DIGITALES ÖSTERREICH

IKT-Sicherheit

Nationale IKT-Sicherheitsstrategie Österreich

Wien, 2012

Impressum:

Medieninhaber, Verleger und Herausgeber:
Bundeskanzleramt, Digitales Österreich,
Ballhausplatz 2, 1014 Wien
www.digitales.oesterreich.gv.at

AutorInnen: Expertinnen und Experten aus Wirtschaft, Wissenschaft und öffentlicher Verwaltung

Gesamtumsetzung: IKT Strategie des Bundes

Lektorat und Layout: Bundespressedienst, Abteilung VII/5

Covergestaltung und grafische Unterstützung (Druckversion): BKA | ARGE Grafik

Fotonachweis (Druckversion): photos.com (Cover)

Druck (Druckversion): BM.I Digitalprintcenter

Barrierefreie Version: Bundespressedienst, Abteilung VII/5

Wien, 2012

Rückmeldungen:
Ihre Überlegungen zu vorliegender Publikation übermitteln Sie bitte an ikt@bka.gv.at.

Inhaltsverzeichnis

Einleitung

IKT-Sicherheit ist ein gemeinsames Ziel und die in Frequenz und Umfang zunehmenden Herausforderungen machen ein koordiniertes Vorgehen unumgänglich. Die Dynamik der Herausforderungen bedeutet allerdings für konventionelle Strategien eine besondere Stresssituation, die eine längerfristige und globalere Sichtweise zur Stabilisierung benötigt.

Die IKT-Sicherheitsstrategie muss daher nicht nur die Einordnung in die Europäische Situation als wichtigen Orientierungspunkt definieren, sondern auch zum Ziel haben, die Stimme Österreichs im Konzert der Mitgliedsstaaten im Bereich IKT-Sicherheit zu stärken. Damit ist ein substantielles Engagement in Europa für eine nachhaltige Entwicklung unabdingbar.

Im KMU-Bereich und im Privatbereich liegt die „Sicherheitsarmutsgrenze“ aufgrund allgemeiner Prioritäten niedrig. Als Land mit einem besonders großen Anteil an kleinen und mittleren Unternehmen (KMU) ist daher spezieller Fokus auf die Bedürfnisse dieser Bereiche zu legen.

Kernziele einer IKT-Sicherheitsstrategie sind die kritischen Informationsinfrastrukturen und deren Schutz. Ausgehend davon sind Maßnahmen zur Festigung und Handlungsschemata umzusetzen, die die Kalkulierbarkeit der Risiken sicherstellen.

Reaktive Strategien wie Cyber Security/Cyber Defense stellen wichtige und integrale Elemente dar. Doch können diese nur wirksam verfolgt werden, wenn sie durch proaktive Strategieelemente großflächig ergänzt werden, die meist einen deutlich höheren Kosten/Wirkungsfaktor aufweisen.

Dies stellt einen besonderen Auftrag dar für die schulischen und außerschulischen Bildungsformen bis hin zu den Vorbereitungsphasen für den Wiedereintritt ins Arbeitsleben aber auch für die Medien – insbesondere Rundfunk und Fernsehen. Dieser Auftrag muss über die derzeit vorhandenen Vorfalls-Meldungen hinausgehen, da hier die Potentiale noch nicht einmal ansatzweise ausgeschöpft sind. In gleicher Weise sind Interessensvertretungen (z. B. Kammern) aufgefordert, bestehende Aktivitäten branchenübergreifend zu bündeln und zu intensivieren.

Zur Sicherstellung kalkulierbarer Risiken in allen Bereichen ist die Zusammenarbeit von Wirtschaft und Sicherheitsforschung massiv zu erhöhen. Dabei sind über die Grenzen hinweg sichtbare Leuchttürme kompetenter Umsetzung (z. B. integrale Sicherheit im österreichischen E-Government) auch in weiteren Bereichen aufzubauen, um damit die Nachhaltigkeit für die österreichische Wirtschaft zu sichern. Eine koordinierte Kooperation mit Bildung und Forschung muss der Dynamik Rechnung tragen, über Technologiebeobachtung aktuelle Entwicklungen rechtzeitig erkennen und die Widerstandsfähigkeit verbessern.

Um das IKT-Risikobewusstsein deutlich über den Anlassfall hinaus zu stärken, wird die Verwaltung IKT-Sicherheit im eigenen Bereich ernst nehmen und kompetent umsetzen müssen. Der gute Ansatz aus dem IKT-Konsolidierungsgesetz weist auf Handlungsbedarf auch in anderen Bereichen hin.

Ausgehend von CIIP-Aktionsplänen, die ein gemeinsames Vorgehen festlegen und durch Übungen zum umfassenden und selbstverständlichen Handlungsschema werden lassen, müssen auf der Basis von internationaler Zusammenarbeit Schutzprofile für Technologien, die

in kritischen Infrastrukturen eingesetzt werden, (z. B. unter Mitwirkung von ENISA/CEN/ETSI ...) entstehen und ein gemeinsames Verständnis für Prüfung/Zertifizierung und Monitoring erzeugen.

Mit einem prozessorientierten Ansatz wurde nunmehr die Basis geschaffen. Darauf aufbauend kann nun die Gesamtstrategie formuliert werden, die Stakeholder identifiziert und ein kontinuierliches Engagement und Zusammenarbeiten dieser Stakeholder zur Erreichung der Ziele institutionalisiert.

Prof. DI Dr. Reinhard Posch,
Chief Information Officer des Bundes

Zusammenfassung

Die Entwicklung der modernen Informations- und Kommunikationstechnologien (IKT) – und allen voran das Internet – haben das gesellschaftliche und wirtschaftliche Leben in einem unvergleichbaren Ausmaß verändert. In Österreich nutzen mittlerweile rund drei Viertel der Bevölkerung regelmäßig das Internet, jeder Zweite bereits täglich. Die Wirtschaft ist im Hinblick auf den elektronischen Geschäftsverkehr und auf die Effizienz ihrer internen Geschäftsprozesse von der IKT abhängig. Für die öffentliche Verwaltung ist die IKT eine unverzichtbare Grundlage geworden wenn es darum geht, ihre Dienstleistungen über den traditionellen Weg hinaus einer breiten Öffentlichkeit zugänglich zu machen.

Das Wohl des Staates hängt heute in erheblichem Maß von der Verfügbarkeit und dem Funktionieren des Cyber-Raums ab. Während Internet-Nutzung, E-Commerce, E-Business und E-Government wesentliche Wachstumsraten verzeichnen und der Bereich der IT-Kriminalität (insbesondere Hacking- und Phishing-Delikte) massiv ansteigt, hat sich das Niveau der Internet- und Computerkenntnisse kaum verändert. Dies hat zu einem massiven Missverhältnis zwischen der tatsächlichen IKT-Nutzung, der zunehmenden IT-Kriminalität, dem notwendigen IT-Wissen und dem Risikobewusstsein geführt.

Attacken aus dem Cyber-Raum sind eine unmittelbare Gefahr für unsere Sicherheit und für das Funktionieren von Staat, Wirtschaft und Gesellschaft. Sie können unser tägliches Leben schwerwiegend beeinträchtigen. Es gehört zu den obersten Prioritäten für Österreich, mit allen zur Verfügung stehenden Mitteln national und international an der Absicherung des Cyber-Raums zu arbeiten. Ein erster Schritt dazu ist es, eine Strategie für die Sicherheit des Cyber-Raums zu definieren.

> Die IKT-Sicherheitsstrategie ist ein proaktives Konzept zum Schutz des Cyber-Raums und der Menschen im virtuellen Raum unter Berücksichtigung ihrer Grund- und Freiheitsrechte. Sie wird Sicherheit und Widerstandskraft der österreichischen Infrastrukturen und Leistungen im Cyber-Raum verbessern, vor allem aber wird sie Bewusstsein und Vertrauen für die österreichische Gesellschaft schaffen.

Mit der Strategie werden Aspekte der Entstehung von IKT-Sicherheitswissen und IKT-Sicherheitsbewusstsein bis zu proaktiven und reaktiven Aktivitäten für Cybervorfälle behandelt. Das Spektrum reicht von Bildung, Forschung, Sensibilisierung, Judikatur, von technischen und organisatorischen Belangen österreichischer Unternehmen bis zur Absicherung strategisch bedeutender Einrichtungen Österreichs.

IKT-Sicherheit wird als zentrale gemeinsame Herausforderung verstanden. Von der Strategie des Vorgehens wurde ein Bottom-up-Ansatz gewählt mit einem breiten, alle relevanten Akteure integrierenden Ansatz. Die strategischen Zielsetzungen und Maßnahmen zur Umsetzung der österreichischen Ziele präsentieren sich damit aus der Perspektive von fünf Kernbereichen:

- **Stakeholder und Strukturen**
- **Kritische Infrastrukturen**

- **Risikomanagement und Lagebild**
- **Bildung und Forschung**
- **Awareness**

Ein nachfolgender Aktionsplan wird zur Umsetzung der österreichischen Ziele sowohl die bereichsspezifischen als auch die bereichsübergreifenden Maßnahmen schärfen und im Kontext von Zeit und Verantwortung implementieren.

Übersicht

Stakeholder und Strukturen

- Optimierung der Cyber-Landschaft in Österreich
  - Öffentliche Cyber-Partnerschaft (Cyber Security-Steuerungsgruppe, Cyber-Krisenmanagement, Cyber Security-Plattform)
  - Cyber-Lagezentrum
- Vernetzung der Stakeholder und Strukturen
- Ausbau des rechtlichen Rahmens für Cyber Security in Österreich
- Förderung der internationalen Kooperationen

Kritische Infrastrukturen

- Ausbau von Cyber-Krisenmanagement
- Ausbau von Risikomanagement und Informationssicherheit
- Informationsaustausch von öffentlichen und privaten Akteuren

Risikomanagement und Lagebild

- Identifizierung von Kernunternehmen in den Sektoren
- Umfassendes Risiko- und Sicherheitsmanagement über Sektoren hinweg
- Sicherstellung von Mindeststandards und Lenkung der Risiko Akzeptanz in Kernunternehmen
- Etablierung Krisen- und Notfallmanagement in IKT-nahen und -fremden Sektoren
- Lagebeurteilung und -management

Bildung und Forschung

- Frühzeitige schulische Ausbildung in IKT, IKT-Sicherheit und Medienkompetenz
- Verpflichtende IKT-Ausbildung aller Studierenden der Pädagogik
- Verstärkte Ausbildung von IKT-SicherheitsspezialistInnen im tertiären Sektor
- IKT-Sicherheit als wichtiger Bestandteil in der Erwachsenenbildung/Weiterbildung
- IKT-Sicherheitsforschung als Basis für nationale Kompetenz
- Vermehrte Einbindung von IKT-Sicherheitsthemen in angewandte IKT-Forschung
- Aktive Themenführerschaft bei internationalen Forschungsprogrammen

Awareness

- Stärkung der IKT-Sicherheitskultur in Österreich
- Positive Positionierung der IKT-Sicherheit
- Abgestimmte und koordinierte Vorgehensweise
- Wirksamkeit und Nachhaltigkeit der Awareness-Maßnahmen

Bereichsübergreifende Themen: Rechtlicher Rahmen, Internationale Kooperation, Öffentliche Cyber-Partnerschaft, Cyber Competence, Standardisierung und Zertifizierung, einheitliche Terminologie und gemeinsame Sprache, eine Informations- und Kommunikationsplattform für alle Handlungsfelder und Zielgruppen / Cyber Security Plattform).

1 Stakeholder und Strukturen

1.1 Ausgangslage

Cyber-Sicherheit ist in seiner spezifischen Ausprägung in einem Land sehr eng verknüpft mit seinen vorhandenen Stakeholdern und Strukturen. Der Begriff umfasst Organisationen, Einrichtungen oder Personen, die ein erhebliches Interesse an dem Thema Cyber-Sicherheit haben oder in maßgeblicher Weise davon betroffen sind.

Eine Betrachtung von 200 Stakeholder und Strukturen und eine detaillierte Analyse der 80 derzeit wichtigsten in Österreich gibt Auskunft über die aktuelle Qualität von Cyber Security im Lande.

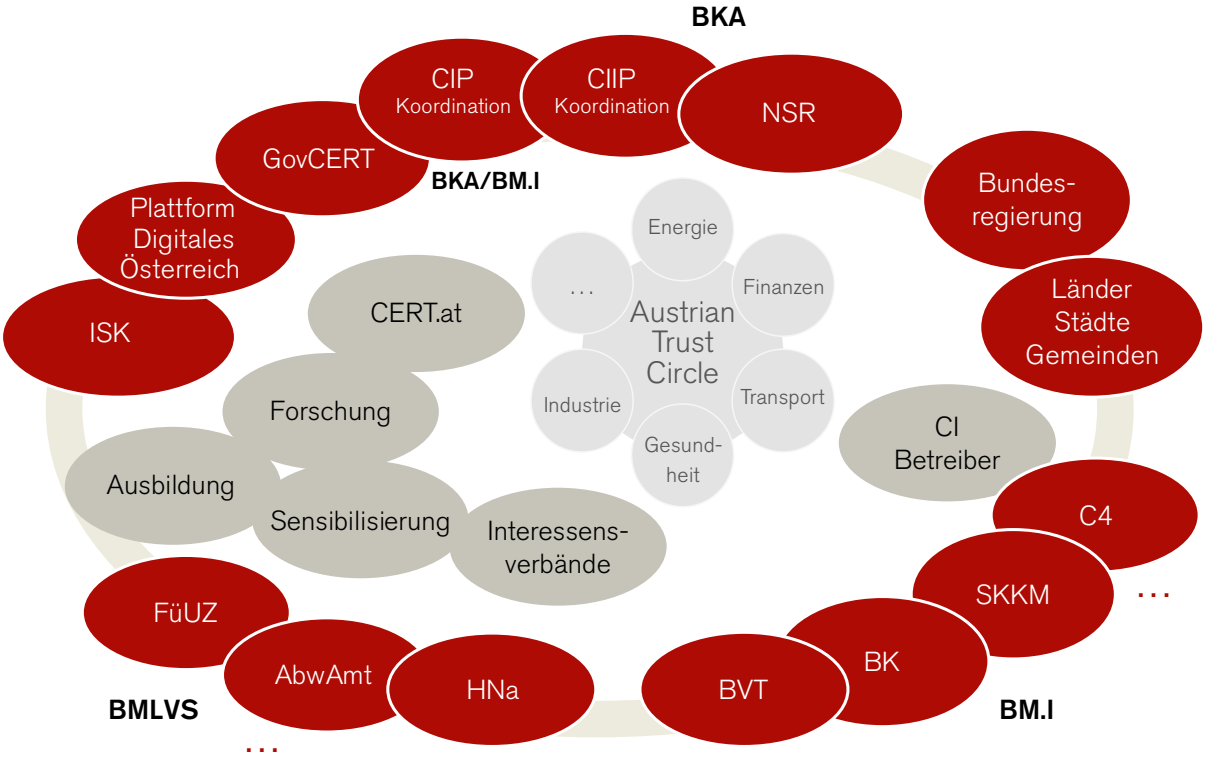
Aufteilung nach Bereichszuordnung: Der Schwerpunkt des Wirkens von Cyber Security in Österreich liegt im öffentlichen Bereich; hier vor allem im Bundesbereich und in den öffentlich finanzierten Einrichtungen. Die öffentliche Verwaltung hat bezüglich Cyber Security in mehreren Ressorts spezialisierte Einrichtungen für unterschiedliche Handlungsfelder und Zielgruppen. Die Einrichtungen sind für ihre Anwendungsbereiche optimiert und leisten einen erheblichen Beitrag zur Cyber Security in Österreich.

Länder, Städte und Gemeinden agieren in kleinerem Rahmen. Übergreifende Strukturen sind nur wenige vorhanden. Die Privatwirtschaft hat im eigenen Unternehmensbereich meist gute Cyber-Strukturen. Je größer der Betrieb ist, desto größer sind auch die Möglichkeiten vorzubeugen und zu schützen. Cyber Security Interessensvertretungen der privaten Wirtschaft sind auf breiter Ebene erst im Entstehen. Dem Bürger/der Bürgerin stehen nur wenige Interessensvertretungen zur Verfügung, die ausschließlich auf sie ausgerichtet sind. Sie müssen auf die Einrichtungen der öffentlichen Verwaltung zurückgreifen.

Aufteilung nach Tätigkeitsbereichen: Die übergreifend agierenden Stakeholder und Strukturen sind in etwa gleichmäßig verteilt auf die Tätigkeitsbereiche Sensibilisierung, Forschung, Prävention, Notfall- und Krisenmanagement. Der sehr spezialisierte Bereich Aufklärung und Strafverfolgung ist ausschließlich in den dafür zuständigen Ministerien angesiedelt. Der Bereich Bildung dagegen ist nur wenig im Bereich Cyber Security tätig; es gibt kaum Akteure, die einen Schwerpunkt Cyber Security anbieten. Gerade dies ist aber enorm wichtig für einen qualitativen Auf- und Ausbau von personellen Kapazitäten – sowohl in den Betrieben als auch bei den Behörden – zum Zweck der Cyber-Sicherheit. Im Bereich Bildung liegt ein enormes Potential für die Zukunft.

Aufteilung nach Kundenorientierung: Staat und Wirtschaft werden als Klientel der österreichischen Stakeholder in etwa gleich stark betreut. Auffallend ist die geringe Anzahl (bzw. Sichtbarkeit) von BürgerInnen-Interessensvertretungen und die geringe Orientierung der Cyber Stakeholder am Staatsbürger/an der Staatsbürgerin als Kundengruppe.

Abbildung 1: Die Stakeholder in Österreich bei Cyber-Schadensfällen



Beschreibung der Abbildung 1: Zu den Stakeholdern zählen: Bundesregierung; Länder, Städte, Gemeinden; BM.I (Bundesministerium für Inneres) mit den Einrichtungen: C4 (Cyber Crime Competence Center), SKMM (Staatliches Krisen- und Katastrophenschutzmanagement), BK (Bundeskriminalamt), BVT (Bundesamt für Verfassungsschutz und Terrorismusbekämpfung), BMLVS (Bundesministerium für Landesverteidigung und Sport) mit den Einrichtungen: HNa (Heeresnachrichtendienst), AbwAmt (Abwehramt), FüUZ (Führungsunterstützungszentrum), BKA (Bundeskanzleramt) mit den Einrichtungen: ISK – Informationssicherheitskommission), Plattform Digitales Österreich, GovCERT, CIP (Critical Infrastructure Protection) Koordination, CIIP (Critical Information-Infrastructure Protection) Koordination, NSR (Nationaler Sicherheitsrat). Weiteres die Bereiche: CERT.at, Forschung, Ausbildung, Sensibilisierung, Interessensverbände, CI Betreiber und die Mitglieder des Austrian Trust Circle (Energie, Finanzen, Transport, Gesundheit, Industrie etc.).

Im Bereich Cyberspace gibt es viele österreichische Strukturen und Stakeholder, die sehr verteilt – jeder für sich – an einer Cyber-Sicherheit arbeiten. Mehrere übergreifend wirkende, ausschließlich auf Cyber Security spezialisierte Organisationen spielen bereits eine wichtige Rolle in Österreich, wie etwa die etablierten CERTs (Computer Emergency Response Team).

Die Prozesse, mit deren Hilfe Cyber-Vorfälle beherrscht werden können, sind allerdings vor allem lokal implementiert. Übergreifende Cyber Security-Abläufe sind derzeit nicht formal abgestimmt oder festgeschrieben. Im Gegensatz zur institutionalisierten und prozessgesteuerten traditionellen Schadensfallbehandlung funktioniert heute eine Behandlung von Cyber-Schadensfällen in Österreich vor allem durch ein persönliches Netzwerk von Kontakten.

Augenfällig ist, dass zwei wesentliche Elemente in den österreichischen Strukturen entweder fehlen oder in einem nur unzureichenden Zustand vorhanden sind:

- Ein zentrales österreichisches Lagezentrum, dessen Leistung heute zum Teil durch die existierenden CERTs abgedeckt wird.
- Jener Bereich der öffentlichen Verwaltung, der mit Cyber Security zu tun hat. Dazu gehören die öffentlichen Stakeholder, ihre spezialisierten Einrichtungen und vor allem die Prozesse der Zusammenarbeit im Rahmen eines umfassenden Cyber Security-Konzepts. Es fehlt heute weitgehend eine übergeordnete Struktur der Cyber Security-Behandlung.

Die Cyber Security Landschaft in Österreich hat in vielen Punkten einen guten Reifegrad entwickelt. In anderen Punkten besteht starker Nachholbedarf.

1.2 Strategische Ziele und Maßnahmen

1.2.1 Ziel 1: Optimieren der „Cyber Security Stakeholder und Strukturen"-Landschaft in Österreich

These: Auf den ersten Blick ist die aktuelle Cyber Security-Landschaft in Österreich engmaschig und umfassend. Betrachtet man die einzelnen Bereiche genauer, so entdeckt man sehr gut und weniger gut funktionierende Strukturen. So gut es ist, erstere zu wissen, so bedenklich sind letztere für unser Land. Nur ein dichtes Netz von Cyber Security Stakeholder und Strukturen gewährleistet einen qualitativ hochwertigen und umfassenden Umgang mit Cyber Security in Österreich.

Strategische Zielsetzung: Ein dichtes Netz an Cyber Security Stakeholder und Strukturen in Österreich muss alle Bereiche, Tätigkeitsfelder und Zielgruppen von Cyber Security berücksichtigen und den kurzen Innovationszyklen der IKT Rechnung tragen. Dazu werden die Stärken der aktuellen Cyber Security-Landschaft in Österreich auf einem qualitativ hohen Niveau gefestigt, die Schwächen nachhaltig beseitigt und die Strukturen auf die notwendige Flexibilität hin optimiert.

Maßnahmen

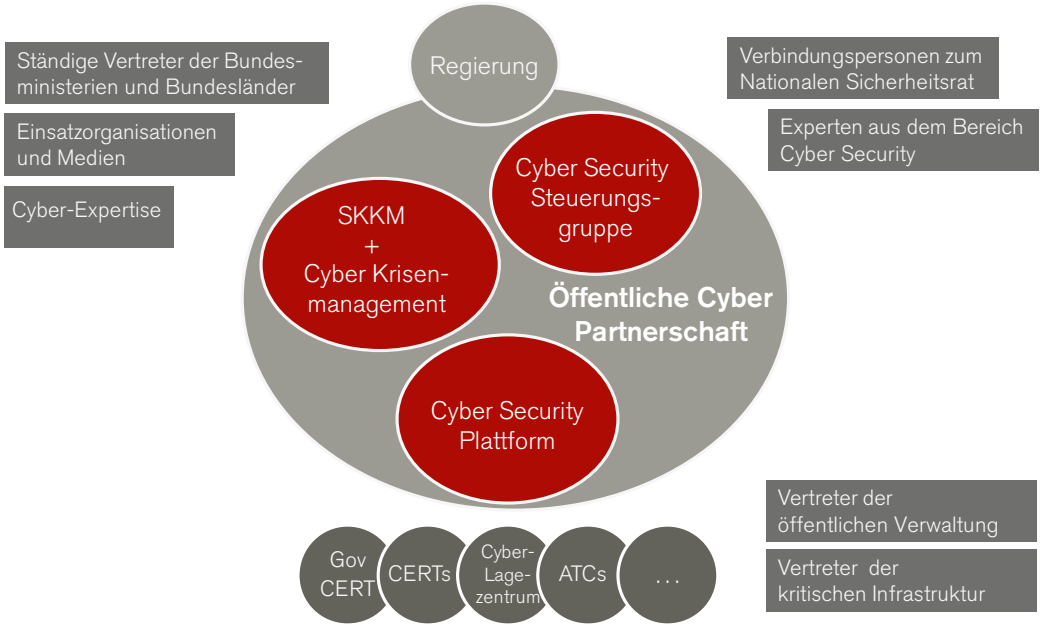
- **Einrichten einer öffentlichen Cyber-Partnerschaft:** Keine einzelne Instanz kann heute alle Aspekte von Cyber Security abdecken. Deshalb ist eine Struktur notwendig, die österreichische Aktivitäten bezüglich Cyber Security bündelt, Kooperationen fördert, Doppelgleisigkeit vermeidet, Synergien nutzt und Initiativen ermöglicht. Aufgrund der nationalen Wichtigkeit des Themas muss der Staat mit seinen Einrichtungen die übergeordnete Koordination wahrnehmen. Die Cyber-Partnerschaft umfasst:
  - **ein öffentliches Cyber-Krisenmanagement**
  - **eine Cyber Security-Steuerungsgruppe**
  - **eine Informationsdrehscheibe für Cyber Security**
- **Einrichten eines Cyber-Lagezentrums:** Um einen Überblick über die aktuelle Cyber-Situation zu erlangen, ist ein permanentes Sammeln, Bündeln und Auswerten von verfügbaren Informationen betreffend Cyber Security notwendig. Diese Funktion nehmen in Österreich zu einem großen Teil verschiedene Einrichtungen wahr, insbesondere die CERTs. Ein zentrales Cyber-Lagezentrum gibt es bislang in Österreich nicht.
- **Strukturen schaffen für Standards, Zertifizierungen, Qualitäts-Assessments:** Eine dauerhafte Verfügbarkeit verlässlicher IKT-Systeme und -Komponenten kann sichergestellt werden, in dem – vor allem in sicherheitskritischen Bereichen – Komponenten eingesetzt werden, die sich einer Zertifizierung unterzogen haben (Stichwort Supply Chain-Sicherheit). Österreich plant die Einrichtung einer Zertifizierungsstelle für Cyber Security Produkte und für Cyber Security Assessoren. Damit wird eine zentrale Instanz zur Koordinierung der Herausgabe von Qualitätsstandards im Bereich Cyber Security für Österreich und von Mindestanforderungen für das Durchführen von Überprüfungen von Cyber-Sicherheitsqualitätsstandards geschaffen. *(Zur Standardisierung siehe auch in Kapitel 1 und 4.)*

Die bedeutenden strukturellen Maßnahmen in Österreich werden in der Folge näher beschrieben.

Öffentliche Cyber-Partnerschaft

Die Cyber-Partnerschaft muss im öffentlichen Bereich eine **krisen-koordinierende**, eine **strategisch-politische** und eine **beratend-operative Ebene** abdecken. Mit der Funktion eines Chief Cyber Security Officer in Österreich, der in enger Vernetzung mit dem Chief Information Officer des Bundes agiert, wird eine zentrale erste Ansprechstelle für Cyber Security-Angelegenheiten des Staates geschaffen.

Abbildung 2 Öffentliche Cyber-Partnerschaft / mit bestehenden Strukturen



Beschreibung der Abbildung 2: In der Mitte ein Kreis für die neue Struktur Cyber-Partnerschaft der Bundesregierung bestehend aus:

- dem öffentlichen Cyber-Krisenmanagement und das SKMM (Staatliches Krisen- und Katastrophenschutzmanagement),
- der Cyber Security Steuerungsgruppe und
- der Cyber Security Plattform.

Umliegend bestehende Strukturen:

- in Nähe der Cyber Security Steuerungsgruppe: Verbindungspersonen zum Nationalen Sicherheitsrat, Experten aus dem Bereich Cyber Security
- in Nähe der der Cyber Security Plattform: Vertreter der öffentlichen Verwaltung, Vertreter der kritischen Infrastruktur; weiters: GovCERT, CERTs, (einzurichtendes) Cyber-Lagezentrum, Mitglieder des Austrian Trust Circle (ATCs) etc.
- in Nähe des Cyber-Krisenmanagements: ständige Vertreter der Bundesministerien und Bundesländer, Einsatzorganisationen und Medien, Cyber-Expertise

Öffentliches Cyber-Krisenmanagement (krisen-koordinierende Ebene)

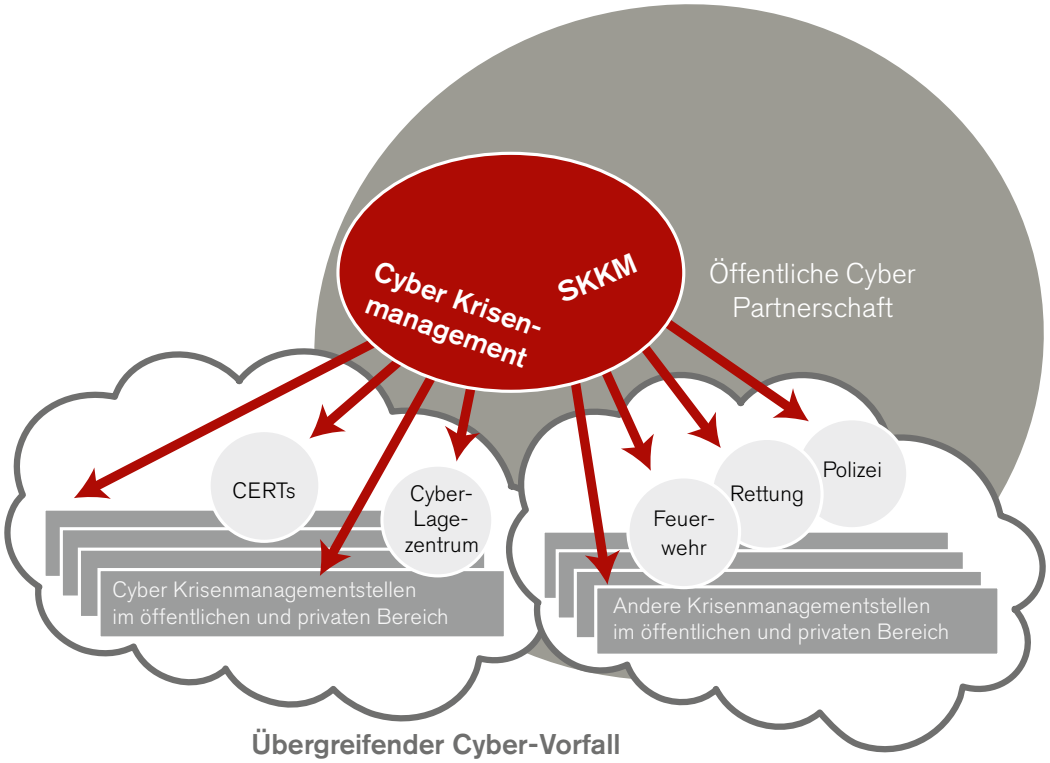
Ein für alle Cyber-Einsatzfälle geeignetes Cyber Security-Krisenmanagement wird für Österreich festgelegt. Bestehende Cyber-Strukturen (z. B. CERTs) sind dabei zu berücksichtigen.

Das Cyber-Krisenmanagement setzt sich zusammen aus VertreterInnen des Staates und der Kritischen Infrastrukturen. Für die Zusammenarbeit von öffentlichen und privaten Krisenstellen sind Regeln und Prozesse zu vereinbaren.

Bei **Cyber-Vorfällen mit lokalem Schadenspotential** übernehmen Einrichtungen der zuständigen Ressorts oder private Einrichtungen die Krisensteuerung in Kooperation mit den CERTs. Diese Einrichtungen sind strikt auf die speziellen Erfordernisse der Cyber Security-Bedrohungen auszurichten. Um für den Notfall gerüstet zu sein, ist wiederholtes Trainieren der gemeinsamen Vorgehensweise von Krisenmanagementstellen und CERTs notwendig.

Die Krisensteuerung im Fall von **übergreifenden Cyber-Vorfällen mit großer Gefahr für die Versorgungssicherheit** von Österreich baut auf den existierenden Krisen- und Katastrophenschutzstrukturen (SKKM) auf. In ergänzender Zusammenarbeit mit dem SKKM soll für die Behandlung der speziellen Cyber-Thematik eine Cyber Security-Expertise als nationales Cyber-Krisenmanagement in Österreich korreliert werden. In Österreich agieren die Cyber Security-Experten als **nationales Cyber-Krisenmanagement**.

Abbildung 3 Cyber-Krisenmanagement und Staatliches Krisen- und Katastrophenschutzmanagement mit Akteuren im Fall eines übergreifenden Cyber-Vorfalls



Beschreibung der Abbildung 3: Das Cyber-Krisenmanagement koordiniert ihre Arbeit mit Cyber-Krisenmanagementstellen im öffentlichen und privaten Bereich – CERTs, Cyber-Lagezentrum. Das Krisen- und Katastrophenschutzmanagement (SKKM) koordiniert deren Arbeit mit anderen Krisenmanagementstellen im öffentlichen und privaten Bereich – Feuerwehr, Rettung und Polizei.

Cyber-Krisenmanagement bedarf einer eindeutigen Verantwortungsstruktur für den Cyber-Krisenfall. Krisenmanagementpläne legen fest, wie Krisenmanagementeinrichtungen bei der Behandlung der wichtigsten Cyber-Bedrohungen vorgehen. Die Krisenmanagementpläne sind

für alle bekannten Vorfälle (Cyber Incidents) gemeinsam auszuarbeiten und müssen laufend an die aktuelle Bedrohungssituation angepasst werden. Regelmäßige Spezial-Übungen (Cyber Exercises) testen das Cyber-Krisenmanagement. Die **Cyber Security-Steuerungsgruppe** verabschiedet die Krisenmanagementpläne.

Cyber Security-Steuerungsgruppe (strategisch-politische Ebene)

Die strategisch-politische Ebene ist die höchste Evaluierungs- und Beratungsebene des Staates im Bereich Cyber Security. Auf dieser Ebene der Cyber-Partnerschaft wird die Steuerungsgruppe als zentrales Beratungsgremium der Bundesregierung in Angelegenheiten der Cyber-Sicherheit Österreichs eingerichtet.

Dieses Gremium befasst sich vorrangig mit ganzheitlichen Ansätzen, Strategien, Krisenmanagement, staatlichen Kooperationen und der internationalen Beteiligung Österreichs an der Thematik Cyber Security. Sie beschließt die umfassende Cyber Security-Strategie Österreichs, überwacht deren Umsetzung und greift – wenn notwendig – korrigierend ein.

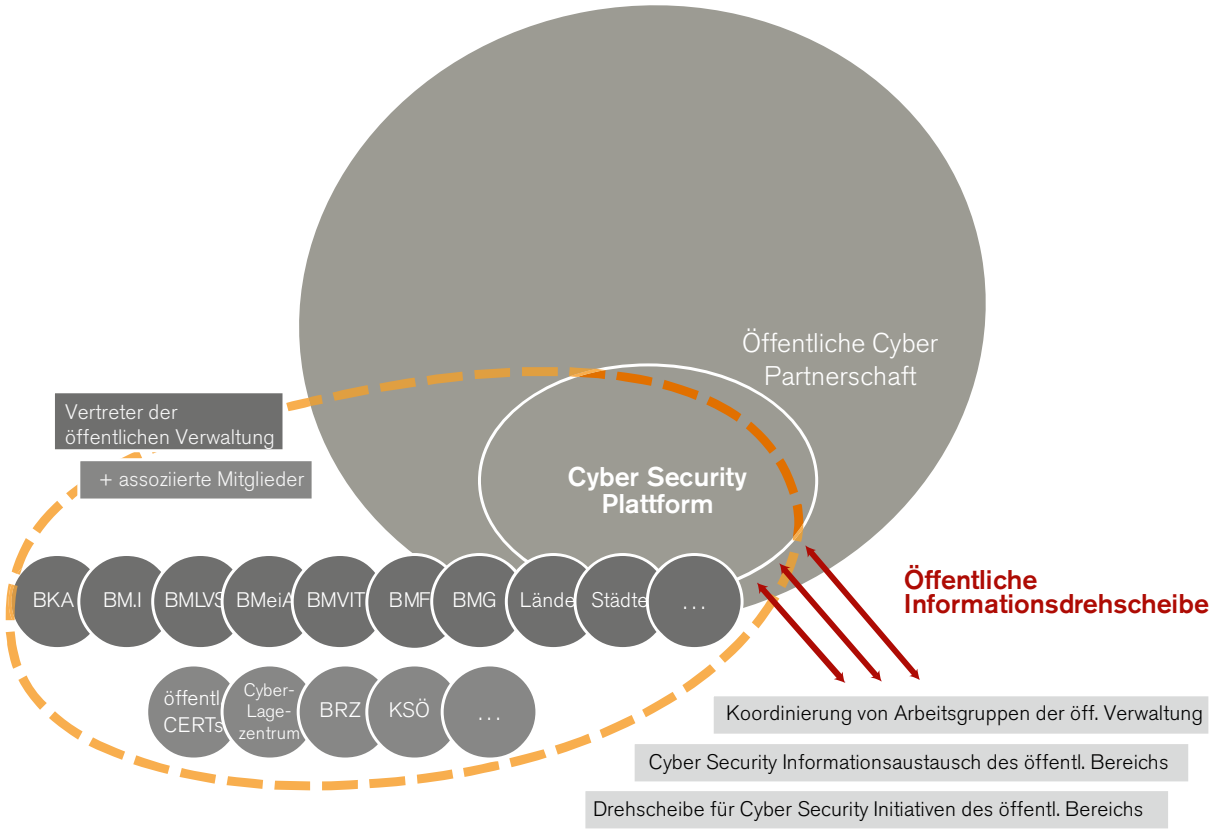
Organisatorisch soll auf das Gremium der Verbindungsleute zum Nationalen Sicherheitsrat aufgesetzt werden. Top Cyber Security-Experten der öffentlichen Verwaltung und der Chief Cyber Security Officer werden Teil dieser Steuerungsgruppe sein. Eine ständige Beteiligung des privaten Sektors in dieser höchsten Cyber-Entscheidungsgruppe in Österreich wird dringend empfohlen.

Informationsdrehscheibe für Cyber Security (beratend-operative Ebene)

Mit der Cyber Security-Plattform wird ein ständiger Informationsaustausch der öffentlichen Cyber-Strukturen in Österreich und der öffentlichen Verwaltung mit den Vertretern der kritischen Infrastruktur, der Wirtschaft, Cyber-Experten und privaten Krisenstellen institutionalisiert (Public Private Partnership für Cyber Security).

Alle wichtigen öffentlichen Stakeholder nehmen in gleichberechtigter Weise teil. Dabei ist auf einen ganzheitlichen Ansatz zu achten, in dem alle Belange der österreichischen Gesellschaft bezüglich Cyber Security berücksichtigt werden. Als Basis für alle Aktivitäten der Cyber Security-Plattform dienen die Grundwerte unserer Gesellschaft im Umgang mit Cyber-Aktivitäten. Diese Grundwerte sollen in einer Präambel festgeschrieben sein, die von der Politik verabschiedet wird.

Abbildung 4 Informationsaustausch der öffentlichen Bereiche



Beschreibung der Abbildung 4: Informationsaustausch über die Cyber Security Plattform mit den Vertretern der öffentlichen Verwaltung (Bundeskanzleramt, Bundesministerium für Inneres, Bundesministerium für Landesverteidigung und Sport, Bundesministerium für europäische und internationale Angelegenheiten, Bundesministerium für Verkehr, Innovation und Technologie, Bundesministerium für Finanzen, Bundesministerium für Gesundheit, Länder, Städte etc.) und assoziierten Mitgliedern (öffentliche CERTs, Cyber-Lagezentrum, Bundesrechenzentrum, Kuratorium Sicheres Österreich etc.). Die öffentliche Informationsdrehscheibe koordiniert Arbeitsgruppen der öffentlichen Verwaltung, tauscht Cyber Security Informationen des öffentlichen Bereichs aus und ist Drehscheibe für Cyber Security Initiativen des öffentlichen Bereichs.

Im Rahmen der Cyber Security Plattform ermöglichen regelmäßige Meetings einen Informationsaustausch aller öffentlichen Bereiche und zwischen öffentlichen und privaten Bereichen. Vertreter der Bereiche Bildung, Forschung und Entwicklung sind verstärkt in den Austausch einzubinden. Arbeitsgruppen und Initiativen behandeln aktuelle Herausforderungen der Cyber Security in Österreich.

Eine Web-Plattform fungiert für alle Zielgruppen in Österreich als die zentrale Anlaufstelle für Themen der IKT-Sicherheit und als grundlegende Informations- und Kommunikationsbasis aller Awareness-Maßnahmen. *(siehe Kapitel 5)*

Als ergänzende Einrichtung der Cyber Security Plattform wird ein **Cyber Competence Center** eingerichtet.

Möglichkeiten eines vertraulichen Informationsaustausches abseits der öffentlich zugänglichen Cyber Security Plattform schaffen weitere Möglichkeiten der Zusammenarbeit der Bereiche Cyber Security, Cyber Crime, Cyber Defense und Cyber Diplomacy.

Cyber-Lagezentrum

Das geplante Cyber-Lagezentrum ist verantwortlich für die Bewältigung von größeren Cyber-Vorfällen innerhalb der Bundesverwaltung sowie auch für besondere Krisen- und Katastrophenlagen auf nationaler Ebene. Assistenzleistungen des Österreichischen Bundesheers (ÖBH) ergänzen das Cyber-Lagezentrum.

Im „Normalbetrieb“ erstellt das Cyber-Lagezentrum öffentliche und nicht-öffentliche Analysen zur Netzsicherheit in Österreich und ist verantwortlich für Simulationen und die Berichterstattung. Im Besonderen ist das Cyber-Lagezentrum für die Frühwarnung zuständig. Kapazitäten für forensische Tätigkeiten werden geschaffen, um Unternehmen auf deren Anfrage hin zu unterstützen. Dazu ist ein 24-stündiges Monitoring, 7 Tage die Woche („24/7“) notwendig, damit die Klientel, insbesondere die Kritischen Infrastrukturen (die einen ähnlichen 24/7-Betrieb ausüben) die notwendige Auskunft zeitgerecht erhalten können.

Um sicherheitsrelevante Informationen in Echtzeit zu erfassen, werden die Netze der öffentlichen Verwaltung und der kritischen Infrastrukturen mit einer Sensorik ausgestattet. Für Netze ohne Sensorik wird ein verpflichtendes Melden von noch zu definierenden Cyber-Anomalien vorgeschrieben.

Dazu ist vorab das rechtliche Umfeld zu analysieren und anzupassen. Verantwortungen und Befugnisse der Cyber-Lagezentren, Meldepflichten und die Weitergabe von Daten aus dem Cyber-Lagezentrum sind gesetzlich zu regeln.

Bei der Organisation des Lagezentrums sollen die in ähnlicher Rolle agierenden Stakeholder eingebunden werden. Strategische und organisatorische Entscheidungen sollen durch einen Lagerat mit den wichtigsten öffentlichen Cyber Security Stakeholdern getroffen werden. Eine Einbindung privater Stakeholder wird dringend empfohlen.

Die Adressaten der Cyber-Lagezentrum-Leistungen sind vor allem Einrichtungen der öffentlichen Verwaltung und Unternehmen der kritischen Infrastrukturen.

1.2.2 Ziel 2: Vernetzung der Stakeholder und Strukturen

These: Cyber Security ist dort wichtig, wo IKT-Systeme in Verbindung mit dem Internet stehen. Das ist in unserer Informationsgesellschaft, wo Menschen vernetzte digitale Geräte direkt oder indirekt nutzen, praktisch überall. Diese digitale Omnipräsenz forciert leider auch kriminelle Machenschaften. Um bei erfolgtem Schaden schnell zu reagieren oder bei überstandenen Schaden die Lehren daraus zur Verfügung zu stellen ist es unverzichtbar, alle Stakeholder und Cyberstrukturen miteinander zu vernetzen. Nur durch ein enges Netz an Kontakten der Stakeholder untereinander wird es möglich, dass Österreich eine robuste Cyber Security-Struktur aufweist.

Strategische Zielsetzung: Es sollen Anreize, Förderungsmaßnahmen und gesetzliche Grundlagen geschaffen werden, um ein enges Vernetzen österreichischer Cyber Security Stakeholder und Strukturen zu fördern. Ziel dabei ist es, den Prozess der Cyber-Vernetzung so zu automatisieren, dass über informationsaustauschende Regelkreise eine umfassende, selbstlernende Cyber Security-Kultur in Österreich entsteht.

Maßnahmen

- **Förderung von bestehender und neuer Vernetzung zwischen Stakeholdern und Strukturen in Österreich:** Stakeholder verstärkt zusammenbringen: innerhalb von Cyber-Tätigkeitsfeldern durch gezielte Fachveranstaltungen; übergreifend in Tätigkeitsfeldern (Sensibilisierung, Bildung, Forschung und Entwicklung, Sicherheitsprävention, Notfalls und Krisenmanagement, Aufklärung und Strafverfolgung) und übergreifend in Bereichen (Öffentliche Verwaltung, Wirtschaft, Universitäten, Interessensvertretungen, Staatsbürger). Der Austausch von Cyber Security Stakeholdern mit Vertretern aus Bereichen, die nur indirekte oder keine Cyber Security-Verantwortung haben, soll verstärkt werden. Bereits existierende Veranstaltungen, Kongresse und Initiativen zum Thema Cyber Security sind weiter zu unterstützen und zu fördern.

- **Untersuchen, welche Beeinflussungs-Regelkreise in Österreich vorhanden sind, um Cyber Security-Kompetenz zu fördern:** Cyber Security-Strategien müssen sich an konstanten wie unvorhersehbaren Veränderungen der Technologien, Anwendungen und Märkte anpassen. Sie müssen ihre Cyber Security-Kompetenz stets aktuell halten. Dabei ist ein Informationsaustausch auf nationaler und internationaler Ebene hilfreich, aber auch das Einrichten von einander mit neuem Wissen und Erkenntnissen versorgenden Regelkreisen. Für letzteres sind Untersuchungen anzustellen und die dafür notwendigen Prozesse (Feedback- und Lernschleifen) einzurichten.

1.2.3 Ziel 3: Ausbau des rechtlichen Rahmens für Cyber Security

These: Um dem Menschen Sicherheit und Vertrauen im Umgang mit vernetzten digitalen Technologien zu geben ist es wichtig, den Cyberspace zu reglementieren. Dabei sind alle

Ausprägungen von digitaler Informations- und Kommunikationstechnik (IKT) in Österreich zu berücksichtigen. In Österreich hat der Gesetzgeber früh auf Besonderheiten der IKT reagiert und in unterschiedlichen Gesetzen Regelungen festgeschrieben. Durch die IKT-Durchdringung der gesamten Welt sind allerdings in letzter Zeit für die Gesetzgebung neue nationale und globale Herausforderungen entstanden. Um mit den schnellen technischen und gesellschaftlichen Prozessen im Internet Schritt zu halten, müssen angepasste Prozesse geschaffen werden, um **„aktuelle" Rechtssicherheit** zu etablieren.

Strategische Zielsetzung: Der rechtliche Rahmen in Österreich für Cyber Security ist entsprechend den Zielen und Erfordernissen der vorliegenden Cyber Security-Strategie anzupassen oder zu entwickeln. Ziel ist eine mit den Veränderungen des Cyberspace schritthaltende Legislative, um Rechtssicherheit im österreichischen Cyberspace zu schaffen. Die österreichische Position wird aktiv in internationalen Arbeitsgruppen der Legislative vertreten.

Maßnahmen

- **Analyse des Status Quo der heutigen Rechtsgrundlagen hinsichtlich Cyber Security und Ergänzung der weißen Flecken in der österreichischen Gesetzgebung:** Es werden alle Bereiche des österreichischen Cyberspace analysiert, die in Österreich durch Verordnungen darzustellen sind. Welche Bereiche werden durch welche Gesetze bereits abgedeckt? Welche Verordnungen zu gleichen Themenbereichen ergänzen einander bzw. existieren parallel? Welche Bereiche werden aktuell in Österreich nicht oder nur unzureichend durch die Legislative adressiert? Widersprüchliche Verordnungen in unterschiedlichen Gesetzen werden beseitigt, Gesetze zu relevanten noch nicht vorhandenen Themen erarbeitet. Dabei soll auch die besondere Verantwortung, die Betreiber von kritischen Infrastrukturen haben, entsprechend berücksichtigt werden.

- **Einrichten einer flexiblen Struktur der Legislative hinsichtlich Cyber Security:** Möglichkeiten einer neuen flexiblen Struktur der Legislative hinsichtlich Cyber Security analysieren. Es soll eine am Puls der Entwicklung des Cyberspace agierende Rechtsstruktur für Cyber Security eingerichtet und gefördert werden.

- **Teilnahme an der Erarbeitung eines internationalen Rechtsrahmens für Cyber Security:** Aktiv in Partnerschaft mit anderen Nationen an der Diskussion und Erarbeitung von internationalen Verordnungen/Empfehlungen von Cyber Security mitarbeiten, um österreichische Grundwerte in internationalen Regelwerken zu verankern.

1.2.4 Ziel 4: Förderung der internationalen Kooperationen

These: Das Internet ist ein globales Phänomen, genauso wie die Bedrohungen aus dem Internet. Der internationale Aspekt der Cyber-Bedrohung nimmt in erschreckendem Ausmaß zu. Um eine nationale digitale Gesellschaft robust zu machen, muss die Strategie dafür strikt

und konsequent international ausgerichtet sein. Die notwendige globale Vernetzung ist ein zentraler Faktor für eine Cyber Security-Strategie. Internationale Organisationen arbeiten heute intensiv daran, Grundrechte unserer Gesellschaft wie Recht auf Privatsphäre oder der Schutz von personenbezogenen Daten auch online wirksam durchzusetzen. Nur durch ein umfassendes aktives Mitmachen an internationalen Prozessen kann das Cyber Security-Wissen aufgebaut werden, um Österreich Vertrauen und Sicherheit im Umgang mit digital vernetzten Strukturen zu geben.

Strategische Zielsetzung: Die Teilnahme des öffentlichen Bereichs an internationalen Organisationen zum Thema Cyber Security wird institutionalisiert und obligatorisch sein. Zusätzlich ist die Teilnahme von Interessenvertretungen des privaten Sektors an internationalen Vereinigungen durch Anreizsysteme der öffentlichen Hand zu fördern. Internationale Ergebnisse und Empfehlungen werden in nationalen Prozessen berücksichtigt.

Maßnahmen

- **Aktive Teilnahme der öffentlichen Verwaltung an internationalen Cyber Security Entwicklungen (OSZE, OSCD, EU, NATO, …)**
- **Förderung der Teilnahme des privaten Bereichs an internationalen Cyber Security Veranstaltungen und Entwicklungen**
- **Aufbau von bi- und multilateralen Netzwerken zur Abwehr von Internetbedrohungen:** Cyber Security-Partnerschaften und Netzwerke (z. B. CERT Netzwerke), intensive Vernetzung im Bereich DACH (Deutschland, Österreich, Schweiz) und bilaterale Cyber Security-Beziehungen mit allen Nachbarstaaten pflegen. Intensiver an internationalen Organisationen zum Aufbau von Cyber Security-Netzwerken teilnehmen.
- **Gemeinsame Erarbeitung von internationalen Strategien zur Sicherung von staatenübergreifenden Grundrechten im Umgang mit digitaler Information und Kommunikation:** Österreichs Grundwerte im Umgang mit digitaler Information und Kommunikation und mit digitalen Netzwerken (wie freier, uneingeschränkter Internet-Zugang und freie Meinungsäußerung im Internet) werden in internationalen Foren vertreten und implementiert.
- **Aktive Beteiligung an länderübergreifenden Cyber Exercises:** Österreich wird die wichtigsten internationalen Cyber-Übungen aktiv mitplanen und daran teilnehmen. Die Erkenntnisse aus den internationalen Übungen fließen direkt in die nationalen Übungen ein.

2 Kritische Infrastruktur

2.1 Ausgangslange

Der Begriff „Kritische Infrastruktur“ oder „Strategische Infrastruktur“ bezeichnet jenen Teil aller staatlichen und privaten Infrastrukturen, die eine wesentliche Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen haben. Ihre Störung oder Zerstörung hat schwerwiegende Auswirkungen auf die Gesundheit, Sicherheit oder das wirtschaftliche und soziale Wohl der Bevölkerung oder die effektive Funktionsweise von staatlichen Einrichtungen.

Die meisten Kritischen Infrastrukturen sind heute in zunehmendem Ausmaß von spezialisierten IT-Systemen abhängig, welche einen möglichst reibungslosen, verlässlichen und durchgehenden Betrieb garantieren sollen. Der IKT-Sektor selbst (und seine IT- und TK-Netze mit ihren Komponenten und Betreibern) und auch die IKT-basierten Infrastrukturen aller anderen Sektoren ermöglichen nicht nur die sektorale Produktion, sondern halten auch den intersektoralen Informationsfluss am Laufen. Verallgemeinert spricht man in diesem Zusammenhang auch von **Kritischen Informationsinfrastrukturen (Critical Information Infrastructure – CII)**. Schutz Kritischer Informationsinfrastruktur (CIIP) ist somit nicht eine Aufgabe des IKT-Sektors allein, sondern rückte in den letzten Jahren vermehrt auch ins Bewusstsein aller anderen Wirtschaftssektoren.

Eine Besonderheit der Kritischen Informationsinfrastrukturen stellt deren Anfälligkeit für verschiedenartige Cyberangriffe dar. Dies zeigt sich insofern, als die CII selbst aktiv als „Angriffskanäle“ gegen andere Kritische Infrastrukturen missbraucht werden könnten. Im Unterschied zu einem Ausfall der Strom- oder Wasserversorgung können Cyberangriffe einen bleibenden, „nachhaltigen“ Schaden verursachen. Dies kann u.a. durch die gezielte Zerstörung oder Manipulation von Maschinensteuerungsdaten erfolgen. .

In Österreich sind Cyber Security-Ziele beim Schutz der Kritischen Informationsinfrastrukturen mit dem etablierten *Austrian Programme for Critical Infrastructure Protection (APCIP)* abzustimmen. Eine übergeordnete Zielsetzung korreliert deshalb zu diesem Programm folgendermaßen:

> „Das APCIP-Programm ist um Cyber Security-Maßnahmen innerhalb und zwischen den Sektoren zu ergänzen, nationale Kapazitäten zur Unterstützung der Informationssicherheit als auch zur Bewältigung von nationalen Krisen- und Katastrophenlagen sind aufzubauen.“

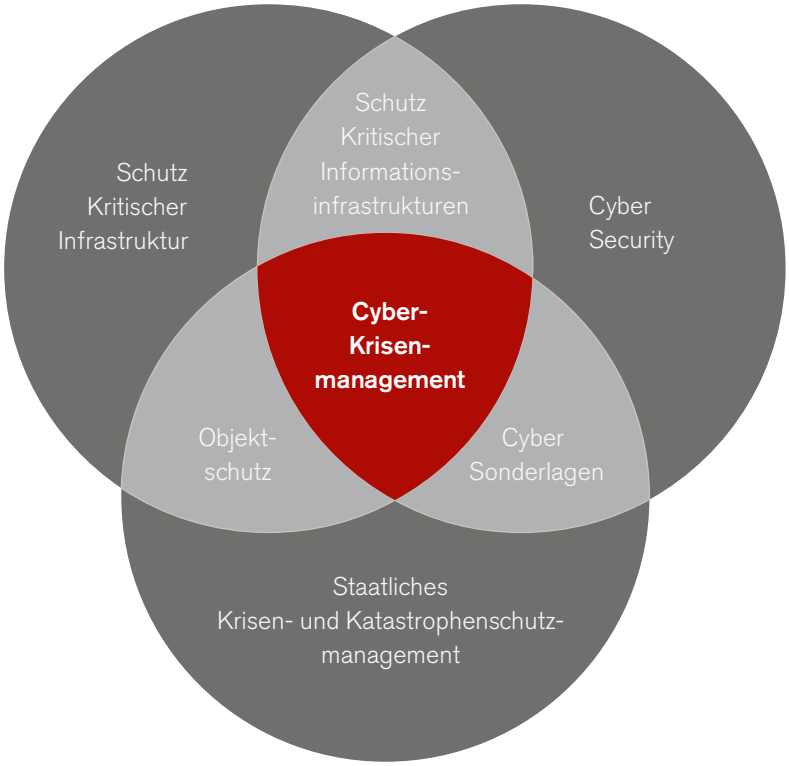
2.2 Strategische Ziele und Maßnahmen

2.2.1 Ziel 1: Cyber-Krisenmanagement

These: Cyber-Krisen und Katastrophenlagen können verheerende Folgen für Staat, Wirtschaft und das öffentliche Leben haben. Im internationalen Vergleich ist es bereits üblich, für solche Anlassfälle besondere übergeordnete Strukturen aufzubauen, die bestehende Strukturen des Krisenmanagements ergänzen.

Strategische Zielsetzung: Reaktive Mittel zu einer bundesweiten Cyber Security-relevanten Katastrophen- und Krisenbekämpfung (Cyber-Krisenmanagement) ausbauen, um Staat, Wirtschaft und das öffentliche Leben vor Schäden zu schützen. Das nationale Cyber-Krisenmanagement ist wichtiger Bestandteil der nationalen Sicherheit.

Abbildung 5 Cyber-Krisenmanagement



Beschreibung der Abbildung 5: Drei Kreise: 1. Schutz Kritischer Infrastruktur, 2. Cyber Security, 3. Staatliches Krisen- und Katastrophenschutzmanagement. In der Schnittmenge von Kreis 1 und 2: Schutz Kritischer Informationsinfrastrukturen. In der Schnittmenge von Kreis 2 und 3: Cyber Sonderlagen. In der Schnittmenge von Kreis 3 und 1: Objektschutz. In der Schnittmenge der drei Kreise: Cyber Krisenmanagement.

Maßnahmen

- **Aufbau einer Struktur zum nationalen Cyber-Krisenmanagement:** Ein nationales Cyber-Sicherheits-Krisenmanagement („Cyber-Krisenmanagement“) unterscheidet sich vom herkömmlichen öffentlichen Katastrophenschutz und Krisenmanagement (SKKM) zum einen durch die besonderen Bedürfnisse und Überschneidungen von Cyber-Sicherheit, zum anderen durch die konstante Zusammenarbeit mit Programmen zum Schutz Kritischer Infrastruktur. Des Weiteren unterscheidet sich das Cyber-Krisenmanagement vom traditionellen SKKM durch den dafür notwendigen Grad der innerstaatlichen sowie internationalen Vernetzung: Cyber-Krisen im Inland können nur mithilfe von staatlichen (öffentlichen) und nicht-staatlichen (privaten) Akteuren bewältigt werden und sind fast immer von internationalen Kooperationen abhängig. *(siehe auch Kapitel 1)*

- **Aufbau eines Cyber-Lagezentrums:** *siehe Kapitel 1 Stakeholder und Strukturen.*

- **Einrichten einer tragfähigen Krisenkommunikation:** Hierbei gilt es, die Kommunikation mit den Organisationen und Firmen zu verstärken, die für den Betrieb der wichtigsten Netzwerke verantwortlich sind. Im Anlassfall müssen gesicherte Kommunikationsanlagen mit öffentlichen und privaten Akteuren im Ausland aufrechterhalten werden können. Der Aufbau eines „Notfallnetzes“ (z. B. mittels DVB-T-Technologie) soll gewährleistet bleiben. Weitere Möglichkeiten von ausfallsicherer Kommunikation (z. B. UKW-Radio) sind in Betracht zu ziehen. Ebenso ist es unerlässlich, bei der Krisenkommunikation die Gesprächspartner verifizieren zu können. Vor allem die Weitergabe von Informationen erfordert eine geeignete Rechtsgrundlage.

2.2.2 Ziel 2: Risikomanagement und Informationssicherheit

These: Die Unterstützung des Selbstschutzes durch proaktive Risikominimierung auf Unternehmens- und Organisationsebene (Risikomanagement und Informationssicherheit) ist eine der effektivsten Methoden, um Cyber Security zu fördern und den alltäglichen Betrieb zu ermöglichen.

Strategische Zielsetzung: Einen möglichst weitreichenden und gestaffelten Einsatz von Methoden des Risikomanagements und der Informationssicherheit innerhalb der identifizierten Kritischen Infrastrukturen schaffen. Dienstleistungen, die von besonderem allgemeinem Interesse sind, haben erhöhten Schutzbedarf.

Maßnahmen

- **Förderung des Risikomanagements innerhalb der KI:** Der Aufbau des IKT-bezogenen Risikomanagements (allg. auch „Informationssicherheit“) gilt als eine der wichtigsten Maßnahmen, die Betreiber von KI zum Selbstschutz ergreifen können. Im Kontext nationaler Cyber-Sicherheit ist es besonders wichtig, dass alle Verantwortlichen **Informationssicherheits- bzw. IKT-bezogene Risikomanagementmaßnahmen** in ihren jeweiligen Be-

trieben einsetzen. Der Staat unterstützt sie dabei durch Informationen zur gemeinsamen Risikoanalyse, Akkreditierung von verschiedenen Risikomanagementmethoden, Angleichung von Ausbildungsmaßnahmen sowie Analysen der Technologiefolgenabschätzungen. Sanktionen und Anreize fördern den Einsatz von Risikomanagementmethoden innerhalb der Privatwirtschaft.

- **Einrichten eines Cyber Competence Centers:** Das Cyber Competence-Center als Teil der Cyber Security Plattform ist die zentrale Anlaufstelle für alle Betreiber der Kritischen Infrastruktur aber auch für Betriebe, die ein Interesse am Risikomanagement/Informationssicherheit-Management (RM/ISM) haben. Es gibt Auskunft über verschiedene RM/ISM-Ansätze und über Akkreditierungsverfahren z. B. nach dem Sicherheitshandbuch 2010 oder ISO 27000. Zusammen mit dem Cyber-Lagezentrum werden quantitative Informationen für die Cyber-sicherheitsbezogene Risikoanalyse aufgearbeitet.

- **Pflege des Informationssicherheitshandbuch als Basis für den Grundschutz:** Das 2010 neu überarbeitete und neu strukturierte „Österreichische Informationssicherheitshandbuch“ (SIHA) beschreibt und unterstützt die Vorgehensweise zur Etablierung eines umfassenden Informationssicherheits-Managementsystems in Unternehmen und der öffentlichen Verwaltung. Das SIHA 2010 ist für die Umsetzung von ISM-Maßnahmen auf Klein- und Mittelbetriebe zugeschnitten. Aufbau und Inhalt orientieren sich an internationalen Vorgaben und erleichtern damit die Umsetzung der ISO/IEC 27000 Normenreihe. Das international anerkannte Handbuch leistet einen wichtigen Beitrag zum Mindestschutz und wird laufend aktualisiert. *(siehe auch Kapitel 4 und 5)*

- **Durchführen von Technologiefolgenabschätzungen:** Im Bereich Cyber-Sicherheit ist alle zwei bis drei Jahre mit einem schwerwiegenden Technologiewandel zu rechnen. Dies erfordert, aktuelle und zukünftige technologische Trends ständig zu beobachten und deren eventuelle Wirkung auf das gesellschaftliche und wirtschaftliche Leben abzuschätzen. Die Technologiefolgenabschätzung ist im Rahmen eines Forschungsprogramms anzusprechen, das mit bestehenden Initiativen (z. B. KIRAS) verknüpft sein kann. *(siehe auch Kapitel 4)*

- **Freiwilliges Registrierungssystem:** Analog zur Freiwilligen Feuerwehr können sich IKT-Spezialisten in ein Registrierungssystem (im Cyber Competence-Center) eintragen lassen, in dem sie ihre fachliche Qualifikation, Identität und Zertifikate bzw. Qualitätsnachweise (z. B. Sicherheitsüberprüfung nach SPG) anführen. Unter Berücksichtigung rechtlicher Rahmenbedingungen erhalten Organisationen und Unternehmen im Krisenfall schnell und unbürokratisch Zugriff auf qualifiziertes Personal.

2.2.3 Ziel 3: Informationsaustausch von öffentlichen und privaten Akteuren

These: Der Informationsaustausch gilt als wichtigster Faktor nationaler Cyber-Sicherheit. Da sowohl die Vielfalt an Akteuren als auch die erhöhte Bedeutung des privaten Sektors eine ausschließlich staatliche zentrale Steuerung undurchführbar machen, ist der ständige Austausch – insbesondere von Bedrohungsinformation – notwendig, um den Selbstschutz der

verschiedenen Akteure zu unterstützen. Hierbei gilt es vor allem, den Zusammenhang mit dem *Austrian Programme for Critical Infrastructure Protection (APCIP)* zu gewährleisten.

Strategische Zielsetzung: Der Informationsaustausch erfolgt zwischen staatlichen Akteuren, zwischen nicht-staatlichen Akteuren und zwischen staatlichen und nicht-staatlichen Akteuren. Die Unterstützung von Public Private Partnership (PPP) als allgemeiner Organisationsrahmen für die Zusammenarbeit zwischen staatlichen und nicht-staatlichen Akteuren ist eine maßgebliche Zielsetzung aller Programme zum Schutz kritischer Infrastrukturen. Der Austausch von Informationen ist mit den Bedürfnissen der Geheimhaltung und dem Datenschutz abzustimmen.

Maßnahmen

- **Unterstützung von Public Private Partnership (PPP):** Die Koordinierung des Schutzes Kritischer Informationsinfrastrukturen bzw. Cyber-Sicherheit erfolgt verstärkt über „trusted" Public Private Partnerships (PPP). Beispiele bereits existierender PPPs sind u. a. CERT.at als „Community-basierte PPP" und Austrian Trust Circle (tauscht Informationen unter den privaten Stellen aus).

- **Rechtssicherheit für Meldepflicht:** Betreiber von kritischen Infrastrukturen haben eine besondere Verantwortung und diese muss bei ordnungspolitischen Maßnahmen besonders berücksichtigt werden. Einerseits werden regulativ verstärkt Anforderungen an die KI gestellt: Zum Beispiel wird empfohlen, bestenfalls alle KI-Betreiber (insbesondere aber jene, die für den Schutz der Kritischen Informationsinfrastruktur verantwortlich sind) zur Anwendung von Risikomanagement- und Informationssicherheitsmaßnahmen rechtlich zu verpflichten. Andererseits thematisiert auch die Privatwirtschaft oft selbst eine Meldepflicht bei Cyber-Angriffen. Eine „freiwillige Meldung" wäre den Betreibern aus Datenschutzgründen oft nicht möglich.

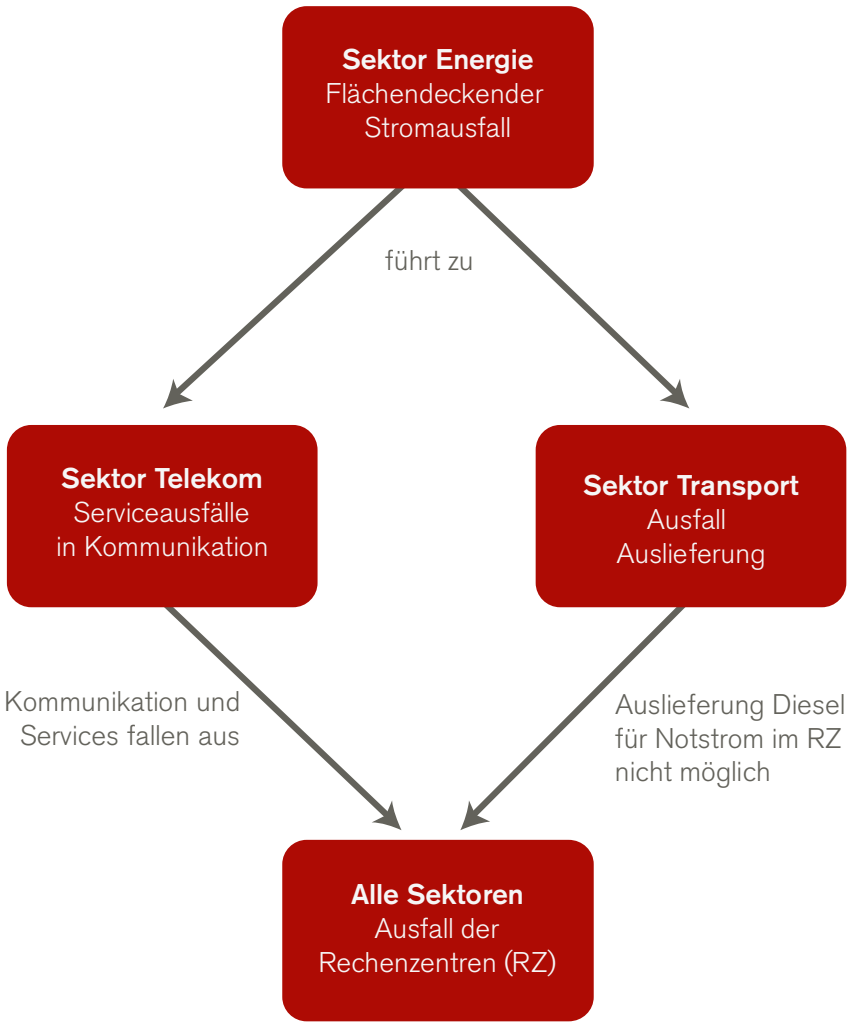
- **Human Sensor Projekt:** IKT-Systemadministratoren werden stufenweise in IKT-Sicherheit ausgebildet und darauf trainiert, Anomalien in ihren IKT Systemen zu erkennen und an IKT-Sicherheitsverantwortliche zu berichten. Die so gewonnenen Erkenntnisse gehen an das Cyber-Lagezentrum und Cyber Competence Center und werden dort weiterverarbeitet, um das Lagebild zu verfeinern.

3 Risikomanagement und Lagebild

3.1 Ausgangslage

Die digitale Gesellschaft bedingt eine große Durchdringung von IKT-Komponenten in allen Bereichen. In klassischen Sektoren wie Energieversorgung, Transport und Industrie spielt IKT heute eine wesentliche Rolle. Reine IKT-Sektoren bedienen sich einer Vernetzung weitreichender Dienstleistungen und Infrastrukturen, die über IKT-Komponenten und Prozesse gesteuert werden. Die Vernetzung der einzelnen Sektoren durch abhängige Leistungs- und Produktübergänge führt zu einer Kettenreaktion bei sicherheitsrelevanten Szenarien.

Abbildung 6: exemplarische Ausfallskette



Beschreibung der Abbildung 6: Ein flächendeckender Stromausfall im Sektor Energie führt einerseits zu Serviceausfällen in Kommunikation im Sektor Telekom (Kommunikation und Services fallen aus) und andererseits zu Ausfällen bei der Auslieferung im Sektor Transport (Auslieferung Diesel für Notstrom in Rechenzentren nicht möglich). Beides führt zum Ausfall der Rechenzentren in allen Sektoren.

Aus dieser Überlegung heraus sind in einer Risiko- und Lagebetrachtung alle Sektoren zu betrachten, besonders genau jedoch die Sektoren Informationsinfrastruktur, Telekommunikation, Energie, Gesundheit, Transport, Zahlungsverkehr und öffentliche Verwaltung. Jeder einzelne Sektor hat ein gut ausgeprägtes Risikomanagement. Die Hauptrisiken werden allerdings vorwiegend dort gesehen, wo sie außerhalb des Einflussbereiches des einzelnen Unternehmens liegen. Dies führt zu dem Schluss, dass die Vernetzung zwischen den Sektoren bzw. über Organisationseinheiten hinaus enorm groß ist und eine übergreifende Risikobetrachtung erfordert.

Die IKT-Risiken befinden sich durch die stark vernetzte Abhängigkeit der Sektoren voneinander jeweils im Kontext einer vor- bzw. nachgelagerten Risikosituation. So ist es auch zu verstehen, dass eine beträchtliche Anzahl von Risiken in einem Unternehmen alleine nicht mehr organisiert und bewältigt werden kann, sondern nur mehr im Verbund bzw. mit staatlicher Unterstützung.

Es ist von zentraler Bedeutung, dass die nicht im IKT-Bereich gelegenen Risiken und Szenarien durch aktuelle Notfall- und Krisenmanagement-Pläne abgesichert sind. Dies ist eine wesentliche Grundlage, um damit die übergreifenden Risiken und Szenarien in der Vernetzung abzufangen.

Ein weiteres Element stellt die Frage des Risikos und Sicherheitsmanagements in den einzelnen Unternehmen dar. Hier ist das Zurückgreifen auf entsprechende Best Practices und Rahmenbedingungen notwendig. In vielen Fällen wird es so weit gehen, dass entsprechende Mindeststandards für diese Kerninfrastrukturen festzulegen sind, die auch einer adäquaten staatlichen Reglementierung bedürfen.

3.2 Strategische Ziele und Maßnahmen

3.2.1 Ziel 1: Identifizierung von Kernunternehmen in den Sektoren

These: Es gibt Risiken, die ein Unternehmen alleine managen kann und es gibt Risiken, die nur im Verbund bzw. mit staatlicher Unterstützung abgedeckt werden können. Die Einschätzung, welche Restrisiken durch ein Unternehmen akzeptiert werden bzw. welche Gegenmaßnahmen als nicht wirtschaftlich sinnvoll angesehen werden, müssen vor dem Hintergrund der Auswirkungen auf andere Sektoren betrachtet werden.

Strategische Zielsetzung: Die Kernsektoren und darin enthaltene Unternehmen müssen identifiziert werden. Es sind einige wenige Kerninfrastrukturen bzw. Kernunternehmen, deren Ausfall Auswirkungen hat, die den jeweiligen Unternehmensbereich bei Weitem übersteigen. Diese sind in die Betrachtung aufzunehmen und in die Risikobewertung einzugliedern.

3.2.2 Ziel 2: Umfassendes Risiko- und Sicherheitsmanagement über Sektoren hinweg

These: Aufgrund der globalen Vernetzung können IKT-Risiken nicht isoliert betrachtet werden.

Strategische Zielsetzung: Ein umfassendes Risiko- und Sicherheitsmanagement muss sich mit allen Risiken beschäftigen und für alle Branchen und Kernunternehmen gelten. Dazu bedarf es Mindeststandards bezüglich der Organisation und der Prozesse.

Maßnahmen

- **Verdichtung des Risikokatalogs** mit ausgewählten Branchenvertretern auf Expertenebene.
- **Definition von Mindeststandards für Risiko- und Sicherheitsmanagement** unter Berücksichtigung von Branchenspezifika und Standards, sowie von Prozessen im Bereich Risiko- und Vorfalls-Management.

3.2.3 Ziel 3: Sicherstellung von Mindeststandards und Lenkung der Risikoakzeptanz in Kernunternehmen

These: Durch den stärker werdenden Wettbewerb bestimmen vermehrt betriebswirtschaftliche Faktoren, welches Risiko Kernunternehmen akzeptieren. Gerade in Kernunternehmen mit hohen Folgeabhängigkeiten kann dies Auswirkungen haben, die über das betroffene Unternehmen weit hinausgehen; dies ist in der Risikobetrachtung zwingend zu berücksichtigen. Bei wesentlichen Auswirkungen auf andere Sektoren ist daher ein Mindeststandard für Risikovorsorge notwendig.

Strategische Zielsetzung: Um erhebliche Auswirkungen durch betriebswirtschaftlich bedingtes Fehlen von Risikovorsorge zu vermeiden, wird Risikoakzeptanz für Kernunternehmen auf übergeordneter Ebene entschieden. Dabei werden Mindeststandards festgelegt und überprüft. Alternativ kann es andere Möglichkeiten geben, um einen gewünschten Lenkungscharakter zu erreichen.

Maßnahmen

- Fragen der Risikoakzeptanz in kritischen Kernunternehmen auf übergeordneter Verantwortungsebene diskutieren sowie klären, in welcher Form Mindeststandards verankert werden (als Gesetze, Richtlinien, Normen, o. ä.), welche Einrichtung das Einhalten prüft und inwieweit branchenübliche Best Practices angewendet werden können.

- Diese Thematik auch auf EU-Ebene einbringen, um die Thematik der Wettbewerbsverzerrung zu adressieren.

3.2.4 Ziel 4: Etablierung von Krisen- und Notfall-Management in den Sektoren

These: Durch die starke Vernetzung müssen IKT-Risiken umfassend betrachtet und eingeschätzt werden, wie sie bewältigt werden können. Notfall- und Krisenpläne sind in den IKT-nahen und fremden Bereichen notwendig.

Strategische Zielsetzung: Prozesse des staatlichen Krisen- und Notfall-Managements hinsichtlich ihrer Risiken überprüfen, die sich aus der zunehmenden Abhängigkeit zahlreicher Kernprozesse von der IKT ergeben.

Krisenorganisationen und -prozesse auf staatlicher und privater Ebene sicherstellen. Darunter fallen etwa Ansprechpartner in Unternehmen (z. B. Krisen- und BCM-Manager) und Notfall- und Kontaktlisten.

Maßnahme

- Aktualität der staatlichen Krisen- und Notfallpläne sowie deren Wartungs- und Testprozesse überprüfen. Mit dem Lagezentrum vernetzen. Krisenorganisationen und -prozesse auf staatlicher und privater Ebene überprüfen, selbige untereinander vernetzen und ggf. weitere geeignete schaffen.

3.2.5 Ziel 5: Lagebeurteilung und -management

These: Derzeit werden Sektoren bzw. Organisationseinheiten einzeln eingeschätzt und beurteilt. Ein persönliches Netzwerk führt sektorenübergreifende Risikobetrachtungen durch. Aufgrund der verketteten Strukturen muss hier eine feste Einrichtung etabliert werden.

Strategische Zielsetzung: Ein Lagezentrum einrichten, das das Zusammenarbeiten der einzelnen Sektoren optimiert. Ein dazugehöriges Meldemanagement nimmt Vorfälle auf und gibt die gewonnen Informationen an Unternehmen der kritischen Infrastruktur weiter. Das Lagezentrum darf keine „Einbahnstraße“ sein. Nur wechselseitige Kommunikation garantiert, dass Informationen rechtzeitig, umfassend und zielgerichtet bereitgestellt werden. Erfahrungen sollen in langfristige Awareness-Maßnahmen fließen.

Maßnahmen

- **Schaffung eines Cyber-Lagezentrums** mit geeigneten Möglichkeiten für Lage-Monitoring mit den dazugehörigen notwendigen Prozessen wie Meldeverpflichtung oder Informationsverpflichtung für die einzelnen Stakeholder. *(siehe Kapitel 1 Stakeholder und Strukturen)*

4 Bildung und Forschung

4.1 Ausgangslage

Bildung und Forschung stellen die Basis für eine erfolgreiche Umsetzung einer bundesweiten IKT-Sicherheitsstrategie dar. Zwei wesentliche Themen sind besonders hervorzuheben: **Ausbildung in IKT-Sicherheit und Medienkompetenz** und **nationale IKT-Sicherheitskompetenz in Lehre und Forschung.**

Der Umgang mit IKT kann heute – neben Lesen, Schreiben und Rechnen – als „4. Kulturtechnik“ bezeichnet werden. IKT und damit eng verbunden IKT-Sicherheit und Medienkompetenz müssen daher bereits in frühen Schulstufen berücksichtigt werden. Die Aufnahme von IKT-(Sicherheits)-Kompetenzen in die Ausbildung an pädagogischen Hochschulen und Universitäten sowie in Weiterbildungsangeboten ist essenziell.

Sicherheitsprobleme in IKT-Systemen entstehen oft durch mangelndes Know-how der beteiligten Entwickler. Da gerade im IKT-Bereich Wissen sehr schnell veraltet, ist ein kontinuierliches Weiterbildungs- und Qualifizierungsprogramm eine wichtige Voraussetzung für die Erhaltung und Produktivität von IKT-Mitarbeitern, aber auch für Zielgruppen im Privatbereich, Einzelunternehmen und KMUs, die nicht im Technologiebereich tätig sind. Besonderer Wert liegt auf der Ausbildung von IKT-SicherheitsspezialistInnen im tertiären Bildungsektor, wobei Österreich auf einem qualitativ hochwertigen Angebot an Studien- und Ausbildungsmöglichkeiten aufbauen kann.

Eine erfolgreiche IKT-Sicherheitsstrategie spiegelt sich in der Forschung wider. Zum einen dient Forschung als Basis für eine Ausbildung auf höchstem internationalem Qualifikationsniveau – Stichwort „forschungsgeleitete Lehre“. Zum anderen benötigt es entsprechendes Know-how im eigenen Land, um Entwicklungen für den nationalen Bedarf zu unterstützen und Entscheidungsgrundlagen für nationale Interessen aufzubereiten. Neben dem Ausbau von Sicherheitsforschungsinstituten und stärkerer Vernetzung ist die vermehrte Einbindung von IKT-Sicherheitsthemen in angewandter IKT-Forschung notwendig. Die Schaffung von Komplementaritäten zu existierenden umfassenden Sicherheitsforschungsprogrammen wie KIRAS sowie eine aktive Themenführerschaft bei EU-Forschungsprogrammen soll die Entwicklung Österreichs zu einer Wissens- und Innovationsgesellschaft unterstützen, um IKT-Sicherheit verstärkt als „Exportprodukt“ zu etablieren.

4.2 Strategische Ziele und Maßnahmen

4.2.1 Ziel 1: Frühzeitige schulische Ausbildung in IKT, IKT-Sicherheit und Medienkompetenz

These: Nur wenn in der Bevölkerung ein breites Verständnis für IKT-Sicherheit und Kompetenz im Umgang mit den neuen Medien vorhanden ist, können Angriffe auf IKT-Infrastrukturen über schlecht geschützte private Systeme sowie der Verlust der Privatsphäre des Einzelnen nachhaltig verhindert werden. Dieses Verständnis muss bereits möglichst frühzeitig in der Schule entwickelt werden.

Strategische Zielsetzung: IKT und IKT-Sicherheit verstärkt in die Lehrpläne und den Unterrichtsalltag ab Volksschulniveau aufnehmen. Mittelfristiges Ziel ist, dass die sichere Benutzung moderner Medien für jeden Bürger selbstverständlich wird – im eigenen Interesse sowie als Basis für den Schutz der nationalen Infrastrukturen.

Maßnahmen

- **Verstärkte Aufnahme von IKT, IKT-Sicherheit und Medienkompetenz in den Unterricht:** Der Umgang mit IKT, den neuen Medien und IKT-Sicherheit muss integraler Bestandteil des Unterrichts in allen Schultypen werden, ein verpflichtendes Unterrichtsfach zur Verbesserung der Medienkompetenz in allen Bereichen eingerichtet werden. Da Kinder in sehr jungen Jahren mit den neuen Medien in Kontakt kommen, muss dieses Thema bereits in den Volksschulen adäquat behandelt werden. Eine Schwerpunktbildung in einzelnen Schultypen, vergleichbar den heutigen Sport-, Musik- bzw. IKT-Hauptschulen, wird empfohlen.

- **Definition von Bildungsstandards für IKT und IKT-Sicherheit:** Ein sinnvolles und hinreichendes IKT-Kompetenzniveau quer über alle Schultypen hinweg sicherstellen.

4.2.2 Ziel 2: Verpflichtende IKT-Ausbildung aller Studierenden der Pädagogik

These: Ein kreativer, sicherer und kritischer Umgang mit IKT und den neuen Medien kann nur dann erfolgreich in den Schulen vermittelt werden, wenn Lehrende entsprechend ausgebildet sind.

Strategische Zielsetzung: IKT-(Sicherheits)-Kompetenzen in die Ausbildung an pädagogischen Hochschulen und Universitäten aufzunehmen ist wichtige Voraussetzung für die Vermittlung dieser Kompetenzen an den Schulen. Entsprechende Weiterbildungsangebote für bereits ausgebildete Lehrkräfte stellen sicher, dass die LehrerInnenausbildung rasch, wirksam und nachhaltig umgesetzt wird.

Maßnahmen

- **Verpflichtende IKT-Ausbildung aller Studierenden der Pädagogik (alle Pädagogischen Hochschulen und Universitäten):** Alle Studierenden der Pädagogik benötigen eine Ausbildung in IKT, die ihnen den sicheren Umgang mit den neuen Technologien und Medien in ihrem Fachbereich ermöglicht und sie fachspezifische Applikationen und Services (z. B. Mathematica, GeoGebra, Google Earth, location based applications, …) im Unterrichtsalltag sicher einsetzen lässt. Besonderer Wert ist auf die Ausbildung von Lehrenden im IKT-Bereich (Lehramtsstudium IKT) zu legen, da diese das Thema IKT generell und damit auch den sicheren Umgang mit IKT den Schülern professionell vermitteln müssen. Ein Ausbau von entsprechenden Lehramtsstudien und innerhalb dieser Studien des Themas IKT-Sicherheit ist essentiell.

- **Weiterbildung der Lehrenden:** Über Angebote der Pädagogischen Hochschulen und der Universitäten zur kontinuierlichen Weiterbildung ist die nachhaltige IKT-Kompetenz der Lehrenden sicherzustellen.

- **Ausbau des Angebotes für Erwachsene, insbesondere Eltern:** Im schulischen Bereich sollen spezielle Angebote für Eltern entwickelt werden, die es diesen ermöglichen, ihren Kindern einerseits kompetente Ansprechpartner zu sein, andererseits auch den Umgang mit den neuen Medien und die Medienkompetenz der Kinder kritisch zu hinterfragen.

4.2.3 Ziel 3: Verstärkte Ausbildung von IKT-SicherheitsspezialistInnen im tertiären Sektor

These: Ein sensibler Bereich wie die nationale Sicherheit benötigt fachspezifisches Know-how und Kompetenzen im eigenen Land. Um das sicherzustellen, muss eine zielgerichtete Ausbildung auf Hochschulniveau erfolgen.

Strategische Zielsetzung: Die bereits vorhandenen Studien- und Ausbildungsangebote – sowohl in Form von Spezialisierungen von generellen IKT-Studiengängen als auch in Form spezifischer IKT-Sicherheitsstudiengänge – werden proaktiv weiterentwickelt. Die Vernetzung und Kooperation der einzelnen Bildungsorganisationen wird gefördert (z. B. gemeinsame Lehrveranstaltungen oder übergreifende Programme).

Maßnahmen

- **Nationales Know-how im IKT-Security-Bereich:** Verstärkung und Etablierung von nationalen interdisziplinären Kompetenzzentren im IKT-Sicherheitsbereich sowie breite Ausbildung nach aktuellem Stand („state-of-the-art“) der Wissenschaft.
- **Förderung der Vernetzung der einzelnen Bildungsorganisationen:** Eine aktive Zusammenarbeit aller Bildungsinstitutionen in Österreich ist essenziell. Lehrpläne sind abzustimmen, um Synergien zu erzielen und Ressourcen sparsam einsetzen zu können. Die Schnittstelle zwischen der Identifikation von Gefährdungen und dem Begegnen systemspezifischer Risiken ist dabei besonders zu beachten.
- **Berücksichtigung von Security-Aspekten in der IKT-Ausbildung:** „Security by design“ als leitendes Querschnittsthema – in allen Bereichen der IKT-Ausbildung soll Security als Querschnittsthema vorkommen.

4.2.4 Ziel 4: IKT-Sicherheit als wichtiger Bestandteil in der Erwachsenenbildung / Weiterbildung

These: Gerade im IKT-Bereich veraltet Spezialwissen sehr schnell. Ein kontinuierliches Weiterbildungs- und Qualifizierungsprogramm ist daher wichtige Voraussetzung für die Erhaltung und Produktivität der MitarbeiterInnen. IKT-AnwenderInnen, etwa in kleinen Firmen oder im Privatbereich, stellen, wenn sie schlecht gesicherte Systeme betreiben, eine potentielle Gefahr für die gesamte IKT-Infrastruktur dar (Stichwort Bot-Netze) und müssen daher entsprechend sensibilisiert und geschult werden.

Strategische Zielsetzung: Basiswissen über IKT-Sicherheit muss in allen Bevölkerungsschichten vorhanden sein. Zielgruppenspezifische Angebote sind zu entwickeln und zu vernetzen. Zu den wesentlichen Zielgruppen gehören: MitarbeiterInnen im IT- und IKT-Bereich im Sinne einer kontinuierlichen Weiterbildung, Einzelunternehmen und KMUs, die nicht im Technologiebereich tätig sind sowie der Privatbereich (etwa die Generation 65+).

Maßnahmen

- **IKT-Sicherheit in der Erwachsenenbildung:** Das bestehende, teilweise sehr gute Angebot besser vernetzen und abstimmen. Insbesondere bildungsbenachteiligte Gruppen sollen erreicht sowie Ressourcen (Räume, IKT-Ressourcen) in Schulen und lokalen Zentren für die Erwachsenenbildung genutzt werden. Betriebe und öffentliche Bibliotheken können als Lernorte fungieren. Standardisierte Ausbildungslevels wie ECDL und ECDL Security forcieren.

- **Kontinuierliche zielgruppenspezifische Weiterbildungsprogramme:** Eine kontinuierliche Weiterbildung für MitarbeiterInnen im IKT-Bereich, aber auch in anderen technologie- und innovationsstarken Bereichen erfordert u. a. die verstärkte Entwicklung zielgruppenspezifischer Angebote, eine Stärkung der Selbstlernkompetenzen (Stichwort: lebensbegleitendes Lernen) sowie die Einbindung von IKT-Sicherheit als Querschnittsthema in nicht-IKT-spezifischen Berufen. Erwachsenenbildungsorganisationen sollen stärker vernetzt und das Weiterbildungsangebot im tertiären Sektor in Kooperation mit Wirtschaft und Industrie ausgebaut werden (berufsbegleitende Studien- und Lehrgänge zur Weiterbildung, spezifische unternehmensbezogene Ausbildungsprogramme etc.).

4.2.5 Ziel 5: IKT-Sicherheitsforschung als Basis für nationale Kompetenz

These: Der sensible Bereich der IKT-Sicherheit erfordert eine ausreichende IKT-Security-Kompetenz auf „state-of-the-art"-Niveau im Land, um für nationale Interessen Entscheidungsgrundlagen aufbereiten und damit Entwicklungen durchführen zu können.

Strategische Zielsetzung: Verstärkte Etablierung von Sicherheitsforschungsinstituten sowie stärkere Vernetzung der Forschungsorganisationen.

Maßnahmen

- **Nationales Know-how in IKT-Sicherheitsforschung:** Nationale Kompetenzzentren im IKT-Sicherheitsforschungsbereich verstärken, neue etablieren, Komplementaritäten zu umfassenden Sicherheitsforschungsprogrammen wie KIRAS (mit einem Forschungssektor „Kommunikation und Information") zur Ressourcenoptimierung schaffen. Einen breiten Ansatz im Bereich der Sicherheitsforschung bzw. zur Erweiterung des nationalen thematischen Schwerpunkts „Schutz kritischer Infrastrukturen" fördern. Neue Forschungsschwerpunkte etablieren (z. B. Entwicklung von robusten Anwendungen und Systemen, Erhöhung der Netzwerkresilienz sowie der sozialen und politischen Resilienz gegenüber IKT-basierten Angriffen). „Common Terms of Reference" mit Standardisierungsinitiativen erarbeiten.

- **Förderung der Vernetzung der einzelnen Forschungsorganisationen:** Bestehende Vernetzungsinstrumente wie die Sicherheitsforschungslandkarte oder die KIRAS-

Innovationsplattformen verstärkt nutzen. Abstimmung und Erfahrungsaustausch zwischen den IKT-Sicherheitsforschungsakteuren zur Bündelung von Umsetzungsmaßnahmen für Sicherheitsforschungsergebnisse.

4.2.6 Ziel 6: Vermehrte Einbindung von IKT-Sicherheitsthemen in angewandte IKT-Forschung

These: IKT-Sicherheit ist integraler Bestandteil von IT-Produkten, Systemen und Lösungen. Daher müssen Sicherheitsaspekte integrierter Bestandteil in IKT-Forschungsvorhaben werden. Umgekehrt sollen auch vermehrt Erkenntnisse aus anderen Wissenschaftsdisziplinen in die IKT-Sicherheitsforschung einfließen – etwa aus der Biologie oder der Psychologie.

Strategische Zielsetzung: Die angewandte IKT-Forschung sowie andere Forschungsbereiche berücksichtigen vermehrt IKT-Sicherheitsthemen, sind mit anderen Wissenschaftsdisziplinen vernetzt und unterstützen die praktische Umsetzbarkeit.

Maßnahmen

- **Security Aspekte in angewandter IKT-Forschung:** In möglichst allen IKT-Forschungsprojekten prüfen, welche IKT-sicherheitsrelevanten Aspekte mitbetrachtet werden müssen, z. B. durch ein zusätzliches Evaluierungskriterium (ähnlich Gender-Aspekten, geistes-, sozial- und kulturwissenschaftlichen (GSK) Aspekten in KIRAS-Projekten oder die Security Considerations bei RFCs). Die Form der Zusammenarbeit zwischen politischen EntscheidungsträgerInnen und Forschungseinrichtungen aus dem Bereich der Technikfolgenabschätzung kann ähnlich TAB in Deutschland oder POST in England institutionalisiert werden.

- **Förderung der Interdisziplinarität im Sicherheitsforschungsbereich und der Umsetzung in der Praxis:** Erkenntnisse und Technologien aus anderen Bereichen (z. B. Biologie) werden auf die IKT-Sicherheitsforschung übertragen. Zur Entwicklung kreativer Lösungen für Sicherheitsprobleme soll eine Forschungslinie zur IKT-Sicherheit mit obligatorischer Einbindung von anderen Wissenschaftsdisziplinen etabliert werden. Schaffung einer Einrichtung, die sich mit der Auswertung und Umsetzung von vorliegenden Ergebnissen aus Sicherheitsforschungsprojekten befasst. Maßnahmen zur Verbesserung der Umsetzung von Ergebnissen aus dem Sicherheitsforschungsbereich in der Industrie bzw. in konkreten Produkten. Ein „Anreizsystem“ (Modell á la „Innovationsscheck“) soll zur Entwicklung von Ideen anregen.

4.2.7 Ziel 7: Aktive Themenführerschaft bei internationalen Forschungsprogrammen

These: Um österreichische Stärken besser zu positionieren, sollen österreichische Programmdelegierte verstärkt national wichtige Sicherheitsforschungsthemen in europäische und internationale Programme einbringen.

Strategische Zielsetzung: Österreich strebt eine aktive Themenführerschaft bei EU-Forschungsprogrammen an.

Maßnahmen

- **Einbringen von für Österreich wichtigen Themen in Forschungsprogramme:** Weitere Forcierung des Einbringens von Sicherheitsforschungsthemen in europäische und internationale Programme (SECURITY, ICT, HORIZON 2020) zur besseren Positionierung österreichischer Stärken. Rechtzeitige Einbindung der jeweiligen österreichischen Programmdelegierten zur Erhöhung des Einbringungserfolgs von Sicherheitsforschungsthemen.

4.2.8 Begleitmaßnahmen

Verstärktes Engagement in internationalen Standardisierungs- und Zertifizierungsaktivitäten: In manchen ausgewählten Standardisierungsbereichen wie der Weiterentwicklung der ISO/IEC 27001 spielt Österreich schon heute eine aktive Rolle. Darüber hinaus soll sich Österreich auch in anderen IKT-Sicherheitsbereichen stärker einbringen: in ISO/IEC JTC1 WG 27 und CEN, bei den Common Criteria, in den europäischen Standardisierungsinitiativen im Sicherheitsforschungsbereich (Mandat M/487 an CEN, CENELEC und ETSI etc.).

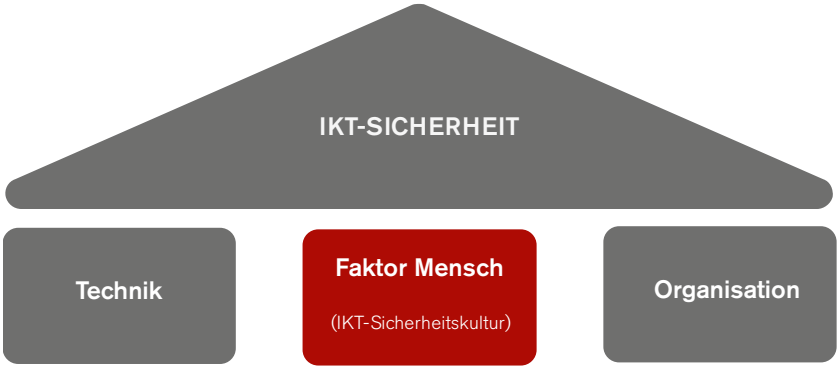
Weiterentwicklung des Österreichischen Informationssicherheitshandbuches: Das Österreichische Informationssicherheitshandbuch unterstützt eine einheitliche Terminologie und Vorgehensweise in der Etablierung von IKT-Sicherheit – sowohl in der öffentlichen Verwaltung als auch in der Wirtschaft. Daher wird das Handbuch als strategisches Rahmenwerk für IKT-Sicherheit in Österreich kontinuierlich weiterentwickelt, um sowohl den sich permanent ändernden technischen Anforderungen als auch den neuen Entwicklungen in der internationalen Standardisierung gerecht zu werden. *(siehe auch Kapitel 2 und 5)*

5 Awareness

5.1 Ausgangslage

Sicherheitsstudien und Lageberichte zur IKT-Sicherheit belegen, dass menschliches Fehlverhalten einen beträchtlichen Anteil der Sicherheitsvorfälle ermöglicht oder sogar verursacht. Was auf den ersten Blick als unverständlich gilt, erklärt sich bei näherer Betrachtung der IKT-Sicherheit. Diese basiert auf drei wesentlichen Säulen: der Technik, der Organisation und dem Faktor Mensch.

Abbildung 7: Säulen der IKT-Sicherheit



Faktor Mensch: Trotz aller sicherheitstechnischen Fortschritte und organisatorischen Regelungen, die die Industrie und die Standardisierung in den letzten Jahren mit sich gebracht haben, stellt der Faktor Mensch immer noch eine wesentliche – wenn nicht die wichtigste – Säule in der IKT-Sicherheit dar. Denn die getroffenen technischen und organisatorischen Sicherheitsmaßnahmen müssen letztendlich durch den Menschen, der als Nutzer der IKT im Zentrum steht, akzeptiert und getragen werden.

IKT-Sicherheitskultur: Eine zukunftsorientierte IKT-Sicherheit muss daher zwangsläufig auf den Faktor Mensch und auf der Stärkung der IKT-Sicherheitskultur aufbauen. Die IKT-Sicherheitskultur bestimmt dabei die Wahrnehmung, das Verständnis, die persönliche Einstellung und das erforderliche Wissen für ein sicherheitsbewusstes Handeln.

Die Sensibilisierung und Bewusstseinsbildung sowie das Wissen aller betroffenen Zielgruppen stellen somit – trotz aller verfügbaren technischen und organisatorischen Sicherheitsmaßnahmen – eine wesentliche Voraussetzung für den Nutzen und den Erfolg der IKT-Sicherheit dar.

Awareness verfolgt drei wesentliche Ziele:

- die Wahrnehmung von IKT Sicherheit als wichtiges Thema stärken, persönliches Interesse und Aufmerksamkeit für die IKT-Sicherheit gewinnen (Sensibilisierung der Zielgruppe),
- die persönliche Einstellung positiv besetzen und das Verständnis für die Notwendigkeit der IKT Sicherheit schaffen (Bewusstseinsbildung auf unterschiedlichen Ebenen) und

- durch konkrete und zielgruppenspezifische Handlungsempfehlungen das Wissen über ein sicherheitsbewusstes Handeln und verantwortungsvollen Umgang mit Informationen und IKT fördern.

Die Awareness-Maßnahmen differenzieren hinsichtlich der Handlungsfelder (wie BürgerIn, Wirtschaft, Verwaltung, Bildung und Forschung, KI) und Zielgruppen (jedenfalls nach AnwenderInnen, EntwicklerInnen und BetreiberInnen der IKT).

5.2 Strategische Ziele und Maßnahmen

5.2.1 Ziel 1: Stärkung der IKT-Sicherheitskultur in Österreich

These: Viele IKT-AnwenderInnen, AuftraggeberInnen und DienstleisterInnen (in Handel, Entwicklung und Betrieb) sind sich der Gefahren im Zusammenhang mit der IKT nicht bewusst. Häufig fehlen Verständnis und Wissen für ein sicherheitsbewusstes Handeln im Cyber-Raum.

Strategische Zielsetzung: Gezielte Awareness-Maßnahmen in allen relevanten Zielgruppen und Handlungsfeldern fördern und festigen die IKT-Sicherheitskultur in Österreich. Die IKT-Sicherheitskultur gewährleistet, dass die Betroffenen der aktuellen Gefährdungslage entsprechend handeln. Die IKT-Sicherheitskultur soll zukünftig – als dritte Säule einer effektiven IKT-Sicherheit – ein der aktuellen Gefährdungslage angemessenes und sicherheitsbewusstes Handeln aller Betroffenen sicherstellen.

5.2.2 Ziel 2: Positive Positionierung der IKT-Sicherheit

These: Häufig werden negative Aspekte der IKT-Sicherheit wahrgenommen wie etwa Mehraufwände, Mehrkosten und Einschränkungen für AnwenderInnen, EntwicklerInnen und BetreiberInnen. Wird nicht informiert, inwieweit die IKT-Sicherheitsmaßnahmen notwendig bzw. angemessen sind, führt dies zu einer ablehnenden Grundeinstellung. Positive Aspekte sind in den Vordergrund zu rücken. Dazu zählen beispielsweise Einhaltung von gesetzlichen und vertraglichen Vorschriften und Vorgaben, Schutz der Vertraulichkeit, Integrität, Verfügbarkeit der verarbeiteten Informationen, Vermeidung von Sicherheitsvorfällen und dadurch entstehende Schäden.

Strategische Zielsetzung: Begleitende Marketing-Maßnahmen stellen im Rahmen der Awareness-Kampagnen eine positive Positionierung der IKT-Sicherheit sowie der Initiativen der nationalen IKT-Sicherheitsstrategie sicher. Die betroffene Zielgruppe nimmt die IKT-Sicherheit zukünftig als positiven und notwendigen Mehrwert wahr.

5.2.3 Ziel 3: Abgestimmte und koordinierte Vorgehensweise

These: Vereinzelt bestehen in Österreich bereits Awareness-Initiativen. Die verschiedenen Stakeholder stimmen sich jedoch nur eingeschränkt ab. Die Umsetzung der geplanten Awareness-Maßnahmen im Rahmen der nationalen IKT-Sicherheitsstrategie erfordert, dass verschiedenste Stakeholder in unterschiedlichen Handlungsfeldern zusammenarbeiten.

Strategische Zielsetzung: Die im Rahmen der nationalen IKT-Sicherheitsstrategie geplanten Awareness-Maßnahmen werden auf Basis einer Vorgehensweise umgesetzt, welche die betroffenen Stakeholder gemeinsam ausgearbeitet haben. Damit sind die notwendige Transparenz, die optimale Nutzung von Synergiepotential und eine höchstmögliche Effizienz der Initiativen sichergestellt.

5.2.4 Ziel 4: Wirksamkeit und Nachhaltigkeit der Awareness-Maßnahmen

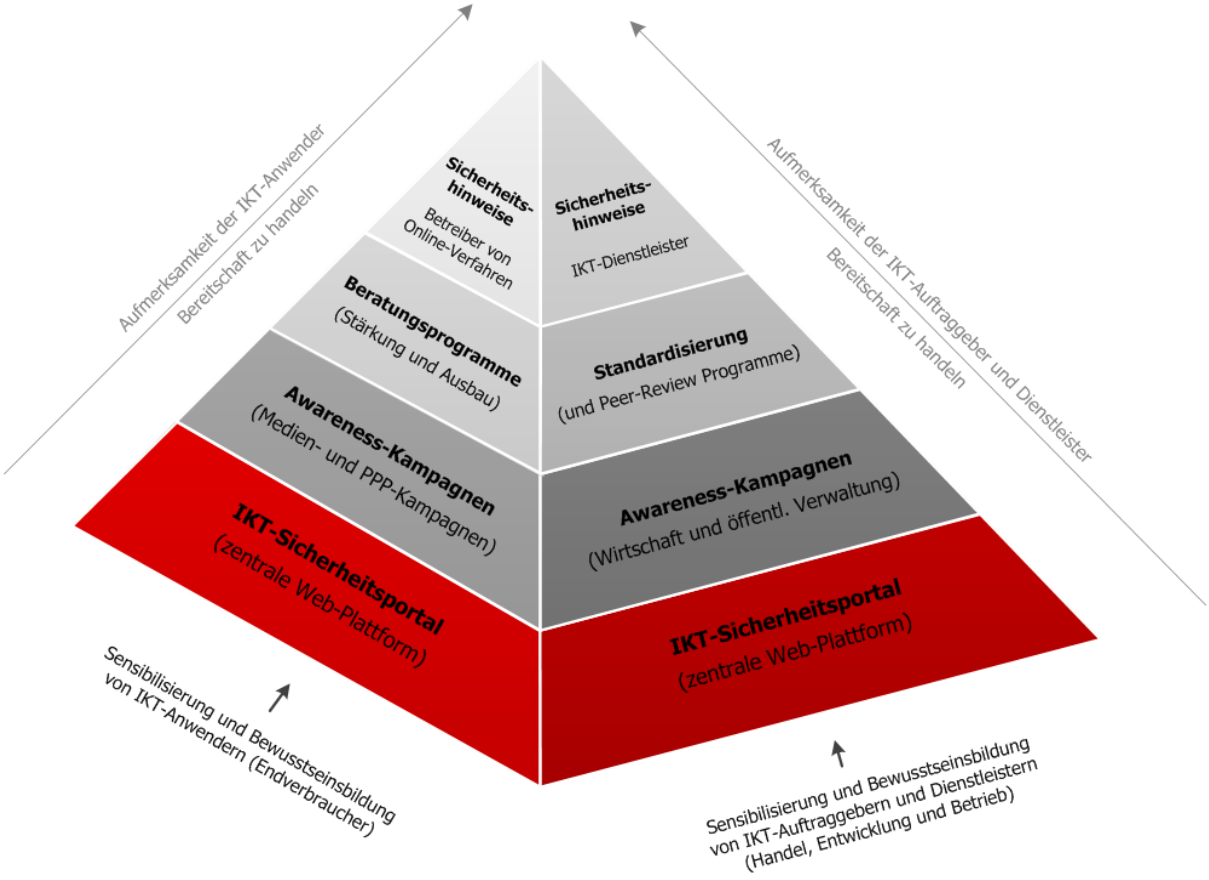
These: Das Wissen über die Akzeptanz und Nutzung der IKT ist in Österreich durch verschiedene statistische Datenbanken und Studien mittlerweile gut erfasst. Dagegen ist Wissen über die bestehende IKT-Sicherheitskultur (Sensibilisierung, Bewusstsein, Wissen und sicherheitsbewusstes Handeln) nur sehr rudimentär vorhanden. Gleiches gilt für tatsächlich eingetretene Sicherheitsvorfälle sowie für ihre Ursachen und Schäden.

Strategische Zielsetzung: Österreich setzt im Sinne der Nachhaltigkeit zukünftig ein Messinstrument ein, das regelmäßig die Wirksamkeit der getroffenen Awareness-Maßnahmen kontrolliert und Auswirkungen auf die Reduzierung von Sicherheitsvorfällen prüft, um im Bedarfsfall durch operative Maßnahmen nachjustieren zu können.

5.2.5 Maßnahmen zur Erreichung der strategischen Ziele

Im Zentrum des bestehenden Maßnahmenkonzepts zur Erreichung der strategischen Ziele stehen gezielte Awareness-Maßnahmen, um die IKT-Sicherheitskultur in Österreich zu stärken. Um eine echte Transformation von der Sensibilisierung und Bewusstseinsbildung zum tatsächlichen, sicherheitsbewussten Handeln zu erzielen, muss die Information und Kommunikation insbesondere dann erfolgen, wenn die Aufmerksamkeit des Einzelnen am größten ist. Daraus resultiert die Notwendigkeit eines mehrstufigen Informations- und Kommunikationskonzepts, das die verschiedenen Zielgruppen in unterschiedlichen Lebenssituationen erreicht und dafür unterschiedliche Medien und Kanäle vorsieht.

Abbildung 8 Awareness-Maßnahmen

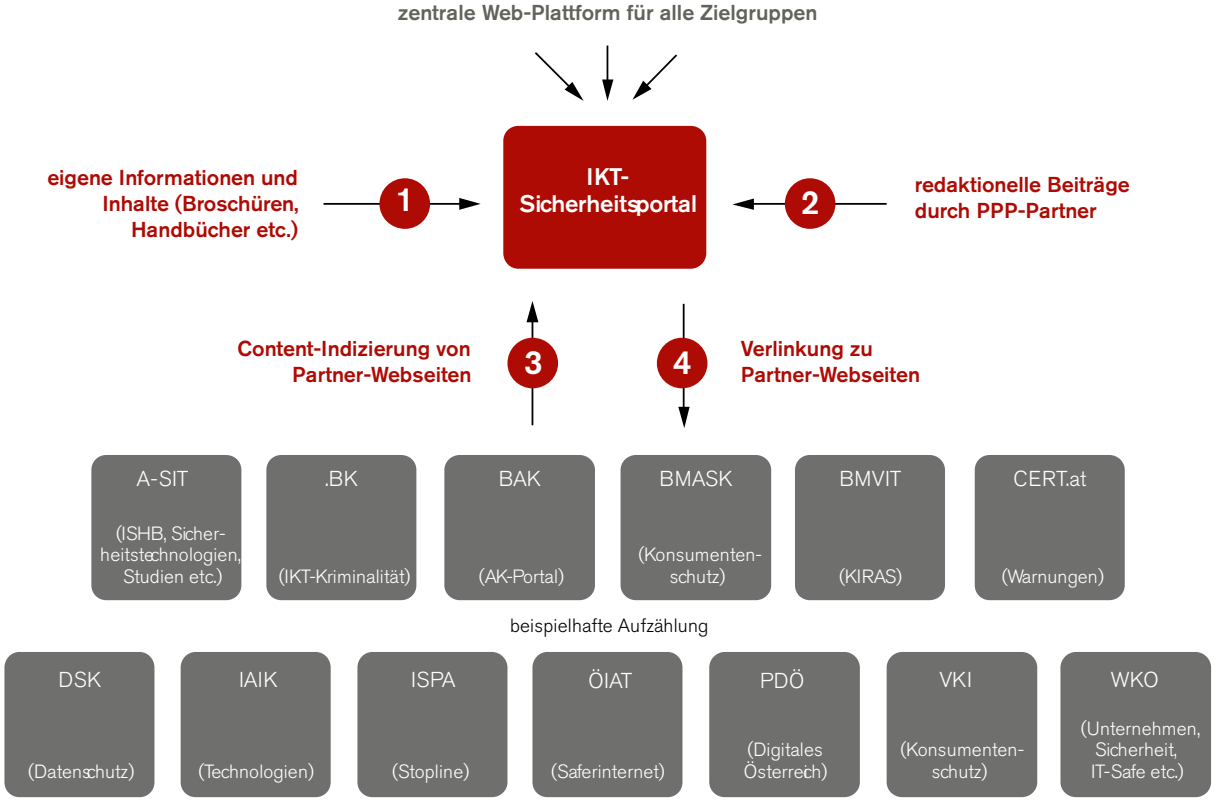


Beschreibung der Abbildung 8:

- Maßnahmen zur Sensibilisierung und Bewusstseinsbildung von IKT-AnwenderInnen: 1. IKT-Sicherheitsportal (zentrale Web-Plattform), 2. Awareness-Maßnahmen (Medien und PPP-Kampagnen), 3. Beratungsprogramme (Stärkung und Ausbau), 4. Sicherheitshinweise (Betreiber von Online-Verfahren). Von 1 bis 4 steigt die Aufmerksamkeit der IKT-AnwenderInnen und deren Bereitschaft zu handeln.
- Maßnahmen zur Sensibilisierung und Bewusstseinsbildung von IKT-AuftraggeberInnen und Dienstleistern (in Handel, Entwicklung und Betrieb): 1. IKT-Sicherheitsportal (zentrale Web-Plattform), 2. Awareness-Maßnahmen (Wirtschaft und öffentliche Verwaltung), 3. Beratungsprogramme (und Peer Review Programme), 4. Sicherheitshinweise (Dienstleister). Von 1 bis 4 steigt die Aufmerksamkeit der IKT-AuftraggeberInnen und Dienstleister und deren Bereitschaft zu handeln.

- **Einrichten eines IKT-Sicherheitsportals:** Das IKT-Sicherheitsportal fungiert in Form einer Web-Plattform für alle Zielgruppen in Österreich als die zentrale Anlaufstelle für Themen der IKT-Sicherheit und als grundlegende Informations- und Kommunikationsbasis aller Awareness-Maßnahmen. Zu den Zielgruppen zählen sowohl IKT-AnwenderInnen als auch IKT-AuftraggeberInnen und IKT-DienstleisterInnen (in Handel, Entwicklung und Betrieb).

Abbildung 9 IKT-Sicherheitsportal



Beschreibung der Abbildung 9: zentrale Web-Plattform für alle Zielgruppen bietet 1. eigene Informationen und Inhalte (Broschüren, Handbücher etc.), 2. Redaktionelle Beiträge durch PPP-Partner, 3 Content-Indizierung von Partner Webseiten und 4. Verlinkung zu Partner-Webseiten. Partner-Webseiten sind (beispielhafte Aufzählung): A-SIT (ISHB, Sicherheitstechnologien, Studien etc.), .BK (IKT-Kriminalität), BAK (AK-Portal), BMASK (Konsumentenschutz), BMVIT (KIRAS), CERT.at (Warnungen), DSK (Datenschutz), IAIK (Technologie), ISPA (Stopline), ÖIAT (Saferinternet), PDÖ (Digitales Österreich), VKI (Konsumentenschutz), WKO (Unternehmen, Sicherheit, IT-Safe etc.)

- **Awareness-Kampagnen:** Aktive Information und Kommunikation zur Stärkung der IKT-Sicherheitskultur in Österreich. Unter Berücksichtigung bereits bestehender Kampagnen und Initiativen gemeinsam mit den Stakeholdern themen- und zielgruppenspezifische Kampagnen erarbeiten, abstimmen und durchführen. Dabei wird die IKT-Sicherheit aus verschiedenen Blickwinkeln betrachtet, auf die relevanten Gefahren hingewiesen, mögliche Auswirkungen und Schäden aufgezeigt und Empfehlungen hinsichtlich geeigneter und sinnvoller Sicherheitsmaßnahmen gegeben. Die Empfehlungen müssen angemessen sein und der Nutzen der IKT-Sicherheit je nach Zielgruppe durch unterschiedliche Motivation (persönliche, ökonomische und rechtliche Aspekte) dargestellt werden. Zu den Kampagnen zählen u. a.: redaktionelle Beiträge in bestehenden Formaten (in Sinn eines Bildungsauftrags) sowie Information und Kommunikation durch PP-Partner in den Bereichen der öffentlichen Verwaltung, der Interessensvertretungen und der Wirtschaft. E-Learning-Programme sollen die Kampagnen ergänzen.
  Derzeit bestehen folgende Themenvorschläge für Kampagnen: IKT-Sicherheit im Privathaushalt, Datenschutz für Betroffene, Datenschutz für Jugendliche, Sicheres Online-Banking, Internet-Ratgeber für Senioren, Sicherer Umgang mit sozialen Medien und Netzwerken, Social Media Ratgeber für Eltern, Vorsicht Internet-Betrug!, Konsumentenschutz im Internet, Gesetzliche Datenschutzbestimmungen für AuftraggeberInnen, Gesetzliche

Datenschutzbestimmungen für DienstleisterInnen, Austrian Trust Circle, IT-Notfallmanagement im Unternehmen, IKT-Sicherheit im Unternehmen, Sichere Online-Verfahren entwickeln und betreiben, Achtung Wirtschaftsspionage, IKT-Sicherheits-Compliance (Check) im Unternehmen.

- **Beratungsprogramme:** Im Bedarf weiterführende und individuelle Beratung durch PP-Partner für verschiedene Zielgruppen: BürgerInnen und private KonsumentInnen, Unternehmen und FirmengründerInnen, IKT-DienstleisterInnen, Organisationen im Bereich der öffentlichen Verwaltung sowie Unternehmen im Bereich der Kritischen Infrastruktur. Bestehende Angebote sollen weiter verstärkt und ausgebaut werden sollen.

Beispiele für das Nutzen von bestehenden Strukturen und Synergiepotential

Awareness-Kampagnen

Redaktionelle Beiträge (Bildungsauftrag) in bestehenden Formaten (wie z.B. Newton, Thema, Konkret das Servicemagazin, ATV-Reportage, etc.)

- durch Rundfunk (wie z.B. ORF und ATV) sowie Print- und Onlinemedien

Information und Kommunikation (aktiver Hinweis auf das Thema IKT-Sicherheit, Aushändigung von Broschüren und elektronische Bereitstellung der Informationen auf deren Webseiten) durch

- PP-Partner im Bereich der öffentlichen Verwaltung mit Parteienverkehr (Polizeidienststellen, kriminalpolizeiliche Beratungsdienst, Finanz- und Zollämter, Bundesheer, Landesverwaltung, Bezirkshauptmannschaften, Schulen, Gemeindeämter, etc.)
- PP-Partner im Bereich der Interessensvertretungen (WKO, AK, VKI, etc.)
- PP-Partner im Bereich der Wirtschaft mit Kundenverkehr (Banken, Internet Service Provider, IKT-Einzelhandelsketten, IKT-Dienstleister, etc.)

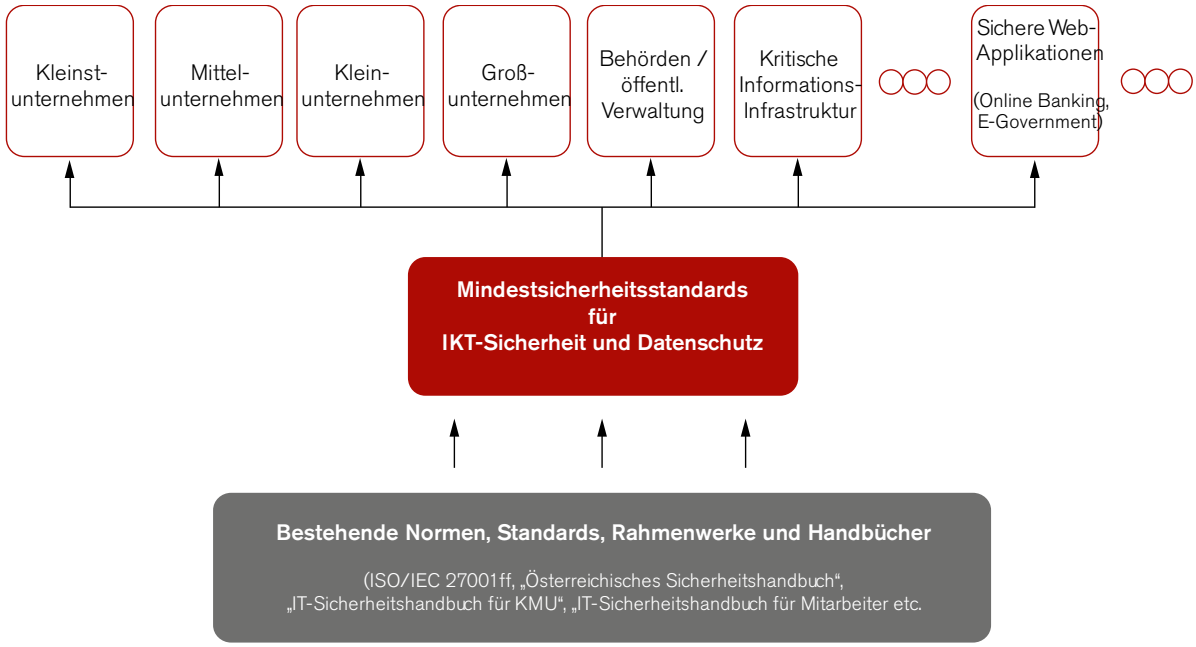
Beratungsprogramme

- Beratung von BürgerInnen und privaten KonsumentInnen (z.B. durch .BK, kriminalpolizeilicher Beratungsdienst, AK, VKI, OCG, etc.)
- Beratung von Unternehmen und Firmengründern sowie spezifische Beratung und Schulungsangebote (sowie etwaige Zertifizierungsangebote) für IKT-DienstleisterInnen im Fachbereich Unternehmensberatung und IT – UBIT (z.B. durch Gründer-Service der WKO, .BK, BMWFJ, A-SIT, etc.)
- Beratung von Organisationen im Bereich der öffentlichen Verwaltung (z.B. durch PDÖ, A-SIT)
- Spezifische Beratung von Unternehmen im Bereich der kritischen Infrastruktur (z.B. durch .BK, WKO, BMWFJ, A-SIT, etc.)

- **Standardisierung:** Im Sinne einer effektiven Sicherheitsprävention und insbesondere zum gemeinsamen Verständnis über aktuelle Anforderungen klare Mindestsicherheitsstandards für die IKT-Sicherheit und den Datenschutz entwickeln und veröffentlichen. Abhängig vom

jeweils vorliegenden Gefährdungspotential soll eine entsprechende Abstufung der Mindestsicherheitsstandards, etwa nach Unternehmensgröße und Branche, sichergestellt werden. Die Entwicklung erfolgt dabei auf Basis des Informationssicherheitshandbuchs und berücksichtigt weitere bestehende Normen, Standards, Rahmenwerke und Handbücher. Freiwillige Sicherheits-Peer Review-Programme durch anerkannte österreichische Universitäten und Forschungseinrichtungen einrichten und fördern. Österreichische Unternehmen und Organisationen können bei Evaluierung der Qualität und Sicherheit ihrer IKT-Dienste und IKT-Produkte durch externe Qualitätsprüfung unterstützt werden. Damit erhalten sie die Möglichkeit mittels Zertifikat, ihre geprüfte IKT-Sicherheit und Einhaltung von Sicherheitsstandards nach außen (ihren Kunden) darzustellen (Wettbewerbsvorteil) und nachzuweisen (Ausschreibungen). Die teilnehmenden (anerkannten) Einrichtungen der Sicherheits-Peer Review-Programme werden auf dem IKT-Sicherheitsportal veröffentlicht.

Abbildung 10 Mindestsicherheitsstandards für die IKT-Sicherheit und den Datenschutz



Beschreibung der Abbildung 10: Basis: Bestehende Normen, Standards und Handbücher (ISO/IEC 27001ff., „Österreichisches Sicherheitshandbuch“, „IT-Sicherheitshandbuch für KMU“, „IT-Sicherheitshandbuch für Mitarbeiter“ etc.). Mindestsicherheitsstandards für die IKT-Sicherheit und den Datenschutz für: Kleinstunternehmer, Mittelunternehmer, Kleinunternehmer, Großunternehmer, Behörden/öffentliche Verwaltung, Kritische Informatinsinfrastrukturen, […], sichere Web-Applikationen (Online Banking, E-Government), […]

- **Sicherheitshinweise:** Seitens IKT-AnwenderInnen besteht die größte Aufmerksamkeit für IKT-Sicherheit bei der Registrierung und Nutzung von Online-Anwendungen. Seitens IKT-AuftraggeberInnen liegt sie beim Kauf von IKT-Produkten und IKT-Diensten, bei der Beauftragung von Entwicklungen, dem Betrieb von IKT-Anwendungen oder der IKT-Infrastruktur. Somit soll die Anwendung von Sicherheitshinweisen für BetreiberInnen von Online-Anwendungen und für IKT-DienstleisterInnen (in Handel, Entwicklung und Betrieb) gesetzlich verpflichtend eingeführt werden. Zu diesem Zweck sollen gemeinsam mit den Interessensvertretungen und unter Berücksichtigung der nationalen und europäischen Gesetzgebung übersichtliche und verständliche Sicherheitshinweise für die unterschiedli-

chen Anwendungsfälle erarbeitet, abgestimmt und den BetreiberInnen von Online-Anwendungen sowie IKT-DienstleisterInnen zur Verfügung gestellt werden. Die Sicherheitshinweise dienen letztendlich dem Schutz der IKT-AnwenderInnen und IKT-AuftraggeberInnen.

5.2.6 Begleitmaßnahmen

- **IKT-Sicherheitslexikon:** Gemeinsame Sprache finden. Das IKT-Sicherheitslexikon soll im ersten Schritt die in der IKT-Sicherheitsstrategie verwendeten Fachbegriffe erklären und regelmäßig erweitert und aktualisiert werden.

- **Entwicklung und Umsetzung eines Marketingkonzepts**: Im Rahmen eines Marketing und Medienkonzepts werden Marke und Styleguide zugunsten einer positiven Positionierung der IKT-Sicherheit, eines professionellen Erscheinungsbildes und eines höchstmöglichen Bekanntheitsgrades und Wiedererkennungswertes gestaltet.

- **Aufbau von Public Private-Partnerschaften:** Die Durchführung der geplanten Awareness-Kampagnen benötigt unterschiedliche Medien und insbesondere verschiedene Kommunikationskanäle. Der Aufbau von Public Private Partnerships mit weiteren Stakeholdern in Österreich gewinnt die für die erforderliche Information und Kommunikation notwendigen Multiplikatoren. Diese Stakeholder werden zudem auf dem IKT-Sicherheitsportal als PP-Partner veröffentlicht.

- **Aufbau einer Koordinationsstruktur:** Um eine abgestimmte und koordinierte Vorgehensweise (Steuerung und Kontrolle) im Zuge der umfassenden Awareness-Maßnahmen sicherzustellen, gilt es zudem, eine geeignete Koordinationsstruktur mit allen beteiligten Stakeholdern aufzubauen. Hierbei sind die entsprechenden Abstimmungs- und Kommunikationskanäle zwischen den einzelnen Stakeholdern, den verantwortlichen Ansprechpartner und den Umsetzungsplänen festzulegen.

- **Entwicklung und Umsetzung von Monitoring-Maßnahmen:** Monitoring-Maßnahmen entwickeln und regelmäßig einsetzen, um die Wirksamkeit und Nachhaltigkeit der getroffenen Maßnahmen sicherzustellen. Dafür sind geeignete Monitoring-Maßnahmen und verantwortliche Stakeholder festzulegen. Bestehende Instrumente und Strukturen sollen genutzt, geeignete Projekte fortgeführt oder erweitert werden.

Abkürzungen und Glossar

ATC	Austrian Trust Circle, Bereichsspezifische Vernetzung der kritischen Informationsinfrastrukturen in Österreich
CERT	Computer Emergency Response Team z. B. http://www.cert.at/
GovCERT	Government Computer Emergency Response Team Österreichs, http://www.govcert.gv.at/
SKKM	Staatliches Krisen und Katastrophenschutzmanagements, http://www.bmi.gv.at/cms/BMI_Zivilschutz/mehr_zum_thema/SKKM.aspx
OSZE	Organisation für Sicherheit und Zusammenarbeit in Europa, http://www.bmeia.gv.at/aussenministerium/aussenpolitik/europa/osze.html
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung, http://www.oecd.org/home/
KIRAS	Nationales Programm zur Förderung österreichischer Sicherheitsforschung, koordiniert vom BMVIT, http://www.kiras.at/
TAB	Büro für Technikfolgenabschätzung in Deutschland, http://www.tab-beim-bundestag.de/de/index.html
HORIZON 2020	Neues Rahmenprogramm für Forschung und Innovation der EU, http://forschungsrahmenprogramm.de/horizon2020.htm
ISO	Internationale Organisation für Standardisierung, http://www.iso.org/iso/home.htm
IEC	Internationale Elektrotechnische Kommission, http://www.iec.ch/
CENELEC	Europäische Einrichtung zur Standardisierung von Elektrotechnik, http://www.cenelec.eu/
CEN	Europäische Einrichtung zur Standardisierung, http://www.cen.eu/
ETSI	Europäisches Institut für Telekommunikationsnormen, http://www.etsi.org/
SIHA	Österreichisches Informationssicherheitshandbuch, https://www.sicherheitshandbuch.gv.at/downloads/Sicherheitshandbuch%20V3-1-001.pdf
CIP	Critical Infrastructure Protection, Abteilung des Bundeskanzleramts und des BM.I zum umfassenden Schutz strategischen Infrastrukturen Österreichs
CIIP	Critical Information-Infrastructure Protection, Koordination der strategischen Informationsinfrastrukturen Österreichs
ISK	Informationssicherheitskommission, Abteilung des Bundeskanzleramts, National Security Authority in Österreich
FüUZ	Führungsunterstützungszentrum, Abteilung des österr. Bundesheeres
AbwAmt	Abwehramt, Abteilung des österr. Bundesheeres
HNa	Heeresnachrichtendienst, Abteilung des österr. Bundesheeres
BVT	Bundesamt für Verfassungsschutz und Terrorismusbekämpfung, Abteilung des BM.I, schützt Einrichtungen des Staates und deren Handlungsfähigkeit
BK	Bundeskriminalamt, Abteilung des BM.I, bundesweite Bekämpfung gerichtlich strafbarer Handlungen http://www.bmi.gv.at/cms/BK/
C4	Cyber Crime Competence Center, Abteilung des BM.I, Koordinierungs- und Meldestelle des BM.I für Cyberkriminalität

Danksagung

Die vorliegende Unterlage wurde im Rahmen von fünf Arbeitsgruppen durch Expertinnen und Experten ausgearbeitet. Dabei haben die Expertinnen und Experten ihr Wissen und ihre breite Erfahrung unentgeltlich eingebracht und zahlreiche Arbeitsstunden investiert.

Das Bundeskanzleramt bedankt sich daher sehr herzlich bei allen Beteiligten im Besonderen bei den Leiterinnen und Leitern der Arbeitsgruppen.

Arbeitsgruppe Risikoeinschätzung/-management – Lagesituation, -monitoring und -folgerungen – Gefährdungslage
Robert Schischka –CERT.at
Thomas Stubbings – Raiffeisen International

Arbeitsgruppe Kritische Infrastruktur
Paul Karrer – Cyber Security Austria
Alexander Pschikal – Bundeskanzleramt

Arbeitsgruppe Bildung und Forschung
Ingrid Schaumüller-Bichl – FH Hagenberg / OCG
Walter Seböck – Donau-Universität Krems

Arbeitsgruppe Stakeholder und Strukturen, nationale und internationale Vernetzung
Daniel Konrad – A-SIT
Wilfried Wöber – Univie/ACOnet

Arbeitsgruppe Awareness
Martina Ertler – Wirtschaftskammer Österreich
Markus Kloibhofer – BMF
Hans-Jürgen Pollirer – Wirtschaftskammer Österreich
Josef Schröfl – BMLVS

Unterstützung der ArbeitsgruppenleiterInnen durch:
Helmut Hummer – Bundeskanzleramt
Alexander Klimburg – OIIP
Roland Ledinger – Bundeskanzleramt
Timo Mischitz – Bundeskanzleramt
Franz Vock – Bundeskanzleramt

Beteiligt in einer der Arbeitsgruppen:

Gerhard Bisovsky
Thomas Bleier
Erwin Bosin
Stefan Brandl
Christian Braunsteiner
Ronald Bresich
Michael Brugger
Gerd Brunner
Barbara Buchegger
Michael Butz
Michael Danzl
Friedrich Dozler
Gerhard Dyduch
Christoph Eberl
Martin Ebner
Ralph Eckmaier
Kurt Einzinger
Rainer Eisenkirchner
Mathias Fahrner
Paul Falb
Eveline Fegerl
Martin Fellhofer
Stefan Fenz
Erhard Friessnik
Andreas Fritz
Anita Fröhlich
Gernot Fuchs
Christian Fuernweger
Thomas Geretschläger
Robert Gottwald
Ernst Graumann
Johann Haag
Helmut Habermayer
Harald Haselbauer
Wolfgang Haumann
Markus Hefler
Sandra Heissenberger
Otto Hellwig
Marcus Hild
Franz Hoheiser-Pförtner
Herbert Höllebauer
Manfred Holzbach
Thomas Hrdinka
Christian Hribernig
Matthias Hudler
Bernhard Jungwirth
L. Aaron Kaplan
Ernst Karner
Nieves Erzsebet Kautny
Joachim Klerx
Roman Kobylka
Leopold Koppensteiner
Manuel Koschuch
Klaus Kraner
Gerhard Krenn
Marco Lang
Martin Langer
Ulrich Latzenhofer
Thomas Latzer
Christoph Lechner
Josef Lechner
Franz Lehner
Wolfgang Liedermann
Jürgen Mang
Johannes Mariel
Georg Melzer
Alexander Mense
Thomas Menzel
Christian Minarovits
Joachim Minichshofer
Philipp Mirtl
Michael Müller
Rupert Nagler
Markus Narrenhofer
Markus Necker
Renate Neumüller
Andrea Nowak
Gerald Obernosterer
Lendl Otmar
Christian Pennerstorfer
Thomas Pfeiffer
Joe Pichlmayr
Helmut Pizka
Ralph Pöchhacker
Christian Polnitzky
Lukas Praml
Manfred Pregartbauer
Karl Preszl
Christian Proschinger
Günter Reiser
Wolfgang Resch
Philipp Reschl
Markus Robin
Karl Rossegger
Wolfgang R. Ryvola
Lambert Scharwitzl
Philipp Schaumann
Manfred Schleinzer
Matthias Schmidl
Rupert Schmutzer
Reinhard Schönthaler
Maximilian Schubert
Jan Schubert
Rainer Schügerl
Helmut Schwabach
Erich Schweighofer
Christian Schwertberger
Armin Selhofer
Alexander Siedschlag
Florian Skopik
Werner Spies
Werner Sponer
Johann Starlinger
Manuel Stecher
Wolfgang Steiner
Jörg Steiner
Barbara Steiner
Jaro Sterbik-Lamina
Matthias Straubinger
Alexander Szönyi
Alexander Talos-Zens
Alfred Tanzer
Simon Tjoa
Wolfgang Trexler
Gerald Trost
Thomas Von der Gathen
Christian Wagner
Thomas Wanasek
Edgar Weippl
Heinz Weiskirchner
Andreas Wespi
Christian Wiesener
Michael Wiesmüller
Martin Winkler
Christian Zagler
Christian Zmaritz