REPUBLIK ÖSTERREICH

Bericht Cyber Sicherheit 2014

BUNDESKANZLERAMT ÖSTERREICH

Bundesministerium für europäische und internationale Angelegenheiten

BM.I REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR INNERES

Bundesministerium für Landesverteidigung und Sport

Impressum

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

Grafische Gestaltung: BKA | ARGE Grafik
Wien, Mai 2014

Inhalt

1 Einleitung **4**

2 Cyber Lage 2013 / Bedrohungsanalyse **5**

2.1 Akteure und deren Intentionen 5

2.2 Methoden 6

2.3 Schwachstellen 8

3 Internationale Entwicklungen **9**

3.1 Europäische Union 9

3.2 Vereinte Nationen 10

3.3 NATO 10

3.4 OSZE 11

3.5 Nationalstaaten 11

4 Nationale Entwicklungen **14**

4.1 Akteure und Strukturen 14

4.2 Umsetzung ÖSCS 16

5 Cyber Übungen **17**

5.1 NATO-Übung »Cyber Coalition 2013« 17

5.2 Combined Endeavor (CE) 17

5.3 Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise« (CWIX) 17

6 Zusammenfassung / Ausblick **18**

1 Einleitung

Die ÖSCS legt fest, dass durch die Cyber Sicherheit Steuerungsgruppe ein jährlicher Bericht Cyber Sicherheit erstellt wird. Der erste Bericht zur Cyber Sicherheit in Österreich soll bis Juni 2014 der Steuerungsgruppe vorgelegt werden. Durch die Steuerungsgruppe wird der Bericht den im Nationalen Sicherheitsrat vertretenen Mitgliedern der Bundesregierung und sonstigen thematisch involvierten Regierungsmitgliedern zur Kenntnis gebracht.

Zielsetzung des Berichtes ist eine **zusammenfassende Darstellung der Cyber Bedrohungen** und wesentlichen sonstigen **nationalen und internationalen Entwicklungen** im jeweils **vergangenen Jahr**. Grundlage sind ressortspezifische Berichte zur Thematik.

2 Cyber Lage 2013 / Bedrohungsanalyse

Die heutige Gesellschaft ist immer mehr von den technischen Errungenschaften und in weiterer Folge von der Vertraulichkeit, Verfügbarkeit 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. Im Zeitalter der »Digital Natives« kann die Fähigkeit eines Einzelnen zu einer möglichen Waffe zur Durchführung von Cyber Angriffen werden.

2.1 Akteure und deren Intentionen

Wesentliche Bedrohungen im Cyber Raum gehen von einzelnen **staatlichen Akteuren** aus. Sie versuchen, den Cyber Raum zur Umsetzung nationaler politischer und wirtschaftlicher Interessen zu nutzen. Gleichzeitig setzen Staaten Cyber Mittel wie z. B. Propaganda über Soziale Medien ein, um Informationsüberlegenheit zu erlangen. Im öffentlichen Fokus stand 2013 vor allem staatlich gesteuerte **Cyber Spionage**. Neben chinesischen Cyber Spionageoperationen sind die Aktivitäten der US National Security Agency (NSA) zu erwähnen. So wurden Informationsbeschaffungsprogramme (wie z. B. Prism), die für die Bekämpfung von Terrorismus eingeführt wurden, ebenfalls zum Zwecke der Cyber Spionage eingesetzt. Neben den USA verfügen auch andere Staaten über ähnliche Programme.

Ein weiteres Kriminalitätsfeld in Zusammenhang mit der missbräuchlichen Verwendung des Internets ist die **Wirtschafts- und Industriespionage**.

Auf nichtstaatlicher Ebene spielen **Cyber Kriminelle** eine wesentliche Rolle. Täter und Täterinnen bedienen sich ausgefeilter Technologien und nutzen das Internet als Tatbegehungsörtlichkeit für ihre weltumspannenden kriminellen Machenschaften. Ihre kriminellen Motive reichen dabei von der Beschaffung von Geld durch Spam[1], Phishing[2] und / oder Pharming[3] über Kreditkartenbetrug bis zum Verkauf vertraulicher Daten. Darüber hinaus stellen kriminelle Organisationen gegen Bezahlung auch technische Mittel (sowohl Hard- als auch Software) zur Durchführung von Cyber Angriffen für »Jedermann« zur Verfügung. Das Internet ist somit Schauplatz nicht nur für Betrugs- und Finanzmittelkriminalität, sondern es bildet auch den »enabling factor« für jegliche Form gefährlicher Cyberattacken auf Behörden, Institutionen und Unternehmen.

1 Massensendungen per E-Mail zu Werbezwecken; machen heutzutage einen erheblichen Anteil des Internetverkehrs aus.

2 Der Versuch, über eine E-Mail (»Klicken Sie auf diesen Link, ansonsten wird Ihr Konto gesperrt!«) Benutzer zu täuschen und dazu zu verleiten, bestimmte Handlungen (z. B. auf einen in der E-Mail enthaltenen Link zu einer schadhaften Webseite zu klicken) zu deren Schaden zu setzen. Das Ziel ist häufig die Extraktion von Zugangsdaten (Username, Passwort), um danach die digitale Identität (Benutzerprofil) übernehmen und für kriminelle Aktivitäten nutzen zu können.

3 Umleitung eines korrekten Webseitenaufrufs (z. B. www.google.com) auf eine gefälschte und sich unter der Kontrolle eines Angreifers befindliche, schadhafte Webseite. Diese ist zumeist täuschend echt der originalen Webseite nachempfunden. Dort getätigte Benutzereingaben (Username, Passwort, TAN-Codes usw.) werden an einen Angreifer, der die gefälschte Webseite kontrolliert, weitergeleitet.

Terroristen nutzen den Cyber Raum vorwiegend zur Radikalisierung, Rekrutierung und Finanzierung von terroristischen Operationen.

»**Hacktivisten**« (**Internet-Aktivisten**) stellen eine besondere Form der Online-Akteure dar. Sie können innerhalb des Cyber Raumes als Online-Demonstranten bezeichnet werden, die meist durch Distributed Denial of Service (DDoS) Angriffe[4] oder Defacements[5] ihren Unmut kundtun. Solch politisch oder gesellschaftlich motivierte Hacker-Aktionen waren 2013 zwar in Österreich präsent, im Vergleich zu den Vorfällen 2012 aber deutlich harmloser. 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.

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.

2.2 Methoden

Zielsetzung von Cyber Angriffen ist es, die Vertraulichkeit, die Integrität und/oder die Verfügbarkeit von Netzwerken, den Geräten in den Netzwerken oder den Daten und Diensten in diesen Netzwerken zu kompromittieren. Sie können in **drei Kategorien** unterteilt werden:

1. **Gezielte Angriffe auf ein bestimmtes Ziel** oder einen ausgewählten Kreis bestimmter Ziele. 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 Informationsabflusses und möglicher Steuerung von außen stellt diese Kategorie von Angriffen (auch »Advanced Persistent Threat« bzw. APT genannt) die **größte Bedrohung** dar.
2. **Zielgerichtete Angriffe** auf einen **bestimmten Personenkreis**. Hier wird eine Gruppe von Personen, deren gemeinsamer Nenner für den Angreifer die Motivation für diesen Angriff ausmacht, angegriffen.
3. **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.

Es gibt eine **Vielzahl an Mitteln und Methoden**, um Angriffe im und über den Cyber Raum erfolgreich durchzuführen. Im Jahr 2013 wurden vor allem **Ausspähung von Zugangsdaten, Einschleusen von Schadsoftware** über Webseiten, **Kompromittierung von Datenbanken** sowie

4 Distributed Denial of Service: Angriffsmethode, bei der Server mit so vielen Anfragen von einer Vielzahl von Systemen ausgehend »bombardiert« werden, bis sie unter der Last der Anfragen zusammenbrechen und die darauf laufenden Services nicht mehr zur Verfügung stehen.

5 Infiltration eines Webservers und Veränderung von sich darauf befindlichen Webseiten.

Störung der Verfügbarkeit einzelner Dienste im Netzwerk erkannt. Diese Attacken wurden teilweise in Kombination, vielfach mit Hilfe bereits bekannter Schadsoftware, in einigen Fällen auch mit eigens für den jeweiligen Angriff konzipierten Programmen umgesetzt.

Die **Infektion von Windows-PCs** ist immer noch das klassische Einfallstor in Firmennetze. Windows selbst stellt dabei jedoch immer weniger das gravierende Problem dar, sondern vielmehr die Programme, mit denen Inhalte aus dem Web dargestellt werden (z. B. PDF-Viewer, Textverarbeitungssoftware, Web-Browser[6] und deren Plug-Ins[7]). Mit Schadsoftware präparierte Dateien werden dabei von Angreifern per E-Mail direkt versendet, per Link referenziert oder in populäre Webseiten mittels Webhacks eingebaut. Über »Social Engineering«[8] (etwa »Öffnen Sie dieses Mahnschreiben/Telekom Rechnung/…«) sind für eine Infektion oft nicht einmal technischen Schwachstellen erforderlich; auch gut implementierte, technische Sicherheitsvorkehrungen lassen sich auf diese Weise umgehen. In Firmen und Behördennetzen kann ein Angreifer auf diese Weise im internen Netzwerk schrittweise bis zu den kritischen Systemen gelangen, um diese ebenfalls zu kompromittieren.

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 in Ihrer Größe und Vielzahl dann die Netzanbindung des Opfers lahm, wodurch das betroffene Online-Service nicht mehr erreichbar ist.

Generell war im Jahr 2013 ein starker Anstieg der auf **Mobiltelefone** ausgerichteten Schadsoftware feststellbar. Außerdem spezialisieren sich Cyber Kriminelle immer stärker auf **soziale Netzwerke** und verwenden diese für die Durchführung und Vorbereitung von Straftaten. Durch die Verbreitung von **Smartphones und Tablets** sind auch diese Geräte als Angriffsziel interessant geworden; vor allem für Android (das am stärksten verbreitete Betriebssystem für Smartphones und Tablets) existiert eine erhebliche Zahl an Schadsoftware. Obwohl technische Lösungen zur Absicherung dieser Endgeräte existieren, ist das Sicherheitsbewusstsein der Benutzer auf diesen Geräten verglichen mit PCs und Notebooks relativ gering.

Die beschriebenen Methoden sind auch und vor allem im Rahmen von **erkannten gezielten Angriffen im Jahr 2013** angewandt worden. In den meisten Fällen konnte beobachtet werden, dass die Angriffe mittels Spear-Phishing[9] per E-Mail mit Schadprogrammen in Anhängen durchgeführt wurden. Es stellte sich jedoch im Laufe des Jahres 2013 heraus, dass einige der Akteure ihre Vorgehensweise erweiterten bzw. wechselten. Außerdem ist auffällig, dass immer mehr verwendete Schadprogramme mit gültigen und überprüfbaren

6 Programm zur Anzeige von Webseiten (z. B. Internet Explorer).

7 Zusatzprogramm für Web-Browser, welches weitere Funktionalität bietet (z. B. Anzeige von Flashvideos in Youtube).

8 Sammelbegriff für Attacken, welche sich nicht gegen technische Systeme (z. B. PCs) richten, sondern gegen deren Anwender.

9 Speziell präparierte Phishing-Attacke auf einen gezielten Opferkreis (z. B. Mitglieder einer bestimmten Mailingliste)

digitalen Zertifikaten[10] ausgestattet sind. Dieses Vorgehen lässt auf eine ansteigende Professionalisierung der Akteure schließen.

2.3 Schwachstellen

Die Hervorhebung 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 **Mobiltelefon / SMS** noch als vertrauenswürdiger Kommunikationskanal nutzbar, so ist das 2013 zunehmend weniger der Fall: Die Komplexität von **Smartphones** und die Proliferation von Apps machen die **Verbreitung von Schadsoftware auf Mobiltelefonen** deutlich einfacher.
- 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.
- 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 wird ab April 2014 ein hoher Anteil an PCs sukzessive verwundbarer, weil bis dorthin unentdeckte Sicherheitslücken nicht mehr bereinigt werden. Dies kann auch durch vorhandene Antivirensoftware nicht abgefedert werden.

10 In der Informationssicherheit dienen digitale Zertifikate als Identifizierungsmerkmal um für die Richtigkeit der Herkunft von Daten zu garantieren.

3 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 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 von Cyber Kriminalität und der Achtung grundlegender Menschenrechte, wie dem Recht auf freie Meinungsäußerung und Informationsfreiheit sowie dem Recht auf Privatleben und Privatsphäre, geachtet werden.

3.1 Europäische Union

Die 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 Kommission 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 GSVP vom Dezember 2013 wiederfindet. Demnach soll einerseits das Fähigkeitsspektrum im Cyber Bereich erweitert und ausgebaut, und andererseits ein EU-Politikrahmen für die Cyberabwehr festgelegt werden.

Unterstützt werden die Aktivitäten in diesem Bereich von der European Network and **Information Security Agency** (**ENISA**), deren Aufgabe es ist, gemeinsam mit den Mitgliedsstaaten und den anderen EU Institutionen die Netzwerk- und Informationssicherheit zu verbessern. Im Rahmen des von ENISA im Oktober auf Initiative der EK organisierten **European Cyber Security Month** wurden vom BMEIA alle E-Mail-mäßig erfassten Auslandsösterreicher, Auslandsösterreicher-Vereine und Honorarkonsulate umfassend informiert.

Am 12. Februar 2013 hat die EK einen Vorschlag für eine Richtlinie des 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 Cybersicherheitsstrategie der EU und wird derzeit im Rat und im EP verhandelt. Folgende Kernforderungen wurden identifiziert:

- Annahme einer nationalen NIS-Strategie, sowie die Aufstellung einer NIS-Behörde und eines GovCERT/CERT (Computer Emergency Response Team) als IT-Notfallteam.
- Verpflichtendes Risikomanagement für kritische Infrastrukturen und Meldeverpflichtung bei Sicherheitsvorfällen.
- Aufbau eines EU-weiten NIS-Kooperationsnetzwerks zum Austausch von Vorfällen und damit zusammenhängender, aufklärungsrelevanter Informationen.

3.2 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.

Im Oktober fand in Seoul die nunmehr dritte **Conference on Cyberspace** statt, an der ca. 90 Delegationen, die Hälfte davon auf Ministerebene, teilnahmen. Österreich war durch das BMEIA und das BM.I vertreten. Der Fokus der Konferenz lag auf den Themen Internet und Wirtschaftswachstum und Entwicklung, sozialer und kultureller Nutzen des Internets, Cyber Sicherheit, Normierung des Cyber Raumes und capacity building. Einmal mehr zeigten sich die bekannten Auffassungsunterschiede zwischen den westlichen, chinesischen und russischen Positionen und die Schwierigkeiten in Hinblick auf eine internationale Normierung im Cyber Bereich.

Darüber hinaus beschäftigen sich 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. Hier brachten Deutschland und Brasilien einen Resolutionsentwurf zum Recht auf Privatsphäre im digitalen Zeitalter ein. Österreich war in den Erarbeitungsprozess intensiv eingebunden und hat – auf Ersuchen von Deutschland und Brasilien – gemeinsam mit einer kleinen Gruppe anderer Länder (darunter Liechtenstein, Schweiz, Frankreich) die Resolution zum frühestmöglichen Zeitpunkt miteingebracht. Die Resolution (A/RES/68/167) wurde Ende November 2013 schließlich im Menschenrechtsausschuss der 68. VN-GV einstimmig angenommen. Sie zielt vor allem auf eine Stärkung des Grundrechts auf Schutz der Privatsphäre und auf die Umsetzung von Art. 17 des Internationalen Paktes über Bürgerliche und Politische Rechte (ICCPR) ab.

Darüber hinaus wurde von Seiten der VN eine offene zwischenstaatliche Sachverständigengruppe – angesiedelt beim VN-Büro für Drogen- und Verbrechensbekämpfung (UNODC) – mit der Erarbeitung einer umfassenden Studie über Cyberkriminalität beauftragt. Im Februar 2013 legte diese ihren Bericht vor, woraufhin einige VN-Mitgliedstaaten den raschen Beginn von Verhandlungen über eine VN-Konvention zur Bekämpfung der Cyberkriminalität verlangten, was jedoch mehrheitlich abgelehnt wurde.

3.3 NATO

Als Verteidigungsbündnis befasst sich die NATO spätestens seit der Verabschiedung ihres neuen strategischen Konzepts von 2010 mit den Verteidigungsaspekten von Cyber. Österreich kooperiert hier als Partnerland eng mit der NATO. 2013 fanden einerseits informelle politische Konsultationen zwischen den sechs westeuropäischen Partnern (WEP-6: Schweiz, Irland, Finnland, Malta, 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.

Bei den NATO-Ukraine Expert Staff Talks on Cyber Defence (November 2013, Jalta) war Österreich, im Rahmen der bilateralen Zusammenarbeit mit der NATO, mit einem Cyber Experten vertreten, welcher der dort die Genese und wesentlichsten Inhalte der ÖSCS vorstellte.

Österreich hat im Rahmen der NATO Partnership for Peace (NATO/PfP) das **Partnerschaftsziel »Cyber Defence«** angenommen. Die diesbezüglichen Vorgaben für 2013 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 BMLVS im **»Cooperative Cyber Defence Center of Excellence« in Tallinn / Estland** seit Oktober 2013.

Am Europäischen Rat im Dezember 2013 wurde 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 Center of Excellence in Tallinn eingehen wird. Selbiges gilt für die mögliche Zusammenarbeit im Rahmen der »Friends of Presidency Initiative on Cyber Issues«, welche seit 2013 zur Unterstützung der Implementierung der EU Cyber Security Strategy aktiviert wurde.

3.4 OSZE

Der Ministerrat der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) bestärkte im Dezember 2013 in Kiew eine Entscheidung des Ständigen Rates zu **vertrauensbildenden Maßnahmen im Bereich der Cyber Sicherheit.** Die Teilnehmerstaaten sollen Kontaktstellen für den Dialog über Sicherheit im und durch den Gebrauch von Informations- und Kommunikationstechnologie nennen. Sie tauschen Informationen über die nationale Organisation von Cyber Sicherheitsplänen, sowohl im staatlichen als auch im privaten Bereich aus, und treffen mindestens dreimal im Jahr im Rahmen des Sicherheitskomitees der OSZE zusammen, um neue Entwicklungen im Bereich der Cyber Sicherheit zu diskutieren. Durch mehr Transparenz und Vertrauen zwischen den OSZE-Staaten, sowie die Vernetzung nationaler Expertinnen und Experten wird die Freiheit des Internets, die freie Meinungsäußerung sowie der Schutz der Privatsphäre in den Vordergrund gerückt.

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 (**OECD-DAC**) sowie im Rahmen von **INTERPOL** statt.

3.5 Nationalstaaten

3.5.1 Vereinigte Staaten von Amerika

Das **Büro für Cyber Sicherheit** ist direkt dem Präsidenten unterstellt und die oberste Stelle für die gesamtstaatliche strategische Ausrichtung. Für den Schutz bundesweiter IKT-Netze, die Kooperation mit den Betreibern von Kritischen Infrastrukturen und die Strafverfolgung von Cyber Kriminellen ist das Heimatschutzministerium verantwortlich. In den US-Streitkräften hat das im Oktober 2010 in Betrieb genommene U.S. Cyber Commmand die Koordinierungsrolle inne.

Die Wichtigkeit, die der Cyber Thematik zugemessen wird, spiegelt sich in den Budgetentwürfen der Regierung wider. So legte Präsident Obama im April 2013 der Regierung einen Budgetvorschlag vor, in dem er mehr als 9,5 Mrd. Euro für Cyber Programme vorsieht. Auch in den US-Streitkräften wurde vermehrt in den Aus- und Aufbau von sowohl offensiven als auch defensiven Maßnahmen investiert.

3.5.2 Russische Föderation

Bereits im Jahr 2000 unterzeichnete Präsident Putin die **Informationssicherheitsdoktrin der Russischen Föderation**, die bis heute gültig ist. Die Russische Föderation vertritt den Standpunkt, dass eine **starke Kontrolle über die nationalen IKT-Infrastrukturen** sowie ein **internationales Abkommen zur Regulierung des Internets** notwendig seien. Um den nationalen Informationsraum besser zu kontrollieren, erließ die russische Regierung z. B. im März 2013 ein Gesetz, welches das Blocken von Internetseiten mit »gefährlichem Inhalt« für Kinder vorsieht. National ist der Inlandsnachrichtendienst FSB für die Cyber Sicherheit verantwortlich. Um Cyber Angriffe möglichst frühzeitig zu erkennen, beauftragte Präsident Putin im Oktober 2013 den FSB, seine Fähigkeiten zur Überwachung von IKT-Netzen auszubauen. Auch die russischen Streitkräfte sind im Begriff, ihre Cyber Fähigkeiten zu erweitern.

3.5.3 Volksrepublik China

Die chinesische Führung erkannte bereits Anfang der 1990er-Jahre die Notwendigkeit, **Informationsüberlegenheit im Cyber Raum** zu schaffen. Für den Schutz der nationalen IKT-Infrastrukturen und deren Überwachung ist das Ministerium für Öffentliche Sicherheit zuständig. Die chinesische Regierung sieht die Notwendigkeit einer gezielten Steuerung des Informationsflusses im Internet, hier v. a. in den Sozialen Medien, zur Wahrung der nationalen Sicherheit. So wurde 2013 ein neues Gesetz verabschiedet, das für die **Verbreitung von Gerüchten über das Internet eine Bestrafung von bis zu drei Jahren Haft** vorsieht.

Im Jänner 2013 bestätigte die chinesische Regierung erstmals die Existenz von Hackereinheiten, sogenannte »Cyber Blue Teams«, in den Streitkräften.

3.5.4 Vereinigtes Königreich

2009 wurde direkt 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 wurden ca. 800 Mio. Euro bis 2015 veranschlagt. Im Juni 2013 gab der britische Schatzkanzler bekannt, dass im nächsten Budget weitere 256 Mio. Euro für das **Nationale Cyber Sicherheitsprogramm** (NCSP) des Cabinet Office zur Wahrung der Interessen des Vereinigten Königreiches vorgesehen seien. Auch die Streitkräfte und Nachrichtendienste (hier v. a. das Government Communications Headquarter GCHQ) bauen ihre Cyber Fähigkeiten aus. So kündigte der britische Verteidigungsminister im September 2013 die Aufstellung einer »**Cyber Reserve**« an. Auf internationaler Ebene strebt das Vereinigte Königreich bilaterale Gespräche v. a. mit wichtigen Handelspartnern an.

3.5.5 Deutschland

2011 gab das Bundesministerium des Inneren (BMI) die »**Cyber Sicherheitsstrategie für Deutschland**« heraus. Für die Umsetzung der nationalen Cyberstrategie sind im Wesentlichen zwei Ministerien verantwortlich. Das BMI, hier v. a. das 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 werden im Nationalen Cyber Abwehr Zentrum (NCAZ) die wesentlichen Informationen zur Cyber Sicherheit zwischen den verantwortlichen Stellen ausgetauscht. Im Februar 2013 z. B. hat der

zuständige Bundesinnenminister einen Gesetzesentwurf zur Erhöhung des IT-Schutzes der Kritischen Infrastruktur (kurz »**IT-Sicherheitsgesetz**«) vorgelegt. Die wesentlichen Punkte dieses Gesetzes sind die Meldung von 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 ist das Bundesministerium der Verteidigung, wo v. a. das Kommando Strategische Aufklärung für Cyber Fähigkeiten zuständig ist. Neben den beiden Ministerien nimmt der Bundesnachrichtendienst (BND) ebenfalls eine wichtige Rolle im Cybersicherheitsbereich ein. Er ist v. a. für die Erstellung eines umfassenden Cyber Lagebildes verantwortlich. Im Juli 2013 wurde ein eigener **Cyber Beauftragter der Bundesrepublik Deutschland** ernannt. Er soll auf diplomatischer Ebene die deutschen Cyber Interessen vertreten.

3.5.6 Niederlande

Die Niederlande veröffentlichte 2013 eine aktualisierte Version seiner Cyber Security Strategie. Nach einer Reihe von DDoS Attacken in den Niederlanden wurden in Kooperation zwischen Banken und dem **nationalen Cybersicherheitszentrum** (NCSC) verstärkt Awareness-Kampagnen gestartet. Das NCSC betreibt neben einer durchgehend erreichbaren Cyber Security Assistance ein umfangreiches Sensornetzwerk, welches zur Analyse und Aufklärung von Cyber Security Fragen und Incidents beitragen soll.

3.5.7 Finnland

Finnland veröffentlichte im Jänner 2013 seine Cyber Security Strategie, in deren Folge ein **nationales Cybersicherheitszentrum** (NCSC) gegründet wurde. Die bislang für nationale Cybersicherheit zuständige FICORA (Finnish Communications Regulatory Authority) wurde in dieses Zentrum integriert, ebenso wie die operative Regierungsverantwortung für die Netz- und Informationssicherheit. Die Budgetmittel wurden erheblich erhöht.

Wichtige Services des NCSC sind neben GovCERT- und den nationalen CERT-Aktivitäten der Einsatz eines speziell auf den öffentlichen Bereich angepassten Systems zur Identifikation von und Warnung vor Cyber Security Bedrohungen und zur graphischen Darstellung möglicher Auswirkungen.

3.5.8 Schweiz

Im Mai 2013 trat in der Schweiz die »**Nationale Strategie zum Schutz der Schweiz vor Cyber Risiken**« in Kraft.

Die Schweizer Melde- und Analysestelle Informationssicherung (MELANI), die auch für die Koordination der Umsetzung der Schweizer Cyber Security Strategie verantwortlich ist, veröffentlichte nach einer Serie schwerer DDoS Attacken eine Reihe von Maßnahmen zur Absicherung der durch solche Attacken betroffenen IT-Infrastruktur.

4 Nationale Entwicklungen

4.1 Akteure und Strukturen

4.1.1 GovCERT und CERT.at

GovCERT ist das nationale CERT der öffentlichen Verwaltung und der kritischen Infrastrukturen und übt sowohl koordinative wie auch operative Funktionen aus. 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.

Es bündelt die sicherheitstechnische Expertise für den Bereich der öffentlichen Verwaltung. Dies umfasst Präventivmaßnahmen, die Sammlung und Bewertung von sicherheitstechnischen Vorfällen sowie bei Bedarf auch Unterstützungsleistung vor Ort. Weitere Aufgaben umfassen Schulungen, die Koordination themenspezifischer Arbeitsgruppen, regelmäßige Awareness-Maßnahmen sowie den Ausbau des österreichischen CERT-Verbunds und die Teilnahme an nationalen und internationalen Cyber Security Übungen.

CERT.at ist das österreichische CERT, dessen Aufgaben sich am ehesten mit denen einer »Internet-Feuerwehr« beschreiben lassen. In erster Linie wird CERT.at im Fall akuter Sicherheitsbedrohungen aktiv, entweder aufgrund eigener Recherchen/Beobachtungen und Bedrohungserkennung oder nach Verständigung durch betroffene Stellen. Auch für Meldungen akuter Sicherheitsprobleme durch Dritte ist CERT.at als Informationsdrehscheibe in Fragen der Cyber Sicherheit ein wichtiger Ansprechpartner. Weitere Aufgabenbereiche von CERT.at umfassen vorbeugende Maßnahmen, wie Früherkennung von Gefahren, Vorbereitung auf Zwischenfälle/Cyber Attacken (»Incidents«), Öffentlichkeitsarbeit und Beratung, sowie die Vernetzung mit ausländischen CERTS.

Zur Wahrnehmung dieser Aufgaben arbeiten GovCERT und CERT.at eng zusammen.

GovCERT und CERT.at waren 2013 aufgrund mehrerer Vorfälle im Einsatz. Dies betraf u. a. Probleme in den Steuernetzen österreichischer Energieversorger (Mai), eine Reihe medienwirksamer DDoS-Attacken (April), eine Welle an Einbrüchen und Defacements auf Webseiten (Januar bis März), Attacken auf die EVN während Unruhen in Bulgarien im Februar, Vorort-Unterstützung bei einem Cyber Vorfall in einem Bundesamt (März) sowie den Fall einer APT-Attacke auf ein Ministerium im Sommer, welcher in enger Kooperation mit internationalen GovCERT-Partnern bearbeitet wurde.

4.1.2 Austrian Trust Circle

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

Aktuell werden im ATC die Sektoren Energie, Finanz, Gesundheit, Industrie, Transport und Kommunikation adressiert. Vierteljährlich finden sektorspezifische Treffen des ATC statt, einmal im Jahr zusätzlich ein sektorenübergreifendes Treffen.

4.1.3 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.

4.1.4 milCERT

Das militärische Computer Emergency Readiness Team (milCERT) wird durch das Abwehramt und das Führungsunterstützungszentrum des Bundesministeriums für Landesverteidigung und Sport betrieben. Es ist aktuell primär für BMVLS-interne Aufgabenstellungen aufgestellt, von der Struktur jedoch prozessorientiert für gesamtstaatliche Aufgaben des BMLVS/ÖBH vorbereitet.

Zu seinen primär 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[11] 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,
- Beobachtung und Evaluierung von Verteidigungs- und Angriffstechnologien,
- 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 minimiert und den Schwachstellen vorab entgegentreten zu können.

4.1.5 Heeresnachrichtenamt (HNaA)

Das HNaA ist für die Erarbeitung des strategischen Lagebildes v. a. in Bezug auf internationale Akteure und Entwicklungen zuständig. Der Beitrag 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, die Angreifer zu identifizieren.

4.1.6 Cyber Crime Competence Center (C4)

Das Cyber Crime Competence Center (C4) des BM.I ist die nationale Koordinierungs- und Meldestelle zur Bekämpfung der Cyberkriminalität. Das Zentrum setzt sich aus technisch und fachlich hochspezialisierten Expertinnen und Experten des Bundeskriminalamtes zusammen. Im Jahr 2013 wurde der organisatorische, personelle und technische Aufbau fortgesetzt und abgeschlossen. Der weitere Ausbau und die Stärkung des C4 erfolgt im Rahmen der Umsetzung der ÖSCS sowie der Cyber Sicherheitsstrategie des BM.I.

---

11 Überprüfung auf potentielle Sicherheitsrisiken.

4.1.7 IKT-Sicherheitsportal

Das IKT-Sicherheitsportal ist eine in der Österreichischen Strategie für Cyber Sicherheit 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 (www.onlinesicherheit.gv.at).

4.2 Umsetzung ÖSCS

Die Umsetzung der in der ÖSCS (Beschluss der Bundesregierung im März 2013) aufgelisteten Maßnahmen zur Erhöhung der nationalen Cyber Sicherheit werden durch die **Steuerungsgruppe Cyber Sicherheit** (bestehend aus den Verbindungspersonen zum nationalen Sicherheitsrat sowie aus Cyber Security Experten aus allen Ressorts) überwacht und auf der operativen Ebene durch eine Kerngruppe geplant und veranlasst. Basis für die Umsetzung stellt ein **Implementierungsplan** dar, welcher im Juni 2013 durch die Steuerungsgruppe Cyber Sicherheit beschlossen wurde.

Im Zuge dieses Beschlusses wurde auch Einvernehmen über vier prioritäre Umsetzungsprojekte erzielt, welche im Laufe des Jahres 2013 durch ressortübergreifende Projektgruppen bearbeitet wurden. Diese sind:

1. Erarbeitung von **Prozessen und Strukturen zur permanenten Koordination auf der operativen Ebene** (bis April 2014, Federführung BM.I und BMLVS).
2. **Bericht ordnungspolitischer Rahmen** (bis Dezember 2014, Federführung durch BKA und BM.I).
3. Konzept und Geschäftsordnung **Cyber Sicherheit Plattform** und Zusammenarbeit mit Betreibern kritischer Infrastrukturen und weiteren Wirtschaftssektoren (bis März 2014, Federführung BKA und BM.I).
4. **Cyber Sicherheit Kommunikationsstrategie** (bis Dezember 2014, Federführung durch BKA und BM.I)

5 Cyber Übungen

5.1 NATO-Übung »Cyber Coalition 2013«

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 Unterstützung des GovCERT an der Cyber Coalition 2013 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

5.2 Combined Endeavor (CE)

Seit 1995 findet alljährlich dieses Vorhaben unter der Leitung von USEUCOM (United States European Command) statt. Dabei handelt es sich um die größte Interoperabilitätsübung für Führungsunterstützungskräfte weltweit. Bis zu 43 verschiedene Nationen (darunter auch AUT) und Organisationen aus Europa und Nordamerika nutzen dieses Umfeld um ihre C4 (Command, Control, Communications and Computers) Systeme in verschiedenen multinationalen Einsatznetzwerken zum Einsatz zu bringen, zu testen und, aufbauend auf die Testergebnisse, weiter zu entwickeln.

5.3 Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise« (CWIX)

Der Zweck dieser im Juni 2013 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. Ziel der nationalen Teilnahme (vier Mitarbeiter des MilCERT) war es, die Auswirkung von Cyberbedrohungen 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 werden.

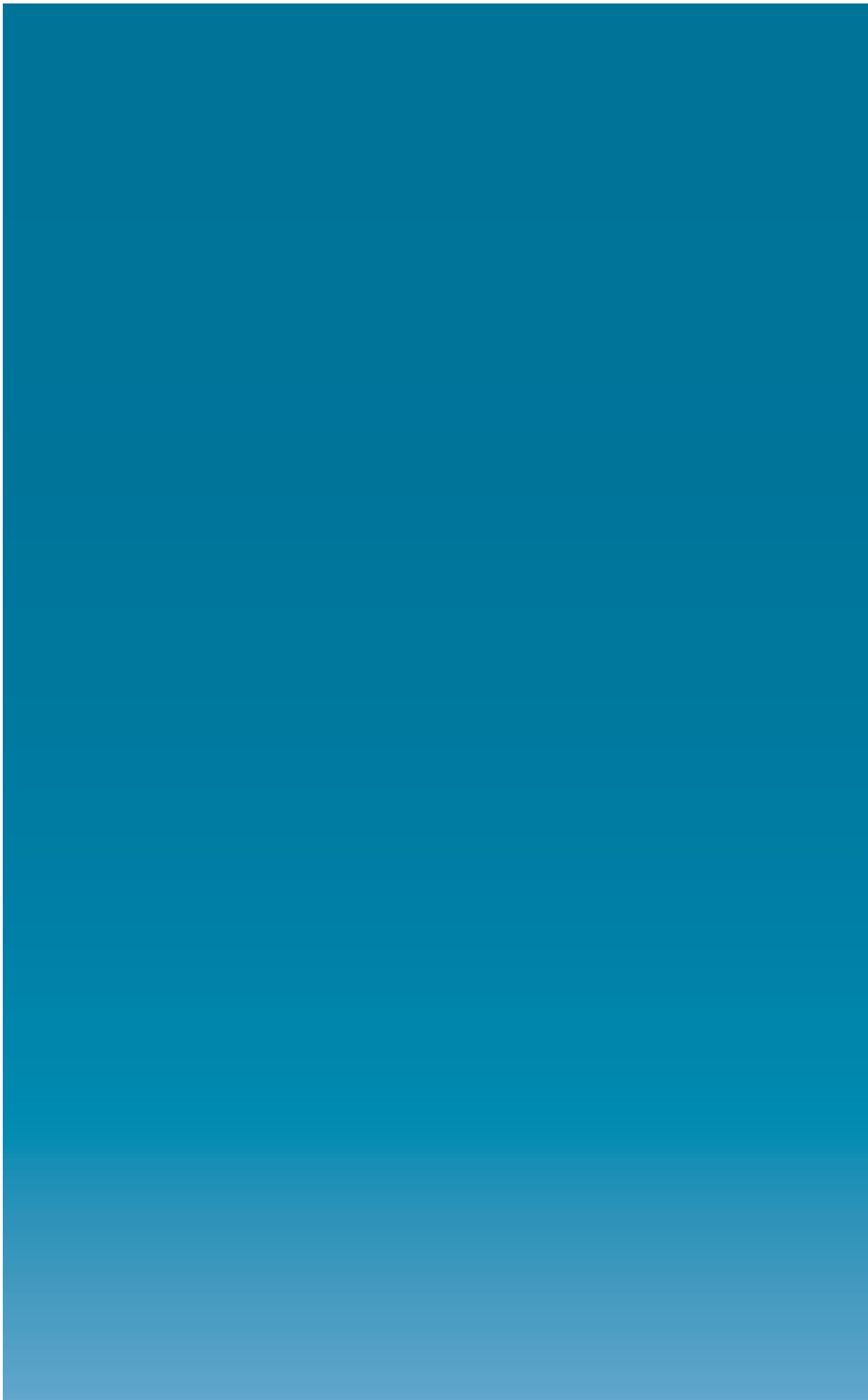
6 Zusammenfassung / Ausblick

Im Jahr 2013 konnte vor allem in den Bereichen Cyber Spionage und Cyber Kriminalität eine signifikante Steigerung der Aktivitäten verzeichnet werden. Angriffe werden immer zielgerichteter gesetzt und auch die Verlagerung von Angriffen in die »Cloud«[12] wird für die nächste Zeit zu erwarten sein. 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 Möglichkeiten 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.

Die Angriffe werden sich nach der Form der Verarbeitung bzw. Speicherung der 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.

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 zunehmend unerlässlich. Breit angelegte und aufeinander abgestimmte technische sowie organisatorische Maßnahmen leisten einen wesentlichen Beitrag, Verarbeitungsanomalien zu identifizieren und passende Gegenmaßnahmen zu entwickeln.

Es kann ein internationaler Trend zur Zentralisierung nationaler Cyber Security Steuerung und Koordination über die Bildung von Cyber Security Centres beobachtet werden. Insgesamt ist davon auszugehen, dass das Interesse der Regierungen an Cyber Sicherheit weiter zunimmt. Dies wird sich in der Veröffentlichung weiterer nationaler Strategiedokumente sowie im Aufbau entsprechender Steuerungs- und Koordinierungsstrukturen manifestieren. Von einer steigenden Bedeutung von Cyber Sicherheit als Gegenstand multinationaler und institutioneller Diskussion ist auszugehen.

Die vorhandenen Aktivitäten und Strukturen in Österreich bilden eine gute Basis um die in diesem Bericht genannten Herausforderungen zu adressieren, bedürfen aber noch eines technischen, organisatorischen und sozialen Capacity Buildings.

12 Überbegriff für Anwendungen und Datenspeicher, welche nicht lokal im Netzwerk liegen, sondern in entfernten Netzwerken. Der Zugriff erfolgt vom lokalen Netzwerk, wie auf eine lokale Ressource.