REPUBLIK ÖSTERREICH

Österreichische Strategie für Cyber Sicherheit

BUNDESKANZLERAMT ÖSTERREICH

Bundesministerium für europäische und internationale Angelegenheiten

BM.I REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR INNERES

Bundesministerium für Landesverteidigung und Sport

Österreichische Strategie für Cyber Sicherheit

Wien, 2013

Impressum

Medieninhaber, Verleger und Herausgeber:
Bundeskanzleramt Österreich
Sektion IV – Koordination
Abteilung IV/6 – Sicherheitspolitische Angelegenheiten
Ballhausplatz 2, 1014 Wien

Grafische Gestaltung: BKA | ARGE Grafik
Wien, März 2013

Inhalt

1 Einleitung 4

2 Chancen und Risiken im Cyber Raum 6

2.1 Chancen 6

2.2 Risiken und Bedrohungen 6

3 Prinzipien 7

4 Strategische Ziele 9

5 Handlungsfelder und Maßnahmen 10

Handlungsfeld 1 – Strukturen und Prozesse 10

Handlungsfeld 2 – Governance 12

Handlungsfeld 3 – Kooperation Staat, Wirtschaft und Gesellschaft 12

Handlungsfeld 4 – Schutz kritischer Infrastrukturen 14

Handlungsfeld 5 – Sensibilisierung und Ausbildung 14

Handlungsfeld 6 – Forschung und Entwicklung 15

Handlungsfeld 7 – Internationale Zusammenarbeit 16

6 Umsetzung 16

Annex 1 18

Cyber-Risikomatrix 2011 18

Annex 2 19

Abkürzungsverzeichnis 19

Annex 3 20

Cyber Sicherheit Glossar 20

1 Einleitung

Die digitale Revolution hat in allen Lebensbereichen der modernen Welt Fuß gefasst. Postindustrielle Gesellschaften und hochentwickelte Staaten nutzen mehr denn je den Cyber Raum für ihre technische, wirtschaftliche, soziale, kulturelle, wissenschaftliche und politische Entwicklung. Digitale Infrastrukturen werden zunehmend zum Rückgrat einer erfolgreichen Wirtschaft, einer lebendigen Forschungsgemeinschaft, eines transparenten Staates sowie einer freien Gesellschaft. Die Entwicklung der modernen Informations- und Kommunikationstechnologien – allen voran das Internet – haben das gesellschaftliche und wirtschaftliche Leben in einem unvergleichbaren Ausmaß verändert. In Österreich nutzen mittlerweile rund drei Viertel der Bevölkerung regelmäßig das Internet, die Hälfte bereits täglich.

Die Wirtschaft ist im Hinblick auf ihre technische Weiterentwicklung und die Effizienz ihrer internen Geschäftsprozesse zunehmend von einer funktionierenden digitalen Infrastruktur abhängig. Für die öffentliche Verwaltung ist das Internet eine unverzichtbare Grundlage geworden, ihre Dienstleistungen über den traditionellen Weg hinaus einer breiten Öffentlichkeit zugänglich zu machen.

Die Bevölkerung muss darauf vertrauen können, dass Daten ihren Adressaten schnellstmöglich und sicher erreichen. Ein offenes und freies Internet, der Schutz personenbezogener Daten und die Unversehrtheit von miteinander verbundenen Netzwerken sind Grundlage für globalen Wohlstand, Sicherheit und Förderung der Menschenrechte.

Die Daseinsvorsorge der Bevölkerung – wie z. B. die Versorgung mit Energie, Wasser, Transporteinrichtungen – ist von einer funktionierenden digitalen Infrastruktur abhängig. Um die Vorteile, die unsere globalisierte und digitalisierte Welt verspricht, nutzen zu können, muss die digitale Infrastruktur verlässlich und sicher funktionieren.

Angriffe aus dem Cyber Raum[1] sind eine unmittelbare Gefahr für unsere Sicherheit und für das Funktionieren von Staat, Wirtschaft, Wissenschaft und Gesellschaft. Sie können unser tägliches Leben schwerwiegend beeinträchtigen. Der Cyber Space kann von nichtstaatlichen Akteuren wie Kriminellen, der organisierten Kriminalität oder Terroristen aber auch durch staatliche Akteure wie Geheimdienste und Militär für ihre Zwecke missbraucht und sein Funktionieren beeinträchtigt werden. Somit sind die Gefahren aus dem Cyber Space ebenso wie dessen positive Nutzung praktisch unbegrenzt. Es gehört somit zu den obersten Prioritäten für Österreich national und international an der Absicherung des Cyber Raums zu arbeiten. Cyber Sicherheit bedeutet Sicherheit der Infrastruktur des Cyber Raums, der im Cyber Raum ausgetauschten Daten und vor allem der Menschen, die den Cyber Raum nutzen.

Die Gewährleistung von Cyber Sicherheit ist eine zentrale gemeinsame Herausforderung für Staat, Wirtschaft und Gesellschaft im nationalen und internationalen Kontext. Die Österreichische Strategie für Cyber Sicherheit (ÖSCS) ist ein umfassendes und proaktives Konzept zum

1 Die Begriffe Cyber Raum, Cyber Space und virtueller Raum werden synonym verwendet.

Schutz des Cyber Raums und der Menschen im virtuellen Raum unter Gewährleistung ihrer Menschenrechte. Sie wird Sicherheit und Widerstandskraft der österreichischen Infrastrukturen und Leistungen im Cyber Raum verbessern, vor allem aber wird sie Bewusstsein und Vertrauen in der österreichischen Gesellschaft schaffen.

Die Strategie für Cyber Sicherheit leitet sich aus der Sicherheitsstrategie[2] ab und orientiert sich an den Prinzipien des Programms zum Schutz kritischer Infrastrukturen[3] .

2 Ministerratsbeschluss vom 1. März 2011

3 Ministerratsbeschluss vom 2. April 2008

2 Chancen und Risiken im Cyber Raum

2.1 Chancen

Der Cyber Raum hat sich zu einem vitalen Aktionsraum für den Staat, die Wirtschaft, die Wissenschaft und die Gesellschaft entwickelt. Für alle ist der Cyber Space bedeutend als

Informations- und Kommunikationsraum: Der Cyber Space ermöglicht die Verbreitung und Übertragung unterschiedlicher Daten- und Informationsbestände und wächst mit rapider Geschwindigkeit: Pro Minute werden derzeit weltweit rund 204 Millionen E-Mails versandt, über zwei Millionen Suchabfragen bei Google eingegeben, sechs Millionen mal Facebook aufgerufen und mehr als 70 neue Domains registriert[1].

Sozialer Interaktionsraum: Der Cyber Raum ist ein allgemeiner sozialer Interaktionsraum, den die Menschen zur Pflege sozialer Beziehungen nutzen. Weltweit gibt es mehr als zwei Milliarden Internetnutzer.

Wirtschafts- und Handelsraum: In verhältnismäßig kurzer Zeit hat sich der Cyber Space zu einem Marktplatz von strategischer Bedeutung entwickelt. Schätzungen zufolge könnte sich der Wert des weltweiten E-Commerce-Geschäfts von 572 Milliarden US $ im Jahr 2012 bis 2014 nahezu verdoppeln.

Politischer Partizipationsraum: Der Cyber Raum beeinflusst das Verhältnis zwischen Staat und Gesellschaft. Mit E-Government erreicht der Staat Bürgerinnen und Bürger und ermöglicht damit vereinfachte Wege zu staatlichen Leistungen. Digitale Formen der Interaktion eröffnen neue Möglichkeiten der politischen Partizipation und der politischen Meinungsäußerung. Voraussetzung dafür ist die Gewährleistung aller Menschenrechte mit gleicher Gültigkeit im virtuellen wie im offline-Bereich.

Steuerungsraum: Eng mit der Funktion als Informationsraum verbunden ist die Rolle des Cyber Space als Steuerungsraum, mit dessen Hilfe so gut wie die gesamte Infrastruktur im Verkehrs-, Wirtschafts- und Industrie-, im Sicherheits-, sowie im Gesundheits- und Bildungsbereich überwacht, betrieben und gewartet werden kann. Schätzungen zufolge könnten im Jahr 2020 bis zu 50 Milliarden Geräte miteinander kommunizieren (»Internet of things«). Umso wichtiger wird es, dass auch diese Kommunikation sicher erfolgt.

2.2 Risiken und Bedrohungen

Der Cyber Raum und die Sicherheit der Menschen im Cyber Raum sind einer Vielzahl von Risiken und Bedrohungen ausgesetzt, weil dieser Raum auch Tatraum ist. Diese reichen von Fehlbedienungen bis zu massiven Angriffen staatlicher und nichtstaatlicher Akteure, die den Cyber Raum als Feld für ihr Handeln nutzen und auch vor Landesgrenzen nicht halt machen; auch militärische Operationen können hinter solchen Angriffen stehen. Die Bandbreite der Risiken und Bedrohungen ist in der Cyber Risikomatrix in Annex 1 dargestellt. Cyber Kriminalität, Identitätsmissbrauch, Cyber Angriffe oder der Missbrauch des Internet für extremistische Zwecke stellen besondere neue Herausforderungen für alle betroffenen Akteure dar. Sie erfordern ein breites Zusammenwirken staatlicher und nichtstaatlicher Stellen auf nationaler und internationaler Ebene.

---

1 Quellen für sämtliche Zahlenangaben in diesem Kapitel: Intel und KSÖ Whitepaper - Cybersicherheit intelligent regulieren; warum, wie und durch wen?«

3 Prinzipien

Moderne Cyber Sicherheitspolitik ist ein Querschnittsthema, das in vielen Lebens- und Politikbereichen mitgedacht werden muss. Sie muss **umfassend** und **integriert** angelegt, **aktiv** gestaltet und **solidarisch** umgesetzt werden.

Umfassende Cyber Sicherheitspolitik bedeutet, dass äußere und innere Sicherheit sowie zivile und militärische Sicherheitsaspekte aufs Engste verknüpft sind. Cyber Sicherheit geht über den Rahmen der klassischen Sicherheitsressorts hinaus und schließt Instrumente zahlreicher weiterer Politikbereiche mit ein.

Integrierte Cyber Sicherheitspolitik muss auf eine Arbeitsteilung zwischen dem Staat, der Wirtschaft, der Wissenschaft und der Zivilgesellschaft achten. Sie umfasst Maßnahmen in den Bereichen politisch-strategische Steuerung, Ausbildung, Risikoabschätzung, Prävention und Abwehrbereitschaft, Erkennung und Reaktion, Folgenminderung und Wiederherstellung sowie den damit verbundenen Aufbau staatlicher und nicht-staatlicher Fähigkeiten und Kapazitäten. Eine integrierte Cyber Sicherheitspolitik muss auf nationaler und internationaler Ebene kooperativ angelegt sein.

Proaktive Cyber Sicherheitspolitik heißt darauf hinzuwirken, dass Bedrohungen des Cyber Raums und der Menschen im Cyber Raum erst gar nicht entstehen oder deren Folgen abgeschwächt werden (Sicherheit gestalten).

Solidarische Cyber Sicherheitspolitik trägt dem Umstand Rechnung, dass auf Grund der globalen Natur des Cyber Raums die Cyber Sicherheit Österreichs, der EU und der gesamten Staatengemeinschaft, heute weitestgehend miteinander verbunden sind. Cyber Sicherheit erfordert daher intensive solidarische Zusammenarbeit auf europäischer und internationaler Ebene.

Die allgemein gültigen **Prinzipien der IKT Sicherheit für ein Digitales Österreich** gelten uneingeschränkt für den Bereich der Cyber Sicherheit: **Vertraulichkeit, Integrität, Verbindlichkeit, Authentizität, Verfügbarkeit sowie Privatsphäre und Datenschutz**[1].

Jedenfalls gelten für den Bereich der Cyber Sicherheit folgende **grundlegende Prinzipien:**

Rechtsstaatlichkeit: Das staatliche Handeln im Bereich der Cyber Sicherheit muss den hohen rechtsstaatlichen Standards der österreichischen Verwaltung entsprechen und die **Einhaltung der Menschenrechte**, insbesondere der Privatsphäre und des Datenschutzes sowie der Meinungsäußerungsfreiheit und des Rechts auf Information, gewährleisten.

Subsidiarität: Cyber Sicherheit ist ein Rechtsgut. Der Staat bekennt sich daher zu einem hohen Engagement zum Schutz dieses Rechtsguts, kann und soll aber nicht die alleinige Verantwortung für den Schutz des Cyber Raums übernehmen. Die Eigentümer und Betreiber von Informations- und Kommunikationstechnologie (IKT) sind in erster Linie für den Schutz ihrer Systeme selbst verantwortlich. Dabei gilt der Grundsatz »Selbstverpflichtung wenn möglich, Regulierung wenn notwendig«.

---

1 Siehe http://www.digitales.oesterreich.gv.at/site/5743/default.aspx#a2

Selbstregulierung: Grundsätzlich sollte angestrebt werden, über Eigeninitiativen das Schutzniveau durch Code of Conducts, Standardisierungen und Zertifizierungen zu erhöhen. Es bleibt aber Aufgabe des Staates, den Ordnungsrahmen für den Schutz der IKT von Unternehmen und Privaten zu schaffen und die Selbstregulierung im privaten Bereich zu begleiten.

Verhältnismäßigkeit: Die Maßnahmen und Kosten zur Erhöhung des Schutzniveaus müssen in einem ausgeglichenen Verhältnis zum jeweiligen Risiko und zu den Möglichkeiten zur Gefahrenminderung stehen.

Aufbauend auf diesen Prinzipien wird eine umfassende und kohärente **Cyber Sicherheitspolitik** entwickelt. Diese umfasst alle Maßnahmen auf nationaler, europäischer und internationaler Ebene

- zur positiven Mitgestaltung des Cyber Space im Interesse der Bürger, der Wirtschaft, der Wissenschaft und des Staates,
- zur Verhinderung des Entstehens oder Wirksamwerdens von Bedrohungen des Cyber Space und der Menschen im Cyber Space (Prävention) sowie
- zum Schutz des Rechtsgutes Cyber Sicherheit gegenüber Bedrohungen bzw. zu deren Bewältigung.

4 Strategische Ziele

Österreich wird sich in Richtung einer **digitalen Gesellschaft** weiter entwickeln, wobei auf die Kompatibilität mit den **Grundwerten einer offenen Gesellschaft** zu achten ist. Der dynamische virtuelle Raum ermöglicht sozialen Wohlstand sowie wirtschaftliche Vorteile im Rahmen von E-Government und E-Commerce und ist auch **Grundlage für Informationsaustausch sowie soziale und politische Partizipation.**

Österreich verfolgt im Rahmen seiner Strategie für Cyber Sicherheit folgende **strategische Ziele**:

- Sowohl Verfügbarkeit, Zuverlässigkeit und Vertraulichkeit des Datenaustausches als auch Integrität der Daten selbst sind nur in einem **sicheren, resilienten und verlässlichen Cyber Raum** gewährleistet. Deshalb muss der virtuelle Raum fähig sein, Risiken zu widerstehen, Schocks zu absorbieren und sich einem veränderten Umfeld anzupassen. Besonders wichtige IKT-Systeme sollen möglichst redundant ausgelegt werden.
- Österreich wird durch einen **gesamtstaatlichen Ansatz der zuständigen Bundesministerien** sicherstellen, dass seine **IKT Infrastrukturen** sicher und resilient gegen Gefährdungen sind. Die staatlichen Stellen werden dabei eng und partnerschaftlich mit dem privaten Sektor zusammenarbeiten.
- Das **Rechtsgut Cyber Sicherheit** wird von den österreichischen Behörden in Zusammenarbeit mit nicht-staatlichen Partnern unter Einsatz wirksamer und verhältnismäßiger Mittel in den Bereichen der politisch-strategischen Steuerung, der Erkennung und Reaktion sowie der Folgenminderung und Wiederherstellung geschützt.
- Durch eine Vielzahl von **Awareness Maßnahmen** wird eine »**Kultur der Cyber Sicherheit**« in Österreich implementiert.
- Durch den Aufbau von Wissen, Fähigkeiten und Kapazitäten werden im Rahmen eines nationalen Dialogs zu Cyber Sicherheit bestehende Kooperationen gestärkt sowie neue Initiativen unterstützt und miteinander verbunden. Damit wird Österreich ein **Wegbereiter bei der Umsetzung von Maßnahmen zur Sicherung der digitalen Gesellschaft.** Das stärkt auch die Attraktivität des Wirtschaftsstandorts Österreich, der sich durch die hohe Verfügbarkeit, Integrität und Vertraulichkeit der benötigten IKT-Infrastruktur auszeichnet.
- Österreich wird eine **aktive Rolle bei der internationalen Zusammenarbeit** auf europäischer und internationaler Ebene spielen, insbesondere im Erfahrungsaustausch, bei der Erstellung internationaler Strategien, bei der Erarbeitung freiwilliger und rechtlich verbindlicher Regelungen, bei der Strafverfolgung sowie bei der Durchführung von transnationalen Übungen und Kooperationsprojekten.
- Das **E-Government** der österreichischen Verwaltung ist sicher und wird weiter ausgebaut; die Sicherheitsmaßnahmen von Bund, Ländern, Städten und Gemeinden werden gestärkt.
- Alle **österreichischen Unternehmen** werden die Integrität der eigenen Anwendungen sowie die Identität und Privatsphäre ihrer Kunden schützen. Die enge und systematische Zusammenarbeit zwischen Unternehmen spielt dabei eine besondere Rolle.
- Die **österreichische Bevölkerung** soll sich der individuellen Verantwortung im Cyber Raum bewusst sein und sich bei allen online Aktivitäten schützen sowie über die notwendigen Fähigkeiten zur elektronischen Authentifizierung und Unterschrift verfügen.

5 Handlungsfelder und Maßnahmen

Handlungsfeld 1 – Strukturen und Prozesse

Zielausrichtung:

Im Bereich Cyber Space gibt es zahlreiche Strukturen und Stakeholder, die – jeder für sich – an Cyber Sicherheit arbeiten. Mehrere ausschließlich auf Cyber Sicherheit spezialisierte Organisationen (z. B. CERTs[1]) spielen bereits jetzt eine wichtige Rolle im Cyber Krisenmanagement. Übergreifende Cyber Sicherheit Abläufe sind jedoch derzeit nicht formal festgelegt. Es sind daher Prozesse und Strukturen festzulegen, die eine übergeordnete Koordination sowohl auf politisch-strtegischer Ebene als auch auf operativer Ebene unter Einschluss aller relevanten Stakeholder im öffentlichen und privaten Bereich sicherstellen.

Maßnahmen:

1) Einrichtung einer Cyber Sicherheit Steuerungsgruppe

- Die mit Ministerratsbeschluss vom 11. Mai 2012 eingerichtete **Cyber Sicherheit Steuerungsgruppe** soll unter Federführung des Bundeskanzleramtes auf politisch-strategischer Ebene die Maßnahmen zur Cyber Sicherheit koordinieren, die Umsetzung der ÖSCS beobachten und begleiten, einen jährlichen Bericht zur Cyber Sicherheit erstellen und die Bundesregierung in Angelegenheiten der Cyber Sicherheit beraten. Die Steuerungsgruppe setzt sich aus den Verbindungspersonen zum Nationalen Sicherheitsrat[2] und Cyber Sicherheit Experten der im Nationalen Sicherheitsrat vertretenen Ressorts zusammen. Insbesondere wird auch der Chief Information Officer des Bundes diesem Gremium angehören. Themenorientiert wird die Steuerungsgruppe um Vertreter weiterer Ressorts und der Länder erweitert. Dazu zählen insbesondere jene Ressorts, in deren Wirkungsbereich die durch die Steuerungsmaßnahmen adressierten bzw. betroffenen Organisationen und Unternehmen fallen. Vertreter relevanter Unternehmen werden in geeigneter Form eingebunden.

2) Schaffung einer Struktur zur Koordination auf der operativen Ebene

- Aufbauend auf bestehende operative Strukturen sowie unter deren Einbindung wird eine **Struktur zur Koordination auf der operativen Ebene** geschaffen. In ihrem Rahmen soll insbesondere ein periodisches und anlassbezogenes **Lagebild Cyber Sicherheit** erstellt und über zu treffende Maßnahmen auf der operativen Ebene beraten werden. Gewährleistet werden soll auch ein kontinuierlicher Überblick über die aktuelle Situation im Cyber Space durch Sammeln, Bündeln, Auswerten und Weitergeben von relevanten Informationen. Dabei ist auch die Wirtschaft in geeigneter Form auf Augenhöhe einzubinden. Der permanent und gemeinsam erarbeitete Status zur Situation im Cyberspace soll allen Beteiligten als Grundlage für zu treffende planerische, präventive und reaktive Maßnahmen dienlich sein. Die Betreiber von kritischen Infrastrukturen werden auf der operativen Ebene und insbesondere bei Störungen im Bereich der Informations- und Kommunikationsstrukturen unterstützt sowie über Gefahren im Netz informiert. Die Operative Koordinierungsstruktur ist so zu gestalten, dass es möglich ist, sie als operatives Ausführungsorgan des übergreifenden Cyber Krisenmanagement zu nützen.

1 Computer Emergency Response Team

2 Bundesgesetz über die Errichtung eines Nationalen Sicherheitsrates § 5 Abs. 1

- Die Arbeiten im Rahmen der **Operativen Koordinierungsstruktur** werden unter Einbindung der Ressorts und operativer Strukturen aus Wirtschaft und Forschung vom BM.I koordiniert (PPP-Modell). Es wird bei der entsprechenden Koordination auf der operativen Ebene vom BMLVS unterstützt, auf das die Federführung im Cyber Defence Fall übergeht. Die operativen organisations-, sektoren- bzw. zielgruppenorientierten Strukturen bleiben im jeweiligen Verantwortungsbereich. Im Rahmen der Operativen Koordinierungsstruktur sollen Einrichtungen zusammenarbeiten, die sich mit der Sicherheit von Computersystemen und des Internets sowie dem Schutz von kritischen Infrastrukturen beschäftigen. Es sind dies im staatlichen Bereich insbesondere GovCERT (Government Computer Emergency Response Team), MilCERT (Military Cyber Emergency Readiness Team) und das Cyber Crime Competence Center (C 4). Darüber hinaus werden in einem zweiten Kreis weitere staatliche Einrichtungen sowie in einem erweiterten Kreis private CERTs (CERT.at, BRZ-CERT, Banken, …), Wirtschaft und Forschung eingebunden.
- Von der Cyber Sicherheit Steuerungsgruppe wird eine **Arbeitsgruppe** eingerichtet, die Vorschläge für notwendige Prozesse und Strukturen zur permanenten Koordination auf der operativen Ebene erarbeitet. Dabei werden auch Vertreter relevanter Unternehmen in geeigneter Weise eingebunden.

3) Einrichtung eines Cyber Krisenmanagements

- Das **Cyber Krisenmanagement** setzt sich aus Vertretern des Staates und der Betreiber von kritischen Infrastrukturen zusammen. Es orientiert sich in seiner Zusammensetzung und Arbeitsweise an dem staatlichen Krisen- und Katastrophenmanagement (SKKM). Aufgrund der über IKT hinausreichenden Betroffenheit und im Sinne der inneren Sicherheit übernimmt für übergreifende Bedrohungen der Cyber Sicherheit das BM.I die Federführung. Im Sinne der äußeren Sicherheit geht die Federführung für den Souveränitätsschutz im Rahmen der militärischen Landesverteidigung (Cyber Defence) auf das BMLVS über.
- **Krisenmanagement- und Kontinuitätspläne** werden auf Basis von Risikoanalysen für sektorspezifische und sektorübergreifende Cyber Bedrohungen in Zusammenarbeit von öffentlichen Einrichtungen und den Betreibern von kritischen Infrastrukturen ausgearbeitet und laufend aktualisiert.
- Regelmäßige **Cyber Übungen** sollen das Cyber Krisenmanagement sowie die Krisenmanagement- und Kontinuitätspläne testen.

4) Stärkung bestehender Cyber Strukturen

- Die Rolle des vom BKA betriebenen **GovCERTs** als staatliches CERT wird erweitert und gestärkt. Verantwortung, Befugnisse und Wirkungsbereich, die Verankerung innerhalb der öffentlichen Verwaltung, die Rolle des GovCERTs im Krisenfall und das Zusammenspiel mit der Operativen Koordinationsstruktur sollen detailliert und neue Anforderungen spezifiziert werden.
- Zur Vorbeugung und Prävention von Cyberkriminalität sowie zur operativen internationalen Kooperation in diesem Bereich wird das vom BM.I betriebene **Cyber Crime Competence Center** (C 4) weiter ausgebaut. Das Center ist die österreichische Zentralstelle zur Wahrnehmung sicherheits- und kriminalpolizeilicher Aufgaben im Bereich der Cyber Sicherheit.
- Zum Schutz der eigenen Netze, zum weiteren Aufbau des Lagebildes Cyber Sicherheit und als Basis operativer Fähigkeiten zur Abwehr von Cyber Angriffen wird das vom BMLVS betriebene **MilCERT** weiter ausgebaut. Aus diesen Fähigkeiten sind u.a. Kapazitäten zur Assistenzleistung im IKT-Bereich zu schaffen.
- Um die nationale Zusammenarbeit im Bereich österreichischer CERTs zu verbessern soll der österreichische **CERT-Verbund** ausgebaut und das **CERT.at** gestärkt werden. Dadurch soll die Entwicklung der CERTs in allen Sektoren gefördert und ein Informations- und Erfahrungsaustausch zu CERT spezifischen Themen intensiviert werden.

Handlungsfeld 2 – Governance

Zielausrichtung:
Die Rolle, die Zuständigkeiten und die Kompetenzen von Staat und nicht-staatlichen Akteuren im Cyber Raum werden festgelegt und Rahmenbedingungen für die Zusammenarbeit aller Akteure geschaffen.

Maßnahmen:

5) Schaffung eines zeitgemäßen ordnungspolitischen Rahmens

- Unter der Leitung der **Cyber Sicherheit Steuerungsgruppe** wird ein umfassender Bericht über die Notwendigkeit der Schaffung zusätzlicher **rechtlicher Grundlagen, regulatorischer Maßnahmen** und nicht-rechtlicher **Selbstverpflichtungen** (Code of Conduct) für die Gewährleistung der Cyber Sicherheit in Österreich erstellt und der Bundesregierung vorgelegt. In diesem Bericht sollen unter anderem die Fragen der Schaffung der notwendigen organisatorischen Strukturen, die behördlichen Aufgaben und Befugnisse, des Informationsaustauschs zwischen Behörden und Privaten, der Meldeverpflichtungen, der Verpflichtung zum Ergreifen von Schutzmaßnahmen und der Supply Chain Sicherheit behandelt werden.
- Bei der Festlegung von Verpflichtungen für nicht-staatliche Akteure ist der **ausgewogene Einsatz von Anreizen und Sanktionen** zu erwägen.

6) Festlegung von Mindestsicherheitsstandards

- Für eine effektive Sicherheitsprävention und zum gemeinsamen Verständnis über aktuelle Anforderungen sollen im Zusammenspiel aller relevanten Stakeholder **Mindestsicherheitsstandards** für die Cyber Sicherheit definiert werden. Die dabei definierten Anforderungen sollen für alle in sicherheitsrelevanten IKT Bereichen eingesetzten Komponenten und Dienstleistungen gelten. Die gültigen Normen, Standards, Verhaltensregeln, Best Practises usw. werden im österreichischen **Informationssicherheitshandbuch** zusammengefasst und laufend aktualisiert.

7) Erstellung eines jährlichen Berichts zur Cyber Sicherheit

- Durch die **Cyber Sicherheit Steuerungsgruppe** wird ein jährlicher Bericht »**Cyber Sicherheit in Österreich**« erstellt.

Handlungsfeld 3 – Kooperation Staat, Wirtschaft und Gesellschaft

Zielausrichtung:
Viele Aufgaben und Verantwortlichkeiten von öffentlichen Verwaltungen, Wirtschaft und Bevölkerung basieren auf Informations- und Kommunikationstechnologie. Die Verantwortung, mit digitaler Technik sorgfältig umzugehen, liegt bei jeder anwendenden Organisationseinheit. Aber erst eine breite Kooperation aller Bereiche und ein permanenter gegenseitiger Informationsaustausch machen die Verwendung von IKT transparent und sicher. Bestehende Kapazitäten und Prozesse in Verwaltung, Wirtschaft und bei den Bürgerinnen und Bürgern sollen durch Zusammenarbeit gestärkt und neue Möglichkeiten generiert werden.

Maßnahmen:

8) Einrichtung einer Cyber Sicherheit Plattform

- Zur laufenden Kommunikation mit allen Stakeholdern aus Verwaltung, Wirtschaft und Wissenschaft wird unter Fortführung und Nutzung bestehender Initiativen (wie z. B. Austrian Trust Circle, Cyber Security Austria, Kuratorium sicheres Österreich, A-SIT[3], …) die **Österreichische Cyber Sicherheit Plattform** als Public Private Partnership betrieben. Mit dieser Plattform soll ein ständiger Informationsaustausch der öffentlichen Verwaltung untereinander sowie der öffentlichen Verwaltung mit Vertretern der Wirtschaft, Wissenschaft und Forschung institutionalisiert werden. Alle Akteure nehmen in gleichberechtigter Weise an der Plattform teil. Die Cyber Sicherheit Plattform berät und unterstützt die Cyber Sicherheit Steuerungsgruppe.
- Die **Zusammenarbeit mit privaten Betreibern kritischer Infrastrukturen und weiteren Wirtschaftssektoren** ist für die Cyber Sicherheit Österreichs von zentraler Bedeutung. Die nähere Ausgestaltung dieser Kooperation wird Gegenstand von weiterführenden Gesprächen der Cyber Sicherheit Steuerungsgruppe mit der Wirtschaft sein.
- Im Rahmen der Cyber Sicherheit Plattform sollen auch umfassende **Kooperationen zwischen den beteiligten Partnern** in den Bereichen Sensibilisierung und Ausbildung sowie Forschung und Entwicklung initiiert werden.
- Um das gegenseitige Verständnis für die Herausforderungen und die Handlungsmöglichkeiten aller an der Cyber Sicherheit beteiligten Partner zu fördern, soll der **Austausch** von Expertinnen und Experten zwischen den beteiligten staatlichen, privatwirtschaftlichen und wissenschaftlichen Organisationen gestärkt werden. Unter Führung der Cyber Sicherheit Steuerungsgruppe und mit Hilfe der Österreichischen Cyber Sicherheit Plattform soll hierfür ein Programm erarbeitet werden.

9) Stärkung der Unterstützung für KMUs

- KMUs werden mit **Schwerpunktprogrammen für Cyber Sicherheit** sensibilisiert und auf Gefährdungssituationen vorbereitet. Interessenvertretungen sollen dazu angehalten werden, auf dem neuen Internetportal IKT-Sicherheit[4] spezifische Informationen für KMUs online zu stellen und Cyber Sicherheit Aktionen für KMUs zu initiieren. Sektor spezifische Informations-Plattformen wie die Austrian Trust Circles sollen zusammen mit staatlichen Stellen branchentypische Cyber Risikomanagementpläne ausarbeiten; Regulierungsbehörden und Interessenvertretungen werden in diesen Dialog eingebunden. Diese Risikomanagementpläne werden mit den staatlichen Krisen- und Kontinuitätsmanagementplänen abgestimmt. Übergreifende Cyber Übungen für KMUs sollen periodisch aufgesetzt und durchgeführt werden. Sektoren der KMUs sollen auf Wunsch an übergreifenden staatlichen Cyber-Übungen teilnehmen können.

10) Ausarbeitung einer Cyber Sicherheit Kommunikationsstrategie

- Zur Optimierung der Kommunikation zwischen den Stakeholdern in der Verwaltung, der Wirtschaft, der Wissenschaft und in der Gesellschaft sind die von den staatlichen Stellen bereits eingerichteten und geplanten Websites im Rahmen einer Cyber Sicherheit Kommunikationsstrategie aufeinander abzustimmen. Die **Kommunikationsstrategie** wird von der Cyber Sicherheit Steuerungsgruppe unter Einbeziehung aller relevanten Stakeholder vorbereitet.

---

3 Zentrum für sichere Informationstechnologie - Austria

4 Vergl. Maßnahme 12

Handlungsfeld 4 – Schutz kritischer Infrastrukturen

Zielausrichtung:

Beinahe alle Infrastrukturen sind heute in zunehmendem Ausmaß von spezialisierten IKT-Systemen abhängig, die einen möglichst reibungslosen, verlässlichen und durchgehenden Betrieb garantieren sollen. In diesem Sinne ist die Erhöhung der Widerstandskraft dieser Informationssysteme gegen Bedrohungen eine vorrangige Aufgabe. Im Rahmen des Programms zum Schutz kritischer Infrastrukturen (APCIP) werden Unternehmen, die kritische Infrastrukturen betreiben, angehalten, eine umfassende Sicherheitsarchitektur zu implementieren. Mit der ÖSCS sollen diese Maßnahmen hinsichtlich Cyber Sicherheit ergänzt und vertieft werden. Dabei ist die Kooperation mit den Betreibern von kritischen Informationsinfrastrukturen vorrangig.

Maßnahmen:

11) Resilienz der kritischen Infrastrukturen erhöhen

- Betreiber von kritischen Infrastrukturen sollen bei **Prozessen des nationalen Cyber Krisenmanagements** eingebunden werden. Diese strategischen Unternehmen sollen eine **umfassende Sicherheitsarchitektur** (Risiko- und Krisenmanagement) einrichten, gefährdungsorientiert aktualisieren sowie über einen Sicherheitsbeauftragten verfügen. Die **Krisenkommunikation** soll ausgebaut und gestärkt werden. In einem partnerschaftlichen Ansatz sollen für diese Unternehmen **Cyber Sicherheitstandards** definiert werden.
- **Schwere Cyber Vorfälle** sollen für Betreiber von kritischen Infrastrukturen meldepflichtig sein. Die entsprechende gesetzliche Grundlage dafür ist nach umfassenden Konsultationen mit den relevanten Stakeholdern zu schaffen.
- Die bestehenden Dispositionen im Bereich des **Schutzes kritischer Infrastrukturen** (**APCIP**) und des **staatlichen Krisen- und Katastrophenmanagements** (**SKKM**) sollen laufend im Hinblick auf neue Cyber Herausforderungen überprüft und bei Bedarf weiterentwickelt werden.

Handlungsfeld 5 – Sensibilisierung und Ausbildung

Zielausrichtung:

Durch Sensibilisierung aller Zielgruppen soll die notwendige Wahrnehmung, das persönliche Interesse und die Aufmerksamkeit für Cyber Sicherheit gestärkt werden. Diese Bewusstseinsbildung soll Verständnis für die Notwendigkeit von Cyber Sicherheit schaffen. Durch konkrete und zielgruppenspezifische Maßnahmen wird das erforderliche Wissen für ein sicherheitsbewusstes Handeln und einen verantwortungsvollen Umgang mit Informationen und der IKT insgesamt vermittelt und gefördert. Mit einer verstärkten Ausbildung in Cyber Sicherheit und Medienkompetenz in Schulen und anderen Bildungseinrichtungen sowie dem Aufbau einer nationalen Cyber Sicherheitskompetenz in der Lehre soll ein sinnvolles und hinreichendes IKT Kompetenzniveau sichergestellt werden.

Maßnahmen:

12) Stärkung der Cyber Sicherheit Kultur[5]

- **Sensibilisierungsinitiativen** werden auf der Grundlage einer gemeinsamen Vorgangsweise unter Berücksichtigung bereits bestehender Programme erarbeitet, abgestimmt und durchgeführt. Dabei sollen Cyber Sicherheit aus verschiedenen Blickwinkeln betrachtet,

5 siehe Nationale IKT Sicherheitsstrategie, Kapitel Awareness

auf relevante Gefahren hingewiesen, mögliche Auswirkungen und Schäden aufgezeigt und Empfehlungen hinsichtlich Sicherheitsmaßnahmen gegeben werden.
- Um verschiedenen Zielgruppen eine weiterführende und individuelle Beratung zu ermöglichen, sollen bestehende **Beratungsangebote** weiter verstärkt und ausgebaut werden.
- Ein **Internetportal IKT-Sicherheit** wird in Form einer Web-Plattform als zentrale Informations- und Kommunikationsbasis für Sensibilisierungsmaßnahmen eingerichtet. Die Koordination des Internetportals IKT-Sicherheit erfolgt durch BMF, BKA und A-SIT, wobei sich die strategische Ausrichtung des Portals an den Prinzipien und Zielen der ÖSCS orientiert.
- Die **Präventionsangebote** zur Vorbeugung von **Cyberkriminalität** werden weiter ausgebaut.

13) Verankerung von Cyber Sicherheit und Medienkompetenz auf allen Ebenen der Aus- und Weiterbildung[6]

- Verstärkte Aufnahme von **IKT, Cyber Sicherheit und Medienkompetenz in den Unterricht**. Der Umgang mit IKT und neuen Medien ist im Unterricht in allen Schularten integriert. IKT-Sicherheitsthemen und Cyber Sicherheit sollen – abgestimmt auf die Lehrpläne der jeweiligen Schulart – **Bestandteil eines Modells** »**Digitaler Kompetenzen**« sein. Dadurch soll Bewusstsein für Sicherheitsthemen geschaffen und zu einem verantwortungsvollen Umgang hingeführt werden. Ziel ist es, ein IKT-Kompetenzniveau quer über alle Schularten hinweg sicherzustellen.
- IKT(Sicherheits-)Kompetenz soll in die **Ausbildung an pädagogischen Hochschulen und Universitäten** als Voraussetzung für die Vermittlung dieser Kompetenz an den Schulen sowie Einrichtungen der Erwachsenenbildung aufgenommen werden.
- Die **Ausbildung von Spezialisten** im staatlichen Bereich zur Erhöhung der Cyber Sicherheit wird in Zusammenarbeit mit nationalen und internationalen Ausbildungseinrichtungen ausgebaut.
- Für das **Erkennen von Cybervorfällen** sollen IKT Systemadministratoren der Bertreiber von kritischen Infrastrukturen in Cyber Sicherheit ausgebildet und darauf trainiert werden, Anomalien in ihren IKT Systemen zu erkennen und an den Sicherheitsbeauftragten zu berichten (**Human Sensor Programm**).

Handlungsfeld 6 – Forschung und Entwicklung

Zielausrichtung:

Zur Gewährleistung von Cyber Sicherheit ist eine technische Expertise erforderlich, die auf aktuellen Forschungs- und Entwicklungsergebnissen basiert. Dazu ist eine vermehrte Einbindung von Cyber Sicherheitsthemen in angewandte Cyber Forschung und in Sicherheitsforschungsprogramme wie KIRAS notwendig. Ebenso ist eine aktive Themenführerschaft bei EU-Sicherheitsforschungsprogrammen anzustreben.

Maßnahmen:

14) Österreichs Forschung im Bereich Cyber Sicherheit stärken[7]

- Im Rahmen der nationalen und der EU-Sicherheitsforschungsprogramme soll **Cyber Sicherheit** einer der zentralen **Forschungsschwerpunkte** sein. Die relevanten Stakeholder in Verwaltung, Wirtschaft und Forschung werden in gemeinsamen Projekten die konzep-

6 siehe Nationale IKT Sicherheitsstrategie, Kapitel Bildung und Forschung

7 Details siehe Nationale IKT Sicherheitsstrategie, Kapitel Bildung und Forschung

tuellen Grundlagen und die technologischen Instrumente zur Hebung des Cyber Sicherheitsstandards in Österreich entwickeln. Maßnahmen, die dazu beitragen, Forschungs- und Entwicklungsergebnisse zügig in marktfähige Produkte zu übertragen, werden dabei besonders beachtet. Bereits bestehende Forschungsarbeiten, wie z. B. die von A-SIT, sollen weiter ausgebaut werden.

- Österreich soll eine **aktive Themenführerschaft bei EU-Sicherheitsforschungsprogrammen** anstreben. Dabei sollen für Österreich wichtige Themen in internationale Forschungsprogramme eingebracht werden.

Handlungsfeld 7 – Internationale Zusammenarbeit

Zielausrichtung:

Globale Vernetzung und internationale Zusammenarbeit sind zentrale Faktoren für die ÖSCS. Sicherheit im Cyber Raum kann nur durch abgestimmte Instrumentarien auf nationaler und internationaler Ebene erreicht werden. Österreich wird daher eine aktive Cyber Außenpolitik betreiben und seine Interessen im Rahmen von EU, VN, OSZE, Europarat, OECD und NATO Partnerschaften koordiniert und gezielt verfolgen. Zudem werden die internationalen Bezüge der Cyber Politik in anderen Politikfeldern konsequent aufeinander abgestimmt.

Maßnahmen:

15) Effektives Zusammenwirken für Cyber Sicherheit in Europa und weltweit

- Österreich wird einen substanziellen Beitrag zur Erarbeitung und Umsetzung der **Cyber Sicherheitsstrategie der EU** leisten und sich umfassend an den strategischen und operativen Arbeiten der EU beteiligen[8].
- Durch die relevanten Ressorts werden die notwendigen Maßnahmen ergriffen, um die **Europaratskonvention über Cyberkriminalität** umzusetzen und voll zu nutzen.
- Österreich setzt sich auf internationaler Ebene für ein freies Internet ein, das die Ausübung aller **Menschenrechte im virtuellen Raum** gewährleisten soll. Insbesondere das Recht auf Meinungsfreiheit und Information darf auch im Internet keinen ungerechtfertigten Einschränkungen unterliegen. Diese Haltung soll in internationalen Foren vertreten werden. Damit wird Österreich aktiv an der Erstellung und Etablierung eines staatenübergreifenden Kodex für staatliches Verhalten im Cyberraum, der auch vertrauens- und sicherheitsbildende Maßnahmen umfasst, mitwirken.
- Österreich wird die begonnene bilaterale Kooperation im Rahmen der **NATO Partnerschaft für den Frieden** fortsetzen und sich in der **OSZE** aktiv für die Erarbeitung einer Liste konkreter vertrauens- und sicherheitsbildender Maßnahmen einsetzen.
- Österreich beteiligt sich aktiv an der Planung und Durchführung von **länderübergreifenden Cyberübungen**. Die Erkenntnisse daraus fließen direkt in Planung und Weiterentwicklung der operativen Zusammenarbeit ein.
- Die im Bereich Cyber Sicherheit relevanten **außenpolitischen Maßnahmen** werden vom **BMeiA koordiniert**. Sofern zweckmäßig, wird der Abschluss von zwischenstaatlichen oder internationalen Vereinbarungen ins Auge gefasst.

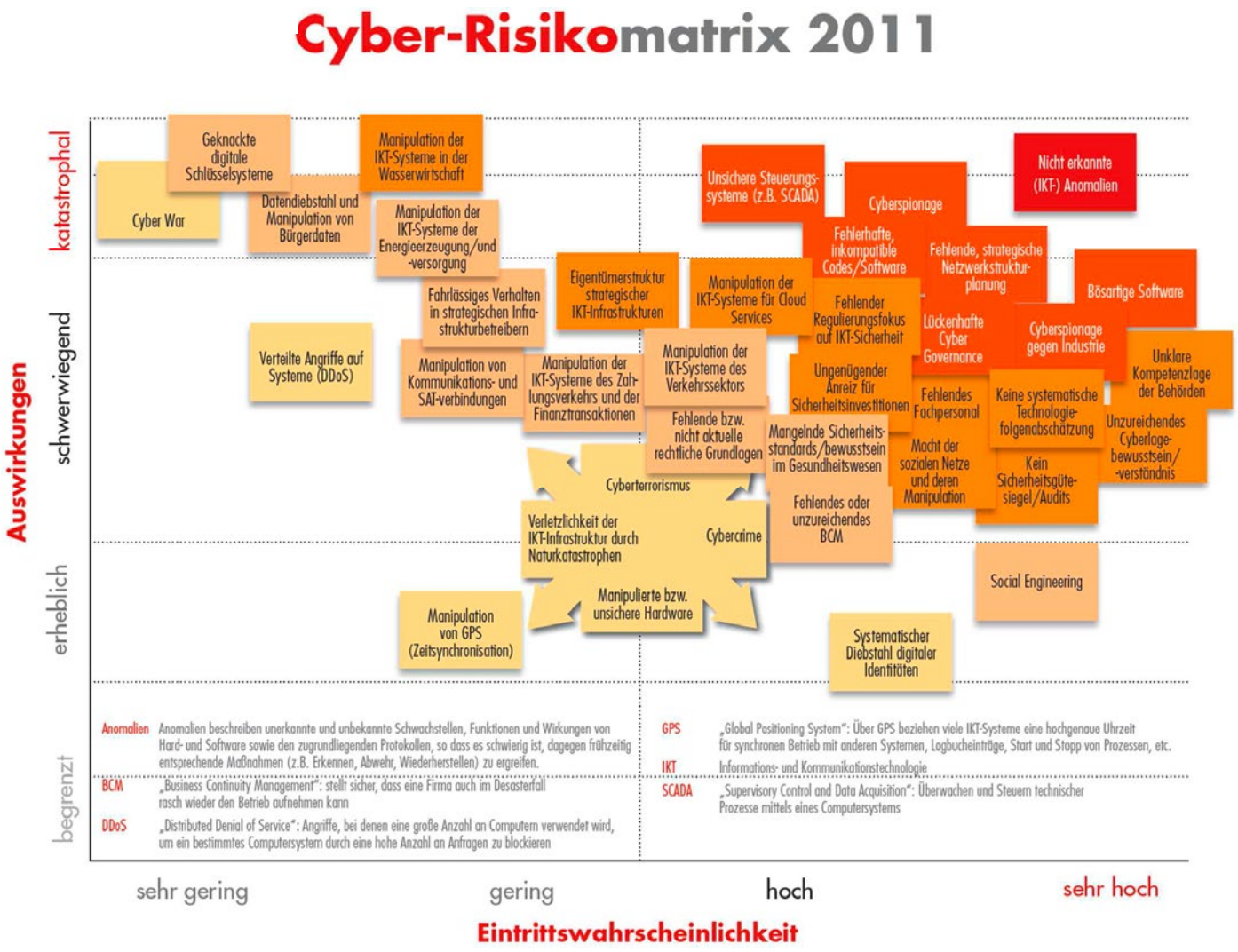
8 Die Europäische Kommission hat am 7.2.2013 die Entwürfe einer Cyber Sicherheit Strategie sowie einer Richtlinie betreffend Maßnahmen zur Sicherstellung eines hohen gemeinsamen Niveaus an Netzwerk- und Informationssicherheit präsentiert.

6 Umsetzung

Die Steuerungsgruppe erarbeitet innerhalb von drei Monaten nach Beschluss der ÖSCS durch die Bundesregierung einen **Implementierungsplan** für die in der Strategie angeführten horizontalen Maßnahmen. Die **Umsetzung** der Maßnahmen ist Angelegenheit der jeweils verantwortlichen Stellen im Rahmen ihres Auftrages. Die **Umsetzung der Maßnahmen** der ÖSCS wird von der Cyber Sicherheit Steuerungsgruppe koordiniert. Auf Grundlage der ÖSCS erarbeiten die betroffenen Ressorts Teilstrategien in ihren jeweiligen Verantwortungsbereichen. Alle zwei Jahre erfolgt durch die in der Cyber Sicherheit Steuerungsgruppe vertretenen Ressorts ein **Umsetzungsbericht** an die Bundesregierung. Gleichzeitig mit dem Umsetzungsbericht wird die **Aktualität** der Österreichischen Strategie zur Cyber Sicherheit überprüft und es werden allenfalls erforderliche Adaptierungen vorgenommen. Die Weiterentwicklung der strategischen Grundlagen erfolgt in Kooperation mit den nicht-staatlichen Partnern.

Annex 1

Cyber-Risikomatrix 2011



Annex 2

Abkürzungsverzeichnis

ACI	Austrian Critical Infrastructure / Österreichische kritische Infrastruktur
APCIP	Austrian Program for Critical Infrastructure Protection / Österreichisches Programm zum Schutz kritischer Infrastruktur
A-SIT	Zentrum für sichere Informationstechnologie – Austria
CERT	Computer Emergency Response Team
CERT.at	Computer Emergency Response Team – Austria
CII	Critical Information Infrastructure / Kritische Informationsinfrastrukturen
GovCERT	Staatliches Computer Emergency Response Team
IKT	Informations- und Kommunikationstechnologie
KMU	Kleine und mittlere Unternehmen
MilCERT	Militärisches Computer Emergency Response Team
MRV	Ministerratsvortrag
ÖSCS	Österreichische Strategie für Cyber Sicherheit
ÖSS	Österreichischen Sicherheitsstrategie
PPP	Public Private Partnership
SKKM	Staatliches Krisen- und Katastrophenschutzmanagement

Annex 3

Cyber Sicherheit Glossar

Awareness
bezeichnet das Sicherheitsbewusstsein aller an der Informationssicherheit mitverantwortlichen Personen. Die dauerhafte Einhaltung und Umsetzung von Sicherheitsregeln ist nur durch Verständnis und Motivation zu erreichen. Zur regelmäßigen Förderung des Bewusstseins über die Wichtigkeit ihrer Tätigkeiten für die Informationssicherheit sind die Mitarbeiter mit gezielten Awarenessmaßnahmen zu unterstützten.

CERT – Computer Emergency Response Team
ist die Bezeichnung eines Notfallteams, das bei Sicherheitsvorfällen zur Abwehr und Wiederherstellung von IKT-Systemen bereitgehalten wird.

Im Wesentlichen werden von Seiten eines CERT/CSIRT drei Dienste zur Verfügung gestellt:

Reaktiver Dienst: Bereitstellung von Notfallteams, die bei Sicherheitsvorfällen zur Abwehr und Wiederherstellung von IKT-Systemen bereitgehalten werden (auch als CSIRT für Computer Security Incident Response Team bezeichnet).

Präventiver Dienst: Die präventiven Aufgaben eines CERT sind die Beobachtung von Entwicklungen der IKT-Sicherheit, die Warnung vor Schwachstellen und erkannten Angriffsmustern. die Unterstützung bei der Schadensermittlung und die Erhöhung der Awareness in ihrem Wirkungsbereich besonders durch Ausbildung und Beratung.

Sicherheitsqualitätsmanagement: Bereitstellen einer fachlichen Know-How-Basis, Audit-Fähigkeiten und eines Lessons-Learned-Zyklus für den eigenen Wirkungsbereich.

Cyberkriminalität (Cyber Crime)
Cyberkriminalität umfasst rechtswidrige Angriffe aus dem Cyber Raum auf oder mittels IKT-Systemen, die strafrechtlich oder verwaltungsstrafrechtlich normiert sind und umfasst somit jede Form von Straftaten, die mit Hilfe von Informationstechnologien und Kommunikationsnetzen begangen werden. Auch die Internetkriminalität zählt dazu[1].

Cyber Angriff, Cyber Spionage, Cyber Sabotage
Ein Cyber Angriff ist ein Angriff mit Mitteln der IT im Cyber Raum, der sich gegen einen oder mehrere andere IT-Systeme richtet und zum Ziel hat, die Schutzziele der IKT Sicherheit als Teil oder Ganzes zu verletzen. Die Ziele der IT-Sicherheit (Vertraulichkeit, Integrität und Verfügbarkeit) können dabei als Teil oder Ganzes verletzt werden. Cyber Angriffe, die sich gegen die Vertraulichkeit eines IT-Systems richten, werden, als Cyber Spionage bezeichnet und stellen somit Spionage auf digitalem Wege dar. Cyber Angriffe gegen die Integrität und Verfügbarkeit eines IT-Systems werden als Cyber Sabotage bezeichnet[2].

1 Textquelle: AG »Cyber« + KSÖ: Cyber Risiko Matrix - Clossar

2 Textquelle: Definition AG »Cyber« nach: Bundesministerium des Innern, »Cybersicherheitsstrategie für Deutschland«, Berlin, 2010 + KSÖ: Cyber Risiko Matrix – Clossar (tlw.)

Cyber Defence

Ist die Summe aller Maßnahmen zur Verteidigung des Cyber- Raumes mit militärischen und speziell dafür geeigneten Mitteln zur Erreichung militärstrategischer Ziele. Cyber Defence ist ein integriertes System und besteht in seiner Gesamtheit aus der Umsetzung der Maßnahmen zur IKT-Sicherheit und der Informationssicherheit, aus den Fähigkeiten des milCERTs, der CNO (Computer Network Operations) und der Unterstützung durch die physischen Fähigkeiten der Streitkräfte.

Cyber Raum / Cyber Space / Virtueller Raum

Der Cyber Raum ist der virtuelle Raum aller auf Datenebene vernetzten IT-Systeme im globalen Maßstab. Dem Cyber Raum liegt als universelles und öffentlich zugängliches Verbindungs- und Transportnetz das Internet zugrunde, welches durch beliebige andere Datennetze ergänzt und erweitert werden kann[3]. Im allgemeinen Sprachgebrauch bezeichnet Cyber Space auch das weltweite Netzwerk von verschiedenen unabhängigen IK-Infrastrukturen, Telekommunikations-netzen und Computersystemen. In der sozialen Sphäre kann bei Benutzung dieses globalen Netzwerkes zwischen Individuen interagiert werden, Ideen ausgetauscht, Informationen verteilt, soziale Unterstützung gewährt, Geschäfte getätigt, Aktionen gelenkt, künstlerische und mediale Werke geschaffen, Spiele gespielt, politisch diskutiert und vieles mehr getan werden. Cyber Space ist ein Überbegriff für alles mit dem Internet verbundene und für die verschiedenen Internet Kulturen geworden. Viele Staaten betrachten die vernetzte IKT und die unabhängigen Netzwerke, die über dieses Medium operieren, als Teil ihrer »Nationalen Kritischen Infrastrukturen«.

Cyber Sicherheit

Cyber Sicherheit beschreibt den Schutz eines zentralen Rechtsgutes mit rechtsstaatlichen Mitteln vor akteursbezogenen, technischen, organisations- und naturbedingten Gefahren, die die Sicherheit des Cyber Space (inklusive Infrastruktur- und Datensicherheit) und die Sicherheit der Nutzer im Cyber Space gefährden. Cyber Sicherheit trägt dazu bei, die Gefährdungen zu erkennen, zu bewerten und zu verfolgen sowie die Fähigkeit zu stärken, Störungen im und aus dem Cyberspace zu bewältigen, die damit verbundenen Folgen zu mindern sowie die Handlungs- und Funktionsfähigkeit der davon betroffenen Akteure, Infrastrukturen und Dienste wieder herzustellen.

Cyber Terrorismus / Missbrauch des Internet für extremistische Zwecke

Unter Cyber Terrorismus wird politisch motivierte Kriminalität staatlicher und/oder nichtstaatlicher Akteure gegen Computer, Netzwerke und die darin gespeicherten Informationen verstanden. Das Ziel ist, eine schwere oder längere Zeit anhaltende Störung des öffentlichen Lebens oder eine schwere Schädigung des Wirtschaftslebens mit dem Vorsatz herbeizuführen, die Bevölkerung auf schwerwiegende Weise einzuschüchtern, öffentliche Stellen oder eine internationale Organisation zu einer Handlung, Duldung oder Unterlassung zu nötigen oder die politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Staates oder einer internationalen Organisation ernsthaft zu erschüttern oder zu zerstören. Dabei handelt es sich somit um organisierte Cybersabotage/-angriffe, die von politisch- fundamentalistischen bzw. terroristischen Gruppen oder Einzeltätern organisiert werden und sich gegen Staaten, Organisationen oder Unternehmen richten[4].

---

3 Textquelle: Definition AG »Cyber« nach: Bundesministerium des Innern, »Cybersicherheitsstrategie für Deutschland«, Berlin, 2010

4 Textquelle: AG »Cyber« + KSÖ: Cyber Risiko Matrix - Clossar

Cyberwar
Unter Cyberwar versteht man die kriegerische Auseinandersetzung im und um den virtuellen Raum mit Mitteln vorwiegend aus dem Bereich der Informationstechnik. In einem weiteren Sinne ist damit auch die Unterstützung militärischer Aktionen in den klassischen Operationsräumen Boden, See, Luft, Weltraum durch Maßnahmen aus dem virtuellen Raum angesprochen. Ganz allgemein werden darunter auch die hochtechnisierten Formen des Krieges im Informationszeitalter gemeint, die auf einer weitgehenden Computerisierung, Elektronisierung und Vernetzung fast aller militärischer Bereiche und Belange basieren[5].

Datenschutz / Data Protection
Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Das Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind[6].

DDOS (Verteilte Angriffe auf Systeme)
Distributed Denial of Services: Angriffe bei denen eine große Anzahl von Computern verwendet wird, um einen bestimmten Computer durch eine hohe Anzahl an Anfragen zu blockieren.

IKT
Überbegriff für alle Computer (IT) und Netzwerk- (KT) basierenden Technologien als auch der damit verbundenen Wirtschaftsbereiche. Informations- und Kommunikationstechnologie wird auch als Deckbegriff definiert, der jegliches Kommunikationsinstrument oder Kommunikations-anwendung beinhaltet, inklusive Radio, Fernsehen, Mobiltelefone (»Handys«), Hardware und Software für Computer und Netzwerke, Satellitensysteme, etc. sowie die verschiedenen Dienstleistungen und Anwendungen, die mit diesen Dingen verbunden sind[7].

IKT-Sicherheit
IKT-Sicherheit ist der Schutzzustand der Informations- und Kommunikations-technologie und der darin verwendeten Informationen, welcher der Art und Schutzwürdigkeit sowie der Art und Intensität einer möglichen Gefährdung entspricht[8].

IKT-System
ist die Zusammenfassung der Kräfte, Mittel und Verfahren für die Verarbeitung, Übertragung und/oder Vermittlung von Informationen zur Erfüllung einer bestimmten Aufgabe. Die Produkte (IKT-Dienstleistungen) eines IKT-Systems können im Wege von Schnittstellen oder bei Eignung im Wege von Services außerhalb der Systemgrenzen zur Verfügung gestellt werden.

Informationssicherheit / Netzwerksicherheit
ist ein Überbegriff zu IKT-Sicherheit und bezieht sich auf alle relevanten Informationen einer Organisation oder eines Unternehmens einschließlich von nicht elektronisch verarbeiteten Informationen. Es bezeichnet somit die Summe der Eigenschaften einer Organisation, die dem Schutz der Vertraulichkeit, Verfügbarkeit und Integrität der Informationen dienen.

---

5 Textquelle: ETH Zürich: »CSS Nr. 71/2010«, Zürich, 2010 + KSÖ: Cyber Risiko Matrix – Clossar + AG »Cyber«

6 Datenschutzgesetz DSG 2000, Artikel 1, Verfassungsbestimmung, Grundrecht auf Datenschutz, § 1. (1)

7 Textquelle: Definition AG »Cyber« nach: Bundesministerium des Innern, »Cybersicherheitsstrategie für Deutschland«, Berlin, 2010

8 Eigendefinition AG »Cyber« (BMLVS/BMI)

Informationen können in Form von gesprochenen Worten, in Dokumenten auf Papier oder sonst direkt lesbaren Medien oder als elektronische verarbeitete Daten in IKT-Systemen vorliegen.

Internet

Das Internet ist ein weltweites System miteinander verbundener Computer, die denselben Protokoll Standard (TCP/IP – transmission control protocol / Internet Protocol) verwenden und das von Milliarden von Benutzern genutzt wird. Es ist ein Netzwerk von Netzwerken, das aus Abermillionen von privaten, öffentlichen, akademischen, geschäftlichen und Verwaltungsnetzwerken besteht, welche auf lokaler wie auch auf globaler Ebene durch ein engmaschiges Netz von elektronischen, funktechnischen und optischen Netzwerktechnologien verbunden sind. Das Internet kennt keine zentralen Instanzen, weder in den technischen Umsetzungen noch in den Bestimmungen über Zugang und Nutzung. Nur die allgemeine Definition der beiden grundlegenden Namensräume im Internet, den Internet Protokoll Adressraum und dem Domain Name System, die von der Internet Corporation for Assigned Names and Numbers (ICANN) verwaltet werden. Das Internet funktioniert plattform- und betriebssystemübergreifend. Typische Dienste im Internet sind World Wide Web (www) und E-Mail.

Kritische Infrastruktur (KI), Critical Infrastructure (CI), Critical Information Infrastructure (CII)

Kritische Infrastrukturen sind jene Infrastrukturen oder Teile davon, die eine wesentliche Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen haben. Ihre Störung oder Zerstörung hat schwerwiegende Auswirkungen auf die Gesundheit, Sicherheit oder das wirtschaftliche und soziale Wohl der Bevölkerung oder die Funktionsweise von staatlichen Einrichtungen[9]. Oftmals wird Kritische Infrastruktur auch mit der Abkürzung des aus dem Englischen entlehnten Substantiv CI (Critical Infrastructure) ausgedrückt. Im internationalen wie nationalen Sprachgebrauch hat sich auch CIP (Critical Infrastructure Protection) um den Schutz kritischer Infrastruktur auszudrücken, durchgesetzt. Konform dazu wird somit auch der Schutz der kritischen Informations Infrastruktur als CIIP (Critical Information Infrastructure Protection) bezeichnet.

Malware

bezeichnet Computerprogramme, die vom Eigentümer des IKT-Systems unerwünschte und meist auch Schaden verursachende Funktionen ausführen. Der Begriff Malware bezeichnet als zusammenfassender Oberbegriff alle Arten von Schadsoftware, wie z. B. Viren, Würmer, Trojaner, Spyware, Backdoors uä.

Sensible Daten

nach dem österreichischen Datenschutzgesetz: Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben[10].

Social Engineering

Im Zusammenhang mit IT-Sicherheit wird dieser Begriff für eine Strategie von Online-Betrügern gebraucht und beschreibt Vorgehensweisen in der direkten Kommunikation des Angreifers mit dem Opfer mit dem Ziel, durch Manipulation an vertrauliche Informationen zu gelangen oder unberechtigt Leistungen in Anspruch nehmen zu können. Indem sie individuell auf ihre Opfer zugehen, steigern sie ihre Erfolgsraten: zuvor ausspionierte Daten wie etwa die Surfge-

9 Textquelle: Austrian Programme for Critical Infrastructure Protection - APCIP

10 www.sicherheitskultur.at, Glossar der Informationssicherheit

wohnheiten oder Namen aus dem persönlichen Umfeld des Opfers werden dafür verwendet, beispielsweise Phishing-eMails persönlich zu formulieren und dadurch Vertrauen zu wecken[11].

Staatliches Krisen- und Katstrophenschutzmanagement (SKKM)

Das SKKM regelt die Katastrophenbewältigung innerhalb Österreichs und die Gesamtheit aller Handlungen zur Abwehr und Bekämpfung der von einer Katastrophe herbeigeführten Gefahren und Schäden. Ziel ist Aufrechterhaltung oder möglichst rasche Wiederherstellung des öffentlichen Lebens, - insbesondere der Ordnung und Sicherheit sowie der lebensnotwendigen Grundversorgung. Sie betrifft demnach sowohl die im öffentlichen Auftrag organisierten Tätigkeiten der involvierten Behörden und Einrichtungen als auch alle privaten Hilfsorganisationen[12].

World Wide Web (www)

Name für die Gesamtheit der über Hyperlinks verknüpften Dokumente im Internet. Oft Synonym für letzteres verwendet[13].

11 Textquelle (tlw.): KSÖ: Cyber Risiko Matrix - Clossar

12 Richtlinie SKKM

13 www.sicherheitskultur.at, Glossar der Informationssicherheit