Strategien für Cybersicherheit

Die Strategien für Österreichs Cyberraum

E-Government Expert Group
18.03 2013
franz.vock@bka.gv.at

AGENDA

- Motivation

- Nationale IKT Sicherheitsstrategie
- Österreichische Strategie für Cybersicherheit

- Cybersicherheitsstrategie der EU
  - Strategie
  - Richtlinie

- Zusammenfassung

- Motivation

- Nationale IKT Sicherheitsstrategie
- Österreichische Strategie für Cybersicherheit

- Cybersicherheitsstrategie der EU
  - Strategie
  - Richtlinie

- Zusammenfassung

Digitale Welt

– großeThemen
– neue Gefahren

Sicherheit im Cyberspace

Um die Vielfalt von Cybersicherheit zu adressieren

braucht man …

Schutz der Gesellschaft vor Cyberbedrohungen

Schutz kritischer Informationsinfrastrukturen

Internationales Zusammenwirken

Standards für Produkte

Sensibilisierung

Cyber Grundschutz

Klare Verantwortungen hinsichtlich “Cyber” definieren

nationales Cyber Abwehrzentrum

Rechtssicherheit

Wirksame Kriminalitätsbekämpfung auch im Cyber-Raum

Verhaltensnormen im Cyberspace

Kooperation von Behörden festlegen

Krisen-management

Öffentlich privates Zusammenarbeiten festlegen

Sichere IT-Systeme in Österreich

Instrumentarien zur Vorbeugung und Abwehr von Cyber Angriffen

IKT-Ausbildung, Forschung, Entwicklung

Strategie

Strategie:
Längerfristig ausgerichtetes Anstreben eines Ziels unter Berücksichtigung der verfügbaren Mittel und Ressourcen

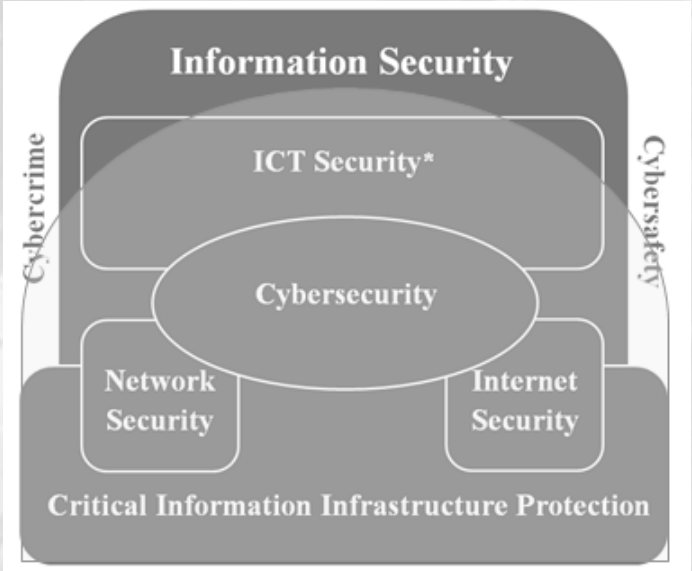
Definition

Cyber Raum / Cyber Space / Virtueller Raum

Der Cyber Raum ist der virtuelle Raum aller auf Datenebene vernetzten IT-Systeme

Cyber Sicherheit

Sicherheit des Cyber Raums



Herangehensweise

Erfahrungen

- Herangehensweise
- Nationale IKT Sicherheitsstrategie
- Österreichische Strategie für Cybersicherheit
- Cybersicherheitsstrategie der EU
  - Strategie
  - Richtlinie
- Zusammenfassung

Der Kickoff …

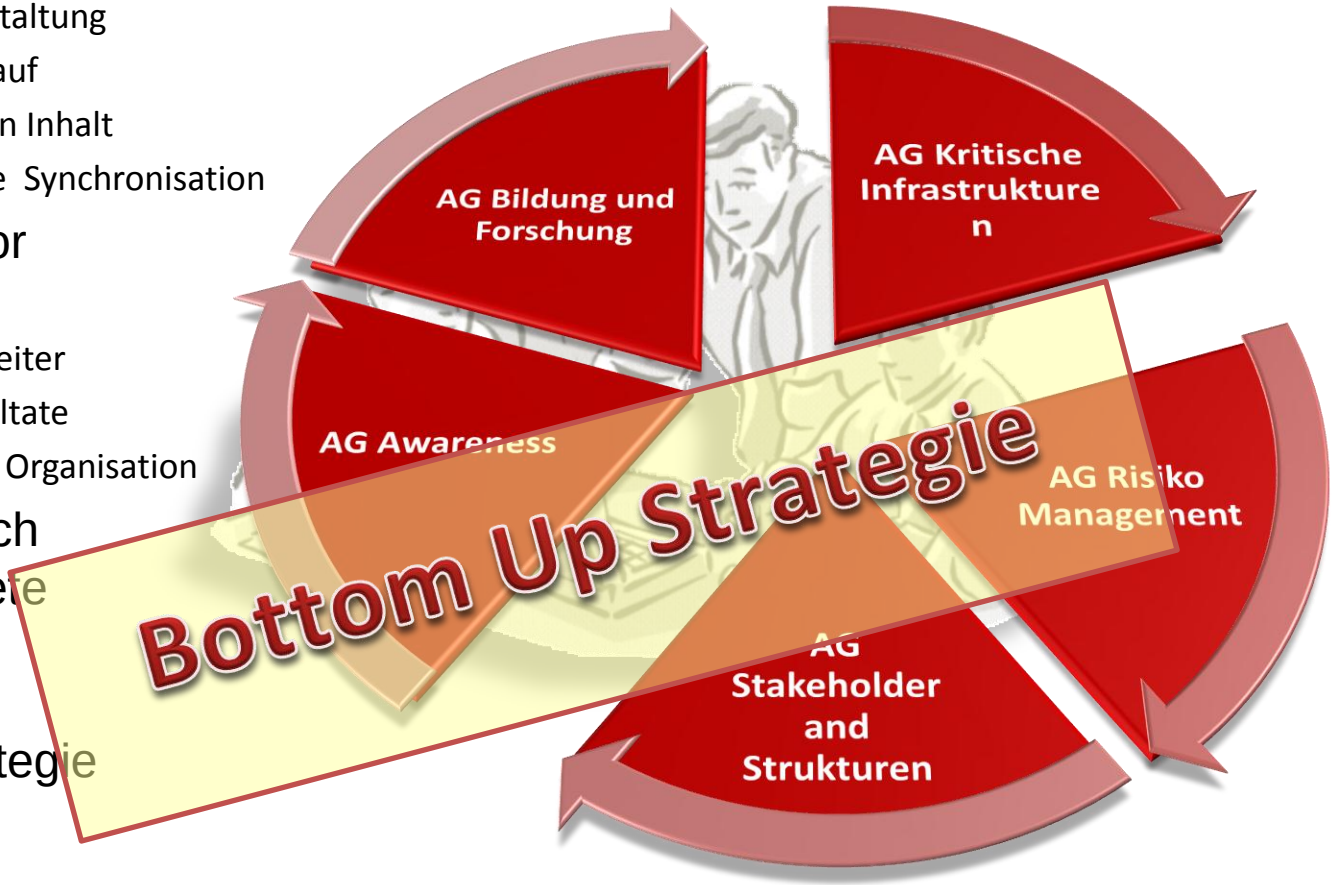
- Am 16. November 2011 startete die IKT Sicherheitsstrategie mit dem Kickoff
- Ca. 200 Teilnehmer
- **Zwei Drittel der Teilnehmer sagten eine aktive Teilnahme zu** die Strategie zu entwickeln.
- So startete die **größten Cyber-sicherheits Initiative in Österreich** mit Teilnehmern aus allen wichtigen Cybersicherheits-Bereichen

Programm Kickoff-Veranstaltung
IKT-Sicherheitsstrategie
16. November 2011

Zeit	Wer
9:30	Eintreffen
10:00-10:15	Begrüßung, Einleitung
10:15-10:45	Keynote Michael Hange Präsident des BSI-Deutschland Bundesamts für Sicherheit in der Informationstechnik IKT Sicherheitsstrategie in Deutschland
10:45-11:15	Keynote Reinhard Posch CIO des Bundes IKT Sicherheitsstrategie Europäische Anliegen und Ansätze
11:15-11:30	Der Prozess der IKT Sicherheitsstrategie
11:30-12:15	Arbeitsgruppenleiter Vorstellung
12:15-12:30	Zusammenfassung
12:30-13:00 bis 14:00	Zuordnung der Arbeitsgruppen und Buffet Raum für Zusammensein, Plaudern, Kennenlernen

IKT-Sicherheitsstrategie – 5 Arbeitsgruppen

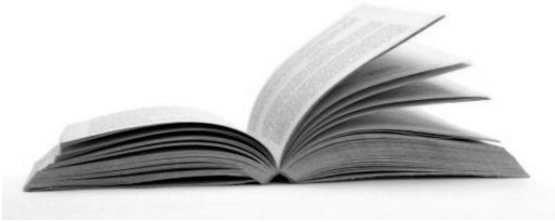
- Zwei Arbeitsgruppenleiter pro Gruppe
  - Frei in der Prozessgestaltung
  - Frei im zeitlichen Ablauf
  - Verantwortlich für den Inhalt
  - Verantwortlich für die Synchronisation
- Ein BKA Koordinator pro Gruppe
  - Unterstützt den AG-Leiter
  - Protokolliert die Resultate
  - Kümmert sich um die Organisation
- BKA is verantwortlich für die übergeordnete Koordination der gesamten IKT Sicherheitsstrategie



IKT-Sicherheitsstrategie– „must have“- Elemente

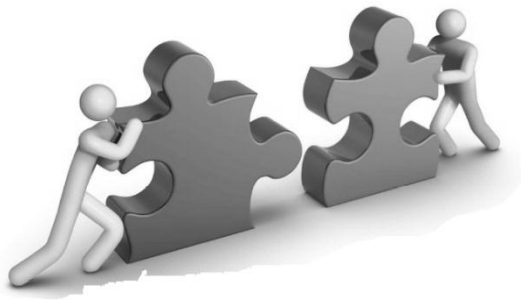
Status Quo

Aktuelle Situation von IKT in Österreich, Bedrohungs- und Risikosituation , der Cyber Rahmen, politische Ziele, Prinzipien, Vision und Mission, abgeleitete Maßnahmen, …



Strategische Ziele

Sensibilisierung, Forschung und Entwicklung, Cyberrisiko Management, Ausbildung, Schutz kritischer Inrfrastrukturen, Sicherheit für Bürger, Wirtschaft, öffentliche Verwaltung, Militär, Diplomatie, Governance, Legislative, abgeleitete Maßnahmen, …
…



Strukturen

Vorhandene und nötige Cyber-Sicherheit Stakeholder und Strukturen, ihre Verantwortungen, ihre Ziele, die Kooperationen und Kommunikationen, angeleitete Maßnahmen, …

Massnahmenkatalog

Maßnahmen abgeleitet von einer Bedrohungsanalyse, Maßnahmen für Krisen- und Katastrophenmanagement, Maßnahmen um die Widerstandsfähigkeit von Informationsstrukturen zu erhöhen, vorbeugende Maßnahmen, Aufsetzen von Partnerschaften, Untersuchung und Strafverfolgung von kriminellen Cyber-Handlungen, Cyberforschung, Cyberausbildung, Cybersensibilisierung Maßnahmen, abgeleitete Maßnahmen ….

IKT-Sicherheitsstrategie – Roadmap

2011			2012										2013	
Okt	Nov	Dez	Jän	Feb	Mär	Apr	Mai	Jun	Jul	Aug	Sep	Okt	Nov	Dez	Jän	Feb

Ausarbeiten der IKT-Sicherheitsstrategie

Detailausarbeitung von Maßnahmen

Maßnahmen

Maßnahmen

Begleitende Koordination und Kommunikation

IKT-Sicherheitsstrategie – Abschlussveranst.

Programm
IKT-Sicherheitsstrategie
15. Juni 2012
Bundeskanzleramt
Ballhausplatz 2, Kongresssaal

Zeit	Wer
9:30	Eintreffen und Kaffee
10:00-10:15	Begrüßung
10:15-10:30	Keynote Prof. Dr. Reinhard Posch CIO des Bundes IKT Sicherheitsstrategie
10:30-11:00	Keynote Dr. Steve Purser ENISA- Head of Technical Competence Dpt. Cyber Security @ ENISA
11:00-11:15	Keynote Mag. Wolfgang Ebner BMI Öffentliche Sicherheit in einer virtuellen Welt
11:15-11:45	Gemeinschaftsfoto und Pause
11:45-13:00	Arbeitsgruppenleiter Vorstellung der Endergebnisse der Arbeitsgruppen
13:00-13:15	Dr. Josef Ostermayer Staatssekretär im Bundeskanzleramt
13:15-13:30	Ing. Roland Ledinger BKA – Leiter IKT-Strategie des Bundes Präsentation der IKT-Sicherheitsstrategie und weiterer Fahrplan

- Am 15. Juni 2012,
  präsentierte die IKT Sicherheitsstrategie im feierlichen Rahmen die finalen **Resultate der AGs** und das Dokument **“Nationale IKT Sicherheits-strategie Österreich”**

Nationale IKT Sicherheitsstrategie Österreich

http://www.digitales.oesterreich.gv.at/DocView.axd?CobId=47986

Die Ergebnisse der Arbeitsgruppe:

Stakeholder und Strukturen

- **Optimierung der Cyber-Landschaft in Österreich**
  Ein dichtes Netz von Cyber Security Strukturen in Österreich muss alle Bereiche, Tätigkeitsfelder und Zielgruppen von Cyber Security berücksichtigen.

- **Vernetzung der Stakeholder und Strukturen**
  Anreize, Förderungsmaßnahmen und gesetzliche Grundlagen fördern ein enges Vernetzen österreichischer Cyber Security Stakeholder und Strukturen.

- **Ausbau des rechtlichen Rahmens für Cyber Security in Österreich**
  Der rechtliche Rahmen in Österreich ist an die Erfordernisse der IKT-Sicherheitsstrategie anzupassen.

- **Förderung der internationalen Kooperationen**
  Aktive Teilnahme und Förderung von allen wichtigen internationalen Organisationen und Aktivitäten zum Thema Cyber Security

Ergebnisse der Arbeitsgruppe:

Schutz kritischer Infrastrukturen

- **Aufbau eines Cyber-Krisenmanagement**
  Reaktive Mittel zur bundesweiten Katastrophen- und Krisenbekämpfung im Bereich Nationaler Cyber Security werden aufgebaut.

- **Ausbau von Risikomanagement und Informationssicherheit**
  Proaktive Risikominimierung wird auf Unternehmens- und Organisationsebene gefördert.

- **Informationsaustausch von öffentlichen und privaten Akteuren**
  Ein fließender Informationsaustausch von öffentlichen und privaten Akteuren schafft für das Risikomanagement die notwendigen Grundlagen und für das Krisenmanagement die erforderlichen Rahmenbedingungen.

Die Ergebnisse der Arbeitsgruppe:

Risikomanagement und Lagebild

- **Identifizierung von Kernunternehmen in den Sektoren**
  Durchführung von Risikobewertungen derjenigen Kernunternehmen, deren Ausfall Auswirkungen haben, die den Unternehmensbereich bei weitem übersteigen.
- **Sicherstellung von Mindeststandards und Lenkung der Risikoakzeptanz in Kernunternehmen**
  Risikoakzeptanz für Kernunternehmen soll auf übergeordneter Ebene entschieden werden, Mindeststandards dafür sollen festgelegt und überprüft werden, alternative Lenkungsinstrumente sollen untersucht werden.
- **Check von etabliertem Krisen- und Notfallmanagement in den Sektoren**
  Prozesse des staatlichen Krisen- und Notfall-Managements sind hinsichtlich ausreichender Bedachtnahme auf Risiken zu überprüfen, die sich aus der zunehmenden Abhängigkeit von zahlreichen Kernprozessen durch IKT-Unterstützung ergeben.
- **Etablieren einer Lagebeurteilung und -management**
  Ein Lagezentrum zur übergeordneten Beurteilung wird institutionell aufgebaut, um den Sektoren eine Basis für Einschätzungen und Entscheidungen zu geben und aus gesamtheitlicher Sicht eine Lagebeurteilung machen zu können.

Ergebnisse der Arbeitsgruppe:

Bildung und Forschung

- **Frühzeitige schulische Ausbildung in IKT, IKT-Sicherheit und Medienkompetenz**
  IKT und IKT-Sicherheit sind verstärkt in die Lehrpläne und den Unterrichtsalltag aufzunehmen.

- **Verpflichtende IKT-Ausbildung aller Studierenden der Pädagogik**
  IKT-(Sicherheits)-Kompetenzen sollen in die Ausbildung an pädagogischen Hochschulen und Universitäten für die Vermittlung dieser Kompetenzen an den Schulen aufgenommen werden

- **Verstärkte Ausbildung von IKT-SicherheitsspezialistInnen im tertiären Sektor**
  Die heute bereits vorhandenen Studien- und Ausbildungsangebote sollen sich pro aktiv weiterentwickeln. Die Vernetzung und Kooperation der einzelnen Bildungsorganisationen soll gefördert werden

- **IKT-Sicherheit als wichtiger Bestandteil in der Erwachsenenbildung / Weiterbildung**
  Entwicklung und Vernetzung zielgruppenspezifischer Angebote als kontinuierliche Weiterbildung für Einzelunternehmen, KMUs und Zielgruppen im Privatbereich soll gefördert werden

Ergebnisse der Arbeitsgruppen:

Awareness

- **Stärkung der IKT-Sicherheitskultur in Österreich**
  Gezielte Awareness-Maßnahmen in allen relevanten Zielgruppen und Handlungsfeldern
  Einrichten eines IKT Sicherheitsportals zur Darstellung von Cyber-Informationen

- **Positive Positionierung der IKT-Sicherheit**
  Begleitende Marketing-Maßnahmen sollen im Rahmen der Awareness-Kampagnen

- **Abgestimmte und koordinierte Vorgehensweise**
  Awareness-Maßnahmen sollen auf Basis einer abgestimmten und zentral koordinierten Vorgehensweise umgesetzt und gemonitort werden

- **Wirksamkeit und Nachhaltigkeit der Awareness-Maßnahmen**
  Es soll ein Messinstrument etabliert werden, dass regelmäßig die Wirksamkeit der getroffenen Awareness-Maßnahmen kontrollieren sowie Auswirkungen auf die Reduzierung von Sicherheitsvorfällen monitoren kann.

Umsetzungsplan

M.1	**Optimieren der Cybersecurity Stakeholder und Strukturen Landschaft in Österreich**
M.1.1	Verbesserung der Abdeckung aller Bereiche, Tätigkeitsfelder und Zielgruppen von Cybersecurity
M.1.2	Vermeidung von Doppelgleisigkeiten
M.1.3	Einrichtung einer öffentlichen Cyber-Partnerschaft
M.1.4	Einrichten eines öffentlichen Cyber-Krisenmanagements
M.1.5	Einrichten einer Informationsdrehscheibe für Cybersecurity
M.1.6	Einrichten eines Cyberlagezentrums
M.1.7	Institutionalisierung einer öffentlich privaten Partnerschaft für Cybersecurity
M.1.8	Forcieren eines nachhaltigen Zusammenarbeitens aller öffentlichen Stellen
M.1.9	Aufbau einer exzellenten Cybersecurity Kompetenz in Österreich
M.1.10	Aufbau eine Cybersecurity Awareness Kultur
M.1.11	Publikation des aktuellen Stands der Cybersecurity Landschaft in Österreich
M.1.12	Forcieren von Strukturen für Standards, Zertifizierungen, Qualitätsassessments
M.2	**Vernetzung der Stakeholder und Strukturen**
M.2.1	Breitangelegte Förderung von bestehender und neuer Vernetzung zwischen Stakeholdern & Strukturen in Österreich
M.2.2	Untersuchung welche Beeinflussungs-Regelkreise in Österreich vorhanden sind, um Cybersecurity Kompetenz zu fördern
M.2.3	Aufbau einer Darstellung und Evaluierung um die Qualität der Vernetzung österreichischer Stakeholder und Strukturen messen zu können
M.3	**Ausbau des rechtlichen Rahmens für Cybersecurity**
M.3.1	Analyse des Status Quos der heutigen Cybersecurity Rechtsgrundlagen
M.3.2	Ergänzung der weißen Flecken in der österreichischen Gesetzgebung hinsichtlich Cybersecurity.
M.3.3	Einrichten einer flexiblen Struktur der Legislative hinsichtlich Cybersecurity
M.3.4	Teilnahme an der Erarbeitung eines internationalen Rechtsrahmens für Cybersecurity
M.4	**Förderung der internationalen Kooperationen**
M.4.1	Aktive Teilnahme der öffentlichen Verwaltung an internationalen Cybersecurity Entwicklungen
M.4.2	Förderung der Teilnahme des privaten Bereichs an internationalen
M.4.3	Aufbau von bi- und multilateralen Netzwerken zur Abwehr von Internetbedrohungen
M.4.4	Gemeinsame Erarbeitung von internationalen Strategien zur Sicherung von staatenübergreifenden Grundrechten
M.4.5	Internationale Vernetzung zum Thema Cybersecurity im Bereich Ausbildung und Training
M.4.6	Internationale Vernetzung zum Thema Cybersecurity im Bereich Sensibilisierung
M.4.7	Internationale Vernetzung zum im Bereich Cybersecurity Forschung
M.4.8	Teilnahme an länderübergreifenden Cyber-Exercises

M.1	**Aufbau einer Struktur zum Cyber-Krisenmanagement**
M.1.1	Cyberlagezentrum
M.1.2	Krisenkommunikation
M.2	**Förderung des Risikomanagements innerhalb der KI**
M.2.1	Cyber Competence Center („C3“)
M.2.2	Informationssicherheitshandbuch/Grundschutzansatz
M.2.3	Technologiefolgenabschätzung
M.2.4	Ordnungspolitische Maßnahmen: Gesetze, Normen, Verordnungen (Meldepflicht,)
M.2.5	Freiwilliges Registrierungssystem
M.2.6	Human Sensor Projekt
M.3	**Unterstützung von Public Private Partnerships (PPP) zum SKI**
M.3.1	„Third-Party-PPP“ – z.B. Austrian Trust Circle
M.3.2	„Community-basierte PPP“ – z.B. CERT.at
M.3.3	„Hierarchische PPP“ – z.B. SOSKII
M.4	**Cybersicherheitsrat**
M.5	**Verfügbarkeit von Personal**
M.6	**Bildung und Awareness**

Die erste große Umsetzung:

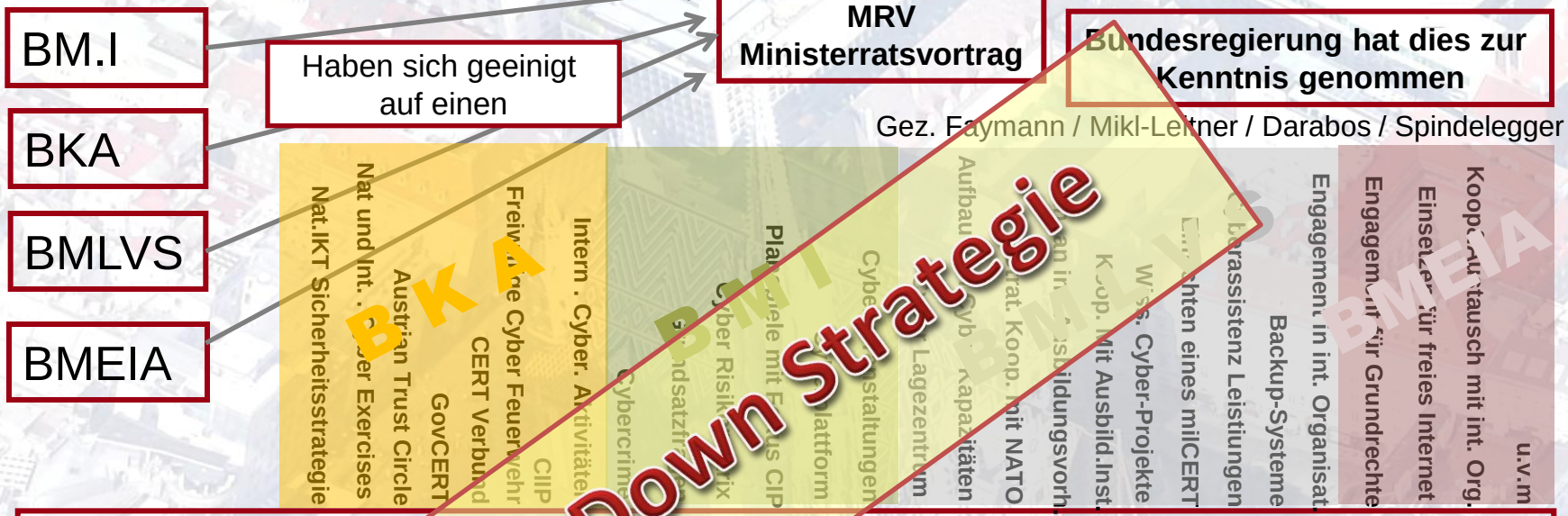
Das Online Sicherheitsportal

Die erste große Umsetzung:

Das Online Sicherheitsportal

- Herangehensweise
- Nationale IKT Sicherheitsstrategie
- ÖSCS – Österreichische Strategie für Cyber Sicherheit
- Cybersicherheitsstrategie der EU
  - Strategie
  - Richtlinie
- Zusammenfassung

MRV Österreichische Strategie für Cyber-Sicherheit

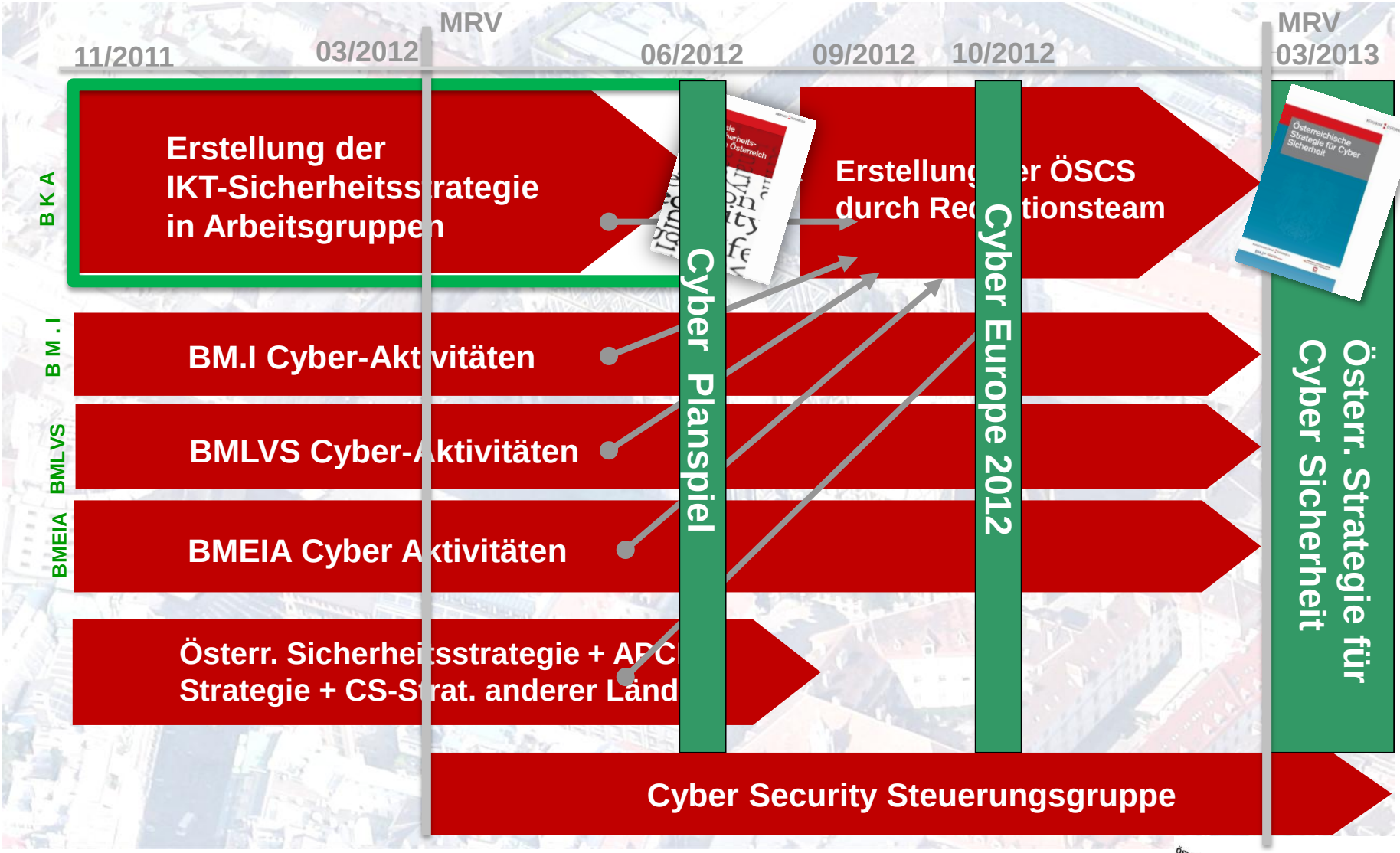


Auf bereits in den Ressorts erarbeitete Ergebnisse zum Schutz des Cyber Space soll aufgebaut werden.

Die Österreichische Strategie zur Cyber-Sicherheit soll durch einen alle Sicherheits-Ministerien integrierenden Ansatz erstellt werden.

Ziel ist die Annahme der Strategie durch die Bundesregierung bis März 2013.

ÖSCS-Roadmap



ÖSCS – Österr. Strategie für Cybersicherheit

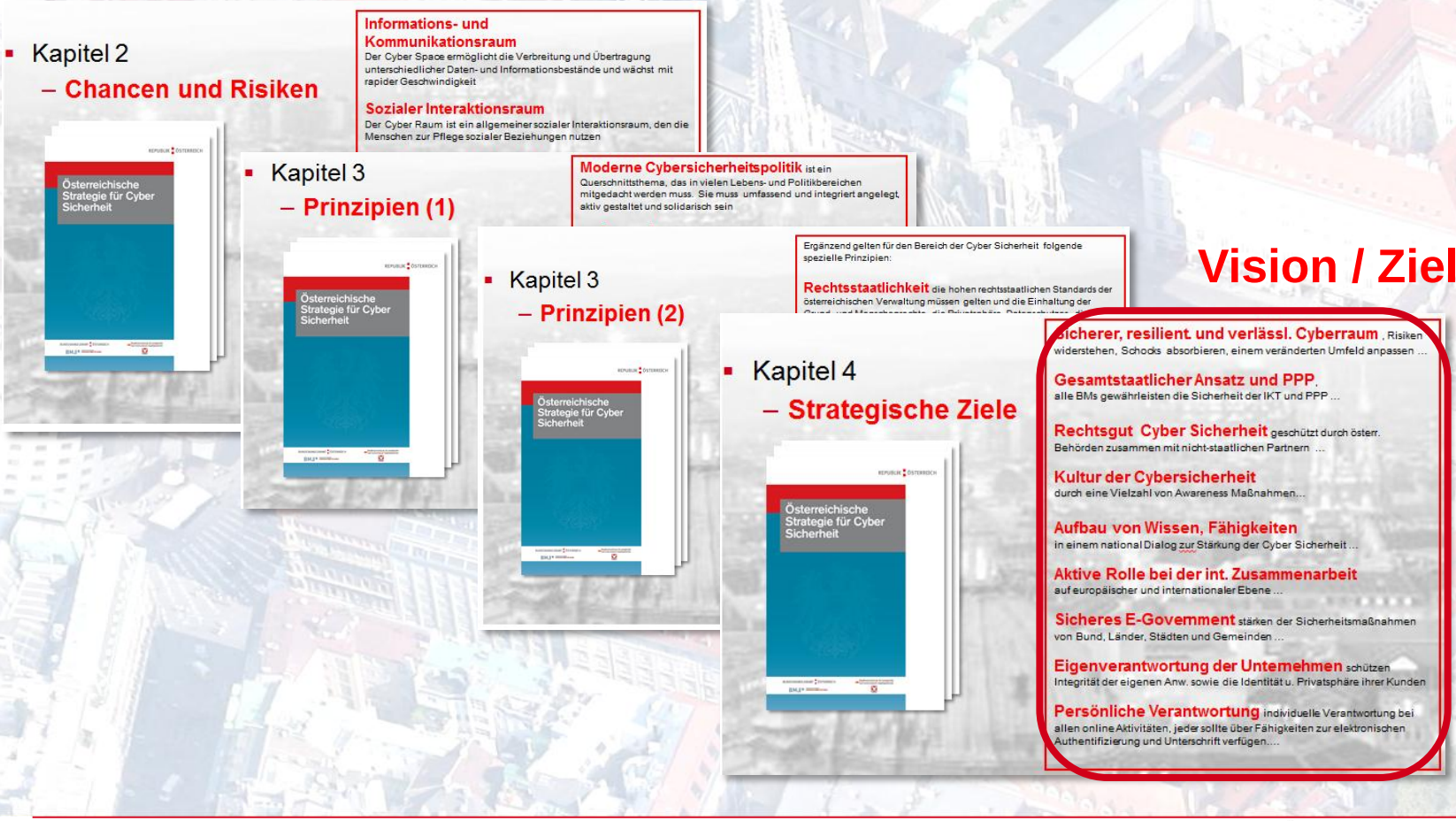
- Kapitel
  1. Einleitung
  2. Chancen und Risiken
  3. Prinzipien
  4. Strategische Ziele
  5. Handlungsfelder und Maßnahmen
  6. Umsetzung

Beschlossen am 20.03.2013 !

http://www.bundeskanzleramt.at/site/7863/default.aspx

ÖSCS – Österr. Strategie für Cybersicherheit

- Kapitel 2,3,4



ÖSCS – Österr. Strategie für Cybersicherheit

- Kapitel 5
  - **Handlungsfelder und Maßnahmen**

HF 1: Strukturen und Prozesse

- Einrichten einer **Cyber Sicherheit Steuerungsgruppe** Koordiniert auf der strategischen Ebene die Maßnahmen der Cybersicherheit in Österreich, berät die Regierung bei allen Angelegenheiten von Cybersicherheit, …

- Einrichten einer **Struktur zur Koordination auf der operativen Ebene**, Erstellt ein periodisches und ereignisbezogenes Lagebild Cybersicherheit in Österreich und koordiniert die Maßnahmen auf der operativen Ebene im Fall eines schweren Cybervorfalls, indem sie bereits existierende Organisationen und Einrichtungen einbindet

- Einrichten eines umfassenden **Cyber Krisen Management** für übergreifende Bedrohungen der Cybersicherheit mit staatsbedrohendem Charakter, inklusive dem Ausarbeiten von Krisenmanagement- und Kontinuitätsplänen

- Stärken von **bestehenden Cyber Strukturen**, insbesonders dem govCERT, dem Cyber Crime Competence Center, dem milCERT und dem nationalen CERT

ÖSCS – Österr. Strategie für Cybersicherheit

- Kapitel 5
  - **Handlungsfelder und Maßnahmen**

HF 2: Governance

- Schaffen eines **zeitgemäßen ordnungspolitischen Rahmens** Untersuchung des derzeit existierenden Rechtsrahmens und Ausarbeitung von zusätzlichen regulatorischen Maßnahmen, und nicht-rechtlichen Selbstverpflichtungen (Code Of Conducts) für die Gewährleistung von Cyber Sicherheit in Österreich…
- **Festlegung von Mindestsicherheits-standards**, Anforderungen sollen für alle im sicherheitsrelevanten Bereiche der IKT eingesetzten Komponenten und Dienstleistungen gelten. Die gültigen Normen, Standards, Verhaltensregeln, Best Practises usw.. werden im österreichischen Informationssicherheitshandbuch zusammengefasst und laufend aktualisiert.
- **Jährlicher Bericht zur Cyber Sicherheit** Durch die Cyber Sicherheit Steuerungsgruppe wird ein jährlicher Bericht „Cyber Sicherheit in Österreich“ erstellt und der Bundesregierung vorgelegt

ÖSCS – Österr. Strategie für Cybersicherheit

- Kapitel 5
  - **Handlungsfelder und Maßnahmen**

HF 3: Kooperation Staat, Wirtschaft und Gesellschaft

- Einrichten einer **Cyber Sicherheit Plattform** soll einen Austausch von Informationen , Aufbau von Kooperationen, … zwischen der öffentlichen Verwaltung und den Vertretern der Wirtschaft, Wissenschaft und Forschung institutionalisieren
- Stärken der **Unterstützung für KMUs** KMUs sollen mit Schwerpunktprogramme für Cybersicherheit unterstützt werden
- Entwicklung einer **Cyber Sicherheit Kommunikationsstrategie** zum Optimieren der Kommunikation zwischen Stakeholders der Administration und Vertretern der Wirtschaft, Wissenschaft und Gesellschaft

HF 4: Schutz krit. Infrastr.

- Erhöhung der **Widerstandskraft der kritischen Infrastrukturen** Einbinden der KI in Prozesse des Cyber Krisenmanagements, Aufbau einer umfassenden Mindest-Sicherheitsarchitektur, Einrichten eines Sicherheitsbeauftragten, Meldepflicht für schwere Cybervorfälle, …

ÖSCS – Österr. Strategie für Cybersicherheit

- Kapitel 5
  - **Handlungsfelder und Maßnahmen**

HF 5: Sensibilisierung und Ausbildung

- Stärkung der **Cybersicherheit Kultur**
  - Sensibilisierungsinitiativen werden auf der Grundlage einer gemeinsamen Vorgangsweise unter Berücksichtigung bereits bestehender Programme erarbeitet, abstimmt und durchgeführt
  - Einrichten eines Online Sicherheitsportals.
    Das Portal soll in Form einer Web-Plattform für alle Zielgruppen in Österreich als zentrale Anlaufstelle für Themen der Cyber Sicherheit fungieren.

- Verankern von **Cybersicherheit und Medienkompetenz auf allen Ebenen der Ausbildung**
  - Aufnahme von IKT, Cyber Sicherheit und Medienkompetenz in den Unterricht
  - Aufnahme von Cybersicherheit in die Ausbildung der Lehrer bei Hochschulen und Universitäten
  - Ausbildung von Cyber Spezialisten im staatlichen Bereich
  - Ausbildung von Systemadministratoren für das frühzeitige Erkennen von Cybervorfällen

ÖSCS – Österr. Strategie für Cybersicherheit

- Kapitel 5
  - **Handlungsfelder und Maßnahmen**

HF 6: Forschung und Entwicklung

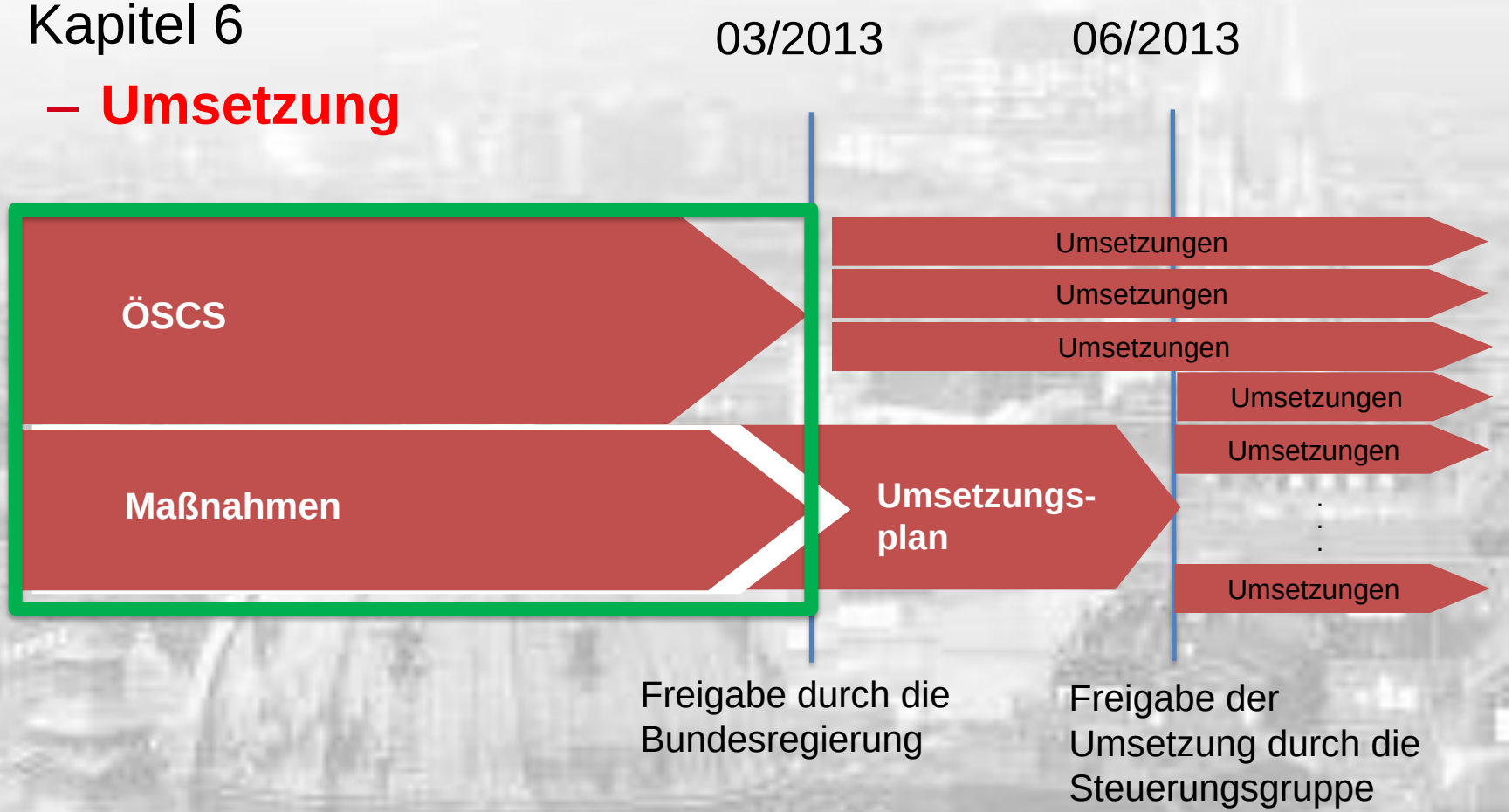
- **Österreichs Forschung stärken** bez. Cybersich.
  - mit zentralen Forschungsschwerpunkten in Österreich
  - mit aktiver Themenführerschaft bei EU Forschungsprogrammen,
  - mit Maßnahmen zur zügigen Übertragung von Forschungs- und Entwickl.Ergebnisse marktfähige Produkte

HF 7: Internationale Zusammenarbeit

- Hinarbeiten auf ein **Effektives Zusammenwirken für Cyber Sicherheit in Europa und weltweit**
  - Beitrag zur Umsetzung einer Europäischen Cyber Sicherheits Strategie
  - Umsetzung und Nutzen der Europaratskonvention bez.Cyberkriminalität
  - Immer und überall einsetzen für grundlegende Menschenrechte im Cyberraum. Insbesondere das Recht auf Meinungsfreiheit und Information ohne Einschränkung
  - paneuropäischen und internationale Cyberübungen,
  - Fortsetzen der NATO Partnerschaft für den Frieden, …

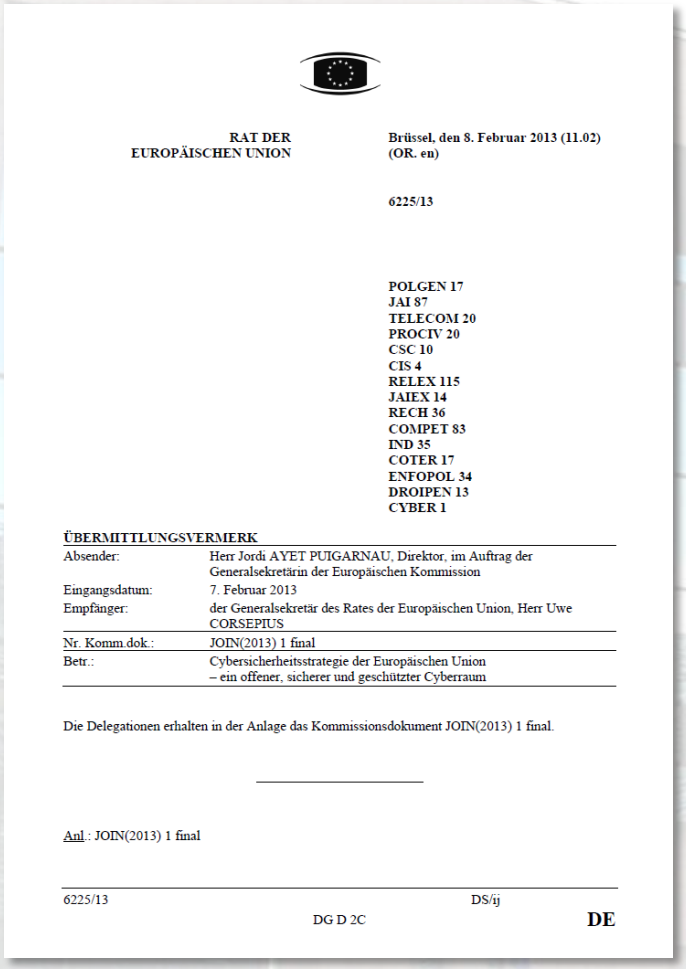
Roadmap ÖSCS

- Kapitel 6
  - **Umsetzung**



- Herangehensweise
- Nationale IKT Sicherheitsstrategie
- Österreichische Strategie für Cybersicherheit
- Cybersicherheitsstrategie der EU
  - Strategie
  - Richtlinie
- Zusammenfassung

Die europäische Strategie für NIS



RAT DER EUROPÄISCHEN UNION

Brüssel, den 8. Februar 2013 (11.02)
(OR. en)

6225/13

POLGEN 17
JAI 87
TELECOM 20
PROCIV 20
CSC 10
CIS 4
RELEX 115
JAIEX 14
RECH 36
COMPET 83
IND 35
COTER 17
ENFOPOL 34
DROIPEN 13
CYBER 1

ÜBERMITTLUNGSVERMERK

Absender:	Herr Jordi AYET PUIGARNAU, Direktor, im Auftrag der Generalsekretärin der Europäischen Kommission
Eingangsdatum:	7. Februar 2013
Empfänger:	der Generalsekretär des Rates der Europäischen Union, Herr Uwe CORSEPIUS
Nr. Komm.dok.:	JOIN(2013) 1 final
Betr.:	Cybersicherheitsstrategie der Europäischen Union – ein offener, sicherer und geschützter Cyberraum

Die Delegationen erhalten in der Anlage das Kommissionsdokument JOIN(2013) 1 final.

Anl.: JOIN(2013) 1 final

6225/13 DS/ij
DG D 2C **DE**

Strategie

http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667

Videos

http://ec.europa.eu/avservices/video/player.cfm?sitelang=en&ref=92446

http://ec.europa.eu/avservices/video/player.cfm?sitelang=en&ref=92529

Catherine ASTHON
Foreign Affairs and Security Policy

Neelie KROES
Digital Agenda

Cecilia MALMSTRÖM
Home Affairs

Vision:
Ein sicherer europäischer Cyberraum
mit den folgenden Zielen

- **Grundwerte der EU gelten in der digitalen Welt** ebenso wie in der realen Welt
- **Schutz der Grundrechte**, der Meinungsfreiheit, der personenbezogenen Daten und der Privatsphäre
- **Allgemeine Zugänglichkeit**
- **Partizipative, demokratische und effiziente Verwaltung**
- **Gemeinsame Verantwortung** im Interesse der Sicherheit

Ziele:
Auf Basis von 5 strategischen Prioritäten

1. **Widerstandsfähigkeit** erhöhen
2. Drastische **Eindämmung der Cyberkriminalität**
3. Entwicklung einer **Cyberverteidigungspolitik und von Cyberverteidigungskapazitäten** im Zusammenhang mit der Gemeinsamen Sicherheits- und Verteidigungs-politik (CSDP)
4. Entwicklung der **industriellen und technischen Ressourcen** für die Cybersicherheit
5. Entwicklung einer **einheitlichen Cyberraumstrategie** der EU auf internationaler Ebene und Förderung der **Grundwerte der EU**

Viele Maßnahmen

Widerstandsfähigkeit

Kommission	• wird 2014 einen **Cybersicherheitswettbewerb** veranstalten
mit ENISA:	• 2013 einen **„Netz- und Informationssicherheits-Führerschein"** vorschlagen (freiwillige Zertifizierung zur Förd.
Kommission	• **NIS-Forschungs** • A/2013 EU co-fina
mit ENI	z.B. mit NIS 2014
	• **paneuropäische**
bittet die Industrie	• **auf allen Ebenen** für die Cybersicherheit zu **sensibilisieren** (Unternehmensebene, Kunden-kontakt, Verantwortung der CXX-Ebene für CS, …)
ersucht das EP	• NIS Vorschlag für
bittet die Industrie	• Führende Rolle bei **Investitionen in eine hohe CS** zu übernehmen, best practice Vorgehensweisen zu entwickeln und Informationsaustausch einzuführen, insbes. PPP

Cyberdefense

Hohe Vertreterin mit MS und Europ. Verteidigungs-agentur	• operative Anforderungen an die Cyberverteidigung der EU **Entwicklung von Cyberverteidigungskapazitäten** und -technologien auf EU-Ebene prüfen. Alle Aspekte des Kapazitätsaufbaus sind zu behandeln (S.15)
	Risikobewertung, Sensibilisierung) • **Dialog** mit Partnern **auf intern. Ebene** (NATO, int.Orgs, multinat. Excellezzentren) pflegen

Cyberkriminalität

ersucht CEPOL (europ. Polizeiakad.)	• Konzipieren und Planen von **Schulungen** zu **koordinieren**
ersucht Europol	• **Hindernisse** für justizielle grenzüberschreitende Zusammenarbeit zu **identifizieren** • **Untersuchung und Verfolgung** von Cyberstraftaten operativ und strategisch zu **unterstützen**
Kommission	• Europäische Zentrum zur Bekämpfung der Cyberkriminalität **(EC3) unterstützen**, dieses soll als Sprachrohr der Strafverfolgungsbehörden insgesamt fungieren. • **Empfehlungen von ICANN** folgen und größere Verantwortung an Registrierstellen für Domänennamen (z.B. Info über Eigentümer von Websites) fördern • Intensiv **Kampf gegen K** einführen einer Strategie eines Globales Bündniss Kindern im Internet
	• die **rasche Umsetzung** und Anwendung der Richtlinien zur riften die bereits inkommen des zu ratifizieren (falls nicht
mit Europol (EC3)	• Gemeinsam **Cybercrim** (Schwerpunkt Kindermis unrechtmässiges Eindringen) • **Reports über Trends** und Bedrohungen **veröffentlichen**, um Cybercrime Bekämpfungs-Prioritäten in den MS zu setzen
	• **Budgetär** die MS beim **Ermittlung von Mängeln** und den **Ausbau der Kapazitäten** gegen Cyberkriminalität unterstützen • empfehlenswerter Vorgehensweisen und die **besten verfügbaren Technologien** dafür mit MS abstimmen (Supp. von JRC) • **Eng** mit Europäischen Zentrum zur Bekämpfung der Cyberkriminalität (EC3), Europol und Eurojust **zusammenarbeiten**

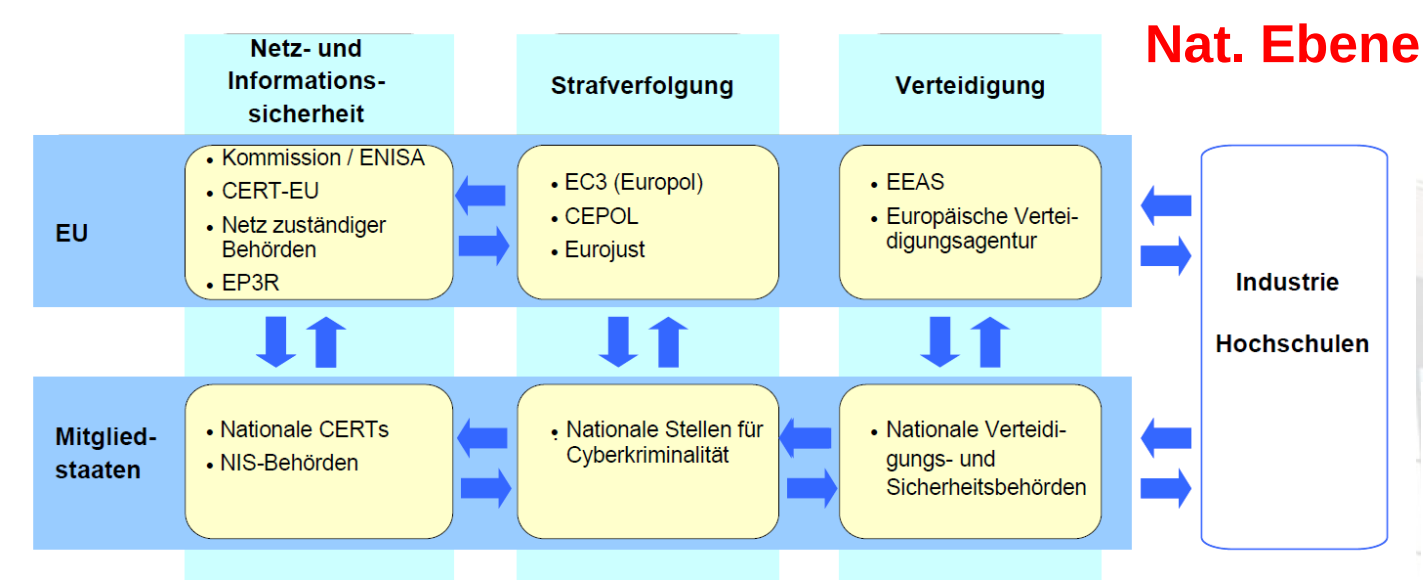
International

Kommission und die Hohe Vertreterin	• eine **einheitliche EU-Cyberraum-Politik** auf int. Ebene hinarbeiten, Cyberthemen in die Gemeinsame Außen- und Sicherheitspolitik integrieren und die Koordinierung globaler Fragen des Cyberraums zu verbessern • Entw. von **Verhaltensnormen** und vertrauensbildenden wenden nkommen rn (S.20) au in Drittländern im Interesse eines leichten Zugangs zu Informationen, einem freien Internet und gegen Cyberbedroh. • **EU-Finanzierungsinstrumente** dafür einsetzen • **Koordination und Informationsaustausch** im Rahmen der int. Netze für NIS und der zust. Behörden verstärken

Industr. Res.

Kommission	• 2013 ei Leben r Gewähr verwend
fordert EUROPOL und die ENISA auf	• neue **Trends in Cyberkriminalität und Cybersicherheit** zu ermitteln, so dass geeignete cyberforensische Werkzeuge und Technologien entwickelt werden können
Kommission	
fordert öffentl. und privaten Sektor auf	• in Zusammenarbeit mit den **Versicherungen harmonisierte metrische Verfahren** für die Berechnung von Risikoprämien ss Unternehmen, die in Sicherheit ingere Versicherungsbeiträge zahlen
beauftragt	
fordert öffe privaten S	
fordert MS auf	**nutzen** um Sicherheitsfunktionen bei IKT Produkten zu stimulieren • die **frühzeitige Einbeziehung von Industrie und Hochschulen** in die Entwicklung und Koordinierung von Sicherheitslösungen fördern. • Forschungspläne von zivilen und militärischen Einrichtungen koordinieren

Aufgaben und Zuständigkeiten



- **EU Ebene**
- **Int. Ebene**
- **Unterstütz. bei großem Cybervorfall**

- MS sollen **Strukturen für CS, Cybercrime und Cyber Defense**
- Sie sollen **notwendige Kapazitäten dafür bereitstellen**
- **Aufgaben** und **Zuständigk.** in der nationalen Cybersicherheitsstrategie festlegen
- **NIS Kooperationspläne** mit eindeutiger Zuweisung von Aufgaben und Zuständigkeiten entwickeln

Fazit und Folgemaßnahmen

- **Verwirklichung** dieser Zielvorstellungen ist **nur durch eine echte**
  zahlreichen Akteuren möglich, die Verantwortung

Begleitende Richtlinie

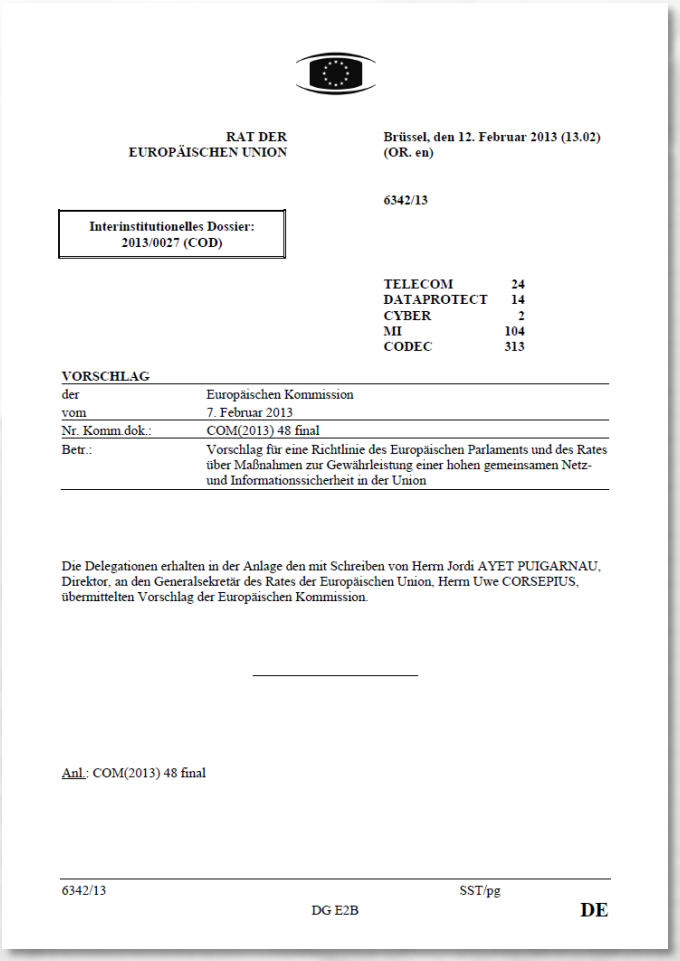
- Herangehensweise

- Nationale IKT Sicherheitsstrategie
- Österreichische Strategie für Cybersicherheit

- Cybersicherheitsstrategie der EU
  - Strategie
  - Richtlinie

- Zusammenfassung

Der Vorschlag für eine NIS Richtlinie



RAT DER
EUROPÄISCHEN UNION

Brüssel, den 12. Februar 2013 (13.02)
(OR. en)

6342/13

Interinstitutionelles Dossier:
2013/0027 (COD)

TELECOM	24
DATAPROTECT	14
CYBER	2
MI	104
CODEC	313

VORSCHLAG

der	Europäischen Kommission
vom	7. Februar 2013
Nr. Komm.dok.:	COM(2013) 48 final
Betr.:	Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union

Die Delegationen erhalten in der Anlage den mit Schreiben von Herrn Jordi AYET PUIGARNAU, Direktor, an den Generalsekretär des Rates der Europäischen Union, Herrn Uwe CORSEPIUS, übermittelten Vorschlag der Europäischen Kommission.

Anl.: COM(2013) 48 final

6342/13 SST/pg
DG E2B DE

Direktive engl.

http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1666

Direktive deutsch

http://ec.europa.eu/dgs/home-affairs/what-is-new/news/news/2013/docs/1_directive_20130207_de.pdf

Impact Assessment

http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1669

Kapitel 2 Nationaler Rahmen für NIS

- Artikel 5: Nat. NIS-Strategie und NIS-Kooperationsplan
  - Jeder MS hat eine **NIS Strategie** mit folgenden Aspekten (1)
    - **Festlegung der Ziele und Prioritäten** der Strategie auf der Grundlage einer aktuellen Analyse der Sicherheitsrisiken und –vorfälle
    - ein **Steuerungsrahmen** zur Erreichung dieser Ziele und Prioritäten, einschließlich einer klaren Festlegung der Aufgaben und Zuständigkeiten der staatlichen Stellen und der anderen einschlägigen Akteure
    - Bestimmung **allgemeiner Maßnahmen** zu NIS plus Mechanismen für die Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor
    - die Aufstellung von **Ausbildungs-, Aufklärungs- und Schulungsprogrammen**
    - **Forschungs- und Entwicklungspläne** und eine Darlegung, wie diese Pläne die Prioritäten widerspiegeln
  - NIS-Strategie hat einen **NIS-Kooperationsplan** mit folgenden Elemente (2)
    - **Risikobewertungsplan** zur Bestimmung der Risiken und zur Bewertung der Auswirkungen pot. Sicherheitsvorfälle
    - Festlegung der **Aufgaben und Zuständigkeiten** der verschiedenen an der Umsetzung des Plans Beteiligten
    - Festlegung von **Kooperations- und Kommunikationsabläufen**
    - **Fahrplan** für NIS Übungen und Schulungen
  - Die nationale NIS-Strategie und der nationale NIS-Kooperationsplan werden der Kommission **innerhalb eines Monats nach ihrer Annahme mitgeteilt** (3)

Kapitel 2 Nationaler Rahmen für NIS

- Artikel 6: NIS zuständige nationale Behörde

  - Jeder MS benennt eine für NIS **zuständige Behörde** (1)
  - NIS Behörden **überwachen die Anwendung** dieser Richtlinie (2)
  - Zuständige Behörde ist mit **angemessenen Ressourcen** ausgestattet, damit sie ihre Aufgaben wirksam und effizient wahrnehmen kann, die MS gewährleisten eine wirksame und effiziente und sichere Zusammenarbeit der zuständigen Behörden (3)
  - **MS gewährleisten** dass die zuständige Behörde die **Meldungen über Sicherheitsvorfälle** von den öffentl. Verwaltungen und den Marktteilnehmern erhalten (4)
  - Zuständige Behörden **konsultieren** gegebenenfalls die **nat. Strafverfolgungsbehörden** und arbeiten mit Ihnen zusammen. (5)
  - **MS teilen unverzüglich der Kommission die zuständige Behörde**, deren Aufgabe und etwaige spätere Änderungen mit. Die MS machen die Benennung der zuständ. Behörde öffentlich bekannt. (6)

Kapitel 2 Nationaler Rahmen für NIS

- Artikel 7: IT Notfallsteam
  - **Jeder MS richtet ein CERT ein**, das die Voraussetzung von Anhang 1 erfüllt. Das CERT kann innerhalb der zuständigen Behörde eingerichet werden. (1)
  - MS gewährleisten eine **CERT- Ausstattung** entspr. Anhang 1 (2)
  - MS gewährleisten eine **sichere nationale IKT Struktur** für die CERTs, kompatibel zu den Artikel 9 (3)
  - MS informieren die Kommission über die **Ressourcen und Prozesse** der CERTs (4)
  - Das **CERT untersteht der Aufsicht der zuständigen Behörde**, die die Angemessenheit der ihm zur Verfügung gestellten Ressourcen, sein Mandat und die Wirksamkeit seines Verfahrens zur Bewältigung von Sicherheitsvorfällen regelmäßig überprüft (6)

Kapitel 3 Zusammenarbeit zwischen den Behörden

- Artikel 8: Kooperationsnetz
  - zuständige Behörden und die Kommission bilden ein Netz (das **Kooperationsnetz**) für die Zusammenarbeit (1)
  - Sie stehen über das Kooperationsnetz **permanent in Verbindung** (2)
  - Die Behörden haben innerhalb dieses Netzes **folgende Aufgaben** (3)
    - Verbreitung von **Frühwarnungen**
    - Gewährleistung einer **koordinierten Reaktion**
    - **Veröffentlichung** nichtvertraulicher Informationen über laufende Frühwarnungen und koordinierte Reaktionen auf einer **gemeinsamen Website**;
    - **Erörterung und Bewertung** von nationalen NIS-Strategien NIS-Kooperationspläne auf Anfrage eines MS oder Kommission
    - **Bewertung der Wirksamkeit der CERTs**, insbesondere bei der Durchführung von NIS Übungen auf Unionsebene auf Anfrage eines MS oder Kommission
    - Zusammenarbeit und Informationsaustausch mit dem **Europäischen Zentrum zur Bekämpfung der Cyberkriminalität**
    - Austausch von **Erfahrungen** und **Best Practices** und Unterstützung beim **Kapazitätsaufbau**
    - regelmäßiger **gegenseitiger Überprüfungen der** Kapazitäten und der Abwehrbereitschaft
    - **Durchführung von NIS-Übungen** auf Unionsebene und Teilnahme an **internationalen NIS-Übungen**
  - Kommission legt mittels **Durchführungsrechtsakten** die erforderlichen Modalitäten für eine Zusammenarbeit zw. den zust. Behörden und der Kommission fest (4)

Kapitel 3 Zusammenarbeit zwischen den Behörden

- Artikel 10: Frühwarnungen
  - **Frühwarnungen über das Kooperationsnetz** für Sicherheitsrisiken und –vorfälle mit mindestens einer der **folgenden Voraussetzungen** (1)
    - sie **weiten sich rasch** aus oder können sich rasch ausweiten
    - sie **übersteigen** die nationale Reaktionskapazität
    - sie betreffen oder können **mehr als einen Mitgliedstaat** betreffen
  - Zust. Behörden und KOM stellen **alle rel. Informationen zur Verfügung** die für die Beurteilung der Sicherheitsrisiken von Nutzen sein können (2)
  - KOM kann auf Anfrage eines MS einen and. MS ersuchen relevante Informationen zur Verfügung zu stellen (3)
  - Bei einem kriminellen Hintergrund informieren die zust. Behörden oder die KOM das Europäische Zentrum zur Bekämpfung der Cyberkriminalität (4)
  - KOM soll delegierte Rechtsakte zur **Präzisierung der Sicherheitsrisiken** und -vorfälle zu erlassen, die Frühwarnungen auslösen (5)

Kapitel 3 Zusammenarbeit zwischen den Behörden

- Artikel 11: Koordinierte Reaktion
  - Im Anschluss an eine Frühwarnung einigen sich die zuständigen Behörden nach einer Bewertung der einschlägigen Informationen auf eine **koordinierte Reaktion gemäß dem NIS-Kooperationsplan** der Union (1)
  - Die verschiedenen auf **nationaler** Ebene im Zuge der koordinierten Reaktion angenommenen **Maßnahmen** werden **dem Kooperationsnetz** mitgeteilt (2)

Kapitel 3 Zusammenarbeit zwischen den Behörden

- Artikel 12: NIS-Kooperationsplan der Union
  - KOM nimmt mittels Durchführungsrechtsakten einen **NIS Kooperationsplan** an (1)
  - Dieser sieht folgendes vor (2)
    - Für das **Frühwarnsystem**
      - Festlegen der Form und des **Verfahrens** für die **Einholung und den Austausch**
      - Festlegen der Verfahren und **Kriterien zur Bewertung** der Risiken und Vorfälle durch das Kooperationsnetz
    - Für die **koordinierte Reaktion**
      - einzuhaltende **Verfahren**, einschließlich der **Aufgaben** und **Zuständigkeiten** und der Kooperationsverfahren
    - **Fahrplan** für NIS-Übungen und –Schulungen
    - **Programm für den Wissenstransfer** zwischen den MS hinsichtl. Kapazitätsaufbau und gegenseitigem Lernen
    - **Programm zur Sensibilisierung** und Schulung der Mitgliedstaaten untereinander
  - Der NIS-Kooperationsplan wird **spätestens ein Jahr nach dem Inkrafttreten dieser Richtlinie angenommen** und regelmäßig überarbeitet (3)

Kapitel 4 Sicherheit der Netze u. Informationssyst.

- Artikel 14: Sicherheitsanforderungen und Meldung von Sicherheitsvorfällen
  - MS stellen sicher, dass öffentl. Verwaltungen und Marktteilnehmer für Netze und Informationssysteme **geeignete und angemessene RM Systeme** einsetzen (1)
  - MS gewährleisten die **Meldung von Sicherheitsvorfällen** mit erheblichem Schadenspotential durch öffentl. Verw. und Marktteilnehmer an die zust. Behörden (2)
  - (1) und (2) gelten für alle Marktteilnehmer, die Dienste in der EU bereitstellen (3)
  - Zuständige Behörde **unterrichtet die Öffentlichkeit** oder verpflichtet die öffentl. Verwaltungen und Marktteilnehmer zur Unterrichtung wenn **öffentl. Interesse** vorliegt
  - Die Zuständige Behörde berichtet dem Kooperationsnetz jährlich über eingeg. Meld. (4)
  - KOM erlässt delegierte **Rechtsakte zur Festlegung der Meldepflicht** (5)
  - Zust. Behörden können **Leitlinien und Anweis. zur Meldepflicht** herausgeben (6)
  - KOM wird ermächtigt Durchführungsrechtsakten bez. Meldeverpfl. festzulegen (7)
  - (1) und (2) gelten nicht für Kleinstunternehmen (8)

Kapitel 4 Sicherheit der Netze u. Informationssyst.

- Artikel 15 Umsetzung und Durchsetzung
  - Die zust. Behörden sollen **alle Befugnisse eingeräumt** werden, die für die Untersuchung von Verstößen gegen die Verpflicht. nach Artik. 14 erforderlich sind (1)
  - Die zust. Behörden sollen gegenüber den öffentl. Verwaltungen und Marktteilnehmern befugt sein folgendes zu verlangen (2)
    - **Alle Informationen und Unterlagen**, die zur Beurteilung der Netzsicherheit erforderlich sind
    - **Eine Sicherheitsprüfung** durch eine qualifizierte unabhängige Stelle oder nat. Behörde zu machen
  - Die zust. Behörden dürfen **verbindliche Anweisungen** geben (3)
  - Die zust. Behörden **melden** kriminelle Delikte an die **Strafverfolgungsbehörden** (4)
  - Die zust. Behörden arbeiten bei Datenschutzverletzungen mit DSK zusammen (5)
  - MS gewährleisten, dass alle Verpflichtungen, die öffentlichen Verwaltungen oder Marktteilnehmern nach diesem Kapitel auferlegt werden, einer **gerichtlichen Nachprüfung** unterzogen werden können (6)

Kapitel 5 Schlussbestimmungen

- Artikel 17 Sanktionen

  – MS erlassen **Vorschriften über Sanktionen für Verstöße** gegen die nach dieser Richtlinie erlassenen Bestimmungen und treffen alle erforderlichen Maßnahmen, um deren Anwendung sicherzustellen. Sanktionen müssen *wirksam, angemessen und abschreckend* sein. Die MS teilen diese Sanktionen spätestens bei der Umsetzung dieser Richtlinie der Kommission mit (1)

  – Die bei Sicherheitsvorfällen mit **Folgen für den Schutz personenbezogener Daten** vorgesehenen Sanktionen müssen **mit bestehenden Sanktionen auf europ. Ebene im Einklang stehen (**Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr) (2)

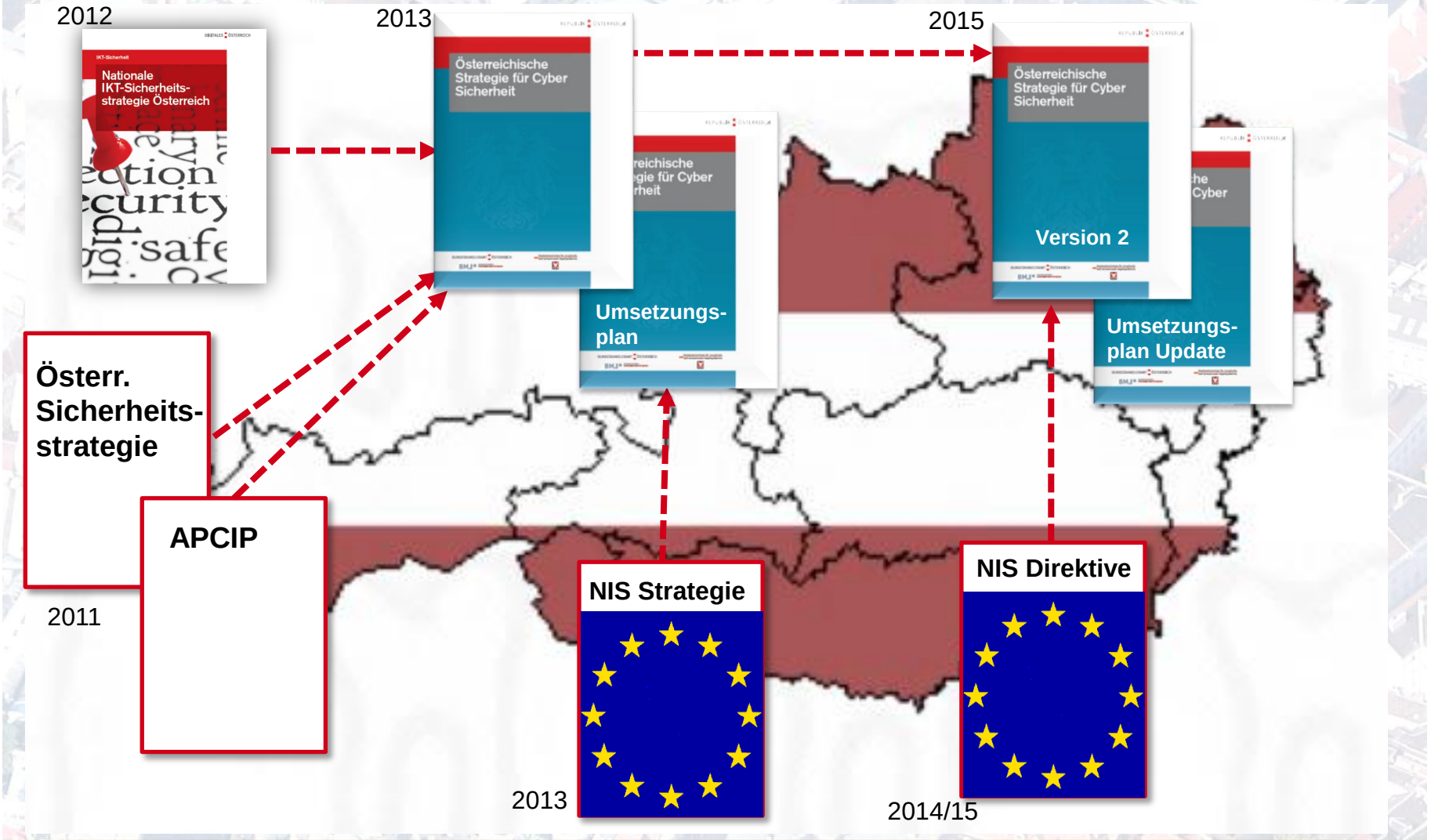
- Herangehensweise

- Nationale IKT Sicherheitsstrategie
- Österreichische Strategie für Cybersicherheit

- Cybersicherheitsstrategie der EU
  - Strategie
  - Richtlinie

- **Zusammenfassung**

Die Strategien für Österreichs Cyberraum



Danke

Franz Vock
Bundeskanzleramt

Abt. **IKT-Strategie des Bundes / E-Government**
Cyber Security, Secure Electronic-Identity, International Issues

Mitglied von **GovCERT Österreich**
franz.vock@bka.gv.at

ÖSCS – Österr. Strategie für Cybersicherheit

- Vergleich Direktive - ÖSCS

Richtlinie	ÖSCS
Artikel 5: Nat. NIS Strategien und NIS Kooperationsplan	ÖSCS als ganzes HF1/Punkt3 Einrichten eines übergreifenden Cyber Krisenmanagement/ Erstellen von Krisen und Kontinuitätspläne NICHT UMFASSEND
Artikel 6: NIS zuständige Behörde	HF1/Punkt2: Schaffung einer Struktur zur Koordination auf der operativen Ebene
Artikel 7: IT Notfallsteam	HF1/Punkt4: Stärkung bestehender Cyber Strukturen
Artikel 8: Kooperationsnetz	KEINE ABBILDUNG
Artikel 9: Sicheres System für Informationsaustausch	KEINE ABBILDUNG

ÖSCS – Österr. Strategie für Cybersicherheit

- Vergleich Direktive - ÖSCS

Richtlinie	ÖSCS
Artikel 10: Frühwarnungen	HF1/Punkt2: Schaffung einer Struktur zur Koordination auf der operativen Ebene – Lagebild Cybersicherheit
Artikel 11: Koordinierte Reaktion	National: HF1/Punkt3 Einrichten eines übergreifenden Cyber Krisenmanagement/ Erstellen von Krisen und Kontinuitätspläne EU-weit: KEINE ABBILDUNG
Artikel 12 NIS Kooperationsplan der Union:	KEINE ABBILDUNG

ÖSCS – Österr. Strategie für Cybersicherheit

- Vergleich Direktive - ÖSCS

Richtlinie	ÖSCS
Artikel 13: Internationale Zusammenarbeit	HF7/Punkt15 Effektives Zusammenwirken für Cyber Sicherheit in Europa und weltweit
Artikel 14: Sicherheitsanforderungen und Meldung von Sicherheitsvorfällen	HF4/Punkt11: Resilienz der kritischen Infrastrukturen erhöhen NICHT UMFASSEND