REPUBLIK ÖSTERREICH

Bericht Cyber Sicherheit 2015

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 2015

Wien, 2015

Impressum

Medieninhaberin, Verlegerin und Herausgeberin:
Bundeskanzleramt Österreich,
Sektion IV – Koordination,
Abteilung IV/6 – Sicherheitspolitische Angelegenheiten
Ballhausplatz 2, 1010 Wien

Grafische Gestaltung: BKA | ARGE Grafik
Druck: BM.I Druckerei
Wien, März 2015

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 erste Bericht wurde im Juni 2014 von der Steuerungsgruppe beschlossen und den thematisch involvierten Regierungsmitgliedern zur Kenntnis gebracht.

Der vorliegende Bericht Cyber Sicherheit 2015 baut auf den Inhalten des letztjährigen Berichtes auf und ergänzt diesen um aktuelle Entwicklungen.

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 Akteure und deren Intentionen

Auch 2014 wurden staatliche Konflikte zusehends im Cyber Raum ausgetragen. Aufdeckungen im Bereich **staatlicher Überwachung und Spionagetätigkeit** waren Mittelpunkt von Kontroversen und öffentlicher Debatte. Staatliche Akteure nutzen den Cyber Raum zur Förderung ihrer politischen, militärischen und wirtschaftlichen Interessen. Es ist davon auszugehen, dass die Aktivitäten in diesem Bereich fortgesetzt werden. Aktuelle Zwischenfälle zeigen jedoch, dass selbst politisch motivierte Attacken sich nicht wie im realen Leben eindeutig einer Organisation oder einem Staat zuordnen lassen. Auch gibt es wenige Informationen darüber, wie derartige Attacken konkret durchgeführt werden, da diese meist zielgerichtet stattfinden. In diesem Bereich wird eine große Dunkelziffer vermutet.

Da die Nachverfolgung von Aktionen und die Identifikation der Akteure im Cyber Raum ausgesprochen schwierig sind, ist die Hemmschwelle für eine Durchführung solcher Aktionen gering. Es ist daher davon auszugehen, dass im virtuellen Raum mehr und gewagtere Aktionen stattfinden als in der realen Welt. Neben den typischen großen **Akteuren** wie den **USA** (gemeinsam mit dem Vereinigten Königreich, Neuseeland, Australien und Kanada im »5 Eyes-Verbund«), **Russland und China** werden zunehmend auch **kleinere Staaten (z. B. Iran, Syrien)** in diesem Feld aktiv. Auch 2014 gab es weitere Enthüllungen zu den Spionageprogrammen der NSA, dieses Thema ist immer noch aktuell und dürfte es auch 2015 bleiben.

Auch das Thema **Wirtschafts- und Industriespionage** war 2014 präsent. Eine Grenze zwischen politischer und wirtschaftlicher Industriespionage kann dabei nicht immer klar gezogen werden. Neben Spionageaktivitäten wird auch versucht, die öffentliche Meinung global zu beeinflussen (internationale **Propaganda**) und die eigene Bevölkerung von ausländischen Medien abzuschirmen.

Auf nichtstaatlicher Ebene spielen **Cyber Kriminelle** eine wesentliche Rolle. Täter und Täterinnen bedienen sich ausgefeilter Technologien und nutzen das Internet als Tatbegehungsort für ihre weltumspannenden kriminellen Machenschaften. Diese reichen von Kleinkriminalität bis hin zu groß angelegten Kampagnen mit Schadenshöhen nahe an der Milliarde Euro. Die Opfer finden sich ebenfalls in allen Bereichen: Sie reichen von Bürgern, Vereinen, KMUs, High-tech Start-Ups, Konzernen bis hin zu öffentlichen Einrichtungen. Das Motiv ist hier meist direkt monetär, die Wege zur Zielerreichung variieren. Cyber Kriminalität ist zu einem arbeitsteilig arbeitenden »Ökosystem« herangewachsen, in dem die »Wertschöpfungskette« von verschiedenen Akteuren erbracht wird. Nicht alle Elemente handeln offensichtlich kriminell, in manchen Fällen wird aber toleriert, dass Dienstleistungen für Cyber Kriminalität benutzt werden.

Terroristen nutzen den Cyber Raum vorwiegend zur Radikalisierung, Rekrutierung und Finanzierung von terroristischen Operationen. Für 2014 sind hier v.a. die Propagandaaktivitäten des »Islamischen Staates« hervorzuheben.

»**Hacktivisten**« (**Internet-Aktivisten**) stellen eine besondere Form von Online-Akteuren dar. Sie können innerhalb des Cyber Raumes als Online-Demonstranten bezeichnet werden, die meist durch »Distributed Denial of Service«-Angriffe oder »Defacements«[1] ihren Unmut über bestimmte Umstände (meist politischer oder gesellschaftlicher Natur) kundtun. Dahingehend motivierte Hacker-Aktionen nahmen jedoch 2014 in Österreich weiter ab. Die bekannteste Hacktivistengemeinschaft ist die Anonymous-Bewegung. In ihren Anfängen vereinten sich Personen unter dem Deckmantel von Anonymous, um gegen globale Themen wie Einschränkungen der Meinungsfreiheit oder für die Freiheit des Internets zu protestieren. Mit der Zeit haben sich vermehrt Anonymous-Gruppierungen gebildet, die sich auf nationale oder regionale Themen fokussieren. Neben den klassischen Hacktivisten haben die sogenannten »patriotischen Hacker« wie z. B. die »Syrian Electronic Army« meist ein gewisses Naheverhältnis zu Regierungen. Es ist davon auszugehen, dass Hackergruppen auch als Deckmantel zur Verschleierung staatlicher Cyber Angriffe eingesetzt wurden und weiterhin werden.

Letztlich sind noch einzelne Hacker bzw. Hackergruppen zu erwähnen, welche aus unterschiedlichen Motiven heraus durch Cyber Attacken erheblichen Schaden anrichten können. Zu beobachten ist jedoch, dass klassische Hacker, die aus Neugier und Spieltrieb in Systeme eindringen, kaum noch eine Rolle spielen.

1.2 Methoden

Zielsetzung von Cyber Angriffen ist es, die Vertraulichkeit, die Integrität und/oder die Verfügbarkeit von Netzwerken, darin befindlichen Geräten oder Daten und Diensten in diesen Netzwerken zu kompromittieren. Bei der **Auswahl der Ziele bzw. Opfer** solcher Attacken kann man **drei Kategorien** unterscheiden:

- **Gezielte Angriffe auf ein bestimmtes Ziel.** Diese Form wird gewählt um gut geschützte Ziele anzugreifen, bei denen die Schadsoftware auf jedes Opfer individuell abgestimmt wird. Dies bedarf einer zeitaufwändigen und ressourcenintensiven Vorbereitung. Hinsichtlich der tatsächlichen Auswirkungen vor allem im Bereich des Informationsabflusses und möglicher Steuerung von außen stellt diese Kategorie von Angriffen (auch »Advanced Persistent Threat« bzw. APT genannt) die größte Bedrohung dar.
- **Zielgerichtete Angriffe auf eine ausgewählte Gruppe bestimmter Ziele**. Hier wird eine ausgewählte Gruppe bestimmter Ziele, deren gemeinsamer Nenner für den Angreifer die Motivation für diesen Angriff ausmacht, angegriffen.
- **Großflächige Angriffe auf möglichst viele Ziele gleichzeitig**. Diese Form wird verwendet, um Informationen von möglichst vielen, nicht näher identifizierten Rechnern zu stehlen. In der Regel werden schwächer geschützte Systeme angegriffen.

Je nach Ziel und intendiertem Effekt wird aus einer **Vielzahl an Mitteln und Methoden** gewählt, um Angriffe im und über den Cyber Raum erfolgreich durchzuführen. Diese kann man folgendermaßen kategorisieren:

1 Optische Veränderung/Verunstaltung einer Webseite, meist im Zusammenhang mit einem gesellschaftspolitischen Hintergrund

- **Kompromittierung von Rechnern des Opfers**: Das reicht von privat betriebenen PCs, über das Netzwerk von Firmen bis hin zu Servern. Meist kommt Schadsoftware zum Einsatz, die eine Fernsteuerung der infizierten Komponenten ermöglicht.
- **Datendiebstahl**: In manchen Fällen erreicht ein Angreifer keine Kontrolle über die IT-Ressourcen seiner Opfer, kann aber Daten abgreifen.
- **Störung der Verfügbarkeit** (»Denial of Service«): Der Angreifer kann sich die Ressourcen des Opfers nicht aneignen, schafft es aber, die Systeme des Opfer so zu stören, dass die legitime Nutzung nicht mehr möglich ist.

Im Jahr 2014 gab es keine bedeutende Änderungen in der Methodik der Angreifer um in Systeme einzugreifen, interessanter sind die Entwicklungen, wie Kompromittierungen zum Vorteil des Täters ausgenutzt werden. Beispiele dafür sind:

- Angriffe auf Banken: Angriffe auf das Online-Banking von Bankkunden (mittels Phishing-Mails/Webseiten oder Malware am Client-PC) können weiter beobachtet werden, inzwischen sind aber auch schon Angriffe bekannt geworden, bei denen Banken selbst kompromittiert wurden und Geld direkt dort gestohlen wurde. So wurden sowohl Geldüberweisungen direkt im Core-Banking als auch die Steuerung von Bankomaten manipuliert.
- Angriffe auf Handelsketten: In mehreren Fällen gelang es Angreifern, soweit in Firmennetze einzudringen, dass Bezahlvorgänge in Kassensystemen manipuliert und Kreditkartendaten ausgespäht werden konnten.
- »Ransomware«: Dazu zählt Malware, die Daten von Nutzern in »Geiselhaft« nimmt (indem gespeicherte Daten verschlüsselt werden) und versucht für eine Freigabe Geld zu erpressen. Ransomware findet sich nicht mehr nur auf PCs, sondern weitete sich auch auf Netzwerkspeicher und Smartphones aus.
- Es gab in Österreich Fälle, wo nach einem Einbruch in ein Firmennetz die E-Mail-Kommunikation des Konzerns mit seinen Vertriebspartnern mitgelesen wurde, um dann gezielt gefälschte E-Mails einzustreuen und Zahlungen umzuleiten.
- Mit »Havex/Dragonfly/Energetic Bear« gab es 2014 auch einen APT, der auf die Netze von industriellen Steueranlagen abzielte.

Die **Infektion von Windows-PCs** ist immer noch das klassische Einfallstor in Firmennetze. Vorrangiges Angriffsziel sind dabei die Programme, mit denen Inhalte aus dem Web dargestellt werden (z. B. PDF-Viewer, Textverarbeitungssoftware, Web-Browser und deren Plug-Ins). Mit Schadsoftware präparierte Dateien werden dabei von Angreifern per E-Mail direkt versendet oder per Link referenziert. Über »**Social Engineering**« (etwa »Öffnen Sie dieses Mahnschreiben/Telekom Rechnung/…«) sind für eine Infektion oft nicht einmal technische Schwachstellen erforderlich; auch gut implementierte technische Sicherheitsvorkehrungen lassen sich auf diese Weise umgehen. So etwa werden wieder Makros in Office-Dokumenten benutzt, um Schadsoftware einzuschleusen: Dies erfordert zwar die explizite Zustimmung des Users, diese lässt sich aber oft über »Social Engineering« erreichen. Auch über manipulierte Webseiten wird versucht, deren Besucher zu infizieren. Bei gezielten Angriffen wurde 2014 ein Trend in Richtung »Watering Hole Attack« identifiziert: Der Angreifer infiziert dabei eine Webseite, die seine Opfer häufig besuchen und versucht über Browser/Plugin-Schwachstellen die Kompromittierung des Ziels zu erreichen. Diese Vorgehensweise kann mit E-Mails kombiniert werden, welche Opfer gezielt auf solche Seiten lenken.

Ist eine initiale Infektion gelungen, kann ein Angreifer z. B. in Firmen- und Behördennetzen weiter vordringen und auf diese Weise im internen Netzwerk schrittweise bis zu den kritischen Systemen gelangen, um diese ebenfalls zu kompromittieren. Das zu verhindern ist technisch und administrativ sehr aufwändig; entsprechende Sicherungsmaßnahmen werden daher nur sehr selten effektiv umgesetzt.

Eine weitere Methode sind Einbrüche über die im Internet erreichbaren Dienste der potentiellen Opfer. Insbesondere die Webseiten von Vereinen, Konzernen und KMUs, Schulen, aber auch Behörden sind Opfer solcher Attacken. In diesen Fällen ist das Opfer für den Angreifer oft weniger interessant als die Ressourcen und die Besucher des attackierten Webservers.

Für Angriffe auf die Verfügbarkeit von Online-Services werden seit 2013 immer häufiger »**Distributed Reflected Denial of Service Attacks**« benutzt. Hierbei fälscht der Angreifer im Namen des Opfers viele kleine Anfragen an legitime Server; die darauf folgenden Antworten legen dann in Ihrer Größe und Vielzahl die Netzanbindung des Opfers lahm, wodurch das betroffene Online-Service nicht mehr erreichbar ist. Wurde 2013 dazu noch primär das »Domain Name Service« missbraucht, so wurden 2014 weitere Protokolle benutzt, etwa das »Network Transfer Protocol« oder das »Simple Service Discovery Protocol«. Mit Stand Ende 2014 sind noch rund 40.000 IP-Adressen in Österreich für solche Angriffe missbrauchbar.[2]

1.3 Schwachstellen

Im Jahr 2014 traten neben der üblichen **Vielzahl an Schwachstellen**[3] auch zwei Probleme auf, welche besonders erwähnenswert sind:

- »Heartbleed«: Dieser Fehler in »openssl«[4] machte viele Dienste im Internet für Datendiebstahl anfällig. Aktuelle Zahlen zum Stand von Heartbleed in Österreich finden sich im Bericht Internet Sicherheit Österreich 2014.[5] Signifikante Vorfälle mittels Heartbleed sind in Österreich jedoch nicht bekannt geworden.
- »Shellshock«: Diese Schwachstelle in »bash«[6] machte zahlreiche Webserver anfällig. Auch wenn der Fehler erst dieses Jahr entdeckt und veröffentlicht wurde, konnte nachvollzogen werden, dass er bereits seit 1989 in »bash« existierte. Die Schwachstelle wurde von Sicherheitsexperten als extrem kritisch beurteilt, da ein Angreifer aus der Ferne mit Hilfe dieser Schwachstelle beliebige Codes am angegriffenen Server ausführen konnte.

Eine Auflistung einzelner technischer Schwachstellen ist aufgrund ihrer zumeist gegebenen Volatilität wenig zielführend. Die folgende Auflistung ist daher bewusst allgemein gehalten:

- Potentielle Angreifer konzentrieren sich immer stärker auf die **Anwenderschicht**, da die Netzwerkebene durch technisch implementierte Sicherheitsmaßnahmen einigermaßen beherrschbar ist. Der Mensch ist hingegen eine permanent existierende Schwachstelle. Oft brauchen Angreifer keine technischen Fehler auszunutzen, wenn sie Anwender z. B. durch »Social Engineering« dazu bringen können, gegen ihre eigenen Interessen zu handeln.
- Schien vor 10 Jahren **Mobiltelefonie** noch als vertrauenswürdiger Kommunikationskanal nutzbar, so ist das 2014 nicht mehr als gegeben anzunehmen: Die Komplexität von Smartphones und die Proliferation von Apps machen die Verbreitung von Schadsoftware auf Mobiltelefonen deutlich einfacher, auch wurden mehrere Angriffsvektoren auf die Übermittlung von SMS-Nachrichten im Mobilfunk gefunden.

2 Siehe CERT Jahresbericht: http://cert.at/reports/report_2014_chap05/content.html
3 Die zentrale Datenbank »Common Vulnerabilities and Exploits (CVE)« der Non-Profit-Organisation Mitre, in der veröffentlichten Schwachstellen eine eindeutige ID gegeben wird, musste für 2014 erstmals 5-stellige Nummern vergeben.
4 Eine Servertechnologie zur Bereitstellung verschlüsselter Webseiten (z. B. Online-Banking)
5 http://cert.at/reports/report_2014_chap05/content.html
6 Ein auf Unix/Linux-Systemen verbreiteter Kommandozeileninterpreter

- Username und Passwort allein sind als **Zugangsschutz** für sensitive Web-Applikationen nicht ausreichend. Die Wiederverwendung von Passwörtern seitens der Anwender ist ein Faktum, welches von Internet-Betrügern vermehrt ausgenutzt wird. Es wurden 2014 mehrmals riesige Datenbanken mit Usernamen und dazugehörigen Passwörtern gefunden.
- Laufende **Software-Aktualisierungen** sind ein massives Management-Problem. Das reicht von Browser-Plugins bei Privat-PCs bis hin zur Webserver-Software bei Unternehmen.
- **Support-Ende von XP**: Aufgrund des Auslaufens des Supports für Windows XP seitens Microsoft wurde ab April 2014 ein hoher Anteil an PCs sukzessive verwundbarer, weil bis dorthin unentdeckte Sicherheitslücken nicht mehr bereinigt wurden. Dies kann auch durch vorhandene Antivirensoftware nicht abgefedert werden.
- Auch im Zunehmen begriffen sind **gezielte Angriffe auf Industrieanlagen und Steuersysteme** (**SCADA**), welche bisher oftmals durch physikalische Trennung zur Außenwelt stark erschwert waren. Neue Technologien und drahtlose Kommunikation führen zusehends zu einer Auflösung dieser Trennung und öffnen so kritische Systeme zur Außenwelt und damit verbundenen Gefahren aus dem Cyber Raum.

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.

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 jedoch 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

2.1.1 Grundlagen

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) eine **EU Cyber Sicherheitsstrategie** vor. Unter dem Titel »An Open, Safe and Secure Cyberspace« finden sich darin eine Reihe von Vorschlägen, unter anderem zum Ausbau von Fähigkeiten, zur Verbesserung von Kooperation und Kommunikation sowie zur Stärkung einer gemeinsamen internationalen Politik der EU im Cyber Bereich. Darüber hinaus soll die gemeinsame Cyber Verteidigungspolitik verbessert werden, eine Forderung, die sich auch in den Schlussfolgerungen des Europäischen Rates (ER) zur Gemeinsame Sicherheits- und Verteidigungspolitik (GSVP) vom Dezember 2013 wiederfindet. Demnach soll einerseits das Fähigkeitsspektrum im Cyber Bereich erweitert und ausgebaut, andererseits ein EU-Politikrahmen für die Cyber Abwehr festgelegt werden.

Am 18. November 2014 wurde durch den Rat der EU ein »**EU Cyber Defence Policy Framework**« angenommen, das die vorrangigen Aufgaben für die GSVP im Cyber Bereich identifiziert, die Rollen der diversen Akteure im europäischen Rahmen klarstellt und die Entwicklung von Cyber Verteidigungsfähigkeiten sicherstellt. Darüber hinaus soll das »EU Cyber Defence Policy Framework« den Schutz der für die GSVP relevanten Kommunikations- und Informationsnetzwerke des Auswärtigen Dienstes und eine verbesserte Kooperation der EU mit dem privaten Sektor wie auch der Nordatlantischen Vertragsorganisation (NATO) gewährleisten.

Der Rat nahm weiters am 10. Februar 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. Es liegt nun ein ausgewogener Text vor, der auf Aspekte wie die Anwendung von Völkerrecht, Menschenrechten und Rechtstaatlichkeit auch im Cyber Raum, Internet Governance, digitale Wirtschaft, Wettbewerbsfähigkeit der EU und Cyber Capacity Building Bedacht nimmt. Die Schlussfolgerungen enthalten Maßnahmen, die die Wahrung der oben genannten Grundsätze gewährleisten, die EU aber auch befähigen sollen, den Grundsatz eines freien Internets mit

Zugang für alle zu schützen, sowie in enger Zusammenarbeit mit wichtigen Partnern und internationalen Organisationen den aus dem Cyber Raum auftretenden Gefahren wirksam zu begegnen.

2.1.2 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 und hat im Jahr 2014 an einer Vielzahl von pan-europäischen Arbeitsgruppen mitgewirkt. Ein Schwerpunkt war 2014 die Arbeitsgruppe zu Nationalen Cyber Security Strategien.

Am 12. Februar 2013 hat die EK zudem einen Vorschlag für eine **Richtlinie des Europäischen Parlaments (EP) und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit (NIS)** an die Mitgliedsstaaten übermittelt. Diese sogenannte »NIS-Richtlinie« ist ein integraler Bestandteil zur Umsetzung der Cyber Sicherheitsstrategie der EU und wird derzeit im Rat und im EP verhandelt. Folgende Kernforderungen wurden darin identifiziert:

- Annahme einer nationalen NIS-Strategie, sowie die Aufstellung einer NIS-Behörde und eines GovCERT/CERT (Computer Emergency Response Team) als IT-Notfallteam (künftig wird auf EU-Ebene statt CERT der Terminus CSIRT, d. i. Computer Security Incident Response Team aufgrund des Bestehens einer Gemeinschaftsmarke verwendet).
- Verpflichtendes Risikomanagement für kritische Infrastrukturen und Meldeverpflichtung bei Sicherheitsvorfällen für wesentliche Dienste.
- Einsatz 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.

2.1.3 Kooperationen

Im Dezember 2013 wurde durch den ER eine **Intensivierung der Zusammenarbeit der EU mit der NATO** beschlossen. Dies lässt im Cyber Bereich erwarten, dass die Europäische Verteidigungsagentur eine verstärkte Kooperation mit dem NATO »Center of Excellence« in Tallinn eingehen wird.

Selbiges gilt für die mögliche Zusammenarbeit im Rahmen der »**Friends of Presidency Initiative on Cyber Issues**«, die 2013 zur Unterstützung der Implementierung der EU Cyber Security Strategy aktiviert wurde. Aufgabe dieser Gruppe ist es, die verschiedenen Cyber Themen in der EU horizontal zu koordinieren. Dabei sollen miteinander verknüpfte Cyber Fragen in ganzheitlicher Weise betrachtet werden, eine übergreifende Zusammenschau bezüglich aller in der EU stattfindenden Cyber Themen stattfinden und die Zusammenarbeit mit allen Organisationen gefördert werden, die sich auf europäischer Ebene mit Fragen der Cyber Sicherheit beschäftigen. Vorrangiges Ziel ist es, die Effektivität von bestehenden Aktivitäten und Beratungsfunktionen zu Cyber Thematiken zu verbessern. Eine Operative Ownership wird dabei nicht übernommen.

Die Arbeitsgruppe wurde als permanente Einrichtung für jeweils drei Jahre mit mindestens drei Veranstaltungen pro Präsidentschaft eingerichtet und genutzt, um die Umsetzung der europäischen Cyber Sicherheitsstrategie zu überwachen. Damit hat die Gruppe enorm an Bedeutung gewonnen und ist nun innerhalb der EU zentrale Drehscheibe zur Darstellung, Diskussion und Verfolgung aller Cyberthemen.

2.1.4 European Cyber Security Month

Der »European Cyber Security Month (ECSM)« ist eine institutionalisierte, alljährlich stattfindende **Kampagne der ENISA zur Bewusstseinsbildung zum Thema Cyber Sicherheit**. Dabei bietet sich den Teilnehmern die Gelegenheit, eigene Aktivitäten zum Thema Cyber Sicherheit öffentlichkeitswirksam zu präsentieren. Österreich beteiligte sich 2014 über das BKA nach 2013 bereits zum zweiten Mal an dieser Kampagne. Dabei konnten in Österreich zum wiederholten Male unter über 30 Teilnehmerländern mit Abstand nicht nur die größte Zahl an Organisationen aus den Bereichen der öffentlichen Verwaltung, der Privatwirtschaft, Banken, Gesundheit und Forschung, sondern auch die meisten Aktivitäten für die Kampagne akquiriert werden. Die Bandbreite dieser Aktivitäten umfasste dabei Awareness-Kampagnen, Trainings, Konferenzen, Workshops, Vorträge, Forschungsveranstaltungen, Hacking-Wettbewerbe und vieles mehr. Unter anderem wurden vom BMEIA im Rahmen dieser Kampagne alle E-Mail-mäßig erfassten Auslandsösterreicher, Auslandsösterreicher-Vereine und Honorarkonsulate in Spanien und im Vereinigten Königreich über das Pilotprojekt »Elektronische Signatur via Mobiltelefon« umfassend informiert.

2.2 Vereinte Nationen

Bereits zur Jahrtausendwende rief die Generalversammlung der Vereinten Nationen (VN-GV) den »**World Summit on the Information Society (WSIS)**« ins Leben. Im Rahmen von WSIS, der organisatorisch bei der International Telecommunication Union (ITU) angesiedelt ist, und an dem neben staatlichen Akteuren auch NGOs, zivilgesellschaftliche Gruppen und der private Sektor beteiligt sind, wird derzeit eine Evaluierung der Fortschritte im vergangenen Jahrzehnt durchgeführt. Diese Evaluierung soll 2015 im Rahmen einer Review zum 10-Jahres Jubiläum (WSIS+10) zum Abschluss kommen.

Im Oktober/November 2014 fand in Busan (Republik Korea) mit der Plenipotentiary Conference die höchstrangige Konferenz der ITU statt, bei der auch der neue ITU-Generalsekretär Houlin Zhao (China) gewählt wurde. Österreich war durch das Bundesministerium für Verkehr, Innovation und Technologie (BMVIT) vertreten. Ein wichtiges Ergebnis aus Sicht der westlichen Staaten war, dass eine Ausweitung des ITU-Mandats zu Cyber Security bei dieser Konferenz verhindert werden konnte.

Es beschäftigen sich auch mehrere **Komitees der VN-GV** mit Cyber Themen. Neben dem Ersten Komitee, das Entwicklungen auf dem Gebiet der Information und Telekommunikation im Kontext der internationalen Sicherheit beobachtet, ist aus österreichischer Sicht vor allem die Arbeit im **Dritten Komitee** von Interesse. Die im Jahr 2014 zum zweiten Mal von Deutschland und Brasilien eingebrachte Resolutionsinitiative zum Recht auf Privatsphäre im digitalen Zeitalter konnte nach langwierigen Verhandlungen wieder im Konsens angenommen werden. Österreich beteiligte sich als Mitglied der Kerngruppe aktiv an den Verhandlungen, wobei vor allem Fragen der Extraterritorialität, zu den Grundsätzen der Verhältnismäßigkeit und Notwendigkeit und zur Massenüberwachung besonders umstritten waren. Mit der Resolution wurde die Grundlage für die Diskussionen über die Einrichtung eines Mandates für einen VN-Sonderberichterstatter zum Schutz der Privatsphäre durch den VN-Menschenrechtsrat im März 2015 geschaffen.

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.

2.3 NATO

Als Verteidigungsbündnis 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. 2014 fanden einerseits 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.

Generell sind die Initiativen der NATO im Zusammenhang mit der im Juni 2014 in Kraft gesetzten »**NATO Enhanced Cyber Defence Policy**« zu sehen.

Österreich hat im Rahmen der NATO Partnership for Peace (NATO/PfP) das Partnerschaftsziel »Cyber Defence« angenommen. Die diesbezüglichen Vorgaben für 2014 konnten allesamt erfüllt werden.

Zusätzlich verstärkte sich die Zusammenarbeit mit der NATO im Bereich der Cyber Defence durch die Beschickung und Mitarbeit eines Offiziers des Bundesministeriums für Landesverteidigung und Sport (BMLVS) im »**Cooperative Cyber Defence Center of Excellence« in Tallinn / Estland** seit Oktober 2013.

2.4 OSZE

Die Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) setzt seit 2013 eine Reihe von vertrauensbildenden Maßnahmen im Bereich der Cyber Sicherheit um. Unter anderem haben die 57 Teilnehmerstaaten 2014 begonnen, sich durch einen strukturierten und transparenten **Austausch von Informationen im Bereich der Sicherheit von Informations- und Kommunikationstechnologie** gegenseitig über Entwicklungen und Probleme auf dem Laufenden zu halten. Die Teilnehmerstaaten richteten Kontaktstellen für den Dialog ein und tauschten Informationen über die nationale Organisation von Cyber Sicherheitsplänen, sowohl im staatlichen als auch im privaten Bereich, aus.

Durch die Schaffung **vermehrter Transparenz** sowie durch die **Vernetzung und Zusammenarbeit** nationaler Expertinnen und Experten soll das Vertrauen der Teilnehmerstaaten unterei-

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

nander gestärkt werden. Für den Krisen- und Konfliktfall sollen gegenseitig Ansprechstellen genannt und zur Verfügung gestellt werden. Für Österreich stehen dabei die Sicherheit und die Freiheit des Internets, der freien Meinungsäußerung aber auch der vor Überwachung geschützten Privatsphäre im Vordergrund.

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 Security und Privacy** Analysen und High Level Empfehlungen erstellt. Dabei werden Trends beobachtet und analysiert, Erfahrungen ausgetauscht, Besonderheiten einzelner Länder thematisiert und schließlich Empfehlungen und Strategievorschläge für Politik, Wirtschaft und Bürger erstellt. Zweimal im Jahr treffen sich dazu Cyber und Privacy Experten aus den OECD Ländern um die Vorschläge zu diskutieren und Informationen auszutauschen. In Österreich nimmt das BKA die koordinative Tätigkeit für diese Gruppe wahr.

2.6 Österreich in anderen Cyber-relevanten internationalen Foren

2.6.1 Freedom Online Coalition

Die »Freedom Online Coalition« ist eine von den Niederlanden im Dezember 2011 gegründete Koalition, die sich weltweit für die **effektive Umsetzung der Menschenrechte online** in unterschiedlichen Foren einsetzt. Zu diesem Zweck haben die Mitglieder der Koalition eine enge Zusammenarbeit auf diplomatischer Ebene (in bi-/multilateralen und multi-stakeholder Foren), mit der Zivilgesellschaft und mit der Wirtschaft, insbesondere im Bereich Informations- und Telekommunikationstechnologie, vereinbart. Österreich ist Gründungsmitglied dieser Koalition gleichgesinnter Staaten, der derzeit 24 Mitglieder angehören. Die vierte Freedom Online-Konferenz, an der auch Österreich teilnahm, fand am 28./29. April 2014 in Tallinn statt. Neben Einschränkungen der Internet-Freiheit durch Russland und die Türkei war die Konferenzdebatte durch die NSA-Affäre und von den vom FOC-Mitglied USA gesetzten Reformmaßnahmen geprägt.

2.6.2 Central European Cyber Security Platform

Diese **Kooperationsplattform** der Länder (und der CERTs/tlw. milCERTs) **der Visegrad-Staaten** (Ungarn, Tschechien, Slowakei und Polen) **und Österreich** wurde im Jahr 2013 in Prag ins Leben gerufen und soll zum Austausch von Informationen zwischen den Mitgliedsstaaten dienen. Im Jahr 2014 hatte Österreich den Vorsitz dieser Initiative inne, wobei die Vorbereitungen zwischen dem Bundesministerium für Inneres (BM.I), dem BMLVS und dem BKA eng koordiniert wurden. Vom 8. bis 10. April 2014 fand dazu eine erste Konferenz für den Austausch aller Mitgliedsstaaten und aller CERTs der Mitgliedstaaten in Wien statt. Im Rahmen dieses Zusammentreffens wurde – neben der Abstimmung der Positionen zu z. B. EU und NATO – auch eine gemeinsame Deklaration verabschiedet. Diese wurde im Rahmen der letzten Meetings dieser Gruppe als Grundlagenentwurf für eine weitere Zusammenarbeit erarbeitet.

2.6.3 Global Conference on Cyberspace

Die Global Conference on Cyberspace ist die wichtigste Konferenz im Bereich **Cyber Diplomatie**. Sie setzt den auf der ersten Cyber Konferenz in London 2011 initiierten London Process (Cyber Space als politische Herausforderung, die eine Diskussion auf hoher Ebene im Rahmen eines umfassenden, strategischen Ansatzes erforderlich macht) fort, und baut auf dem in der Seoul Konferenz 2013 etablierten **Seoul Framework** (Wirtschaftswachstum und sozialer Nutzen, Cyber Kriminalität, Cyber Sicherheit, Internationaler Frieden und Sicherheit sowie Capacity Building) auf. Die nächste Konferenz findet in Den Haag vom 16.–17. April 2015 statt.

Weitere für Österreich relevante Aktivitäten im Cyber Bereich finden im Rahmen der UNESCO, des Europarates, des Ausschusses für Entwicklungshilfe in der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung sowie im Rahmen von INTERPOL statt.

2.7 Nationalstaaten

2.7.1 Vereinigte Staaten von Amerika

Im Nationalen Sicherheitsrat (Weißes Haus) wurde die Funktion eines **Sonderbeauftragten für die Planung und Entwicklung der nationalen Strategie für Cyber Sicherheit** eingerichtet (Special Assistant to the President and Cybersecurity Coordinator Michael Daniel). Dieser ist neben der Koordinierung der Ressorts auch für die Zusammenarbeit mit den anderen Gebietskörperschaften, Unternehmen und NGOs zuständig. Für die Abwehr von Angriffen auf die inländische IKT-Infrastruktur ist das Heimatschutzministerium zuständig, wo eine entsprechende Abteilung besteht (Office of Cybersecurity and Communications).

Ermittlungen bei Vorliegen von Angriffen werden vom Federal Bureau of Investigation (FBI, nachgeordnete Dienststelle des Justizministeriums) durchgeführt. Im Bereich der militärischen Verteidigung besteht ein United States Cyber Command als nachgeordnetes Kommando des US Strategic Command. Daneben befasst sich auch die National Security Agency (NSA) mit Cyber Sicherheit. Im jüngsten Budgetentwurf des Präsidenten sind für das Fiskaljahr 2016 (ab. 1. Okt. 2015) in Summe Aufwendungen in Höhe von USD 14 Mrd. für Cyber Sicherheit vorgeschlagen.

2014 setzten die USA zahlreiche Maßnahmen, um die Cyber Sicherheit sowohl national als auch international weiter zu erhöhen. Wie auch 2013 war die Kooperation zwischen öffentlichen und privaten Stellen ein wesentliches Thema. Trotz intensiver Bemühungen ist es der US-Regierung aber noch nicht gelungen, die Zusammenarbeit zwischen dem zivilen und dem staatlichen Bereich tatsächlich gesetzlich umfassend zu regeln. Das Weiße Haus veröffentlichte im Februar 2014 die vom National Institute of Standards and Technology ausgearbeiteten **Cyber Sicherheitsstandards für die Industrie**. Dieses »Cybersecurity Framework 2.0« beinhaltet freiwillig zu adaptierende Richtlinien. Außerdem unterzeichnete Präsident Obama Ende des Jahres fünf Cyber Sicherheitsgesetze für die öffentliche Verwaltung.

2014 wurde das Cyber Budget der Streitkräften im Vergleich zu 2013 um fast 30 % erhöht. Die im März 2014 veröffentlichte Quadrennial Defense Review spiegelte die zunehmende Fokussierung der US-Streitkräfte auf Technologie wider, im Oktober veröffentlichte das Pentagon zudem eine Cyber Doktrin. Zentrale Themen der US-Streitkräfte 2014 waren der Erhalt von Humankapital, die Entwicklung eigener Laufbahnbilder für Cyber Soldaten und die Aufstellung einer eigenen Truppengattung Cyber in der US Army.

Zentrale Eckpunkte der internationalen Bemühungen der USA sind die Erarbeitung von vertrauensbildenden Maßnahmen, die Anwendbarkeit des internationalen Rechts und der Schutz von Menschenrechten im Cyber Raum, der Aufbau von Cyber Fähigkeiten in Drittstaaten und der multi-stakeholder Ansatz zu Internet Governance.

2.7.2 Russische Föderation

Bereits im Jahr 2000 unterzeichnete Präsident Putin die **Informationssicherheitsdoktrin der Russischen Föderation (RF)**, die bis heute gültig ist. Anfang 2015 hat der Nationale Sicherheitsrat angeregt, die Informationssicherheitsdoktrin zu überarbeiten. Die RF vertritt den Standpunkt, dass eine starke Kontrolle über die nationalen IKT-Infrastrukturen sowie ein internationales Abkommen zur Regulierung des Internets notwendig seien. Die RF ist auch bemüht, den **nationalen Informationsraum besser zu kontrollieren**. Eine Reihe an restriktiven Gesetzen haben in den letzten Jahren die Befugnisse der Generalstaatsanwaltschaft und der Medienaufsichtsbehörde Roskomnadzor (föderaler Dienst für die Aufsicht im Bereich der Telekommunikation, Informationstechnologie und Massenkommunikation) zur Blockierung oder Löschung von Websites ausgeweitet. So erließ man z. B. im März 2013 ein Gesetz, welches das Blocken von Internetseiten mit »gefährlichem Inhalt für Kinder« vorsieht. Im Dezember 2013 wurde durch eine weitere Gesetzesverschärfung das Blocken von Internetseiten ermöglicht, die extremistische Inhalte bzw. Informationen über nicht genehmigte Protestaktionen verbreiten. Seit August 2014 fallen Blogger, die täglich mehr als 3.000 Zugriffe auf ihre Seiten bekommen, in dieselbe Kategorie wie Massenmedien und müssen den Behörden gegenüber entsprechend detaillierte Informationen offenlegen. Mitte 2014 wurde ein weiteres Gesetz zur besseren Kontrolle über das Internet verabschiedet: Ausländische Unternehmen, die Daten russischer Nutzer sammeln (wie Google, Facebook, Twitter) müssen diese künftig auf Servern in der RF speichern. Roskomnadzor ist laut Gesetz bevollmächtigt, den Zugang zu Online-Diensten wie Yahoo, Google etc. über die Internetprovider einschränken zu lassen, wenn die Speicherung von personenbezogenen Daten innerhalb des Landes nicht sichergestellt werden kann.

National ist der Inlandsnachrichtendienst FSB im Bereich Cyber Sicherheit federführend. Um Cyber Angriffe möglichst frühzeitig zu erkennen, beauftragte Präsident Putin im Oktober 2013 den FSB, seine Fähigkeiten zur Überwachung von IKT-Netzen auszubauen.

In den russischen Streitkräften wurde 2014 der Ausbau von Cyber Fähigkeiten weiter vorangetrieben. So wurden Mitte Oktober 2014 in den strategischen Raketentruppen eigene Einheiten zur Erkennung und Frühwarnung von Cyber Angriffen gebildet. Kurz darauf erklärte der russische Verteidigungsminister Sergei Shoigu, dass Russland in den nächsten Jahren ca. 440 Mio. € für die Aufstellung von zusätzlichen Cyber Einheiten in den Streitkräften investieren würde. Im Anfang Dezember eröffneten nationalen Kontrollzentrum des Verteidigungsministeriums werden auch Aspekte der Cyber Verteidigung bzw. Cyber Kriegsführung bearbeitet.

Auf internationaler Ebene strebte Russland **Kooperationsabkommen mit internationalen Partnern** an. So wurde im April 2014 ein Abkommen zur Kooperation im militärtechnischen Bereich mit Ecuador abgeschlossen, das einen Erfahrungsaustausch bei der Cyber Verteidigungsausbildung vorsieht. Auch mit China wurde 2014 eine Reihe von Kooperationsabkommen im IT-Bereich abgeschlossen. Auf multilateraler Ebene verfolgte Russland weiterhin den Ansatz der supranationalen Kontrolle des Internets mit einem festgelegten Verhaltenskodex.

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. Die Rolle der Kommunistischen Partei (KP) wurde

im August 2014 mittels Umwandlung des Staatlichen Internet Informationsbüros in eine Abteilung der Partei, die »Cyberspace Administration of China«, aufgewertet. Diese ist für die Ausarbeitung neuer Gesetze und Regulierung sowie die Überwachung des Internets zuständig. Unter ihrer Führung wird eine **nationale Strategie für die Entwicklung des Internets und zur Cyber Sicherheit** ausgearbeitet. Präsident und KP-Vorsitzender Xi Jinping leitet darüber hinaus die im Februar 2014 gegründete »Leading Small Group on Cyber Security and Internet Managment«, die auf höchster Ebene Direktiven für die Bekämpfung von Cyber Straftaten und Cyber Terrorismus gibt.

Die Kontrolle aller Aspekte des Internets wird laufend intensiviert, zahlreiche ausländische Webseiten etwa von Medien, Social Media und Suchdiensten, sowie inländische Social-Media-Accounts werden blockiert bzw. zensuriert. Seit dem Start einer Kampagne zur »Förderung der Cyber-Sicherheit« 2011 wurden rund 30.000 Personen wegen Online-Aktivitäten verurteilt. Seit 2013 drohen wegen »Verbreitung von Gerüchten online« (die mehr als 5.000mal angeklickt werden oder mehr als 500mal wiedergepostet werden) bis zu 3-jährige Haftstrafen.

Ende August 2014 beauftragte Präsident Xi die militärische Führung des Landes mit der Ausarbeitung einer **Strategie zur Informationskriegsführung**.

Auf internationaler Ebene verfolgt China einen ähnlichen Ansatz wie die RF. So befürwortet China ebenfalls das weltweite Internet unter die Kontrolle einer internationalen Institution wie der International Telecommunications Union (ITU) der VN zu stellen. Weiters bemühte sich China 2014 sowohl bi- als auch multilaterale Kooperationen im Cyber Raum einzugehen bzw. auszubauen, u. a. mit der EU.

2.7.4 Deutschland

Im Februar 2011 beschloss das Bundeskabinett die »**Cyber Sicherheitsstrategie für Deutschland**«. Ziel der Strategie ist es, Cyber Sicherheit auf einem der Bedeutung und der Schutzwürdigkeit der vernetzen Informationsinfrastrukturen angemessenen Niveau zu gewährleisten, ohne die Chancen und den Nutzen des Cyber Raums zu beeinträchtigen.

Für die Umsetzung der nationalen Cyberstrategie sind im Wesentlichen zwei Ministerien verantwortlich. Das Bundesministerium des Innern, hier v. a. das nachgeordnete Bundesamt für Sicherheit in der Informationstechnik (BSI), ist für die Veröffentlichung von Leitfäden und Richtlinien zu Schutzmaßnahmen für den privaten Sektor zuständig. Unter der Federführung des BSI bilden das Bundesamt für Verfassungsschutz, das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, das Bundeskriminalamt, die Bundespolizei, das Zollkriminalamt, der Bundesnachrichtendienst und die Bundeswehr das nationale Cyber Abwehrzentrum. In diesem Zentrum werden alle Informationen zu Cyber Angriffen, welche diese Behörden im Rahmen ihrer Zuständigkeiten eruieren, zusammengeführt. So bewertet das BSI einen Cyber Angriff aus technischer Sicht, das Bundesamt für Verfassungsschutz befasst sich mit der Frage, ob der Angriff möglicherweise von einem ausländischen Nachrichtendienst ausgegangen ist und das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe bewertet die Auswirkungen von möglichen Angriffen auf Infrastrukturen.

Zur sichtbaren Stärkung der Zusammenarbeit innerhalb der Bundesregierung sowie zwischen Staat und Wirtschaft wurde ein **Cyber Sicherheitsrat** eingerichtet. Aufgabe dieses Rates ist es, auf der politisch-strategischen Ebene zwischen Staat und Wirtschaft die präventiven Instrumente und die übergreifenden Politikansätze für Cyber Sicherheit zu betrachten.

Im Dezember 2014 verabschiedete das Bundeskabinett den »Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme« (kurz »**IT-Sicherheitsgesetz**«). Die wesentlichen Punkte dieses Gesetzes sind die verpflichtende Meldung von erheblichen IT-Sicherheitsvorfällen an den Staat, die Verbesserung des Schutzes der in den Kritischen Infrastrukturen eingesetzten IT und eine Stärkung der Aufgaben und Kompetenzen des BSI.

Das zweite wesentliche Ministerium im Kontext der Cyber Sicherheit ist das Bundesministerium der Verteidigung, wo insbesondere das Kommando Strategische Aufklärung für Cyber Angelegenheiten zuständig ist. Neben den beiden Ministerien nimmt der Bundesnachrichtendienst ebenfalls eine wichtige Rolle im Cyber Sicherheitsbereich ein. Er ist hauptsächlich für die Erstellung eines umfassenden Cyber Lagebildes verantwortlich.

Darüber hinaus wurde 2013 im Auswärtigen Amt ein eigener **Sonderbeauftragter für Cyber Außenpolitik** samt Arbeitsstab eingesetzt. Er soll auf internationaler Ebene die deutschen Cyber Interessen vertreten.

2.7.5 Vereinigtes Königreich

2009 wurde im **Cabinet Office das Büro für Cyber Sicherheit** eingerichtet. Dieses Büro veröffentlichte 2011 die **Nationale Cyber Sicherheitsstrategie**, die als wesentliche Eckpunkte den Schutz der Wirtschaft und der Kritischen Infrastrukturen sowie die Bekämpfung von Cyber Kriminalität beinhaltet. Zur Umsetzung der Strategie stehen für das Nationale Cyber Sicherheitsprogramm des Cabinet Office insgesamt ca. 1,16 Mrd. Euro bis 2016 zur Verfügung. Auch die Streitkräfte und Nachrichtendienste (insb. das Government Communications Headquarter) bauen ihre Cyber Fähigkeiten aus. Im Rahmen der National Crime Agency wurde die National Cyber Crime Unit eingerichtet. Im Mai 2013 stellte das Verteidigungsministerium eine »Cyber Reserve« auf. Im Dezember 2014 wurde der zweite nationale Fortschrittsbericht veröffentlicht sowie der zweite Cyber Security Governance Health Check durchgeführt. Auf internationaler Ebene verstärkt das Vereinigte Königreich Partnerschaften wie z. B. mit dem Europarat oder der Organisation Amerikanischer Staaten zur Stärkung der internationalen Ressourcen zur Bekämpfung von Cyber Kriminalität insbesondere zur grenzüberschreitenden Strafverfolgung, inklusive zusätzlicher Unterstützung von Europol und Interpol.

Im Juni 2014 z. B. wurde das Vereinigte Königreich Vollmitglied des NATO Cooperative Cyber Defense Centre of Excellence, im gleichen Monat wurde das 50. Treffen der Internet Cooperation for Assigned Names and Numbers mit 3.000 Teilnehmern in London abgehalten.

2.7.6 Frankreich

Anfang 2014 veröffentlichte die zentrale Stelle für die Koordination von Cyber Angelegenheiten in Frankreich, die »Agence Nationale de la Sécurité des Systèmes d'Information«, zwei Berichte zur Erhöhung der Cyber Sicherheit der Industriekontrollsysteme. Diese Berichte wurden in Zusammenarbeit mit dem Privatsektor erarbeitet.

Im Jänner 2014 kündigte Verteidigungsminister Jean-Yves Le Drian eine geplante Investition von ca. 1 Mrd. € über 5 Jahre in Cyber Verteidigungsmaßnahmen an. Ein Monat später veröffentlichte das Verteidigungsministerium das Dokument »**Pacte Défense Cyber**« worin Maßnahmen zur Steigerung der Cyber Sicherheit in den Streitkräften erläutert werden. Im Oktober 2014 wurde von Le Drian ein **Kompetenzzentrum für Cyber Verteidigung** in Bruz eröffnet. Dort sollen bis 2017 rund 250 Techniker ein »centre d'excellence« im Cyber Bereich bilden.

2.7.7 Niederlande

Die Niederlande veröffentlichte 2013 eine aktualisierte Version seiner Cyber Security Strategie. Das nationale Cybersicherheitszentrum betreibt neben einer durchgehend erreichbaren Cyber Security Assistance ein umfangreiches Sensornetzwerk, welches zur Analyse und Aufklärung von Cyber Security Fragen und Vorfällen beitragen soll.

Ende 2014 veröffentlichte das Cybersicherheitszentrum zudem seinen alljährlichen Bericht über die Cyber Sicherheitslage in den Niederlanden (»Cyber Security Assessment Netherlands«). Im Zuge einer steigenden Abhängigkeit von IKT in der Gesellschaft und den damit verbundenen Herausforderungen für Sicherheit und Schutz der Privatsphäre erkennt dieser Bericht u. a. die fortschreitende Entwicklung des sogenannten »Internet of Things«[8] sowie die Sammlung von »Big Data«[9] als wesentliche Herausforderungen für Cyber Sicherheit in naher Zukunft.

Aufgrund einer europäischen Vorreiterrolle der Niederlande und des NSCS in Angelegenheiten der Cyber Sicherheit erfolgte die Veröffentlichung dieses Berichtes unter hoher internationaler Beachtung.

2.7.8 Schweiz

Seit dem Jahr 2013 läuft in der Schweiz die Umsetzung der »**Nationalen Strategie zum Schutz der Schweiz vor Cyber Risiken**«. Die darin enthaltenen 16 Maßnahmen sollen bis 2017 dezentral von verschiedenen Bundesstellen, den Kantonen sowie den Betreibern kritischer Infrastruktur umgesetzt werden.

Die **Schweizer »Melde- und Analysestelle Informationssicherung«** ist für die Koordination der Umsetzung der Schweizer Cyber Security Strategie verantwortlich und übernimmt im operativen Bereich eine Leit- und Koordinationsfunktion.

2.7.9 Israel

Israel ist einer der führenden Cyber Sicherheitsanbieter weltweit. Seit Jahren sind israelische Netze im Fokus von staatlichen und nicht-staatlichen Cyber Angreifern. Vor allem während den regelmäßig aufflackernden regionalen Konflikten sind israelische Regierungsnetzwerke Ziel internationaler Hacktivisten. Aufgrund der konstanten Bedrohung bemüht sich Israel, einen ganzheitlichen Ansatz in der Cyber Verteidigung zu verfolgen. So gab Ministerpräsident Netanyahu im Rahmen einer Kabinettssitzung im September 2014 die **Schaffung einer nationalen Behörde für Cyber Defense** bekannt. Diese soll Sicherheitsbemühungen zwischen Regierung, Industrie und zivilen Bereichen koordinieren und damit sowohl militärische als auch zivile Schlüsseleinrichtungen vor Cyber Angriffen schützen.

Neben dem Aufbau von Cyber Sicherheitsstrukturen, sowohl auf ziviler als auch militärischer Seite, ist noch auf die besonders enge Kooperation zwischen dem privaten Sektor, hier v. a. den lokalen Cyber Sicherheitsanbietern und den israelischen Behörden, die für Cyber Sicherheit zuständig sind, hinzuweisen.

8 Verbindung unterschiedlicher Geräte mit dem Internet zur Bereitstellung zusätzlicher Funktionalität (z. B. Fernseher, Auto).

9 Sammlung großer Mengen von Daten, z. B. zur Erstellung von statistischen Prognosen oder Benutzerprofilen für zielgerichtete Werbung.

3 Nationale Entwicklungen

3.1 Akteure und Strukturen

3.1.1 Operative Strukturen

Von der Bundesregierung wurde im März 2013 die Österreichische Strategie für Cyber Sicherheit (ÖSCS) beschlossen. Gemäß der ÖSCS ist aufbauend auf den bestehenden operativen Strukturen sowie unter deren Einbindung eine **Struktur zur Koordination auf der operativen Ebene** zu schaffen. Diese Struktur stellt den raschen **Austausch aktueller Informationen** über Cyber Sicherheitsvorfälle sicher und unterstützt die Umsetzung entsprechender Gegenmaßnahmen. Sie stellt außerdem das **Cyber Lagebild Österreich** bereit, unterstützt und koordiniert gesamtstaatliche Notfallmaßnahmen im Rahmen des **Cyber Krisenmanagements** (CKM) und leistet damit einen essentiellen Beitrag zur Erhöhung der Cyber Sicherheit in Österreich. Die operativen Strukturen binden einerseits die Ressorts mit Cyber Sicherheitsagenden (BKA, BM.I, BMLVS, BMEIA), andererseits operative Strukturen aus Wirtschaft und Forschung ein. Sie werden vom BM.I koordiniert, das dabei von den anderen Ressorts unterstützt wird. Im Cyber Defence Fall geht diese Zuständigkeit auf das BMLVS über.

Im Jahr 2014 wurden in interministeriellen Arbeitsgruppen die konzeptuellen Grundlagen für die Einrichtung der operativen Koordinierungsstruktur und des Cyber Krisenmanagements geschaffen. Mit der **operativen Koordinierungsstruktur** soll sichergestellt werden, dass

- eine zentrale Stelle jederzeit über den aktuellen Cyber Status in Österreich verfügt und entsprechende generelle Maßnahmen vorbereiten kann,
- eine zentrale Stelle zur Koordination aller Akteure bei größeren Vorfällen verfügbar ist,
- es eine klare Aufgaben- und Rollenverteilung zwischen Meldestellen und dem Koordinationsgremium gibt,
- dieselbe Information zur selben Zeit bei allen relevanten Akteuren vorliegt und dadurch gesamtstaatliche Synergieeffekte erzielt werden können,
- durch schnelle Reaktion rasche und nachhaltige Maßnahmen gesetzt werden können.

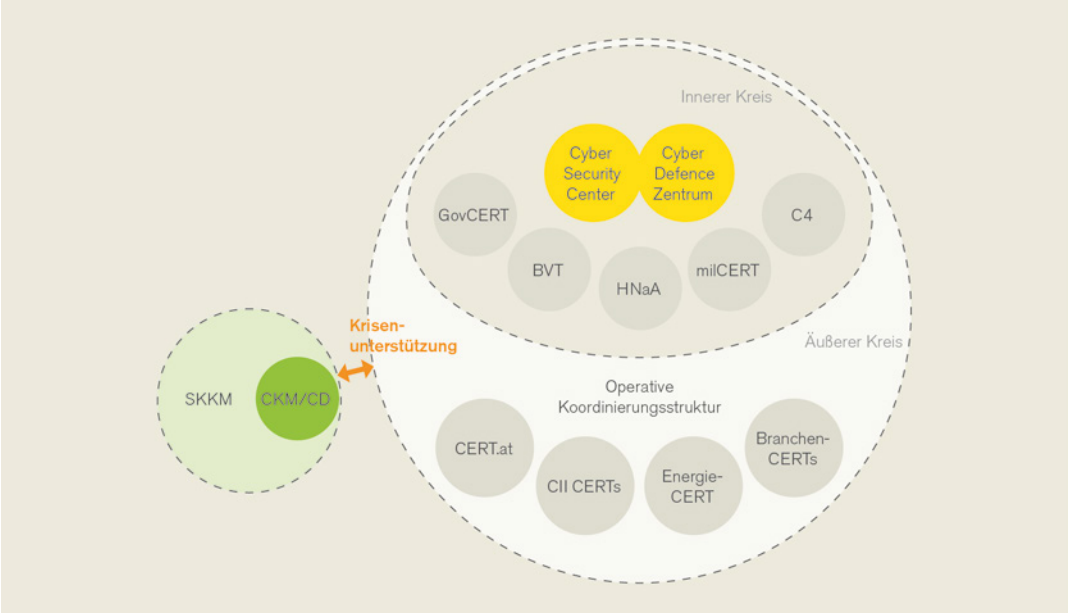

Abbildung 1: Operative Koordinierungsstruktur

Aus der fortschreitenden Umsetzung der ÖSCS erwuchs der Bedarf nach dem Aufbau sektorspezifischer CERTs (äußerer Kreis). Deren Rolle als Anlaufstelle für die Meldung von Cyber Vorfällen innerhalb individueller Sektoren wurde in den operativen Strukturen institutionalisiert. Ihre Aufgabe besteht in der Aufnahme von Vorfällen und damit verbundener Informationen aus den jeweiligen Sektoren und der Weiterleitung dieser Daten in anonymisierter Form an die koordinierende Stelle (**Cyber Security Center – CSC / Cyber Defence Zentrum – CDZ**). Weiters fungieren die CERTs innerhalb der Sektoren als Kommunikationsdrehscheiben und nach außen als Kontaktstellen (Single Points of Contact).

Als erstes sogenanntes »Branchen-CERT« konnte während der Cyber Übung »CE.AT 2014« erstmals die Rolle eines Energie-CERTs erfolgreich getestet werden. Diese Entwicklung wird von den hauptverantwortlichen Ressorts (innerer Kreis) unterstützt, es ist zu erwarten, dass aufgrund der Umsetzung der ÖSCS und durch den Ausbau des CERT-Verbunds weitere solche »Branchen-CERTs« dem Energie-CERT folgen werden.

Die operative Koordination sieht vor, dass die Betreiber von kritischen Infrastrukturen insbesondere bei Störungen im Bereich der Informations- und Kommunikationsstrukturen auf operativer Ebene unterstützt werden. Ausgehend von dieser in der ÖSCS vorgesehenen Unterstützung bei der Krisenbewältigung ergibt sich das folgende **Eskalationsszenario Cyber Sicherheit:**

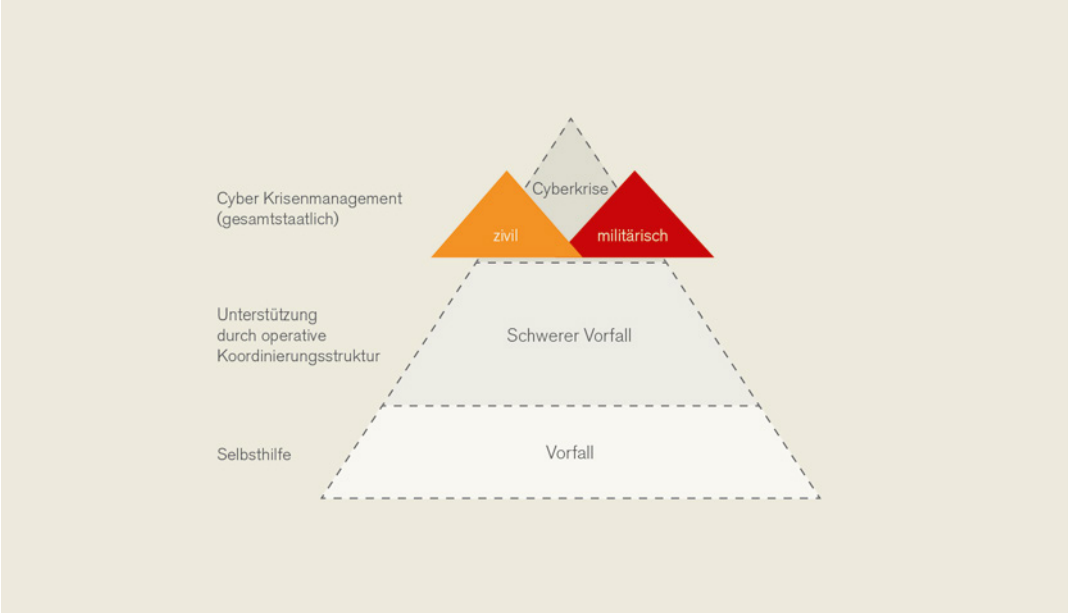

Abbildung 2: Eskalationsszenario Cyber Sicherheit

Die Mechanismen des CKM sollen sich eng an die bereits erprobten Abläufe des Staatlichen Krisen- und Katastrophenschutzmanagements (SKKM) anlehnen. Die Auslösung erfolgt somit durch den Vorsitzenden des CKM nach vorherigen Konsultationen mit den Kernressorts des CKM.

3.1.2 GovCERT und CERT.at

GovCERT ist das **nationale CERT** (Computer Emergency Response Team) **der öffentlichen Verwaltung** und ist Teil des inneren Kreises der operativen Koordinierungsstrukturen. Als österreichischer Cyber Security Point-of-Contact (PoC) ist das GovCERT mit internationalen Organisationen und Ansprechpartnern wie der European GovCERT Group oder der Central European Cyber Security Plattform vernetzt. Zur Wahrnehmung seiner Aufgaben arbeitet das GovCERT eng mit dem österreichischen CERT (CERT.at) in Form einer Public-Private-Partnership zusammen. CERT.at übernimmt dabei operative Aufgaben des GovCERT.

CERT.at und GovCERT bieten im Anlassfall auch Hilfe vor Ort – unbürokratisch und ohne weitere Kosten. 2014 kam es beispielsweise zu einem Einsatz bei einem Unternehmen aus dem Energie-Sektor. Hier wurden die Experten von CERT.at/GovCERT um Unterstützung gebeten, nachdem von externer Seite ein Einbruch auf einem Server festgestellt wurde. Gemeinsam mit dem betroffenen Unternehmen konnte sichergestellt werden, dass der Server-Einbruch keine weiteren Auswirkungen auf andere Systeme hatte, und auch nicht versucht wurde, durch diesen Server Schaden auf anderen Systemen anzurichten. Weiters wurde auch gemeinsam eine Strategie für Medienkommunikation und PR-Arbeit ausgearbeitet, da auch hier die Erfahrungen aus mehreren Vorfällen in der Vergangenheit wertvollen Input lieferten.

GovCERT und CERT.at präsentierten am 15.1.2015 gemeinsam den »Jahresbericht Internet-Sicherheit Österreich 2014«.

3.1.3 CERT-Verbund

Der CERT-Verbund wurde 2011 als **Kooperation österreichischer CERTs** sowohl **aus öffentlichen wie auch privaten Sektoren** gegründet. Ziel ist die Bündelung der verfügbaren Kräfte und die optimale Nutzung des gemeinsamen Know-hows zur Gewährleistung einer bestmöglichen

IKT-Sicherheit. Mitglieder des CERT-Verbunds sind: A1-CERT, ACOnet-CERT, BRZ CERT, CERT.at, GovCERT, milCERT, R-IT CERT, Wien CERT.

Themen 2014 waren neben dem gegenseitigen operativen Informations- und Erfahrungsaustausch die zukünftige Ausrichtung des CERT Verbundes, die Umsetzung der ÖSCS, rechtliche Herausforderungen von CERTs, die neue österreichische Cyber Architektur, Information Sharing, Cyber Exercises, Cyber Entwicklungen im nationalen und internationalen Umfeld, laufende Berichte und Diskussionen von Ereignissen sowie Cyber Veranstaltungen und Publikationen.

3.1.4 milCERT

Das militärische Computer Emergency Response Team (milCERT) wird durch das Abwehramt und das Führungsunterstützungszentrum des BMLVS betrieben. Es ist aktuell primär für BMVLS-interne Aufgabenstellungen aufgestellt, von der Struktur jedoch prozessorientiert zur **Erfüllung von gesamtstaatlichen Aufgaben des BMLVS/ÖBH** vorbereitet.

Zu seinen militärischen Hauptaufgaben zählen u. a.:

- Ausarbeitung periodischer und anlassbezogener operativer Cyber Lagebilder sowie Beitrag zur Erstellung des Lagebildes Cyber Sicherheit,
- Evaluierung von Angriffs- und Verteidigungstechnologien und Erstellung resultierender konzeptioneller Empfehlungen,
- Durchführung technischer und organisatorischer Sicherheitsüberprüfungen,
- Penetration Testing[10] und Sicherheitsaudits von Anwendungen und Systemen,
- Statische und dynamische Code-Analyse bei möglichen Schadcodeuntersuchungen und Erarbeitung von Gegenmaßnahmen,
- Entwicklung umfangreicher Sicherheitseinrichtungen in den Bereichen Netzwerke, Server und Endgeräte,
- Reaktion auf und Behandlung von IT-Sicherheitsvorfällen,
- Ausarbeitung und Umsetzung von Cyber Defence Maßnahmen.

Das milCERT zielt primär auf die proaktive und vorzeitige Erkennung und Erforschung von Schwachstellen und Verwundbarkeiten von IKT-Systemen ab. Dies mit dem Ziel, bereits vor Eintreten von Sicherheitsproblemen und konkreten Bedrohungen die Risiken zu minimieren und Schwachstellen vorab entgegentreten zu können.

3.1.5 Heeresnachrichtenamt

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

3.1.6 Cyber Crime Competence Center

Das Cyber Crime Competence Center (C4) des BM.I ist die **nationale Koordinierungs- und Meldestelle zur Bekämpfung der Cyber Kriminalität.** Das Zentrum setzt sich aus technisch und fachlich hochspezialisierten Expertinnen und Experten des Bundeskriminalamtes zusammen. Im Jahr 2014 konnte der organisatorische und technische Aufbau abgeschlossen werden. Die

10 Überprüfung auf potentielle Sicherheitsrisiken

Umsetzung des Personal- und Raumkonzeptes ist für 2015/2016 geplant. Um auf dem Stand der Technik und damit im hoch innovativen technischen Umfeld schlagkräftig zu bleiben, wird der weitere Ausbau und die Stärkung des C4 im Rahmen der Umsetzung der ÖSCS sowie der Cyber Sicherheitsstrategie des BM.I erfolgen.

3.1.7 Cyber Sicherheit Plattform

Das Handlungsfeld 3 der ÖSCS beschreibt die Kooperation zwischen Verwaltung, Wirtschaft und Gesellschaft. Eine der wesentlichsten Maßnahmen aus diesem Feld ist die Implementierung einer nationalen **Austauschplattform zwischen Wirtschaft, Wissenschaft und Verwaltung.** Durch die **Cyber Sicherheit Plattform** (CSP) soll der Erfahrungs- und Informationsaustausch im Bereich Cyber Sicherheit weiter intensiviert werden. Zusätzlich wird die Plattform ein **Dach für bereits bestehende Kooperationsformate** im Bereich der Cyber Sicherheit bilden. Darüber hinaus wird die Cyber Sicherheit Steuerungsgruppe (CSS) in strategischen Fragen der Cyber Sicherheit beraten und unterstützen.

Konzept und Geschäftsordnung für die Cyber Sicherheit Plattform wurden im Jahr 2014 durch die CSSe beschlossen. Nach der im März 2015 erfolgten Konstituierung der Plattform wird diese im Laufe des Jahres 2015 ihre Arbeit aufnehmen.

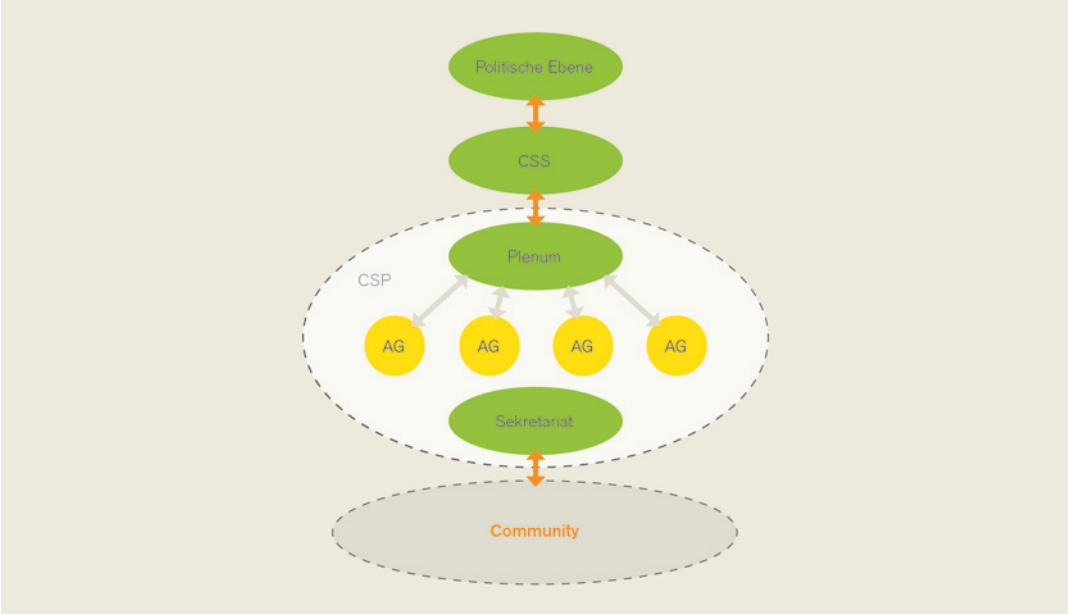

Abbildung 3: Cyber Sicherheit Plattform

3.1.8 Austrian Trust Circle

Der 2010 gegründete Austrian Trust Circle (ATC) ist eine **Initiative von CERT.at und dem BKA.** 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.

Vierteljährlich finden sektorspezifische Treffen des ATC statt, zu denen sich mittlerweile mehr als einhundert IT- und InformationssicherheitsexpertInnen einfinden, um neben Fach- und Impulsvorträgen den fachlichen Austausch mit KollegInnen aus der Branche zu pflegen. Einmal im Jahr findet zusätzlich ein sektorenübergreifendes Treffen statt. Die gebildete Vertrauensbasis innerhalb dieses Forums ermöglicht es, auch über Erfahrungen aus Sicherheitsvorfällen offen

zu diskutieren. Diese Form des (inter)sektoriellen Austauschs bietet somit eine einzigartige Möglichkeit, Einblicke in die Arbeitsweisen, Denkweisen und Herausforderungen der einzelnen Sektoren zu bekommen um dabei Gemeinsamkeiten aller Sektoren zu identifizieren und die Zusammenarbeit zu fördern.

3.1.9 IKT-Sicherheitsportal

Das IKT-Sicherheitsportal 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.

2014 umfassten die Aktivitäten auf dem IKT-Sicherheitsportal insgesamt die Verfassung von 217 Newsartikeln, 98 Publikationseinträgen, 32 Veranstaltungseinträgen, 10 Fachartikeln und vier Online Ratgebern.

3.2 Umsetzung ÖSCS

Die Umsetzung der in der ÖSCS aufgelisteten Maßnahmen zur Erhöhung der nationalen Cyber Sicherheit werden durch die CSS koordiniert. Basis für die Umsetzung stellt ein **Implementierungsplan** dar, welcher im Juni 2013 durch die CSS beschlossen wurde und seitdem laufend aktualisiert wird.

Im Laufe des Jahres 2014 wurden die Arbeiten an den im Jahr 2013 beschlossenen prioritären Umsetzungsprojekten weitgehend abgeschlossen und von der CSS genehmigt:

- Prozesse und Strukturen zur **permanenten Koordination auf der operativen Ebene** (operative Koordinierungsstruktur)
- **Konzept Cyber Krisenmanagement** (inkl. Cyber Defence)
- **Konzept und Geschäftsordnung** für die **Cyber Sicherheit Plattform**
- Abschlussbericht der Arbeitsgruppe **Cyber Sicherheit Kommunikationsstrategie**
- Zwischenergebnisse der Arbeitsgruppe **ordnungspolitischer Rahmen**.

Im ersten Halbjahr 2015 wird die CSS der Bundesregierung einen Umsetzungsbericht zur ÖSCS vorlegen.

4 Cyber Übungen

4.1 Nationale Cyber Übung »CE.AT 2014«

Bereits seit 2010 führt Österreich alle zwei Jahre erfolgreich unter der Federführung des BKA eine nationale **Cyber Übung »CE.AT (Cyber Europe Austria)**« durch. Diese ist ein Ableger der internationalen ENISA-Übung »Cyber Europe« (CE). 2012 und 2014 erfolgte die nationale Teilnahme über eine Schnittstelle zur internationalen Übung »Cyber Europe«. 2014 baute sie auf deren Szenario (Bedrohung des Energiesektors durch politisch motivierte Cyber Attacken) auf.

Die Ziele der internationalen Übung »CE 2014« waren unter anderem die **Überprüfung der standardisierten Kooperationsverfahren und -mechanismen**, um Cyber Krisen in Europa zu bewältigen, die Verbesserung der Fähigkeiten auf nationaler Ebene, sowie das Erkunden der bestehenden Zusammenarbeit zwischen dem privaten und öffentlichen Sektor. 2014 nahmen mehr als 200 Organisationen und 400 Cyber Sicherheitsexperten aus 26 EU und drei EFTA Staaten an der »CE 2014« teil, die in drei Phasen (technisch, operativ, strategisch) abgehalten wurde[11].

Für die erste, technische Phase der Übung (Technical Level Exercise) in Österreich konnte das BKA als planungsverantwortliche und koordinierende Institution Ende April 2014 sieben österreichische Teilnehmer aus Energiewirtschaft und öffentlicher Verwaltung für eine aktive Teilnahme gewinnen.

Die Teilnahme an der zweiten, operativen Phase der »Cyber Europe 2014« (Operational Level Exercise) fand am 30. Oktober 2014 in Form der nationalen Cyber Übung »CE.AT 2014« in Österreich statt. Diese war mit 29 teilnehmenden Organisationen aus den Bereichen öffentliche Verwaltung, Gas- und Stromwirtschaft sowie Internet Service Provider die größte sektorübergreifende Übung in Österreich bisher.[12]

Während der »CE.AT 2014« zeigte sich die Notwendigkeit einer umfangreichen Kooperation zwischen Wirtschaft und öffentlicher Verwaltung in der Bewältigung einer Cyber Krise. Diese wurde im Zuge der Übung durch den Vertrauensausbau zwischen den teilnehmenden Organisationen ermöglicht. Neben der guten Zusammenarbeit zeigte sich weiters, dass bei großen Vorfällen eine koordinierte Medienarbeit von hoher Bedeutung ist. Diese Koordination der Medienarbeit wurde während der Übung durch den Pressedienst des BKA wahrgenommen. Auch wurden im Rahmen der »CE.AT 2014« erstmals Teilaspekte der operativen Koordinierungsstrukturen, wie etwa Branchenmeldestellen und das Cyber Security Center, beübt.

Die »Cyber Europe 2014« wurde am 24. und 25.2. 2015 durch die dritte Phase (Strategic Level Exercise) abgeschlossen. Während dieser Phase erörterten die internationalen Teilnehmer in Form eines Workshops mögliche Maßnahmen und Handlungsempfehlungen zur besseren internationalen Zusammenarbeit auf strategisch-politischer Ebene während der Bewältigung einer internationalen Cyber Krise.

11 http://www.enisa.europa.eu/media/press-releases/cyber-europe-2014-findet-heute-statt
12 http://www.bundeskanzleramt.at/site/cob__57674/currentpage__1/7949/default.aspx

4.2 Übung der Central European Cyber Security Platform

Eine der ersten gemeinsamen Aktionen der Central European Cyber Security Platform (vgl. Kapitel 2.6.2) war im Juni 2014 eine Übung, die unter der Federführung Ungarns den Zweck hatte, bei regionalen Cyber Krisen die **Kooperation und die Kollaboration der beteiligten Staaten** zu testen. Die Ziele der Übung waren einerseits einander kennenzulernen und Vertrauen aufzubauen und andererseits mögliche Ansprechpartner für den Fall einer plötzlichen Krise zu haben. Weitere Ziele waren das Testen des Informationsaustauschs sowie von Tools und Methoden, das Experimentieren mit einem länderübergreifenden Krisenmanagement und das Ausprobieren des Starts und der Funktionalität einer Cyber Kollaboration.

Österreich beteiligte sich an der Übung mit einem technischen und juristischen Fokus. Die Ergebnisse der Übung wurden evaluiert und werden in den Aufbau einer länderübergreifenden CECSP Kommunikations-/Kollaborations-/Krisenmanagement Plattform einfließen.

4.3 NATO-Übung »Cyber Coalition 2014«

Seit 2008 führt die NATO jährlich eine Übungsserie mit dem Ziel durch, Entscheidungsprozesse, technische und operationelle Abläufe sowie die Zusammenarbeit zwischen den Teilnehmern zu üben. Österreich nahm unter Leitung des milCERT und mit Unterstützung des GovCERT an der Cyber Coalition 2014 teil. Die nationalen Experten konnten dabei eine im internationalen Vergleich hervorragende Leistung erbringen. Die österreichische Teilnahme an dieser Übung durch milCERT und GovCERT war auch durch Erreichung des **nationalen Ziels – Aufbau einer Notfall-Kommunikationsinfrastruktur zwischen milCERT und GovCERT** – erfolgreich.

Die Übung schaffte erneut Kenntnisgewinn über die benötigten Organisationsstrukturen und Abläufe, um Cyber Angriffe auf das österreichische Bundesheer entsprechend bearbeiten bzw. abwehren zu können und dient daher als wesentlicher Motor für den Fähigkeitenaufbau des milCERT. Der Zweck der Teilnahme lag weiters im Test und der **Verbesserung bestehender Cyber Defence Fähigkeiten**, der Kommunikation zwischen NATO und Partnern sowie der Partner untereinander, dem Test der Kommunikationslinien, der Ablauforganisation, der Bearbeitungsprozesse und der technischen Fähigkeiten sowie der Beobachtung der internationalen Entwicklungen im Fachbereich. Im Zuge des Vorhabens wurden erstmals Milizangehörige in die Übung eingebunden und zum wiederholten Male eine Notfallkommunikation durch die Streitkräfte bereitgestellt. Eine Einbindung staatlicher und privater Stakeholder wurde dieses Jahr ausgesetzt. Die bisherige Einbindung des GovCERT als einen der wichtigsten Partner blieb davon unbenommen und wird schon seit 2012 erfolgreich durchgeführt. Es konnten die wesentlichsten nationalen Übungsziele erreicht werden und die Erreichung der Ersten Einsatzbereitschaft des milCERT abermals bestätigt werden.

4.4 SCUDO-Übung

In allen Dingen hängt der Erfolg von den Vorbereitungen ab – dieser Leitsatz begleitete das Sicherheitsforschungsprojekt SCUDO (Schutzübung für Computerbasierte Unternehmensübergreifende Desaster Logistik) durch die gesamte Projektzeit. Im Rahmen des Sicherheitsforschungsprojektes war es das Ziel einen **Baukasten zur Vorbereitung, Durchführung und Evaluation von IT-getriebenen Notfallsübungen zu erstellen** und deren Wirksamkeit und Einsetzbarkeit zu erforschen. Der Erfolg des Projektes konnte in insgesamt sieben durchgeführten Übungen mit einzelnen Organisationen und 2014 einer groß angelegten Übung gemeinsam mit dem BKA, BMLVS, BM.I, CERT.at und Organisationen aus den auch im Rahmen des Austrian Trust Circle adressierten Sektoren gezeigt werden.

4.5 Combined Endeavor

Seit 1995 findet alljährlich die Übung Combined Endeavor unter der Leitung des United States European Command statt. Dabei handelt es sich um die größte **Interoperabilitätsübung für Führungsunterstützungskräfte** weltweit. Bis zu 43 verschiedene Nationen (darunter auch Österreich) und Organisationen aus Europa und Nordamerika nutzen dieses Umfeld um ihre Führungs- und Führungsunterstützungssysteme in verschiedenen multinationalen Einsatznetzwerken zum Einsatz zu bringen, zu testen und, aufbauend auf den Testergebnissen, weiter zu entwickeln. Im Jahr 2014 wurde die Übung um den Übungsbereich Cyber in einem eigenen Übungsumfeld »Cyber Endeavor« erweitert um so auch auf die aktuellen Bedrohungen reagieren zu können, welche sich aus dem hohen Vernetzungsgrad von IKT-Systemen und dem Bedarf an Information Sharing ergeben.

4.6 Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise (CWIX)

Der Zweck dieser im Juni 2014 in Polen stattgefundenen Übung liegt generell in der **Durchführung von technischen und operationellen Tests mit einsatzorientierten Systemen, Services und Applikationen** als Teil der Sicherstellung der Fähigkeit »Interoperabilität« in laufenden und zukünftigen internationalen Einsätzen. Der Cyber Bereich der CWIX 2014 hat im Vergleich zum vorigen Jahr stark an Bedeutung gewonnen. Sowohl die Beteiligung von anderen Nationen, als auch die Ziele der Cyber Focus Area wurden ambitionierter und leistungsfordernder. Die Rolle des Cyber Component Commander wurde durch Österreich unter Beteiligung des ungarischen Teams innerhalb des Szenarios bereitgestellt. Durch den Cyber Component Commander wurde auf Computer-Vorfälle reagiert, Angriffe erkannt und mitigiert.

Ziel der nationalen Teilnahme (vier Mitarbeiter des milCERT) war es, die Auswirkung von Cyber Bedrohungen auf Einsatzsysteme zu erforschen und zu testen. Dadurch konnten wesentliche Ableitungen für die Bewertung von Schutzmechanismen gegen Angriffe von innen und außen und den sicheren Betrieb von Führungsinformationssystemen gewonnen und gleichzeitig technisch auf tiefster Detailebene im internationalen Umfeld an Lösungen gearbeitet werden.

4.7 KSÖ Planspiel

Das »Kuratorium Sicheres Österreich (KSÖ)« veranstaltete heuer zum wiederholten Mal eine Cyber Übung. 12 Teilnehmer aus verschiedenen Sektoren der kritischen Infrastrukturen (darunter Finanzen, Transport und öffentliche Verwaltung) sowie CERT.at und CSC nahmen an diesem Planspiel teil, das sich nicht nur auf die technische Abwicklung, sondern auch auf die Kommunikation zu Medien und die rechtliche Beurteilung der gesetzten Aktionen konzentrierte. Im Rahmen des Planspiels wurde auch unter der Federführung des CSC ein Krisenlagebild unter Mitwirkung der beteiligten Unternehmen erstellt und präsentiert. Die Rückmeldungen aus dem Lagebildprozess sowie die Fragestellungen aus den Bereichen Recht und Kommunikation bilden eine wertvolle Grundlage für die weiteren Schritte beim Aufbau des CSC.

5 Zusammenfassung / Ausblick

Im Jahr 2014 hat sich der Trend hin zu einer signifikanten Steigerung von Aktivitäten vor allem in den Bereichen Cyber Spionage und Cyber Kriminalität fortgesetzt. Staatlich gesteuerte Cyber Spionage stand auch 2014 im öffentlichen Fokus.

Die Nutzung des Cyber Raumes für terroristische Aktivitäten, z. B. zum Zwecke der Radikalisierung und Rekrutierung hat sich 2014 insbesondere in den Propagandaaktivitäten des Islamischen Staates manifestiert. Soziale Medien wie Facebook oder Twitter spielen eine zunehmend wichtige Rolle in diesem Kontext.

Aktivitäten im Cyber Raum werden sich zunehmend nach der Form der Verarbeitung bzw. Speicherung der betroffenen Daten richten und sich somit in den nächsten Jahren vor allem auf Cloud-Dienste und Social Networks konzentrieren. Der stetige Zuwachs an mobiler Nutzung des Internets über Smartphones und Tablets wird diesen Trend verstärken.

Angriffe werden immer zielgerichteter gesetzt. Aufgrund einer erkennbaren »Erfolgsrate« für den Täter werden seitens aller Akteure, unabhängig von deren Motivation (Erlangung von finanziellen Mitteln, Beschaffung von Informationen, Schädigung eines Gegners in seiner Einsatzbereitschaft) künftig noch mehr Investitionen in Forschung und Entwicklung von zielgerichteten Angriffen erfolgen. Methoden und Mittel werden dazu weiterentwickelt und die Erforschung von Schwachstellen vorangetrieben. Es ist sowohl von einer quantitativen Steigerung von Angriffen, wie auch einer qualitativen Erhöhung der dafür eingesetzten Fähigkeiten auszugehen. Die Erkennung solcher Angriffe gestaltet sich nicht zuletzt aufgrund ihrer Individualität sowie der eingesetzten und teils hoch entwickelten Schadsoftware als überaus schwierig.

Angesichts dieser Entwicklungen sind ein geeigneter Schutz und die Zusammenarbeit für den Bereich der Informations- und Kommunikationstechnologie und der darin verarbeiteten Informationen von stark zunehmender Bedeutung. Umfassende Ansätze unter Einbindung staatlicher und nichtstaatlicher Akteure sind dabei unerlässlich. Breit angelegte und aufeinander abgestimmte technische sowie organisatorische Maßnahmen leisten einen wesentlichen Beitrag, Verarbeitungsanomalien zu identifizieren und passende Gegenmaßnahmen zu entwickeln.

Vor diesem Hintergrund haben sich die bereits 2013 aufgezeigten Trends zur Zentralisierung nationaler Cyber Security Steuerung und Koordination sowie das zunehmende Interesse von Regierungen an Cyber Angelegenheiten auch 2014 weiter fortgesetzt. Der vermehrten Einbindung des privaten Sektors in Cyber Sicherheitsangelegenheiten wird in diesem Kontext besondere Bedeutung beigemessen. International hält der Trend zur Kooperation auf bi- und multinationaler Ebene ebenfalls weiter an.

Die vorhandenen Aktivitäten und Strukturen in Österreich wurden 2014 in Einklang mit den Vorgaben aus der ÖSCS weiterentwickelt, wobei ein Schwergewicht auf die Vernetzung bestehender Aktivitäten und Strukturen gelegt wurde. Im den folgenden Jahren wird es darauf ankommen, die bestehenden und neu etablierten Strukturen, sowohl im öffentlichen als auch im nicht-öffentlichen Bereich, auf das gemeinsame Ziel der Steigerung der Sicherheit des Cyber Raumes hin auszurichten und zum bestmöglichen Zusammenwirken zu bringen.

Anlage A - Abkürzungsverzeichnis:

APT	Advanced Persistent Threat
ATC	Austrian Trust Circle
BKA	Bundeskanzleramt
BMEIA	Bundesministerium für Europa, Integration und Äußeres
BM.I	Bundesministerium für Inneres
BMLVS	Bundesministerium für Landesverteidigung und Sport
BMVIT	Bundesministerium für Verkehr, Innovation und Technologie
BSI	Bundesamt für Sicherheit in der Informationstechnik
C4	Cyber Crime Competence Center
CDZ	Cyber Defence Zentrum
CE	Cyber Europe
CERT	Computer Emergency Response Team
CKM	Cyber Krisenmanagement
CSC	Cyber Security Center
CSP	Cyber Sicherheit Plattform
CSS	Cyber Sicherheit Steuerungsgruppe
CSIRT	Computer Security Incident Response Team
ECSM	European Cyber Security Month
EK	Europäische Kommission
ENISA	European Network and Information Security Agency
EP	Europäisches Parlament
ER	Europäischer Rat
EU	Europäische Union
FBI	Federal Bureau of Investigation
GovCERT	Government Computer Emergency Response Team
GSVP	Gemeinsame Sicherheits- und Verteidigungspolitik
HNaA	Heeresnachrichtenamt
ITU	International Telecommunication Unit
KP	Kommunistische Partei
KSÖ	Kuratorium Sicheres Österreich
milCERT	militärisches Computer Emergency Response Team
NATO	Nordatlantische Vertragsorganisation
NGO	Nichtregierungsorganisation
NIS	Netz- und Informationssicherheit
NSA	National Security Agency
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
OSZE	Organisation für Sicherheit und Zusammenarbeit in Europa
ÖSCS	Österreichische Strategie für Cyber Sicherheit
PfP	Partnerschaft für den Frieden
SKKM	Staatliches Krisen- und Katastrophenschutzmanagement
VN-GV	Generalversammlung der Vereinten Nationen
WSIS	World Summit on the Information Society