MASTERPLAN 2014
Österreichisches Programm zum Schutz kritischer Infrastrukturen (APCIP[1])

1. Hintergrund

Moderne Gesellschaften mit hochentwickelter Dienstleistungs- und Industriewirtschaft zeichnen sich durch einen hohen Grad an Arbeitsteilung und intensiver Teilnahme an der Globalisierung aus, wobei dies nur durch Nutzung unterschiedlichster Infrastrukturen möglich ist. Österreich nimmt diese Chancen wahr und ist sich der Herausforderungen bewusst, die diese Abhängigkeiten von Infrastrukturen mit sich bringen. Sowohl die **Daseinsvorsorge für die Bevölkerung** als auch die Voraussetzungen für einen **attraktiven Wirtschaftsstandort** bauen auf der ständigen Verfügbarkeit und dem reibungslosen Ablauf vielfältiger Infrastrukturen auf. Österreich verfügt über leistungsfähige Infrastrukturen und kann zu Recht auf einen hohen Grad an Versorgungsicherheit bei Lebensmitteln, Verkehrs-, Telekommunikation-, Energie- und Finanzdienstleistungen wie auch auf eine gesicherte Versorgung mit Sozial- und Gesundheitsdienstleistungen verweisen.

Die Gesellschaft muss sich aber bewusst sein, dass die Funktionsfähigkeit von Infrastrukturen unter anderem durch Naturkatastrophen insbesondere bedingt durch den Klimawandel, technische Unfälle, menschliches Versagen, Gefahren im Cyber Raum, Kriminalität und Terrorismus gefährdet ist. Der Schutz kritischer Infrastrukturen gewinnt somit zunehmend an Bedeutung.

Die Bundesregierung hat daher am 2. April 2008 das **Österreichische Programm zum Schutz kritischer Infrastrukturen[2]** beschlossen (Masterplan APCIP 2008). Der Masterplan APCIP 2014 soll die bereits abgeschlossenen Arbeiten dokumentieren und

[1] APCIP = Austrian Program for Critical Infrastructure Protection

[2] „Schutz kritischer Infrastrukturen“ und der englische Begriff „Critical Infrastructure Protection“ werden im Masterplan als „Schutz und Sicherung kritischer Infrastrukturen“ verstanden, also in einem weiteren Begriffsfeld. Im Masterplan wird jedoch aus Vereinfachungsgründen nur der Begriff „Schutz“ verwendet.

den bisherigen Masterplan auf Basis der Erkenntnisse der letzten Jahre weiterentwickeln. Dies entspricht auch dem Auftrag zur Erfüllung des Teilziels 6 „Evaluation und follow up“ des Masterplans von 2008.

Der Schutz kritischer Infrastrukturen kann nur in vertrauensvoller Kooperation zwischen den staatlichen Stellen und den Unternehmen und Organisationen, die kritische Infrastrukturen betreiben und am APCIP teilnehmen (im Folgenden „strategische Unternehmen“) gelingen und erfolgreich erfüllt werden. Damit ist die Leitlinie dieses Programms vorgegeben:

Staat und Wirtschaft leisten gemeinsam einen wesentlichen Beitrag zur Steigerung der Resilienz und Sicherheit Österreichs.

Die Präsentation des **Europäischen Programms zum Schutz kritischer Infrastrukturen[3] (EPCIP)** durch die Europäische Kommission im Jahr 2006 und die folgende Entwicklung waren der Impuls zum Aufbau des nationalen Programms APCIP.

Auf Basis des Masterplans 2008 wurde der staatliche Gesamtprozess zur Implementierung und Umsetzung des Österreichischen Programms zum Schutz kritischer Infrastrukturen vom BKA gemeinsam mit dem BM.I unter Einbindung der betroffenen Bundesministerien, der Bundesländer, der Interessenvertretungen sowie der strategischen Unternehmen erfolgreich koordiniert.

Seit April 2008 haben sich wesentliche **Entwicklungen auf europäischer und nationaler Ebene** ergeben:

- Am 8. Dezember 2008 wurde vom Rat der Europäischen Union (EU) die **Richtlinie 2008/114/EG** über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen (ECI) und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern[4] beschlossen.

- Im Jahre 2011 wurden mit Deutschland, der tschechischen und der slowakischen Republik **bilaterale Vereinbarungen** abgeschlossen, die den Schutz europäischer kritischer Infrastrukturen in den jeweiligen Ländern verbessern soll.

[3] Siehe: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:DE:PDF
[4] Siehe: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:DE:PDF

- Am 15. Februar 2011 wurde mit der Meldung an die Kommission die **Richtlinie EPCIP in Österreich umgesetzt**.

- Anfang 2012 wurde die Identifikation jener **Unternehmen und Organisationen mit strategischer Bedeutung für Österreich** (strategische Unternehmen) in Absprache mit den relevanten Bundesministerien und Interessenvertretungen abgeschlossen.

- Seit März 2013 stehen den Mitgliedstaaten der EU das von der Europäischen Kommission betriebene **Critical Infrastructure Warning and Information Network (CIWIN)** als technische Plattform für den Informationsaustausch zwischen allen relevanten Stakeholdern zur Verfügung.

- Auf der technischen Plattform des CIWIN haben das BKA und das BM.I mit Unterstützung der Europäischen Kommission das Portal CIWIN-AT eingerichtet.

- In der am 20. März 2013 von der Bundesregierung beschlossenen **Österreichischen Strategie für Cyber Sicherheit (ÖSCS)**[5] sind umfassende Maßnahmen zum Schutz kritischer Infrastrukturen vor Risiken und Bedrohungen im Cyber Space vorgesehen.

- Am 8. Mai 2013 wurde im Bundeskanzleramt unter Anwesenheit der Bundesministerin für Inneres der **Leitfaden „Sicherheit in Unternehmen mit strategischer Bedeutung für Österreich“** der Öffentlichkeit vorgestellt und in der Folge an alle identifizierten Unternehmen und Organisationen verteilt. Teile des Leitfadens, z.B. zur IKT Sicherheit, wurden in fachspezifischen Foren den Unternehmen zur Selbstevaluation zur Verfügung gestellt.

- Der am 2. Juli 2013 von der Bundesregierung angenommene **Bericht zur Reform des Wehrdienstes**[6] unterstreicht die Bedeutung des Schutzes kritischer Infrastrukturen für die Bevölkerung Österreichs.

- In der am 3. Juli 2013 vom Nationalrat verabschiedeten **Österreichischen Sicherheitsstrategie (ÖSS)**[7] wird die Bundesregierung ersucht, ein gesamtstaatliches Konzept zur Steigerung der Resilienz Österreichs (Wiederherstellung von Staat und Gesellschaft nach Krisen) und zum Schutz kritischer Infrastrukturen zu erarbeiten.

---

[5] Bundeskanzleramt Österreich (Hg.): Österreichische Strategie für Cyber Sicherheit, Wien 2013, S. 14 http://www.bka.gv.at/DocView.axd?CobId=50748,

[6] Bundesministerium für Landesverteidigung und Sport (Hg.): Bericht zur Reform des Wehrdienstes, Wien 2013 bzw. http://www.bmlv.gv.at/download_archiv/pdfs/bericht_reform_wehrdienst.pdf

[7] Bundeskanzleramt Österreich (Hg.): Österreichische Sicherheitsstrategie. Sicherheit in einer neuen Dekade – Sicherheit gestalten. S. 17, http://www.bka.gv.at/DocView.axd?CobId=52099

- Am 28. August 2013 wurde nach eingehender Diskussion und mehreren Studien zur **Weiterentwicklung von EPCIP** das Commission Staff Working Document „on a new approach to the European Programme for CIP-Making European Critical Infrastructure more secure“ vorgelegt.

- Das **Arbeitsprogramm der Bundesregierung vom Dezember 2013** sieht im Kapitel 06 „Sicherheit und Rechtsstaat“ vor: „*Der Schutz kritischer Infrastrukturen (SKI) und die Gewährleistung von „Cyber Sicherheit“ sind von besonderer Bedeutung für die Gesundheit, Sicherheit, das wirtschaftliche und soziale Wohl der Bevölkerung, das Funktionieren staatlicher Einrichtungen und die Nutzung des „Cyber Raumes“, der immer mehr zum vitalen Aktionsraum für Staat, Wirtschaft, Wissenschaft und Gesellschaft wird*“.[8]

2. Der strategische und konzeptuelle Rahmen von APCIP

2.1. Definitionen

Kritische Infrastrukturen im Sinne dieses Masterplans sind jene Infrastrukturen (Systeme, Anlagen, Prozesse, Netzwerke oder Teile davon), die eine wesentliche Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen haben und deren Störung oder Zerstörung schwerwiegende Auswirkungen auf die Gesundheit, Sicherheit oder das wirtschaftliche und soziale Wohl großer Teile der Bevölkerung oder das effektive Funktionieren von staatlichen Einrichtungen haben würde.

Resilienz ist die Fähigkeit eines Systems, einer Gemeinschaft oder einer Gesellschaft, welche(s) Gefahren ausgesetzt ist, deren Folgen zeitgerecht und wirkungsvoll zu bewältigen, mit ihnen umzugehen, sich ihnen anzupassen und sich von ihnen zu erholen, auch durch Bewahrung und Wiederherstellung seiner bzw. ihrer wesentlichen Grundstrukturen und Funktionen[9].

[8] Bundeskanzleramt (Hg.): Arbeitsprogramm der österreichischen Bundesregierung 2013 – 2018. Erfolgreich. Österreich. Wien 2013, S. 78, http://www.bka.gv.at/DocView.axd?CobId=53264

[9] United Nations International Strategy for Disaster Reduction (UNISDR, 2009). http://www.unisdr.org/we/inform/terminology#letter-r. Übersetzung BM.I.

2.2. Die Österreichische Sicherheitsstrategie als Rahmen für APCIP

Die Weiterentwicklung und Umsetzung von APCIP ist ein wichtiger Beitrag zur Erarbeitung eines gesamtstaatlichen **Konzepts zur Steigerung der Resilienz Österreichs**, wie dies in der ÖSS vorgesehen ist. In der ÖSS finden sich im Empfehlungsteil in den Kapiteln *Allgemeine Empfehlungen*, *Innere Sicherheit* und *Verteidigungspolitik* noch weitere Hinweise auf den Schutz kritischer Infrastruktur.

Die ÖSS sieht vor, dass ein gesamtstaatliches Konzept zur **Steigerung der Resilienz Österreichs** erarbeitet werden soll. Der Schutz kritischer Infrastrukturen im Rahmen des APCIP ist neben Katastrophenschutz und Schutz vor technischen/industriellen Gefahren[10] sowie Maßnahmen zur Erhöhung der Cyber Sicherheit ein wesentlicher Beitrag zur Steigerung der Resilienz Österreichs im Sinne der **ÖSS.**

Bei der Weiterentwicklung von APCIP ist sicher zu stellen, dass inhaltliche und organisatorische Doppelgleisigkeiten mit den Bereichen Katastrophenschutz und Schutz vor technischen/industriellen Gefahren sowie Cyber Sicherheit vermieden und Synergien genützt werden.

2.3. APCIP und EPCIP

Österreich beteiligt sich aktiv an der Umsetzung des EPCIP und unterstützt die Europäische Kommission bei der Weiterentwicklung des Programms. Die Komplementarität und Kompatibilität zwischen APCIP und EPCIP ist daher sicherzustellen.

2.4. APCIP und Programme der Bundesländer

Die Bundesländer entwickeln eigene Programme zum Schutz ihrer regionalen kritischen Infrastrukturen und motivieren auch die Städte und Gemeinden lokale Programme zu schaffen. Bund und Länder tauschen in regelmäßigen Workshops ihre Erfahrungen aus. Dadurch soll die Komplementarität zwischen APCIP und den Länderprogrammen sichergestellt werden. Die Bundesbehörden unterstützen im Rahmen ihrer Zuständigkeiten

[10] Maßnahmen in diesen Bereichen werden im Rahmen des Staatlichen Krisen- und Katastrophenschutzmanagement koordiniert.

die Länder bei der Umsetzung der Länderprogramme nach Maßgabe der zur Verfügung stehenden Ressourcen und der aktuellen Bedrohungslage.

2.5. Zusammenspiel mit dem Staatlichen Krisen- und Katastrophenschutzmanagement (SKKM)

Das SKKM ist ein gesamtstaatliches Verfahren, das in umfassender Weise die Koordination der Maßnahmen der relevanten Akteure auf der Ebene des Bundes, der Länder und der Gemeinden im Bereich der Katastrophenprävention, -vorsorge, -hilfe und Beseitigung von Katastrophenfolgen (Begrenzung des Schadensausmaßes) zum Ziel hat. Das SKKM bezieht kritische Infrastrukturen in genereller Form in die Prävention und Vorsorge mit ein, wobei hier auf Vorfälle von erheblicher Schwere (Katastrophen) abgezielt wird. Das APCIP geht über diese Vorsorgemaßnahmen hinaus und entwickelt im Dialog zwischen Staat und Betreibern strategischer Unternehmen maßgeschneiderte und umfassende Konzepte zum Risiko-, Krisen- und Sicherheitsmanagement. Staatliche Maßnahmen zur Bewältigung von Katastrophen und die Beseitigung von Katastrophenfolgen, sind vom APCIP nicht vorgesehen und verbleiben daher in der Zuständigkeit der SKKM-Akteure.

3. Prinzipien und strategische Zielsetzungen APCIP

Prinzipien:

a) **„Operator based approach“:** Auf eine Aufzählung der kritischen Sektoren wird bewusst verzichtet, da damit die Interdependenzen einer komplexen Wirtschaft nicht abgebildet werden können. Österreich hat sich bei der Identifizierung von kritischen Infrastrukturen für einen an den Betreibern von strategischen Unternehmen orientierten Zugang entschieden.

b) **Subsidiarität und Selbstverpflichtung der Unternehmen**: Die Eigentümer und Betreiber von strategischen Unternehmen sind in erster Linie für die Aufrechterhaltung ihrer Leistungen und den Schutz ihrer Anlagen und Einrichtungen selbst verantwortlich. Da ein nationales Interesse an der Versorgungsfunktion dieser Unternehmen besteht, sollen sich diese in einer (freiwilligen) Selbstverpflichtung zu einer erhöhten Resilienz

und damit zu Schutzstandards bekennen, die für ihre Branche gemeinsam definiert wurden. Deshalb sind Politik und Verwaltung für die Gestaltung der Rahmenbedingungen verantwortlich, damit ein klar definiertes Schutzniveau erreicht wird.

c) **Komplementarität**: Bestehende Maßnahmen und Pläne sollen weiter genutzt und den neuen Bedrohungen angepasst werden.

d) **Vertraulichkeit**: Informationen sollen auf Basis von Vertraulichkeit ausgetauscht werden und nur in jener Informationstiefe vorliegen, die die jeweilige Aufgabenstellung erfordert.

e) **Kooperation**: Die Zusammenarbeit aller Stakeholder, d.h. Unternehmen und Interessenverbände, öffentliche Verwaltung und Regulatoren, aber auch Normungsinstitute und Medien haben einen angemessenen Beitrag zur Weiterentwicklung und Umsetzung von APCIP zu leisten.

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

g) **All-hazards-Ansatz:** Kritische Infrastrukturen sollen vor einem breiten Spektrum möglicher Risiken gesichert werden. Die Maßnahmen sind aus einem **umfassenden Sicherheitsverständnis** abzuleiten und sollten daher das Risiko krimineller Akte und terroristischer Anschläge genauso berücksichtigen wie Naturgefahren und von Menschen verursachte Katastrophen bzw. technisches Versagen.

Resiliente Unternehmen als strategisches Ziel

Der Schwerpunkt von APCIP liegt in der Unterstützung der strategischen Unternehmen zur Implementierung einer umfassenden Sicherheitsarchitektur. Dazu ist es für diese Unternehmen notwendig:

- über die eigene Verwundbarkeit Bescheid zu wissen und eine **Risikoanalyse** durchzuführen,
- daraus Maßnahmen abzuleiten, um **Risiken zu vermeiden,** zu **mindern oder zu überwälzen (Risikomanagement zur Verringerung der Verletzlichkeit)**,

- über die Fähigkeit zu verfügen, durch ein Krisenmanagement **Störungen und Notfälle** besser zu **bewältigen** (**Business Continuity Management** zur Begrenzung des Schadensausmaßes) sowie
- ein **Sicherheitsmanagement** einzurichten.

Strategische Unternehmen leisten damit einen gesellschaftlich wertvollen Beitrag zur Aufrechterhaltung der Daseinsvorsorge und zur Gewährleistung eines attraktiven Wirtschaftsstandorts.

4. Handlungsfelder und Maßnahmen

Handlungsfeld 1 - Governance

Ziele:

Der Schutz kritischer Infrastruktur ist eine komplexe Herausforderung, bei der die Aktivitäten der unterschiedlichen Akteure in Staat und Wirtschaft koordiniert und APCIP mit anderen Bereichen des Nationalen Risikomanagements (Katastrophenschutz und Schutz vor technischen/industriellen Gefahren, Cyber Sicherheit), verstärkt abgestimmt werden muss.

Akteure:

BKA und BM.I sind gemeinsam mit der Umsetzung von APCIP beauftragt. Sie werden dabei von anderen staatlichen Akteuren aus den Bereichen der Bundesverwaltung und der Länder beraten und unterstützt.

Maßnahmen:

1) Strategische Steuerung und Weiterentwicklung

- Der staatliche **Gesamtprozess** zur Umsetzung des Masterplans APCIP wird vom BKA gemeinsam mit dem BM.I unter Einbindung der betroffenen Bundesministerien, der Bundesländer sowie sonstiger Stakeholder koordiniert.

- BKA und BM.I betreiben gemeinsam die strategische Planung von APCIP und legen einvernehmlich fest, welche Unternehmen und Organisationen von strategischer Bedeutung für den Bund sind und somit auf die **ACI-Liste** gesetzt werden (Maßnahme 6).

- BKA und BM.I betreiben gemeinsam das Portal **CIWIN-AT** (Maßnahme 18).

- BKA und BM.I arbeiten mit den Betreibern strategischer Unternehmen im Rahmen einer **Public Privat Partnership** zusammen (Maßnahmen 18 - 22).

- Das BM.I ist für die Umsetzung des **sicherheitspolizeilichen Teils von APCIP** zuständig.

- Alle betroffenen Ressorts und staatlichen Stellen beteiligen sich an der Umsetzung und Weiterentwicklung von APCIP nach Maßgabe ihrer ressortmäßigen Zuständigkeiten und sind stärker in den Planungs- und Umsetzungsprozess miteinzubinden.

- BKA und BM.I arbeiten mit der EU im Rahmen des **EPCIP** zusammen.

2) Abstimmung mit anderen staatlichen Stellen

- Die interministerielle Projektgruppe APCIP/EPCIP „Schutz kritischer Infrastruktur", welche auf Grund des Ministerratsvortrag 2008 eingerichtet wurde, wird in den „**Beirat APCIP**" umgewandelt.

- Zur Mitwirkung im Beirat sind insbesondere Vertreter von BMLVS, BMWFW, BMVIT, BMF, BMLFUW und BMG sowie die Bundesländer einzuladen. Vertreter der Interessenvertretungen, der Wirtschaft und der Regulatoren werden zu bestimmten Themen beigezogen.

- **BKA und BM.I berichten regelmäßig dem Beirat** über die Fortschritte bei der Umsetzung von APCIP und EPCIP. Der Beirat berät und unterstützt das BKA und das BM.I bei der Umsetzung und Weiterentwicklung von APCIP und EPCIP und sorgt für eine Abstimmung des Programms mit relevanten anderen Bereichen (Katastrophenschutz und Schutz vor technischen/industriellen Gefahren, Cyber Sicherheit). Der Beirat kann themenspezifische Arbeitsgruppen einsetzen.

3) Ordnungspolitischer Rahmen

- Die **Mitarbeit der Betreiber** strategischer Unternehmen am APCIP erfolgt auf **freiwilliger Basis** in Form einer **Selbstverpflichtung** (Public Private Partnership).

- Die freiwillige Zusammenarbeit sowie insbesondere der Austausch und der Schutz der Informationen zwischen den Sicherheitsbehörden und diesen Betreibern soll in rechtlich nicht verbindlichen **Kooperationsvereinbarungen** geregelt werden.

- Die **Aufgaben und Befugnisse der Sicherheitsbehörden** zum Schutz kritischer Infrastrukturen sollen gesetzlich geregelt werden. Unter anderem soll die Möglichkeit geschaffen werden, auf begründetes Ersuchen behördliche Sicherheitsüberprüfungen durchführen zu lassen. Dazu ist bis Ende 2014 ein Bericht des BM.I vorzubereiten.

- Im Rahmen der derzeit laufenden Arbeiten zur **Anpassung des Strafrechts** sollen qualifizierende Bestimmungen zur Ahndung von Störungen bei Unternehmen und Organisationen der Daseinsvorsorge vorgesehen werden, seien diese intentional geplant oder grob fahrlässig herbeigeführt.

4) Information der Bevölkerung, Zusammenarbeit mit den Medien

- Die Konsumenten wirken mit ihren Kaufentscheidungen direkt auf die Gestaltung des Waren- und Dienstleistungsangebots ein und somit auch darauf, wieviel „Sicherheit“ an Verfügbarkeit diese bieten. Die Medien sind bei der Vermittlung dieses Sachthemas der Dreh- und Angelpunkt in einer Informationsgesellschaft. BKA und BM.I werden eine **Informations- und Kommunikationsstrategie** zu APCIP vorbereiten.

5) Handbuch APCIP

- BKA und BM.I fassen die grundsätzlichen Dokumente für den Schutz kritischer Infrastrukturen in einem **Handbuch APCIP** zusammen. Das Handbuch wird auf dem Portal CIWIN-AT allen Stakeholdern zu Verfügung gestellt.

Handlungsfeld 2 – Aufgaben der staatlichen Stellen

Ziele: Daseinsvorsorge und Wirtschaftsstandort sichern

Im Sinne der staatlichen Sicherheitsvorsorge ist es die Aufgabe der staatlichen Stellen, strategische Unternehmen auszuweisen, gemeinsam mit diesen deren Risiken zu bewerten und die strategischen Unternehmen zu informieren, zu unterstützen und anzuhalten, ihrer Versorgungsfunktion nachzukommen. Dabei spielen insbesondere die Versorgung mit Lebensmitteln und Wasser, aber auch die Verfügbarkeit von Gesundheits-, Finanz- und Verkehrsdienstleistungen, von Energie sowie von Informations- und Kommunikationsdienstleistungen eine besondere Rolle. Lagebedingt kann die

Unterstützung der Betreiber von der Beratung und Information bis hin zum physischen Schutz von Objekten der strategischen Unternehmen gehen.

Akteure:

Der Schutz kritischer Infrastrukturen ist eine gesamtstaatliche Aufgabe von Bund, Ländern und der strategischen Unternehmen. Die beteiligten Ressorts tragen im Rahmen ihrer Zuständigkeiten zur Umsetzung von APCIP bei. Die operative Umsetzung des APCIP in Bezug auf die sicherheitspolizeilichen Bedrohungen erfolgt durch die Sicherheitsbehörden auf der Grundlage ihrer sicherheitspolizeilichen Aufgaben und Befugnisse. Bei Bedarf unterstützt das Österreichische Bundesheer im Rahmen von Assistenzeinsätzen die Sicherheitsbehörden.

Maßnahmen:

6) Ausweisung ACI

- Durch BKA und BM.I wurden die strategischen Unternehmen, die kritische Infrastrukturen betreiben, erfasst und in der **ACI-Liste** ausgewiesen. Kriterien und Methoden zur Erstellung der ACI-Liste wurden erarbeitet und sind im Handbuch APCIP dargestellt.

- Durch BKA und BM.I werden gemeinsam die Verfahren zur Erstellung, Aktualisierung und Weitergabe der ACI-Liste festgelegt.

7) Staatliche Risikoanalysen

- Als Grundlage für die Festlegung der Schutzstandards für strategische Unternehmen und die Planung weiterer Maßnahmen (z.B. Lagebilder, Beratungen,…) sind von den zuständigen staatlichen Stellen **branchenweise** Risikoanalysen durchzuführen.

- Diese Risikoanalysen sind mit den Methoden und Verfahren der Nationalen Risikoanalyse abzustimmen und orientieren sich an **internationalen Standards**.

8) Leitfaden

- Der im Rahmen des Masterplans 2008 entwickelte **Leitfaden „Sicherheit in Unternehmen mit strategischer Bedeutung für Österreich“** soll bei den Betreibern

das notwendige Bewusstsein der Verletzlichkeit des Betriebes schaffen, das die Voraussetzung zur Implementierung einer umfassenden Sicherheitsarchitektur ist.

- Die strategischen Unternehmen sollen bei der Erstellung einer umfassenden Sicherheitsarchitektur unterstützt und begleitet werden. Der Leitfaden ist die Grundlage für diese **Beratungsgespräche** (siehe Maßnahme 10).

- Der Leitfaden wird vom BKA und vom BM.I regelmäßig auf seine **Aktualität überprüft**. Bei Bedarf wird eine neue Version erstellt.

9) Kontakt- und Meldestelle KI

- Im BM.I wird die **Kontakt- und Meldestelle KI** eingerichtet. Damit soll eine 24/7 Erreichbarkeit für die strategischen Unternehmen gewährleistet werden.

10) Beratung und Information strategischer Unternehmen

- Die **Sicherheitsbehörden informieren und beraten die strategischen Unternehmen** auf der Grundlage des Leitfadens, der Risikoanalysen und der Lagebilder.

- Zur Sicherstellung der Effektivität und Effizienz der Beratung und Information der strategischen Unternehmen wird vom BM.I ein **Präventionskonzept** entwickelt[11].

- Die Beratungs- und Informationsangebote von APCIP werden von BKA und BM.I in einer **Informationsbroschüre** zusammengefasst.

- In Absprache mit den zuständigen Stellen wird schrittweise das **Beratungs- und Informationsangebot** auf Risiken durch Naturgefahren und technische Störungen (z. B. Blackout) sowie Gesundheitsrisiken **erweitert**.

11) Lagebilder

- Für **intentionale Bedrohungen** werden auf der Grundlage sicherheitspolizeilicher Analysen und der Meldungen der strategischen Unternehmen (siehe Maßnahme 16)

[11] Dieses Präventionskonzept berücksichtigt auch die bestehenden Normen (z.B. ONR 2420: Corporate Security Management: Anforderungen an Konzepte zum Schutz von Objekten vor intentionalen Gefahren, ONR 2450 - Umgang mit klassifizierten Informationen – Anforderungen an den Schutz von Verschlusssachen.

vom BM.I regelmäßige und anlassbezogene **Lagebilder** erstellt und den strategischen Unternehmen zur Verfügung gestellt.

- **Weitere Lagebilder** werden bei Bedarf an die strategischen Unternehmen weitergeleitet.

12) Frühwarnsystem

- Die **Kontakt- und Meldestellte KI** informiert strategische Unternehmen über **aktuelle Risiken und Bedrohungen**.

13) Objektschutz

- Nach Maßgabe sicherheitspolizeilicher Analysen werden Objekte kritischer Infrastrukturen in Absprache mit den Betreibern in den vom BM.I geführten **Objektschutzkatalog** aufgenommen.

- Zur Vorbereitung des physischen Schutzes werden gemeinsam mit den strategischen Unternehmen **Objektschutzblätter** erstellt.

- Der Schutz der Objekte erfolgt bei Bedarf auf der **Grundlage des Sicherheitspolizeigesetzes** nach Maßgabe der aktuellen Bedrohungslage. Dazu können auch Kräfte des ÖBH im Assistenzeinsatz zur Unterstützung der Sicherheitsbehörden herangezogen werden.

- Die **Beitragsleistung des ÖBH** zum Schutz kritischer Infrastrukturen und zum Objektschutz ist im Rahmen des in der ÖSS vorgesehenen gesamtstaatlichen Planungsprozesses festzulegen und regelmäßig fortzuschreiben.

Handlungsfeld 3 – Aufgaben der Betreiber von strategischen Unternehmen

Ziele:

Strategisches Ziel von APCIP sind resiliente Unternehmen. Die strategischen Unternehmen sollen mit Hilfe des Leitfadens „Sicherheit in Unternehmen mit strategischer Bedeutung für Österreich“ (siehe Maßnahme 8) eine umfassende betriebliche

Sicherheitsarchitektur einrichten und den Sicherheitsbehörden auf freiwilliger Basis Vorfälle melden, die das Unternehmen in seiner Leistungsfähigkeit einschränken.

Akteure:

Die strategischen Unternehmen tragen die primäre Verantwortung für das Funktionieren ihrer Anlagen und Systeme sowie bei Schadensereignissen das unternehmerische Risiko und die Haftungsrisiken. Dies ist eine gesamtunternehmerische Aufgabe, die der Unterstützung aller Ebenen bedarf.

Maßnahmen:

14) Einrichtung einer umfassenden Sicherheitsarchitektur

- Unter Nutzung des Leitfadens "Sicherheit in Unternehmen mit strategischer Bedeutung für Österreich" (siehe Maßnahme 8) soll, unter Beachtung der im Rahmen von APCIP definierten Schutzstandards (siehe Maßnahme 21) sowie der bestehenden rechtlichen Verpflichtungen, von den strategischen Unternehmen eine **umfassende Sicherheitsarchitektur im Unternehmen** aufgebaut werden.

- Diese umfassende Sicherheitsarchitektur soll alle notwendigen Maßnahmen vom **Risikomanagement**, dem **Business Continuity Management** zur Bewältigung von und der Erholung nach Störungen mit schwerwiegenden Auswirkungen sowie ein **Sicherheitsmanagement** umfassen.

15) Implementierung von Schutzstandards

- Im Rahmen ihrer Selbstverpflichtung setzen die strategischen Unternehmen die für ihre Branche **gemeinsam definierten Schutzstandards** (siehe Maßnahme 21) um und erhöhen damit die Resilienz ihrer Unternehmen.

- Darüber hinaus soll den strategischen Unternehmen im Rahmen der Beratung empfohlen werden, die Umsetzung der oben genannten **Schutzstandards** als Teil ihres Compliance Managements von einer akkreditierten Stelle **zertifizieren** zu lassen.

- Die verpflichtende Umsetzung gesetzlich vorgeschriebener Normen und Standards durch die strategischen Unternehmen, werden durch diese freiwillige Umsetzung von Schutzstandards im Rahmen von APCIP nicht berührt.

16) Meldung von Vorfällen

- Unbeschadet sonstiger gesetzlicher Melde- und Informationsverpflichtungen **melden die strategischen Unternehmen Vorfälle mit schwerwiegenden Auswirkungen** auf die Versorgungsfunktion des strategischen Unternehmens an die Melde- und Kontaktstelle KI.

- Welche Vorfälle gemeldet werden sollen, wird in der **Kooperationsvereinbarung (**siehe Maßnahme 20) festgelegt.

17) Nominierung von Points of Contact für die staatlichen Stellen

- Durch die strategischen Unternehmen sind Ansprechpartner (**Point of Contact**) für die staatlichen Stellen zu benennen und Änderungen bekannt zu geben.

Handlungsfeld 4 – Public Private Partnership

Ziele:

Die funktionierende Zusammenarbeit zwischen Staat, Wirtschaft und Wissenschaft ist zentral für den Erfolg von APCIP.

Akteure:

Die Partner sind einerseits jene staatliche Stellen, die mit der Umsetzung von APCIP auf strategischer und operativer Ebene beauftragt sind und andererseits die strategischen Unternehmen, Wissenschaft und Forschung die diesen Prozess begleiten.

Maßnahmen:

18) Einrichtung und Betrieb CIWIN-AT

- Die **Stärkung des Informationsaustausches** und des **laufenden Dialogs mit und zwischen den strategischen Unternehmen** ist eines der wesentlichsten Ziele von APCIP. Zu diesem Zweck wurden von BKA und BM.I gemeinsam das Portal **CIWIN-AT** auf der **EU Informationsplattform CIWIN**[12] eingerichtet.

[12] Critical Infrastructure Warning and Information Network.

- BKA und BM.I entscheiden über den Zugang von staatlichen Stellen und von strategischen Unternehmen zum Portal CIWIN-AT.

19) PPP-Veranstaltungen

- Die strategischen Unternehmen und andere Stakeholder werden in Informationsveranstaltungen, Workshops, Seminaren usw. über neue Entwicklungen informiert. Bei der Organisation solcher Veranstaltungen sollen auch Synergien mit anderen Bereichen wie z.B. **SKKM** und **Cyber Sicherheit** entwickelt werden.

20) Kooperationsvereinbarungen mit den Sicherheitsbehörden

- Zwischen den Sicherheitsbehörden und den strategischen Unternehmen können **Kooperationsvereinbarungen** abgeschlossen werden. Diese Vereinbarungen sind die Grundlage einer engen operativen Zusammenarbeit einschließlich des Austauschs von Informationen. Weiters können die Aufgaben der Betreiber strategischer Unternehmen sowie die diesbezügliche Unterstützung durch staatliche Stellen festgehalten werden.

21) Gemeinsame Definition von Schutzstandards

- Aufbauend auf den Ergebnissen der branchenspezifischen Risikoanalysen sind von den staatlichen Stellen und den strategischen Unternehmen gemeinsame generische **Maßnahmen zur Reduzierung der identifizierten Risiken** zu entwickeln und in Form von gemeinsam definierten Schutzstandards festzuhalten. Bei der Definition der Standards sollen bestehende Normen Berücksichtigung finden und es ist darauf zu achten, dass die Verhältnismäßigkeit bei der Umsetzung sichergestellt ist.

- Die bestehenden und noch zu definierenden **Schutzstandards von strategischen Unternehmen** sind von den staatlichen Stellen als Grundlage für ihre Beratungstätigkeit zu nutzen.

- Für die Zertifizierung der freiwilligen Umsetzung der oben genannten Schutzstandards sollen **Konformitätsbewertungsstellen** im Sinne des Akkreditierungsgesetzes 2012 benannt werden.

22) Übungen

- In regelmäßigen **Übungen** soll das Zusammenspiel zwischen staatlichen Stellen, wie Sicherheitsbehörden, dem ÖBH sowie Blaulichtorganisationen und strategischen Unternehmen erprobt werden.

- BKA und BM.I werden ein **Konzept zur Evaluierung** von Übungen erstellen, in dem Kriterien und Methoden zur Bewertung einer Übung festgeschrieben werden. Die Ergebnisse von Übungen werden vom Beirat APCIP evaluiert.

23) Ausbildung von Beratern und Dienstleistern in der Sicherheitswirtschaft

- Das Arbeitsprogramm der Bundesregierung 2013 - 2018 sieht vor, dass **Qualitäts- und Ausbildungsstandards** für private Sicherheitsdienstleister festgelegt werden. In enger Zusammenarbeit von Beirat APCIP und den beruflichen Interessenvertretungen soll überlegt werden, ob solche Standards nicht nur für private Sicherheitsdienstleister, sondern auch für Berater im Risikomanagement, Business Continuity Management und Sicherheitsmanagement entwickelt werden, um eine verstärkte Kooperation von Staat und Wirtschaft zu fördern.

24) Bevorzugte Versorgung

- Durch den Beirat wird geprüft, ob für ausgewählte strategische Unternehmen, je nach Anlass, Bedarf und entsprechend den technischen Möglichkeiten, eine **bevorzugte Versorgung** (z.B. mit elektrischer Energie oder Erdgas) **zur Sicherstellung der Daseinsvorsorge** vorgesehen werden kann.

Handlungsfeld 5 – Forschung

Ziele:

Zum Schutz kritischer Infrastruktur sind organisatorische und technische Maßnahmen notwendig. Diese sollen auf aktuellen Forschungs- und Entwicklungsergebnissen basieren. Für das österreichische Sicherheitsforschungsprogramm KIRAS[13] ist der Schutz kritischer Infrastrukturen ein zentrales Forschungsthema und soll helfen, APCIP auf dem letzten Stand der Forschung zu halten.

[13] Nationales Sicherheitsforschungsprogramm KIRAS

Die sich auf europäischer Ebene bietende Möglichkeit, analog zu KIRAS das European Security Research Programme[14] (ESRP) zur Forschung zum Schutz kritischer Infrastruktur gemeinsam mit gleichgesinnten EU-Mitgliedstaaten und assoziierten Staaten zu betreiben, soll genutzt werden. Dies soll helfen die komplementäre und kompatible Entwicklung von APCIP und EPCIP im Rahmen des Handlungsfelds 6 zu unterstützen.

Akteure:

Bedarfsträger aus dem staatlichen Bereich, der Wirtschaft und der Wissenschaft sind die Träger der nationalen wie europäischen Sicherheitsforschung. Nur durch enges Zusammenspiel dieser Akteure ist eine innovative Weiterentwicklung der Sicherheitstechnologien möglich.

Maßnahmen:

25) Forschungsprojekte

- Die Optimierung der Sicherheit und der Schutz vernetzter Systeme (Infrastruktur) ist ein zentraler Schwerpunkt von KIRAS und ESRP. Die **Projekte der Sicherheitsforschung sollen verstärkt zur Umsetzung des Masterplans** auf nationaler Ebene sowie zur Stärkung der internationalen Zusammenarbeit **beitragen**.

Handlungsfeld 6 – Internationale Zusammenarbeit

Ziele:

Auf Grund des transnationalen Charakters vieler kritischer Infrastrukturen ist eine internationale Vernetzung von zentraler Bedeutung. Dies gilt insbesondere für die EU, da APCIP und EPCIP komplementär und kompatibel weiter zu entwickeln sind. Mit den Nachbarstaaten ist durch Austausch von Erfahrungen und Best Practices eine Grundlage für zukünftige operative Kooperationen zu schaffen.

Akteure:

Die Europäische Kommission ist ein wichtiger Partner bei der Weiterentwicklung von EPCIP. Mit gleichgesinnten EU-Mitgliedstaaten ist die Zusammenarbeit zu vertiefen. Mit

[14] Societal Challenge 7, Secure Societies, des 8. EU-Forschungsrahmenprogramms Horizont 2020.

den Nachbarstaaten gibt es zwei Kooperationskreise. Einerseits mit Deutschland und der Schweiz im Rahmen der D-A-CH-Zusammenarbeit, anderseits mit den Staaten des Forum Salzburg[15].

Maßnahmen:

26) Mitwirkung an der Umsetzung und Weiterentwicklung des EPCIP

- Österreich beteiligt sich aktiv an der **Umsetzung und Weiterentwicklung von EPCIP**. Dazu ist die enge Zusammenarbeit mit der Europäischen Kommission und gleichgesinnten Staaten zu suchen. Angebote wie das CIWIN oder des Fonds Innere Sicherheit (ISF) sind zu nutzen.

27) Regionale Kooperationsformate

- Im Rahmen der **D-A-CH Kooperation** sollen regelmäßig gemeinsame Veranstaltungen organisiert werden. Schrittweise sollten die Themen auch auf Bereiche wie SKKM und Cyber Sicherheit ausgedehnt werden.

- Österreich wird den Schutz kritischer Infrastrukturen als eines der Themen des **Forum Salzburg** etablieren. In gemeinsamen Workshops sollen die nationalen Erfahrungen ausgetauscht und konkrete Kooperationsmöglichkeiten identifiziert werden. Auf der Ebene der Europäischen Union soll das Forum Salzburg nach Möglichkeit gemeinsame Positionen zur Umsetzung und Weiterentwicklung von EPCIP vertreten.

28) Bilaterale Kooperationen

- Aufbauend auf den Arbeiten im Rahmen der EU und den regionalen Formaten, sind mit **Nachbarstaaten operative Kooperationen aufzubauen**. Die im Jahr 2011 mit Deutschland, der Tschechischen Republik und der Slowakei abgeschlossenen bilateralen Vereinbarungen sollen vertieft werden. Dazu sollen auf der Grundlage bestehender Abkommen z.B. zur polizeilichen Zusammenarbeit spezielle Vereinbarungen zur Zusammenarbeit im Bereich des Schutzes kritischer Infrastrukturen getroffen werden.

[15] Das Forum Salzburg ist eine Kooperation zwischen Österreich, Bulgarien, Kroatien, Polen, Rumänien, der Slowakei, Slowenien, der Tschechische Republik und Ungarn im Bereich der inneren Sicherheit.

Handlungsfeld 7 – Umsetzung und Evaluierung

Ziele:

Um die kohärente Umsetzung von APCIP sicher zu stellen, ist eine vorausschauende Planung der Aktivitäten und ein laufendes Monitoring der Umsetzung und der dabei erzielten Wirkungen notwendig.

Akteure:

BKA und BM.I planen im Auftrag der Bundesregierung die Umsetzung und steuern und bewerten diese. Bei der Bewertung der erzielten Erfolge werden sie vom Beirat APCIP unterstützt.

Maßnahmen:

29) Jährliche Arbeitsprogramme

- Durch BKA und BM.I werden **jährliche APCIP-Arbeitsprogramme** erstellt, die auch die Grundlage für das Monitoring der Umsetzung darstellen.

30) Monitoring der Umsetzung

- **BKA und BM.I berichten regelmäßig dem Beirat APCIP** über die Fortschritte bei der Umsetzung des Österreichischen Programms.

31) Regelmäßige Berichte an die Bundesregierung

- Alle zwei Jahre legen BKA und BM.I der Bundesregierung einen **Bericht über die Umsetzung des Masterplans** vor. Dabei werden auch Vorschläge für konkrete Maßnahmen sowie zur allfälligen Weiterentwicklung des Masterplans unterbreitet. Der Bericht soll als Paket mit weiteren Berichten zur Umsetzung der ÖSS vorgelegt werden.

Anlage A Abkürzungsverzeichnis

ACI	Österreichische kritische Infrastruktur (Austrian Critical Infrastructure)
APCIP	Österreichisches Programm zum Schutz kritischer Infrastruktur (Austrian Program for Critical Infrastructure Protection)
BCM	Business Continuity Management
BM.I	Bundesministerium für Inneres
BKA	Bundeskanzleramt
B-VG	Bundes-Verfassungsgesetz
CIP	Critical Infrastructure Protection
CIWIN	Critical Infrastructure Warning and Information Network
CIWIN-AT	Österreichisches Portal im CIWIN
D-A-CH	Deutschland, Österreich, Schweiz
ECI	Europäische kritische Infrastruktur (European Critical Infrastructure)
EG	Europäische Gemeinschaften
EPCIP	Europäisches Programm zum Schutz kritischer Infrastruktur (European Program for Critical Infrastructure Protection)
EU	Europäische Union
IKT	Informations- und Kommunikationstechnologie
KI	Kritische Infrastruktur
NRA	Nationale Risikoanalyse
ÖBH	Österreichisches Bundesheer
ÖSS	Österreichische Sicherheitsstrategie
ÖSCS	Österreichische Strategie für Cyber Sicherheit
OK	Organisierte Kriminalität
SKI	Schutz kritischer Infrastruktur
SKKM	Staatliches Krisen- und Katastrophenschutzmanagement
UNISDR	United Nations International Strategy for Disaster Reduction

Anlage B Handlungsfelder und Maßnahmen in der Übersicht

HF 1 Governance	HF 2 Aufgaben Staat	HF 3 Aufgaben Betreiber	HF 4 Public Private Partnership SKI	HF 5 Forschung
1. Strategische Steuerung und Weiterentwicklung 2. Abstimmung mit anderen staatlichen Stellen 3. Ordnungspolitischer Rahmen 4. Information der Bevölkerung, Zusammenarbeit mit den Medien 5. Handbuch APCIP	6. Ausweisung ACI 7. Staatliche Risikoanalysen 8. Leitfaden 9. Kontakt- und Meldestelle KI 10. Beratung und Information strategischer Unternehmen 11. Lagebilder 12. Frühwarnsystem 13. Objektschutz	14. Einrichtung einer umfassenden Sicherheitsarchitektur 15. Implementierung von Sicherheitsstandards 16. Meldung von Vorfällen 17. Nominierung von Points of Contact für die staatlichen Stellen	18. Einrichtung und Betrieb CIWIN-AT 19. PPP-Veranstaltungen 20. Kooperationsvereinbarungen mit den Sicherheitsbehörden 21. Gemeinsame Definition von Schutzstandards 22. Übungen 23. Ausbildung von Beratern und Dienstleistern in der Sicherheitswirtschaft 24. Bevorzugte Versorgung	25. Forschungsprojekte **HF 6 Intern. Zusammenarbeit** 26. Mitgestaltung an der Umsetzung und Weiterentwicklung des EPCIP 27. Regionale Kooperationsformate 28. Bilaterale Kooperationen **HF 7 Umsetzung** 29. Jährliche Arbeitsprogramme 30. Monitoring der Umsetzung 31. Regelmäßige Berichte an Bundesregierung