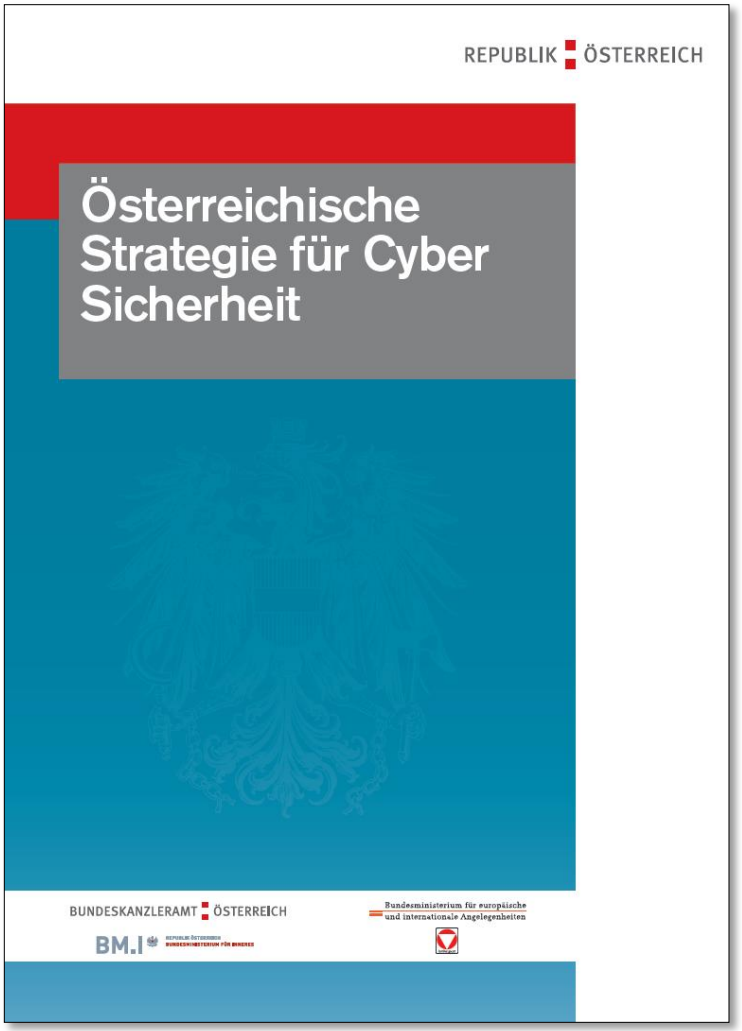
Branchenspezifische Aktivitäten im Kontext der ÖSCS

franz.vock@bka.gv.at

Bundeskanzleramt

28. Juni 2016

… im Kontext der ÖSCS



Verweise auf Branchenspezifische Aktivitäten

Kapitel 3 Prinzipien

- **Integrierte Cyber Sicherheitspolitik** muss auf eine **Arbeitsteilung zwischen dem Staat, der Wirtschaft, der**

Integrierte Cyber Sicherheitspolitik

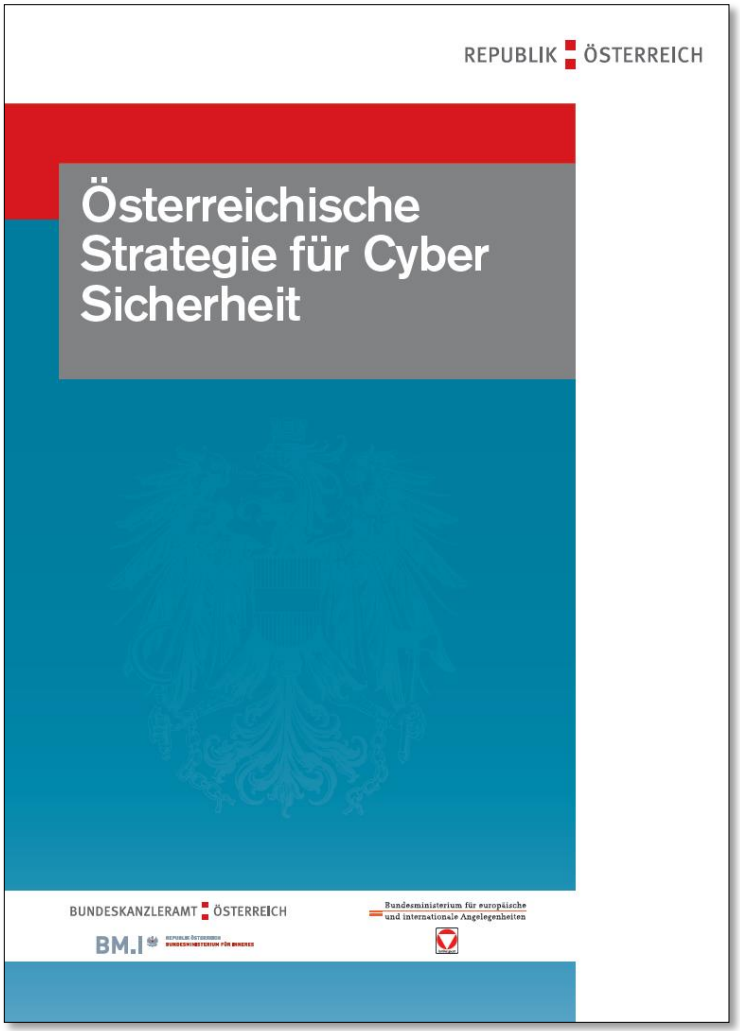
Arbeitsteilung zwischen dem Staat, der Wirtschaft, der Wissenschaft und der Zivilgesellschaft achten

… Aufbau staatlicher und **nicht-staatlicher Fähigkeiten und Kapazitäten**. Eine integrierte Cyber Sicherheitspolitik muss auf nationaler und internationaler Ebene kooperativ angelegt sein.

Subsidiarität

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.

- **Kommunikationstechnologie (IKT) sind in erster Linie für den Schutz ihrer Systeme selbst verantwortlich**. Dabei gilt der Grundsatz Selbstverpflichtung wenn möglich, Regulierung wenn notwendig.



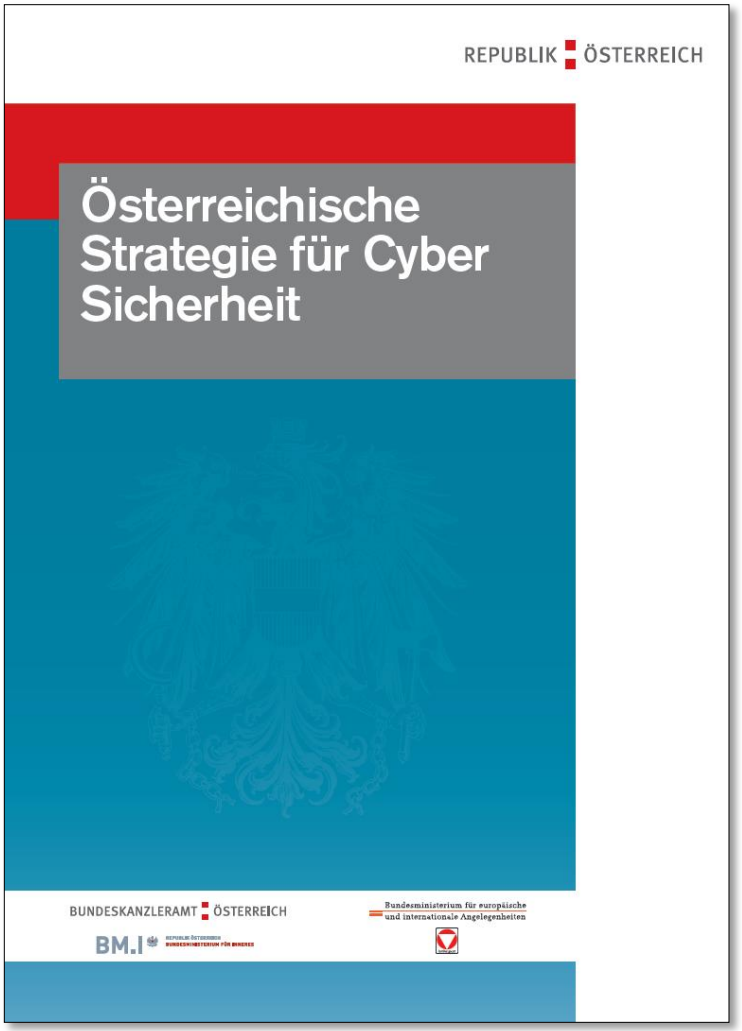
Verweise auf Branchenspezifische Aktivitäten

Kapitel 3 Prinzipien

- **Selbstregulierung**
  Grundsätzlich sollte angestrebt werden, **über Eigeninitiativen das Schutzniveau** … 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**

Kapitel 4 Strategische Ziele

- 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**.



Verweise auf Branchenspezifische Aktivitäten in der ÖSCS

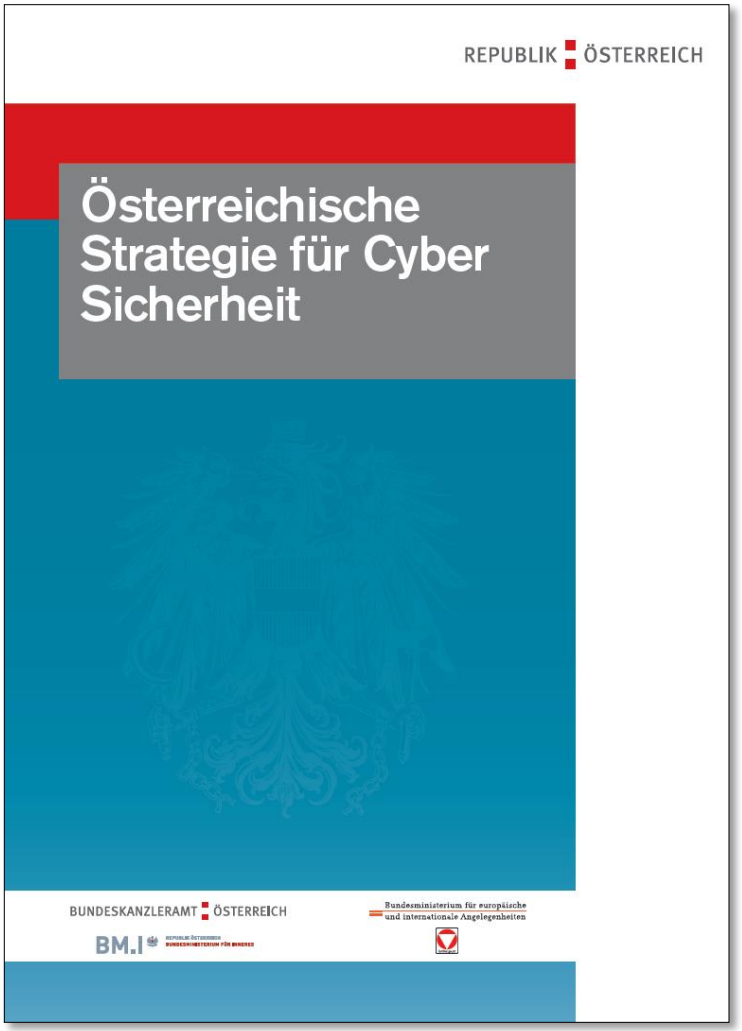
Kapitel 4 Strategische Ziele

- Durch den Aufbau von Wissen, Fähigkeiten und Kapazitäten

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. …

Vertraulichkeit der benötigten IKT-Infrastruktur auszeichnet.

- 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**



Branchenspezifische Aktivitäten

Kapitel 5 HF1 – Strukturen und Prozess

Punkt 1: Einrichtung einer Cyber Sicherheit Steuerungsgruppe

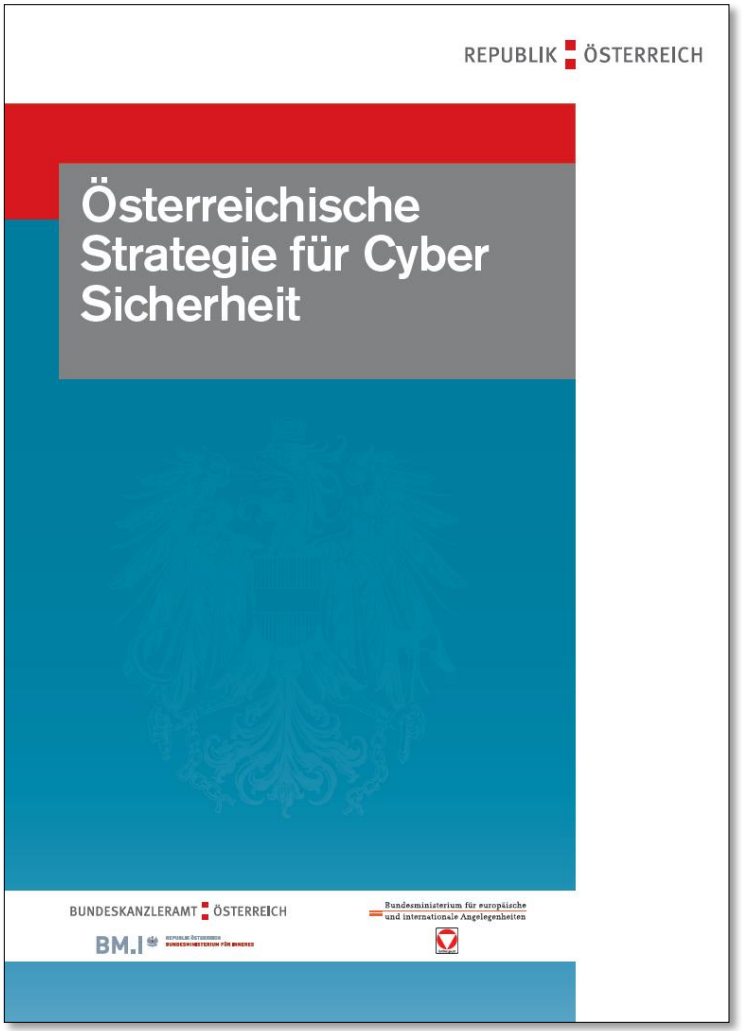
- Die mit Ministerratsbeschluss vom 11. Mai 2012 eingerichtete **Cyber Sicherheit Steuerungsgruppe** soll unter Federführung des Bundeskanzleramtes auf politisch-strategischer Ebene die Maßnahmen zur Cyber Sicherheit koordinieren, die Umsetzung

Cyber Sicherheit Steuerungsgruppe

…

Vertreter relevanter Unternehmen werden in geeigneter Form eingebunden

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**.



Cyber Sicherheit Steuerungsgruppe

Themen der CSS:

Umsetzungen der ÖSCS
(CSS, CSP, CKM, …)
Entwicklungen bei CSC und CVZ

Cyber-APCIP, KMU-Initiativen, NIS Direktive, LEG-AG, Bundesgesetz für Cybersicherheit, Berichte über operative Umsetzungen, Lagebild…

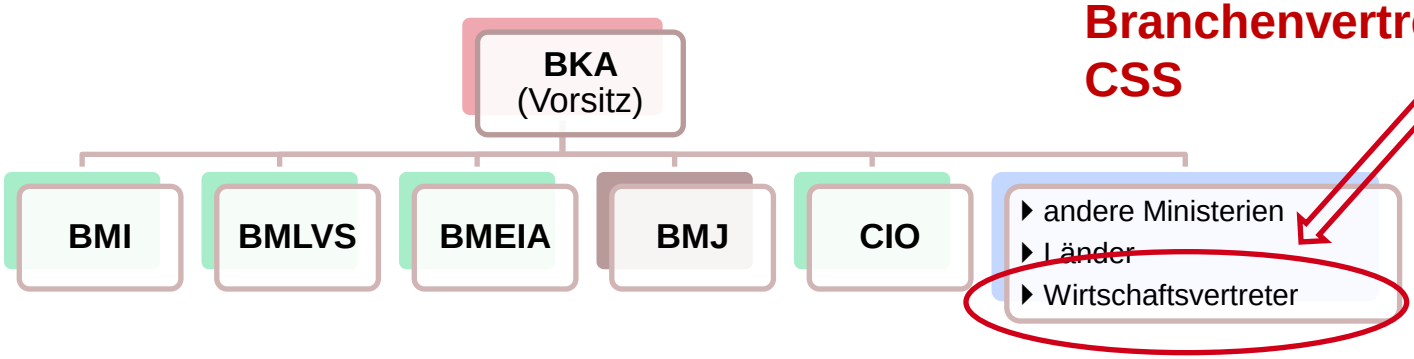
Koordination und Vorbereitung von Cybersicherheit Themen durch ein Core Team von den 4 NSR

Dieses Team versucht alle relevanten Cyber Sicherheit Themen in Österreich zu adressieren

Cyber Sicherheit Steuerungsgruppe

Seit 05/2012

Einbindung von Branchenvertretern in die CSS



Die **Cyber Sicherheit Steuerungsgruppe** (CSS) hat bisher neun Sitzungen abgehalten. Zur Vertiefung der Kooperation mit der Wirtschaft sind Vertreter aus den Sektoren Energie, Finanzen, **Internet Service Provider**, Industrie, Gesundheit. Transport und Kommunikation eingebunden

Branchenspezifische Aktivitäten

Kapitel 5 HF1 – Strukturen und Prozess

Punkt 2: Schaffung einer Struktur zur Koordination auf der operativen Ebene

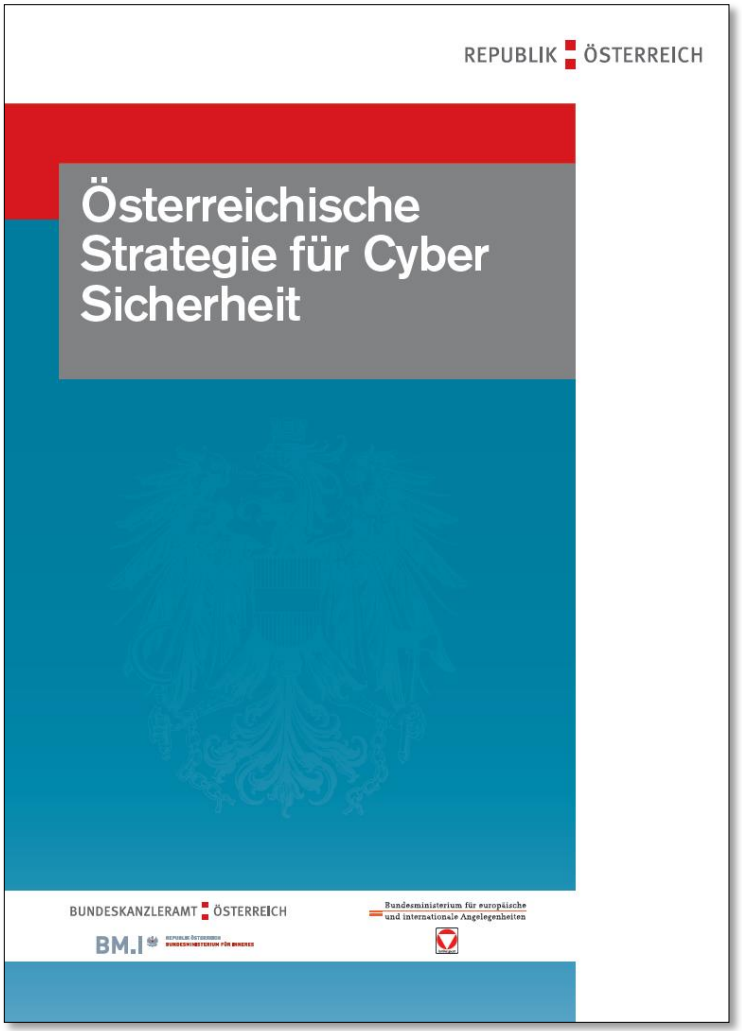
- Aufbauend auf bestehende operative Strukturen sowie unter deren Einbindung wird eine **Struktur zur Koordination auf der operativen Ebene** geschaffen. In ihrem Rahmen soll insbesondere ein periodisches und anlassbezogenes **Lagebild** … auf … soll … im … die … en. … on im Cyberspace soll allen Beteiligten 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. …

Struktur zur Koordination auf der operativen Ebene **…**

…

Dabei ist auch die Wirtschaft in geeigneter Form auf Augenhöhe einzubinden

…



Branchenspezifische Aktivitäten

Kapitel 5 HF1 – Strukturen und Prozess

Struktur zur Koordination auf der operativen Ebene **…**

…

Im Rahmen der Operativen Koordinierungsstruktur sollen **Einrichtungen zusammenarbeiten, die sich mit** … dem **Schutz von kritischen Infrastrukturen** beschäftigen

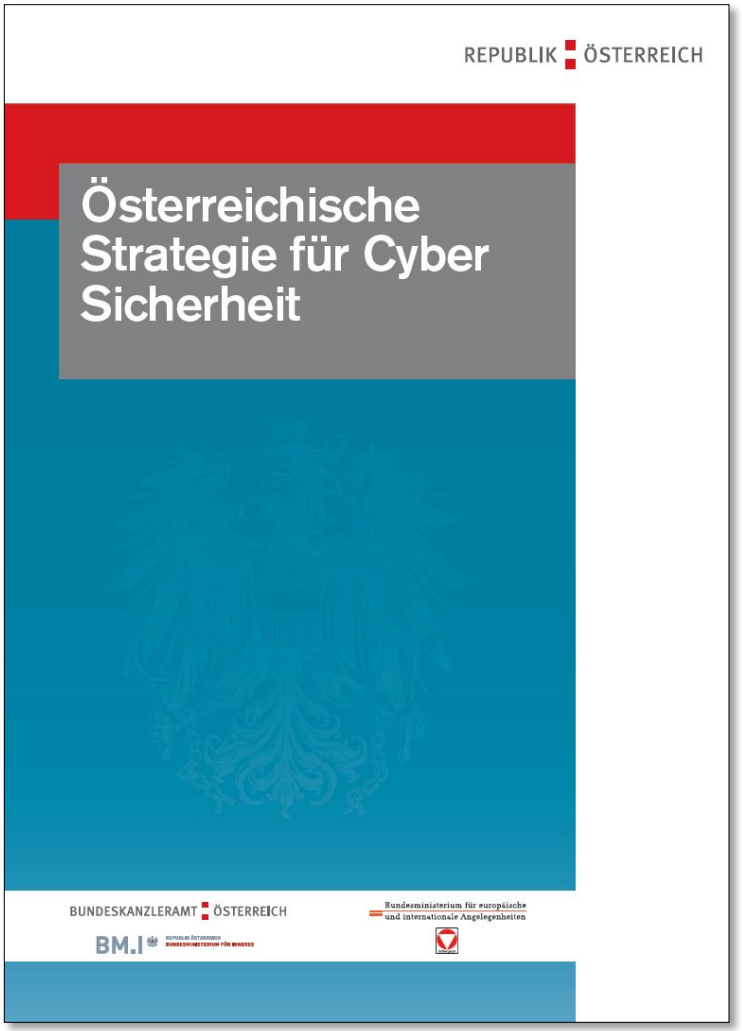
…

Struktur zur Koordination auf der operativen Ebene **…**

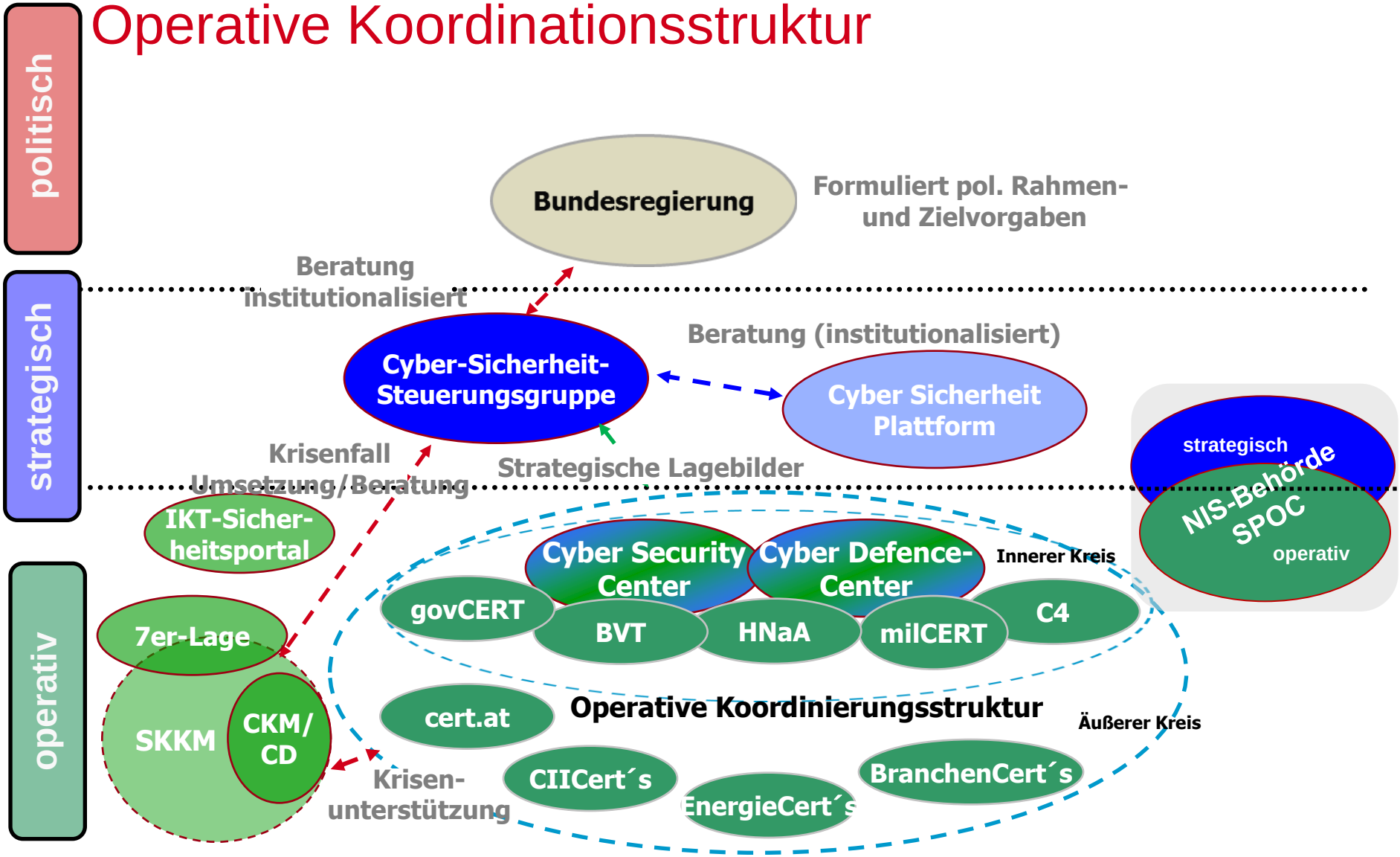
…

Darüber hinaus werden in einem zweiten Kreis **private CERTs, Wirtschaft und Forschung eingebunden**

…



Operative Koordinationsstruktur



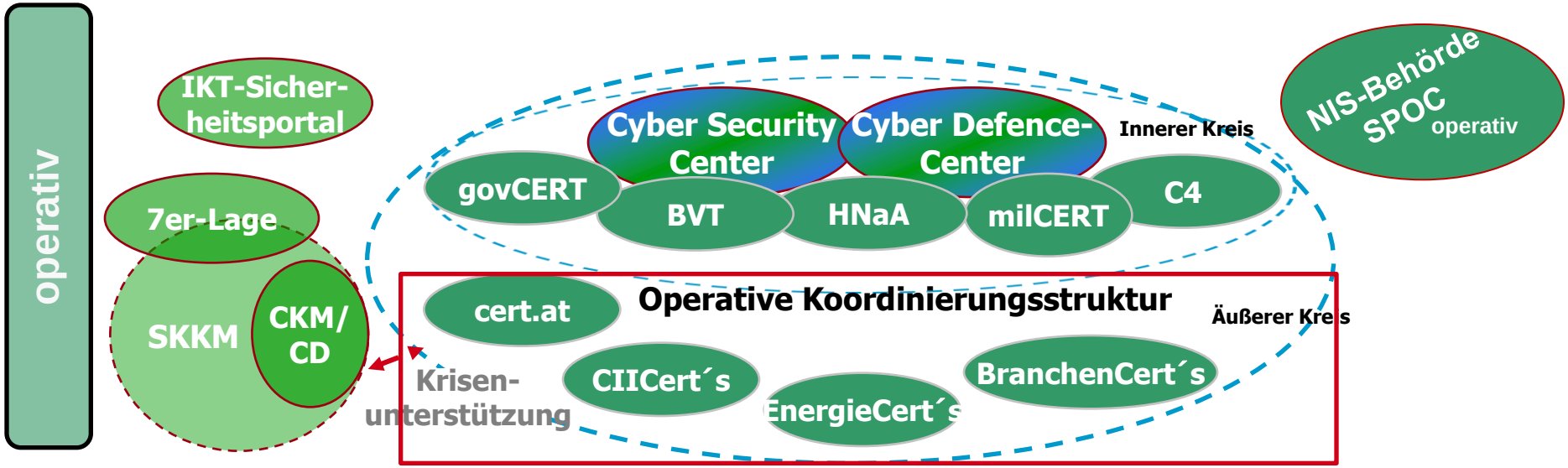
Operative Koordinationsstruktur

Branchenspezifische Aktivitäten

… als Teil des äußeren Kreises der operativen Koordinierungsstrukur

… als Teil des Cyberkrisenmanagements

… als Meldestelle für freiwillige und verpflichtende Meldungen



Branchenspez. Aktivitäten ergeben sich aus den Zielen der opKoord

- Rascher Informationsaustausch
  - und in Folge Umsetzung entsprechender Maßnahmen, basierend auf dieser Information
- Mitarbeit bei der Bereitstellung eines Cyber Lagebilds Österreich
  - basierend auf exakter, hochqualitativer Information und Analysemethoden
- Empfehlungen für proaktive, österreichweite Cyber Sicherheitsmaßnahmen
- Unterstützung und Koordination von staatlichen Notfallmaßnahmen im Falle
  - eines schweren Cybervorfalls
  - einer Cyber Krise

  in Österreich
- Einbindung etablierter öffentlicher und privater Branchen-CERTs in die operative Koordinierungsstruktur
- Etablierung von
  - Cyber Security Centre (CSC)
  - Cyber Defense Zentrum (CDZ)

  als Koordinationsplattformen der operativen Koordinierungstrukturen
  - Beide sind Teil des Arbeitsprogramms der Bundesregierung

Branchenspez. Aktivitäten ergeben sich aus dem Nutzen der opKoord

- Eine koordinierende Plattform (CSC/CDZ)
  - hat Übersicht in Echtzeit über den Status der Cyber Sicherheit in Österreich und kann entsprechend Maßnahmen ergreifen
  - koordiniert im Falle eines schweren Cybervorfalls
- Sektor-spezifische Incident-Meldestellen (Branchen-CERTs) bringen Vorfallsinformationen anonymisiert ein
  - Entgegennahme hereinkommender Vorfallsmeldungen von den Mitgliedern ihrer Branche
  - Durchführung koordinierter Maßnahmen für ihren Sektor
- Klar definierte Aufgaben und Verantwortlichkeiten zwischen
  - Sektor-spezifischen Incident-Meldestellen (Branchen-CERTs)
  - Zentralisierter Koordinationsplattform (CSC)
- Kommunikation auf Augenhöhe zwischen allen staatlichen Stellen
  - Bidirektional, keine Einwegkommunikation
  - Alle Stakeholder erhalten dieselbe Information so rasch als möglich
- **Die operative Koordinierungsstruktur bietet**
  - **Kurze Reaktionszeit im Falle eines schweren Cybervorfalls, und**
  - **Ergreifen koordinierter Gegenmaßnahmen**

Branchenspezifische Aktivitäten

Kapitel 5 HF1 – Strukturen und Prozess

Cyber Krisenmanagement

…

setzt sich aus Vertretern des Staates und der **Betreiber von kritischen Infrastrukturen** zusammen **…**

Cyber Krisenmanagement

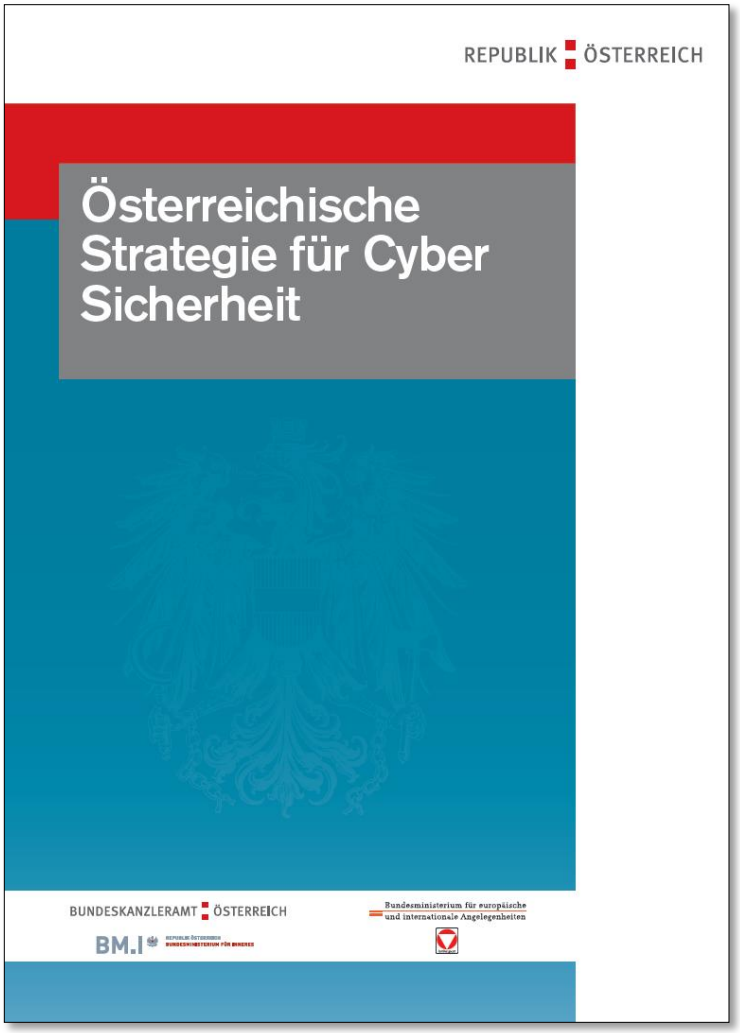
…

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 **…**

Cyber Krisenmanagement

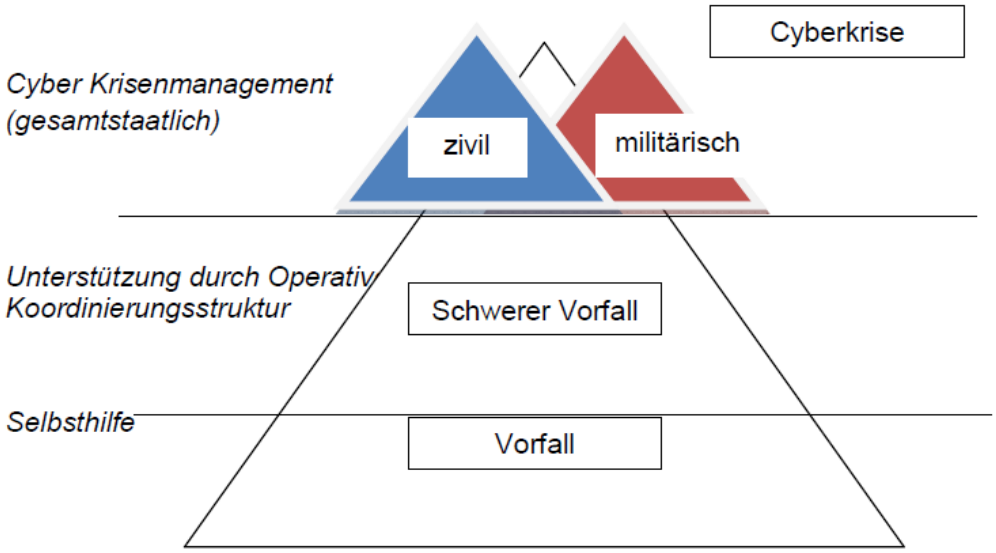
…

Regelmäßige Cyber Übungen sollen das Cyber Krisenmanagement sowie die Krisenmanagement- und Kontinuitätspläne testen



Cyber Krisen Management (CKM)

*„**Cyberkrise** ist eine schwere Anomalie im Cyber Raum, die eine gegenwärtige und unmittelbare Gefahr für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen darstellt und schwerwiegende Auswirkungen auf die Gesundheit, Sicherheit oder das wirtschaftliche und soziale Wohl großer Teile der Bevölkerung oder das effektive Funktionieren von staatlichen Einrichtungen nach sich ziehen kann“.*



Aufgaben:

- Gesamtstaatlicher Koordinations- und Kooperations-Mechanismus
- Bei schweren Cyber Krisen
- Teil des SKKM
- Risiko Manager
  + Operative Koordination
- Führung = zivil oder militärisch, abhängig von der Natur des Cyber Angriffs

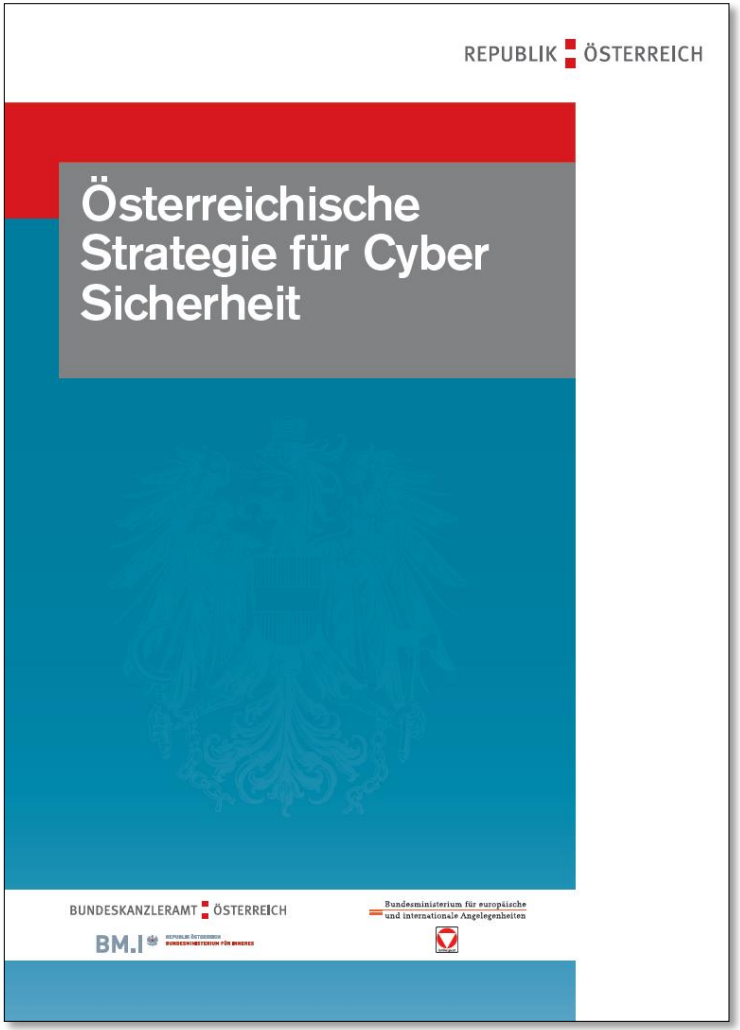
Branchenspezifische Aktivitäten

Kapitel 5 HF1 – Strukturen und Prozess

Punkt 4: Stärkung bestehender Cyber Strukturen

Stärkung bestehender 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



GovCERT-branchenspezifische Aktivitäten

- **Informationsdrehschreibe** für den operativen Bereich Cyber Sicherheit der definierten Branche
- Bündelung der **branchenspezifischen sicherheits-technischen Expertise** für den Bereich der Branche
- Setzen von **Präventivmaßnahmen** in der Branche
- **Unterstützungsleistung vor Ort** falls angefordert
- Sammlung und Bewertung von **sicherheitstechnischen Vorfällen**
- Teilnahme an der **operativen Koordinierungsstruktur**

GovCERT AUSTRIA

Branchenspezifische Aktivitäten

Kapitel 5 HF2 – Governance

Punkt 5: Schaffung eines zeitgemäßen ordnungspolitischen Rahmens

Schaffung eines zeitgemäßen ordnungspolitischen Rahmens

Breite Einbindung der Kritischen Infrastrukturen, der Wirtschaft und der Akademien in den Diskussionsprozess zur Gestaltung des Bundesgesetzes für Cybersicherheit

- U… wird
  e… g
  z…
  M… ode
  o…
  Ö… sem

Bericht sollen unter anderem die Fragen der Schaffung der notwendigen organisatorischen Strukturen, die behördlichen Aufgaben und Befugnisse, des **Informationsaustauschs** **…n, der** …on Sch… …t werd…

…ngen

Akteure ist der **ausg…** **…zen und Sanktionen** zu erwägen.

KSÖ Rechts- und Technologiedialog zur Cybersicherheit

AUSTRIAN TRUST CIRCLE

KSÖ RTD-Whitepaper

AG Ordnungs-politischer Rahmen

Legistische AG

Branchenspezifische Aktivitäten

Kapitel 5 HF2 – Governance

Punkt 6: Festlegung von Mindestsicherheitsstandards

Festlegung von Mindestsicherheitsstandards

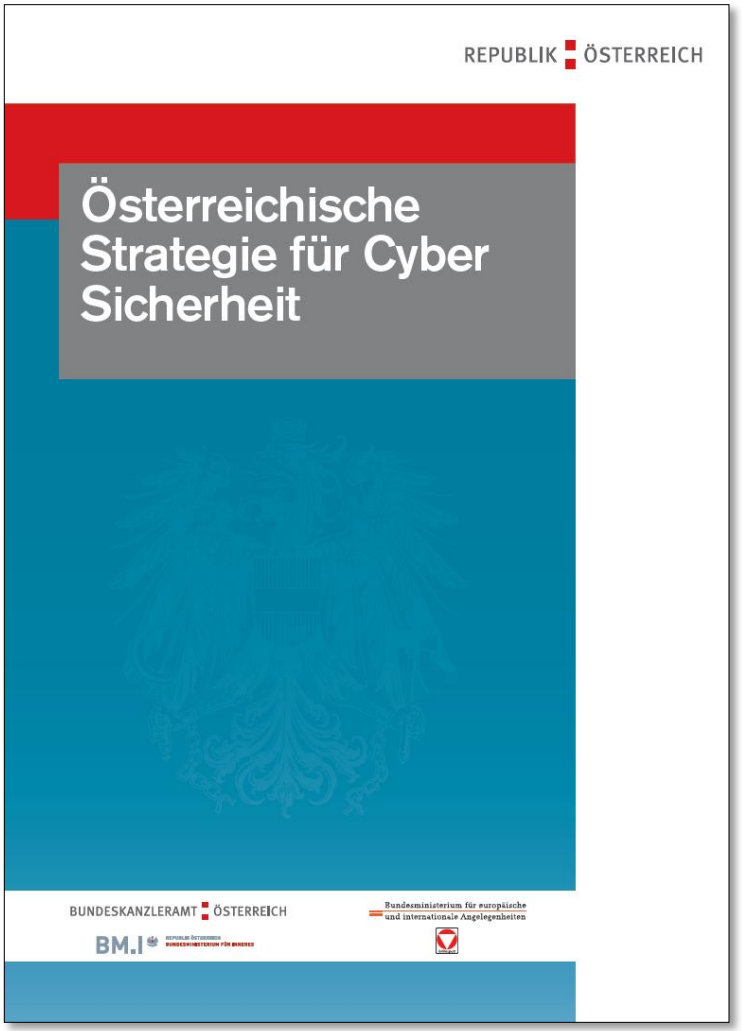
Für eine effektive Sicherheitsprävention und zum gemeinsamen Verständnis über aktuelle Anforderungen sollen **im Zusammenspiel aller relevanten Stakeholder Mindestsicherheitsstandards** für die Cyber Sicherheit definiert werden.

…

- F… …en
  V…
  Z…
  M… …iert
  w…
  si… …ten
  u…
  Verhaltensregeln, Best Practises usw. werden im österreichischen **Informationssicherheitshandbuch** zusammengefasst und laufend aktualisiert.

KIRAS Sicherheitsforschung

enisa



Branchenspezifische Aktivitäten

Kapitel 5 HF3 – Kooperation Staat, Wirtschaft und Gesellschaft

Punkt 8: Einrichtung einer Cyber Sicherheit Platt

Cyber Sicherheit Plattform

…

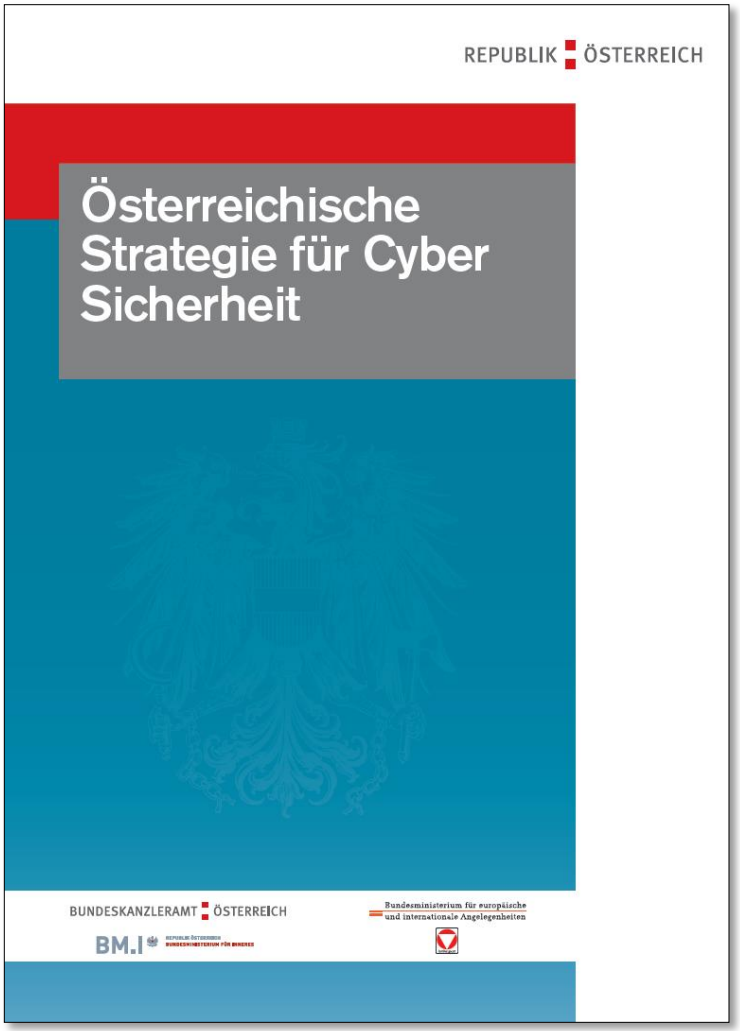
die Österreichische Cyber Sicherheit Plattform als **Public Private Partnership**.

- Zu … ng
  Circle, Cyber Security Austria, Kuratorium sicheres Österreich, A-SIT, …) die **Österreichische Cyber Sicherheit Plattform als** … ll … ng … der … den.
- …

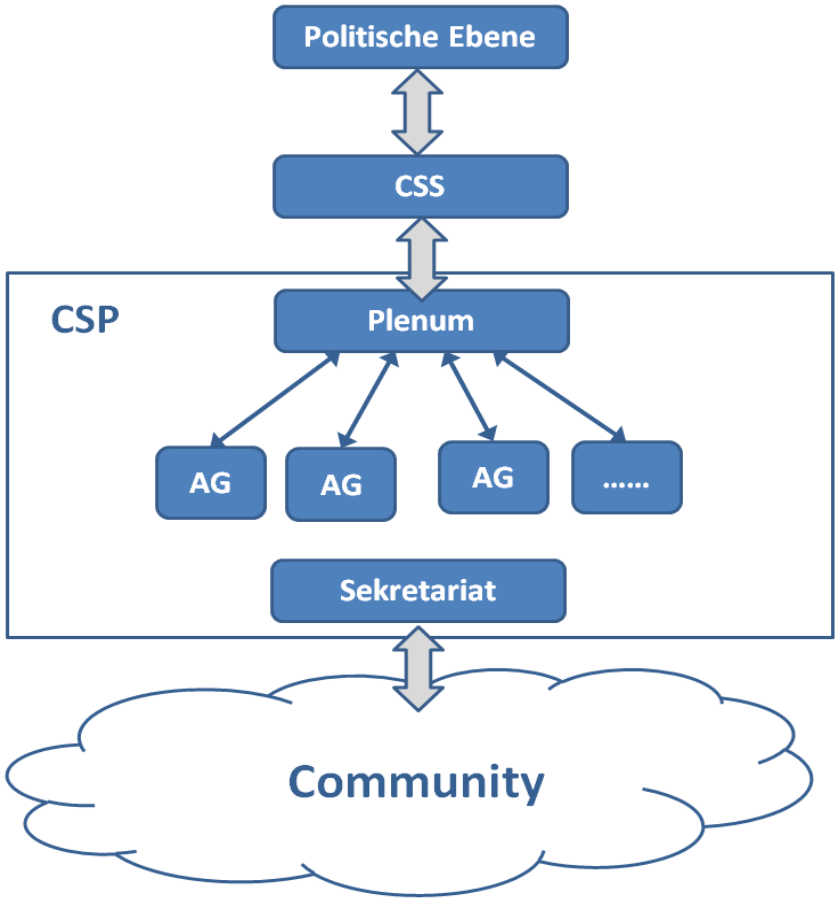
Cyber Sicherheit Plattform

…

Alle Akteure nehmen **in gleichberechtigter Weise an der Plattform tei**



Cyber Sicherheit Plattform (CSP)

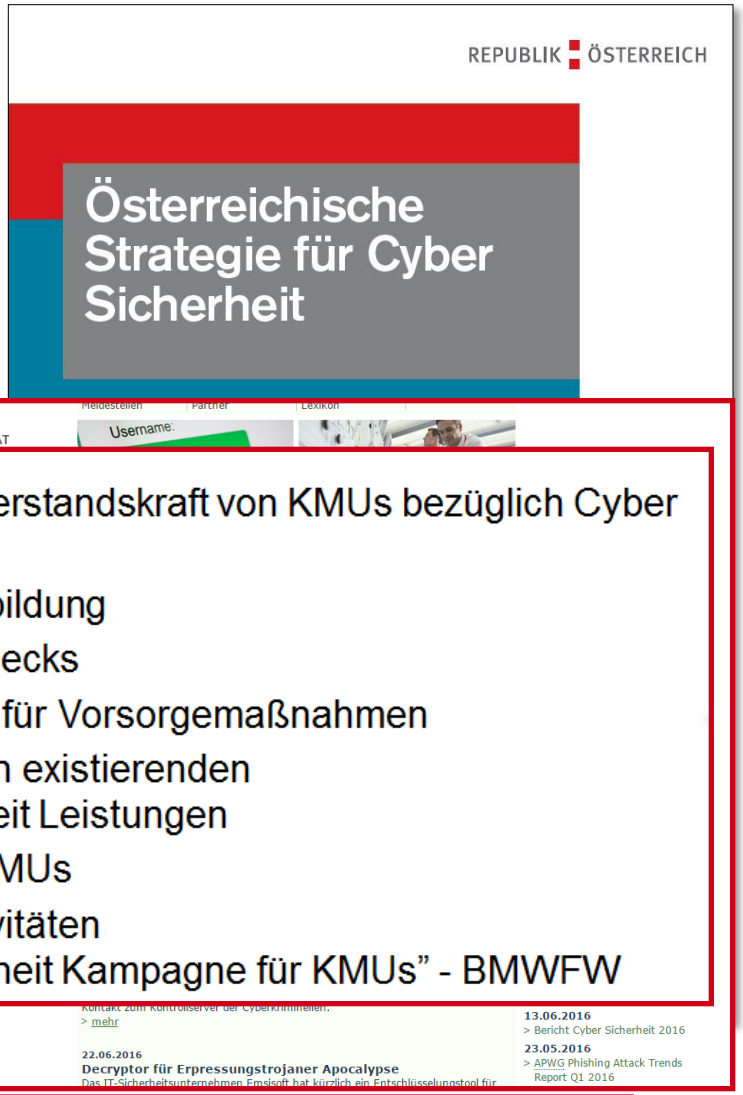


Aktivitäten

- Aufbau von Vertrauen
- Informationsaustausch Verwaltung/Wirtschaft/Wissen-schaft
- Beratung der Cyber Sicherheit Steuerungsgruppe (CSS)
- Dach für bestehende Kooperationsformate (ATC, KSÖ, A-SIT, CSA, …)

Branchenspezifische Aktivitäten

Kapitel 5 HF3 – Kooperation Staat, Wirtschaft und Gesellschaft



KMUs

KMUs werden mit **Schwerpunktprogrammen für Cyber Sicherheit** sensibilisiert und auf Gefährdungssituationen vorbereitet

- Erhöhung der Widerstandskraft von KMUs bezüglich Cyber Bedrohungen
  - Bewusstseinsbildung
  - Sicherheits-Checks
  - Empfehlungen für Vorsorgemaßnahmen
  - Darstellung von existierenden Cyber Sicherheit Leistungen
  - Übungen für KMUs

⇨ Verschiedene Aktivitäten
z.B. „Cyber Sicherheit Kampagne für KMUs" - BMWFW

"Aber sicher!"

Cyber Security Offensive für KMU

Stellen **branchentypische Cyber Risikomanagementpläne ausarbe… Regulierungsbehörden und Interessenvertretungen** werden in diesen Dialog eingebunden …

Branchenspezifische Aktivitäten

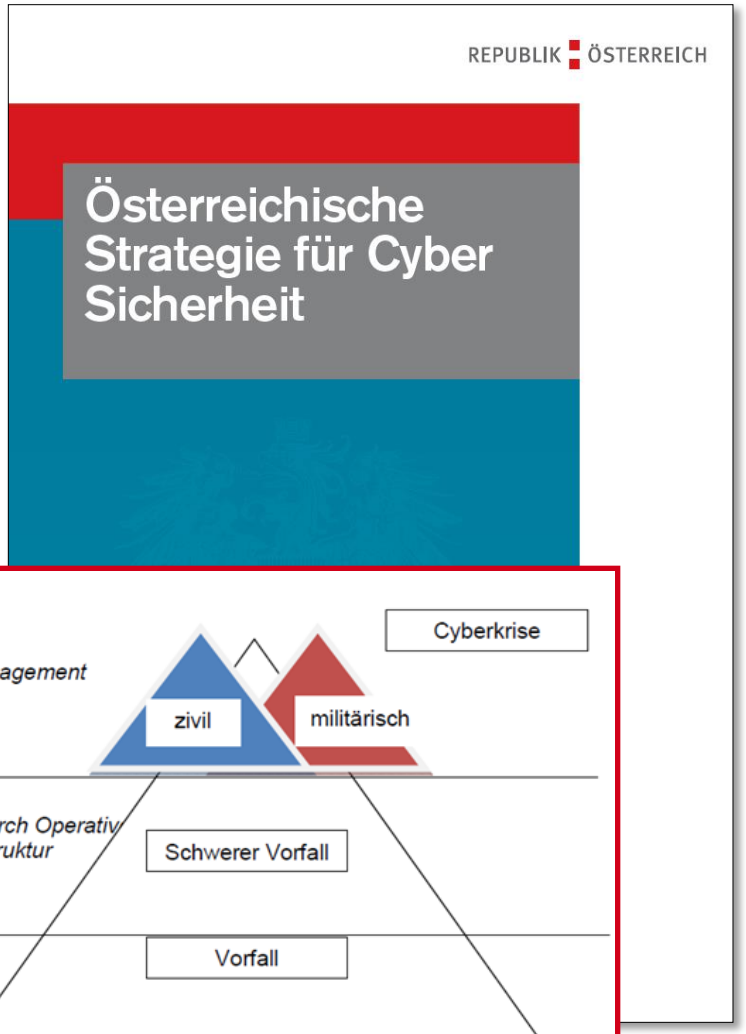
Kapitel 5 HF4 – Schutz kritischer Infrastrukturen

Punkt 11: Resilienz der kritischen Infra

Resilienz Kritische Infrastrukturen

Betreiber von kritischen Infrastrukturen sollen bei Prozessen des nationalen Cyber Krisenmanagements eingebunden werden.

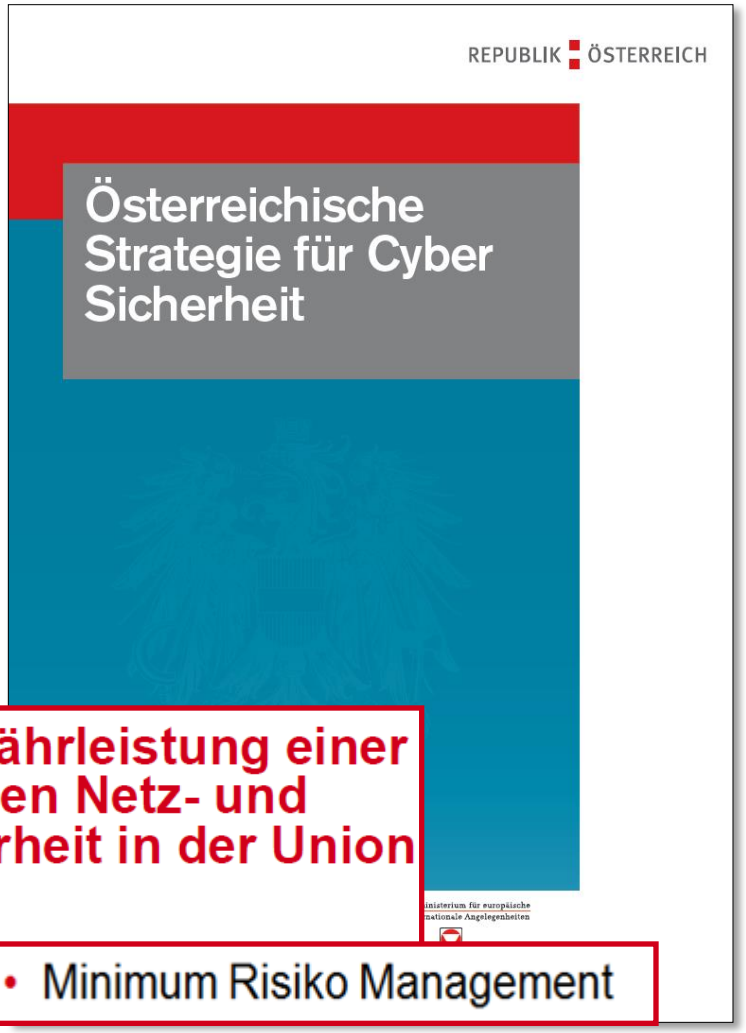
- B… …sen d… w… u… Krisenmanagement) einrichten, gefahrdungsorientiert aktualisieren sowie über einen Sicherheitsbeauftragten verfügen. Die **Krisenkommunikation** soll ausgebaut und gest… In einem partnerschaftlichen Ansatz sollen für diese **Cyber Sicherheitstandards** definiert werden.
- **Schwere Cyber Vorfälle** sollen für Betreiber von kri… Infrastrukturen **meldepflichtig** sein. Die entsprechen… gesetzliche Grundlage dafür ist nach umfassenden K… mit den relevanten Stakeholdern zu schaffen.
- Die bestehenden Dispositionen im Bereich des **Schu… kritischer Infrastrukturen (APCIP)** und des **staatli… und Katastrophenmanagements (SKKM)** sollen la… **Hinblick auf neue Cyber Herausforderungen übe…** Bedarf weiterentwickelt werden.



Branchenspezifische Aktivitäten

Kapitel 5 HF4 – Schutz kritischer Infrastrukturen

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



Richtlinie zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union

„NIS-RL“

- Minimum Risiko Management

Branchenspezifische Aktivitäten

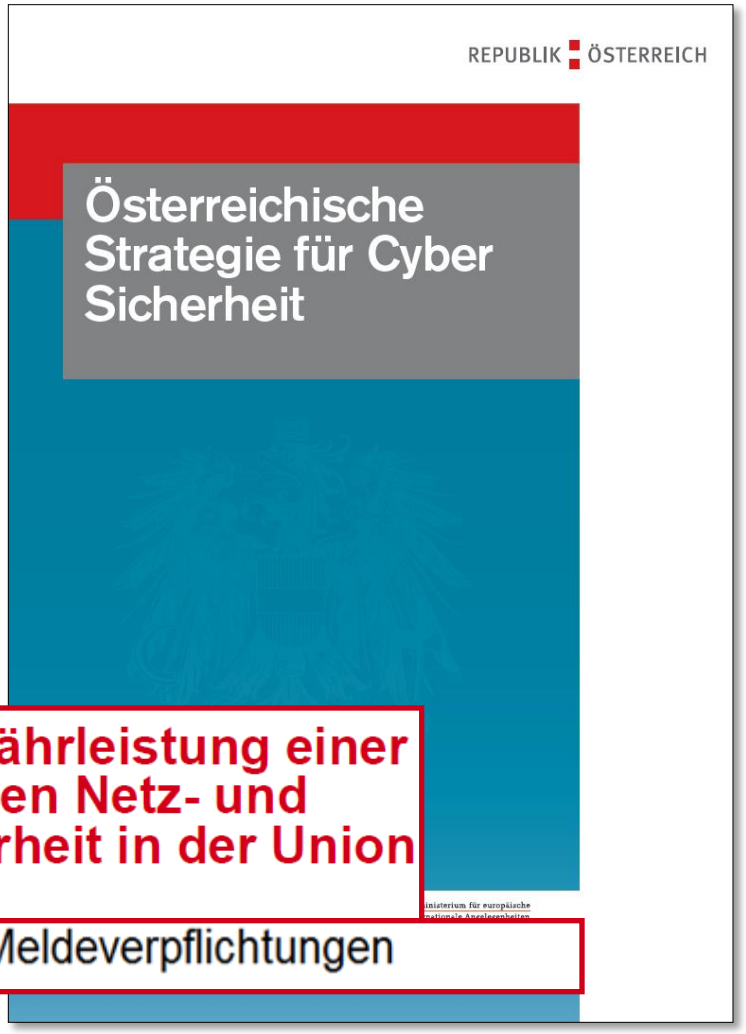
Kapitel 5 HF4 – Schutz kritischer Infrastrukturen

Punkt 11: Resilienz der kritischen Infrastrukturen erhöhen

- **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

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 **kritischer Infrastrukturen (APCIP) und Katastrophenmanagements** werden im **Hinblick auf neue Cyber Herausforderungen überprüft** und bei Bedarf weiterentwickelt werden.



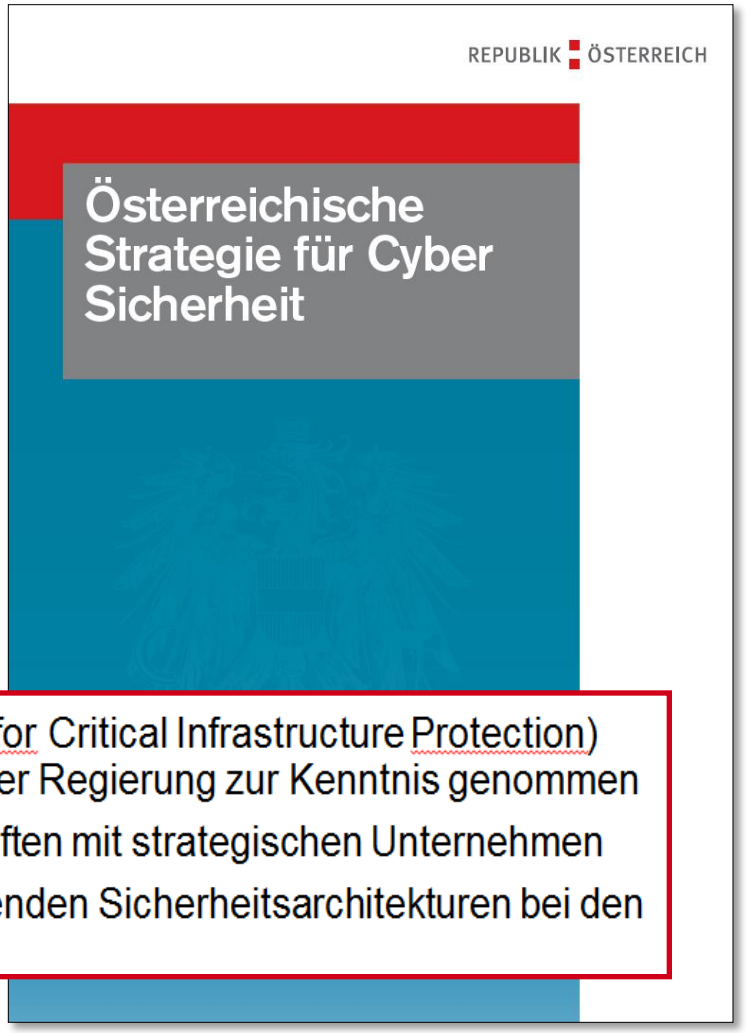
Branchenspezifische Aktivitäten

Kapitel 5 HF4 – Schutz kritischer Infrastrukturen

Punkt 11: Resilienz der kritischen Infr

- **B** …ssen …
  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** s… Infrastrukturen **meldepflic**… gesetzliche Grundlage daf… mit den relevanten Stakeh…
- Die bestehenden Dispositi… **kritischer Infrastrukturen** … **und Katastrophenmanag**… **Hinblick auf neue Cyber Herausforderungen überprüft** und bei Bedarf weiterentwickelt werden.

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.



- **APCIP** (Austrian Program for Critical Infrastructure Protection) wurde am 4.11.2014 von der Regierung zur Kenntnis genommen
  - Sicherheitspartnerschaften mit strategischen Unternehmen
  - Einrichten von umfassenden Sicherheitsarchitekturen bei den KIs

Danke…

Fragen?