs hat die Aufgabe die nationale Zusammenarbeit zwischen österreichischen CERTs zu verbessern und CERT Aktivitäten in Österreich zu fördern. Ein flächendeckendes Netz an CERTs ist das wirksamste Mittel zum Absichern 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 und die optimale Nutzung des gemeinsamen Know-hows zur Gewährleistung von bestmöglicher IKT-Sicherheit.

Die Teilnahme 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 25 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 das Aufbauen von Vertrauen untereinander. Dadurch kann jedes CERT im Notfall sicher sein, dass es niemals alleine ist und für jeden Cyber Krisenfall rasch eine zusätzliche Expertise bereitsteht.

3.7 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. Weiters 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.

3.8 Cyber Crime Competence Center

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. Nach dem Aufbau des Bereiches für Mobile Forensik sind die nächsten Schwerpunkte Ausbildung von Spezialisten und die Schaffung der erforderlichen Infrastruktur in den neuen Themenbereichen KFZ- und Multimediaforensik. 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 Zusam-menhang mit Cyber Crime.

In Reaktion auf das Phänomen Ransomware wurde 2016 die SOKO Clavis ins Leben gerufen. Sie konzentriert die diesbezüglichen Ermittlungen an zentraler Stelle und koordiniert die internationale Zusammenarbeit. Sie setzt aus erfahrenen Kriminalbeamtinnen und Kriminalbeamten, einem BitCoin Spezialisten sowie einem hochqualifizierten Techniker zusammen.

3.9 Cyber Sicherheit Plattform

Die Cyber Sicherheit Plattform (CSP) stellt eine nationale Austausch- und Kooperationsplattform zwischen Wirtschaft, Wissenschaft und Verwaltung dar, im Wege derer der Erfahrungs- und Informationsaustausch im Bereich Cyber Sicherheit mit besonderem Fokus auf den kritischen Infrastrukturen, weiter intensiviert werden soll. Darüber hinaus berät und unterstützt die CSP auch die Cyber Sicherheit Steuerungsgruppe (CSS) in strategischen Fragen der Cyber Sicherheit.

Im Jahr 2016 hat die CSP ihre zweite und dritte Arbeitstagung abgehalten. Die Arbeitsgruppe Standardisierung&Zertifizierung hat die Ergebnisse ihrer Arbeit präsentiert, eine weitere Arbeitsgruppe zur Erarbeitung einer Agenda Cyber Sicherheit wurde eingesetzt. Mit der Agenda Cyber Sicherheit sollen wesentliche nationalen Zielsetzungen für den Bereich Cyber Sicherheit definiert und Grundlagen für eine Überarbeitung der Österreichischen Strategie für Cyber Sicherheit geschaffen werden. Die CSP hat sich im Rahmen ihrer beiden Arbeitstagungen zudem intensiv mit dem Thema Cyber Sicherheitsgesetz auseinandergesetzt und einen intensiven Austausch zwischen Wirtschaft und staatlichen Stellen in dieser zentralen Angelegenheit ermöglicht.

3.10 Austrian Trust Circle

Der 2010 gegründete Austrian Trust Circle (ATC) ist eine Initiative von CERT.at und dem Bundeskanzleramt und besteht aus Teilnehmern aus über 70 Organisationen der strategischen Infrastruktur. Der Austrian Trust Circle setzt sich aus sektorspezifischen Security Information Exchanges zusammen – ein strukturierter und formeller Rahmen für den informellen Informationsaustausch bezüglich Informations- und IT-Sicherheit.

Wesentliche Zielsetzung ist der Aufbau von Vertrauen zwischen den handelnden Personen und Organisationen in den einzelnen Bereichen strategischer Infrastruktur. Dadurch soll der Austausch sicherheitsrelevanter Erfahrungen und im Anlassfall ein rasches gemeinsames Agieren gefördert werden. 2016 wurde erstmals zusätzlich die öffentliche Verwaltung als eigener Sektor adressiert. Die Vernetzung zwischen öffentlichem und privatem Bereich fand regen Zuspruch und wird daher 2017 fortgesetzt. Neben regelmäßigen Treffen innerhalb der einzelnen Sektoren wird

der Austausch zwischen den Sektoren einmal im Jahr Rahmen einer zweitägigen Veranstaltung gefördert. Das Vertrauen, das bei diesen Veranstaltungen gebildet werden kann, stellt einen entscheidenden Vorteil beim Bewältigen von möglichen sicherheitsrelevanten Vorkommnissen dar. Im Jahr 2016 wurden unter anderem Themen, wie die EU-NIS Richtlinie, die Erkennung von Sicherheitsvorfällen, Erfahrungen aus dem Bereich von Krisenkommunikation behandelt.

3.11 IKT-Sicherheitsportal

Das IKT-Sicherheitsportal onlinesicherheit.gv.at ist eine in der ÖSCS definierte Maßnahme, die als interministerielle Initiative in Kooperation mit der österreichischen Wirtschaft eingerichtet wurde. Die Web-Plattform, welche im Jahr 2013 online gegangen ist, dient Sensibilisierungsmaßnahmen und ist Informations- und Kommunikationsbasis für verschiedene Zielgruppen.

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 Experten.

2016 umfassten die Aktivitäten auf dem IKT-Sicherheitsportal insgesamt die Verfassung von 190 Newsartikeln, 65 Publikationseinträgen, 23 Veranstaltungseinträgen und 23 Fachartikeln. Im Servicebereich wurde ein Online-Ratgeber der Wirtschaftskammer zur IT-Sicherheit von Unternehmen integriert und es werden laufend gratis Sicherheitstools und wichtige Tipps, die von den Kooperationspartnern des IKT-Sicherheitsportals zur Verfügung gestellt werden, veröffentlicht.

4 Cyber Übungen

4.1 Cyber Europe und Cyber Europe Austria 2016

Die Europäische Agentur für Netzwerk- und Informationssicherheit (ENISA) organisiert regelmäßig die größte pan-europäische IT-Notfall- und Krisenübung, »Cyber Europe«. Unter Beteiligung der EU- und EFTA-Staaten beübt diese alle zwei Jahre stattfindende Cyber Übung die Krisen- und Notfallpläne bestimmter, adressierter Sektoren, welche in Form eines auf diese Sektoren zugeschnittenen, fiktiv-simulierten Krisenszenarios auf die Probe gestellt werden. 2016 fand diese Übung bereits zum vierten Mal statt. Das von der ENISA vorgegebene Übungsszenario adressierte dabei die Sektoren der öffentlichen Verwaltung, Telekommunikation und der Cyber Sicherheitsindustrie.

Österreich beteiligt sich seit 2010 unter der Koordination des Bundeskanzleramts, das die nationale Übungsleitung innehat, an der Cyber Europe. Die nationale Abhaltung dieser Übung findet in Form einer parallel abgehaltenen, nationalen Übung namens »Cyber Europe Austria« (kurz »CE.AT«) statt. Die Übungsleitung der CE.AT übernimmt dabei die Vorgaben des internationalen Übungsszenarios der ENISA, adaptiert diese und reichert sie entsprechend der nationalen Gegebenheiten der an der Übung beteiligten, österreichischen Sektoren an, um so ein möglichst realistisches Szenario für die österreichischen Teilnehmer zu schaffen, ohne dabei die internationale Komponente der ENISA-Übung »Cyber Europe« zu vernachlässigen.

2016 unterteilte sich die internationale Cyber Europe in zwei Phasen. Während der ersten Übungsphase, die von April bis Oktober 2016 lief, konnten die Teilnehmer in Eigenverantwortung eine Vielzahl unterschiedlicher Sicherheitsvorfälle und Angriffsszenarien zu Übungszwecken innerhalb einer sicheren Übungsumgebung, bereitgestellt durch ENISA, analysieren. Diese Phase stimmte die über 700 Cyber SicherheitsexpertInnen aus über 300 Organisationen in 30 EU- und EFTA-Staaten auf die zweite, große Hauptphase der Cyber Europe, welche am 13. und 14. Oktober 2016 stattfand, ein.

Während dieser zweiten Phase, die in Österreich in Form der CE.AT 2016 umgesetzt wurde, waren die internationalen Teilnehmer gefordert, Lösungsansätze für Vorfälle bzgl. Drohnen, Cloud Computing, mobile Malware oder Ransomware zu finden sowie sich im Zuge dieser Lösungsfindung auf nationaler und europäischer Ebene auszutauschen. Dabei nahmen Faktoren wie die mediale Berichterstattung während einer solchen Cyber Krise, ihre Auswirkung auf Unternehmen und den öffentlichen Sektor sowie die sozialen Medien eine wichtige Rolle ein, was dem Szenario eine hohe Glaubwürdigkeit verlieh.

Das vorrangige Ziel der Cyber Europe 2016 war die Verbesserung der Kooperation auf europäischer Ebene. Dies war für die Teilnehmerstaaten insofern herausfordernd, als diese sich neben der nationalen Prozess- und Kooperationsmechanismen auch mit der EU-Netzwerk- und Informationssicherheitsrichtlinie und den daraus resultierenden Strukturen und Prozessen auseinandersetzen mussten. Wie auch andere Mitgliedsstaaten arbeitet Österreich derzeit unter Federführung des Bundeskanzleramts an der Verfassung eines Bundesgesetzes, das diese Richtlinie in nationalem Recht abbildet. Obwohl dieser Prozess noch nicht abgeschlossen ist, konnten nicht erst 2016, sondern schon bei der vorangegangenen Übung (CE.AT 2014) sich daraus ergebenden Prozesse und Strukturen – welche damals bereits teilweise vorhanden,

teilweise aber auch erst im Aufbau waren – beübt werden. Während der CE.AT 2016 konnte dies anhand der fortgeschrittenen Umsetzung dieser Prozesse und Strukturen nun – zwei Jahre später – erneut beübt werden. Dies führte zu wertvollen Erkenntnissen für eine verbesserte Zusammenarbeit der österreichischen Cyber Sicherheit Stakeholder aus dem staatlichen sowie dem Privatsektor.

Die CE.AT 2016 wurde in Österreich durch das Bundeskanzleramt am 13. Oktober 2016 bereits zum dritten Mal parallel zur pan-europäischen »Cyber Europe«, erfolgreich durchgeführt. Im Vorfeld der Übung wurden zwei wesentliche Ziele definiert: Erstens die darüber erwähnte Fortsetzung des Optimierungsprozesses der Kollaborations- und Koordinationsstrukturen zwischen privaten und staatlichen AkteurInnen, und zweitens das Aufzeigen von übergreifenden Stärken und Schwächen bei der Kommunikation und Kollaboration zwischen den TeilnehmerInnen selbst. An der CE.AT 2016 nahmen insgesamt zehn Organisationen aus dem öffentlichen und dem privaten Sektor teil.

Neben simulierten Cyber Angriffen auf Webseiten und Online Anwendungen der öffentlichen Verwaltung und der Internet Service Provider, machten darüber hinaus die Auswirkungen der Attacken auf die mediale Öffentlichkeit einen wesentlichen Bestandteil der CE.AT 2016 aus, wodurch auch die Krisenkommunikation gegenüber der Öffentlichkeit für den Ernstfall geprobt wurde.

Auf Basis der Ergebnisse und durch die Erfüllung der im Vorfeld definierten Übungsziele konnten durch die CE.AT 2016 erneut wichtige Erkenntnisse für die Zukunft gewonnen werden. Dazu gehört, dass das Vorhandensein und die reibungslose Zusammenarbeit von Strukturen für den Austausch von Informationen und für die Erstellung eines Gesamtlagebilds (etwa durch die in der ÖSCS definierte Operative Koordinierungsstruktur) von maßgeblicher Bedeutung für die erfolgreiche Bewältigung einer Cyber Krise ist. Auch der Sektor-übergreifende Informationsaustausch und die Kooperation zwischen Stakeholdern stellen einen Schlüssel für ein funktionierendes Frühwarnsystem und die Bewältigung von groß angelegten Cyber Angriffen dar. Die Ergebnisse der CE.AT 2016 konnten an jene der vergangenen Übungen aus den Jahren 2012 und 2014 anschließen und belegen damit den Erfolg der Durchführung dieser Cyber Übung.

Trotz solcher Erfolge kann jedoch festgehalten werden, dass erst durch eine regelmäßige Abhaltung solcher Cyber Übungen, welche eine wichtige Rolle in der Verbesserung der Zusammenarbeit der beteiligten Stakeholder spielen, sichergestellt werden kann, dass Österreich mit den fortschreitenden Entwicklungen von Cyber Bedrohungen Schritt halten kann. Um dabei eine Kontinuität zu schaffen, arbeitet das Bundeskanzleramt derzeit an einem Konzept für Cyber Sicherheitsübungen. Dadurch soll einerseits die Abhaltung solcher Übungen in Österreich strukturiert und andererseits den Beteiligten wertvolle Unterstützung in der Planung und Abhaltung von Cyber Übungen geboten werden.

4.2 Cyber Coalition

Seit 2008 führt die NATO jährlich eine Cyber Verteidigungsübung mit dem Namen »Cyber Coalition« durch, um Entscheidungsprozesse, technische und operationelle Abläufe sowie die Zusammenarbeit zwischen den Teilnehmern zu üben. Es sind an der Übungsserie rund 600 internationale Teilnehmer aus 28 NATO-Nationen und 7 NATO Partnerstaaten (darunter auch Österreich) beteiligt. Das BMLVS war 2016 durch MilCERT und das Cyber Verteidigungszentrum vertreten. Primäre Übungsziele waren die Verbesserung von Entscheidungsprozessen sowie von technischen und operationellen Abläufen. Die im Rahmen der Übung zu bewältigenden Aufgabenstellungen waren (auszugsweise):

- Schadsoftware erkennen
- Forensische Analyse (Funktion der Malware, ggf. Infektionsweg ermitteln (Attribution – »wer steckt dahinter?«)
- Analyse von Smart Devices
- Erkennen einer Infektion eines SCADA Systems
- Zusätzlich zu den technischen Herausforderungen die Bereitstellung einer umfassenderen rechtlichen Beurteilung

4.3 Locked Shields

Bei dieser größten technischen Übung (besteht seit 2008, rund 400 internationale Teilnehmer) im Cyber Verteidigungsbereich liegt generell die Detektion und Abwehr von Angriffen im Fokus, mittlerweile werden auch die aktiven Verfahren geübt. Dies ist inbesondere von Relevanz, da – wie auch bei konventionellen Angriffen – die Kenntnisse über die Angriffe und deren Methoden für die Erkennung und Abhaltung notwendig sind.

Das BMLVS war 2016 durch MilCERT und das Cyber Verteidigungszentrum vertreten.

5 Zusammenfassung / Ausblick

Auch im Jahr 2016 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.

DoS (Denial of Service) und DDoS (Distributed Denial of Service) Attacken, sowohl kriminell als auch politisch motiviert, zählen derzeit zu den häufigsten und wirksamsten Cyber Attacken. Darüber hinaus zeichnen Ransomware, CEO Fraud und Phishing-Angriffe für eine signifikante Anzahl an Vorfällen verantwortlich.

In den genannten Vorfallsarten ist neben steigenden Vorfallszahlen auch ein Trend hin zu einer zunehmenden Professionalisierung zu beobachten. So stieg die Anzahl an Ransomware durch »Geschäftsmodelle« wie Ransomware-as-a-Service sprunghaft an. Auch Versuche von CEO Frauds wurden zunehmen aufwändiger und vermehrt auf die jeweiligen Opfer maßgeschneidert. »Crime as a Service«-Geschäftsmodellen kommt in diesem Zusammenhang steigende Bedeutung zu. Konsequenterweise ist bei befragten Unternehmen der kritischen Infrastruktur das für IT-Security zur Verfügung stehende Budget gegenüber dem Jahr 2015 entweder gestiegen oder zumindest gleich geblieben.

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 wurden im Lauf des Jahres 2016 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.

Fragen der Cyber Sicherheit werden weiterhin im Rahmen von EU, VN, OSZE, NATO, OECD und Europarat sowie in multilateralen Foren (Global Conference on Cyberspace, Central European Cyber Security Platform, Freedom Online Coalition) unter aktiver Beteiligung von Österreich thematisiert. Mit der neuen globalen Strategie der EU wurde dem Bereich Cyber ein entsprechendes Gewicht im außen- und sicherheitspolitischen Handeln der EU eingeräumt. Mit 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) soll das Cyber Sicherheitsniveau in allen EU-Mitgliedsstaaten gehoben werden.

Im Bereich der nationalen Akteure und Strukturen war das Jahr 2016 vom Übergang der neu aufgestellten bzw. nach aktuellen Bedürfnissen adaptierten Elemente in den Regelbetrieb gekennzeichnet. Die Anpassung nationaler Strukturen und Prozesse an die neuen Herausforderungen im Cyber Raum wurde damit fortgesetzt. Insbesondere der operationellen Zusammenarbeit zwischen den unterschiedlichen Stakeholdern im Rahmen des inneren Kreises der operativen Koordinierungsstrukturen wurde im Jahr 2016 erhöhte Aufmerksamkeit geschenkt. Zusätzlich wurde die Zusammenarbeit zwischen staatlichen und privaten Strukturen, vor allem auch im Lichte der Umsetzung der EU-NIS-RL, 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. Die Arbeiten an der Umsetzung der EU-NIS-RL in nationale Gesetzgebung werden im Laufe des Jahres 2017 im Rahmen der im Bundeskanzleramt angesiedelten Arbeitsgruppe sowie in Form eines Begutachtungsverfahrens weitergeführt. Darüber hinaus haben Vorarbeiten zur Neufassung der Österreichischen Strategie für Cyber Sicherheit begonnen. Wesentliche Inputs für die strategische Neuausrichtung im Bereich der Cyber Sicherheit werden aus der Zusammenarbeit zwischen dem öffentlichen und dem privaten Bereich, insbesondere im Rahmen der Cyber Sicherheit Plattform, erwartet.