University of Fribourg
international institute
of management in technology

Kompetenzbildungsangebote im Umgang mit Cyber-Risiken (Massnahme 7 NCS)

➢ Ergebnisse Experteninterviews

Bd de Pérolles 90 1700 Fribourg Switzerland T.+41 26 300 84 30 F.+41 26 300 97 94 www.iimt.ch
iimt@unifr.ch

Kontakt
international institute for management in technology - iimt
Universität Fribourg
Boulevard de Pérolles 90
1700 Fribourg
Switzerland
Telefon: +41 26 300 84 30
Fax: +41 26 300 97 94
Email: iimt@unifr.ch

Autoren
Dominic Feichtner
Dr. Bernd Teufel
Prof. Dr. Stephanie Teufel

Inhalt

Abkürzungsverzeichnis

(D)Dos	(Distributed) Denial of Service
AG	Auftraggeber
BAKOM	Bundesamt für Kommunikation
BFS	Bundesamt für Statistik
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAS	Certificate of Advanced Studies
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
C-Level	Erste Führungsebene eines Unternehmens
CSIRT	Computer Security Incident Response Team
CSO	Chief Security Officer
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
EPA	Eidgenössisches Personalamt
EU	Europäische Union
iimt	international institute of management in technology (Universität Fribourg)
IKT	Informations- und Telekommunikationstechnologie
ISACA	Information System Audit and Control Association
ISB	Informatiksteuerungsorgan des Bundes
ISBO	Informatiksicherheitsbeauftragter Organisation
ISO	International Organization for Standardization
IT	Informationstechnik
KI	Kritische Infrastruktur
KMU	Klein und mittlere Unternehmen
KOBIK	Koordinationsstelle zur Bekämpfung der Internetkriminalität
MELANI	Melde- und Analysestelle Informationssicherung

NCS	Nationale Strategie des Bundesrates zum Schutz der Schweiz vor Cyber-Risiken
ÖV	Öffentlicher Verkehr
SANS	SANS Information Security Training
SAS	SAS Institute Inc.
SKP	Schweizerische Kriminalprävention
u.a.	unter anderem

1. Management Summary

Der Schutz der Informations- und Kommunikationsinfrastrukturen vor Cyber-Risiken liegt im nationalen Interesse. Die Sensibilisierung der Gesellschaft und insbesondere der Akteure aus Wirtschaft und Behörden bezüglich Cyber-Risiken ist ein entscheidender Faktor im Risikomanagement.

Im Allgemeinen werden unter Cyber-Risiken jede Art von Risiken im Zusammenhang mit Informations- und Kommunikationstechnologien (IKT) verstanden: Nicht ein spezielles Risiko ist gemeint, sondern eine Gruppe von Risiken, die sich aus den unterschiedlichen angewendeten Technologien, aus den Angriffsprofilen sowie aus nichtbeeinflussbaren, von aussen wirkenden Umständen zusammensetzen. In die Risikobetrachtung gehen demzufolge nicht nur kriminelle Aktivitäten ein, sondern auch beispielsweise Naturkatastrophen. Dementsprechend wird zwischen Abwehr- und Schutzmethoden unterschieden.

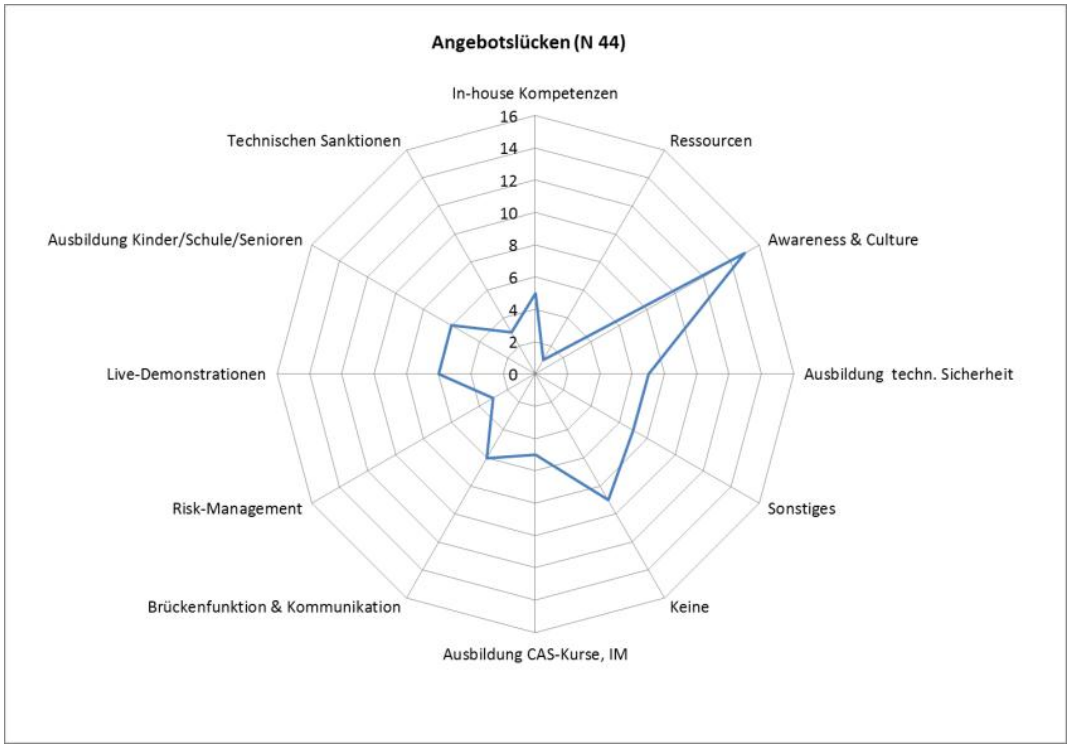
In einem ersten Mandat wurden die Zielgruppen identifiziert und spezifiziert. Aus den einzelnen Segmentierungsstufen wurden Expertinnen und Experten sowie gute Beispiele in diesem Themenfeld identifiziert. Zudem wurde ein Interview-Leitfaden zur Befragung der Expertinnen und Experten aus den Zielgruppen entwickelt.

Auf dieser Basis wurden durch das Bundesamt für Kommunikation (BAKOM), das Informatiksteuerungsorgan des Bundes (ISB), economiesuisse und durch das international institute of management in technology der Universität Fribourg (iimt) Expertinnen und Experten aus den unterschiedlichen Zielgruppen der Gesellschaft zum Themenkreis Cyber-Risiken befragt.

Die durchgeführte Umfrage ist nicht-repräsentativ angelegt, sie kann aber sehr wohl Trends erkennen lassen und ein tieferes Verständnis generieren. Für die Umfrage wurden vornehmlich Expertinnen und Experten aus Wirtschaft und Verwaltung befragt. Dieses qualitative Vorgehen hat durch den ausschliesslichen Einbezug von hochqualifizierten Fachleuten jedoch hinsichtlich der genannten Angebotsdefizite durchaus eine nicht zu unterschätzende Aussagekraft. Tendenziell hat sich gezeigt, dass ein grundsätzliches Bewusstsein der Gefahrenlage existiert. Die Bekanntheit von Schulungsmassnahmen und speziell deren Anwendung scheint eher unterproportional zu sein.

Hervorzuheben ist, dass aus den drei Zielgruppen Wirtschaft, Verwaltung und Bevölkerung sowohl in der Zielgruppe Wirtschaft als auch in der Zielgruppe Verwaltung die wahrgenommenen Cyber-Risiken sich vor allem durch die Nennungen

„unbefugte Datenbeschaffung“ und „unbefugtes Eindringen in ein Datenverarbeitungssystem“ zu charakterisieren scheinen. Des Weiteren sind die Nennungen zu „Hacking“ und „(Distributed) Denial of Service“ (DoS/DDoS) in diesen Zielgruppen beachtenswert, wenngleich anzumerken ist, dass beispielsweise zwischen „Hacking“ und „unbefugte Datenbeschaffung“ eine gewisse Korrelation besteht.



Wie die oben stehende Grafik (vgl. Abb. 8, S.27) zeigt, ist bei den genannten Angebotslücken ein Mangel an Ausbildungsangeboten vom freien Markt identifiziert. Dabei zeigt sich vor allem auch, dass insbesondere Nachholbedarf im Bereich „Ausbildung Sicherheitskultur & Kommunikation“ angemahnt wird, wie sich in dem entsprechend hohen Ausschlag im Cluster „Awareness & Culture“ wiederspiegelt.

2. Projektziele

Der Schutz der Informations- und Kommunikationsinfrastrukturen vor Cyber-Risiken liegt im nationalen Interesse. Im Rahmen der nationalen Strategie des Bundesrates zum Schutz der Schweiz vor Cyber-Risiken (NCS) sollen alle Akteure aus Wirtschaft, Gesellschaft und Behörden für Cyber-Risiken sensibilisiert und soweit ausgebildet werden, dass sie Risiken erkennen und Maßnahmen zur Minimierung ihrer Risikoexponierung treffen können. Dazu braucht es eine Definition von zielgruppengerechten Basis- und Kernkompetenzen für den Umgang mit Cyber-Risiken sowie gute Beispiele, die veröffentlicht werden können, um den Bekanntheitsgrad zu steigern.

Im Rahmen eines Vorgängerprojektes[1] wurde ein Interview-Leitfaden[2] für Experteninterviews entwickelt. Anhand dieses Leitfadens wurden durch BAKOM, ISB, economiesuisse und iimt Expertinnen und Experten aus den unterschiedlichsten Branchen zum Themenkreis Cyber-Risiken befragt. Ziel dieses Folgemandates war die Auswertung und Darstellung des gesammelten Materials. Das Material wurde durch ein weiteres Experteninterview (durchgeführt vom iimt) komplettiert.

Die im Rahmen der verschiedenen Aktivitäten erhobenen Daten mussten zur Auswertung und Darstellung geeignet zusammengeführt und strukturiert werden. Basierend auf

- dem iimt Abschlussbericht des Erstmandates,
- den von iimt, BAKOM, ISB und economiesuisse durchgeführten Experten-Interviews

erfolgte eine zielgruppengerechte Auswertung und Darstellung des Datenmaterials unter Berücksichtigung wissenschaftlicher Anforderungen.

Bezüglich des Datenmaterials ist anzumerken, dass zur Identifizierung der relevanten Cyber-Risiken, der erforderlichen Kompetenzen sowie der bedarfsgerechten Kompetenzbildungsangebote für jede der definierten Zielgruppen eine Expertenbefragung erfolgte.

Insgesamt wurde ein qualitatives Verfahren als Vorgehensmodell gewählt. Daher wird explizit darauf hingewiesen, dass hiermit keine repräsentativen Aussagen getroffen werden können.

[1] D. Feichtner et al. NCS M7 Abschlussbericht. iimt, Universität Fribourg, 2014.

[2] Vgl. Anhang 1.

3. Interviewleitfaden für Experteninterviews

Als Interviewtyp wurde ein halbstrukturiertes Leitfadeninterview gewählt, um den Expertinnen und Experten einerseits möglichst grossen Antwortspielraum zu lassen, andererseits gibt diese Interviewform die Möglichkeit, Muster in der diversifizierten Grundgesamtheit zu erkennen. Auf Grund der Vorgabe, dass die Interviews selbst möglichst kurz gehalten werden, wurden die Befragungen grösstenteils telefonisch durchgeführt.

Die Erhebung war gemäss den Projektzielen qualitativ angelegt. Die Auswertung kann jedoch trotz der qualitativen Natur Trends erkennen lassen und ein tieferes Verständnis generieren. Signifikant gültige Aussagen auf die Grundgesamtheit können mit dem gewählten Stichprobenumfang aber nicht getroffen werden. Dieses qualitative Vorgehen hat durch den ausschliesslichen Einbezug von hochqualifizierten Fachleuten jedoch eine nicht zu unterschätzende Aussagekraft die eine ausreichende Basis für eine spätere empirische Untersuchung darstellt.

Der Interviewleitfaden deckt die folgenden Bereiche ab:

- Relevante Cyber-Risiken
- Erforderliche Kompetenzen
- Gute Beispiele
- Angebotslücken

Die im Einzelnen gewählten Fragestellungen sind in Anhang 1 – Interviewleitf zu finden.

4. Untersuchungsdesign – Zielgruppenbeschreibung

Für die Umfrage wurden die in Abbildung 1 dargestellten Branchen in die Umfrage mit einbezogen. Für Details wird auf Anhang 2 verwiesen.

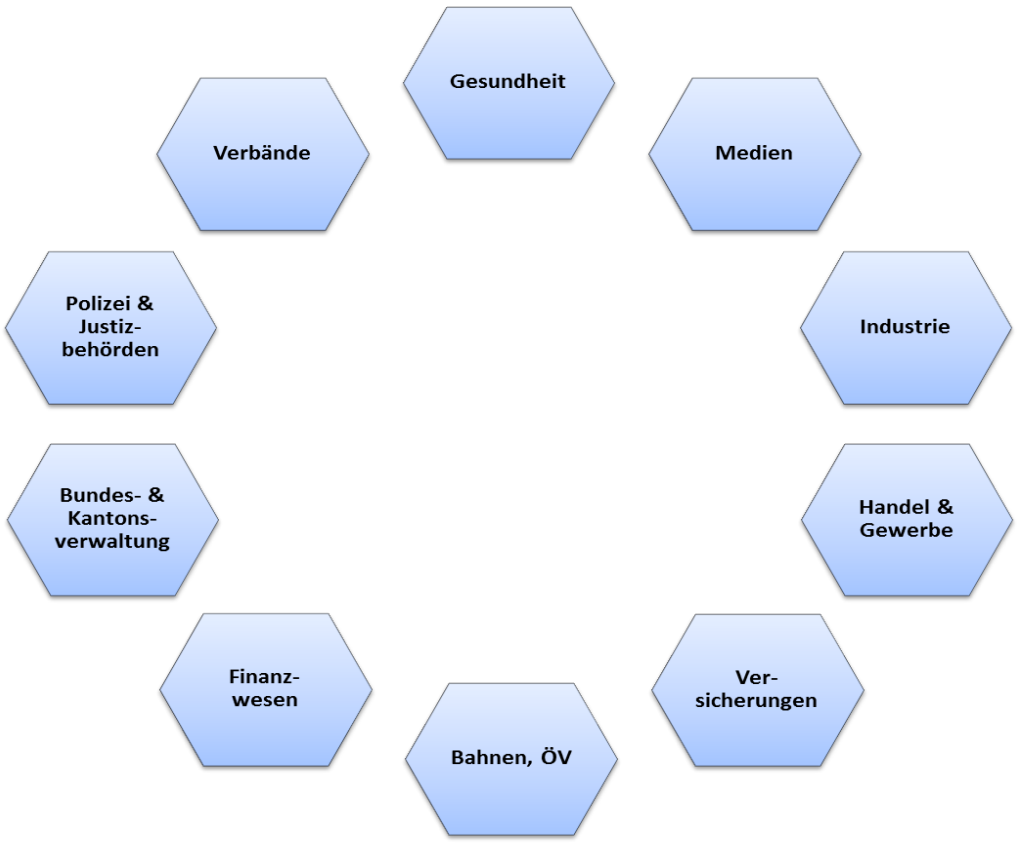


Abbildung 1: Branchen der Umfrage.

Um die bedarfsgerechten Kompetenzbildungsangebote zu identifizieren, wurde für jede der Zielgruppen eine Erhebung in Form einer Expertenbefragung vorgenommen. Die Wahl dieses qualitativen Verfahrens bedeutet, dass keine repräsentativen Aussagen gemacht werden können. So ist auch die Nennung der Kompetenzbildungsangebote mit hoher Qualität, die von den Expertinnen und Experten für ihre Zielgruppen empfohlen werden, eine exemplarische und nicht eine abschliessende.

Die Auswahl der rund 40 Expertinnen und Experten erfolgte unter Rücksprache mit verschiedenen Schlüsselpersonen der Zielgruppen. Pro Zielgruppe wurde mindestens eine Expertenbefragung durchgeführt. Die Befragten sind entweder für eine zielgruppenspezifische Organisation tätig oder sind als Intermediäre für die Vermittlung von Inhalten an diese Zielgruppe verantwortlich (z.B. Lehrpersonen als

Intermediäre zu Kindern und Jugendlichen). Zur Vermeidung von Interessenskonflikten bei der Empfehlung von guten Kompetenzbildungsangeboten wurden Vertreter von Bildungsinstitutionen nicht als Intermediäre einer Zielgruppe befragt.

Die Expertenbefragung, welche im November 2014 abgeschlossen wurde, haben die Koordinationsstelle NCS (ISB/MELANI), das BAKOM, das EDA und der Dachverband economiesuisse durchgeführt. Zudem hat das iimt der Universität Fribourg im Auftrag des BAKOM die Befragung einer ausgewählten Gruppe von Grossen Unternehmen sowie Kleinen und Mittleren Unternehmen (KMU) vorgenommen.

Die Befragung wurde auf Deutsch oder Französisch durchgeführt. Die Form waren persönliche Interviews, Telefoninterviews oder schriftliche Interviews. Die Dauer der Befragung belief sich in der Regel auf eine halbe Stunde. Als Instrument diente ein Interviewleitfaden, den das iimt für diesen Zweck erstellt hat und welcher für spezifische Zielgruppen angepasst wurde.[3]

[3] Vgl. Anhang 1.

5. Zusammenfassung der Expertenbefragung

Abbildung 2 stellt die Zusammensetzung des Untersuchungsgegenstands (Samples) dar. Die Gruppe „Grosse Unternehmen" stellt mit etwa 25% der Gesamtheit die grösste Einzelzielgruppe dar, dies kann auf die getroffenen Aussagen die Gesamtheit betreffend zu Verzerrungen führen. Die Verzerrung ist jedoch in der Einbettung der wahrgenommenen Cyber-Risiken zu vernachlässigen, da die Trends der Aussagen sich über alle Zielgruppen ähnlich verteilen.

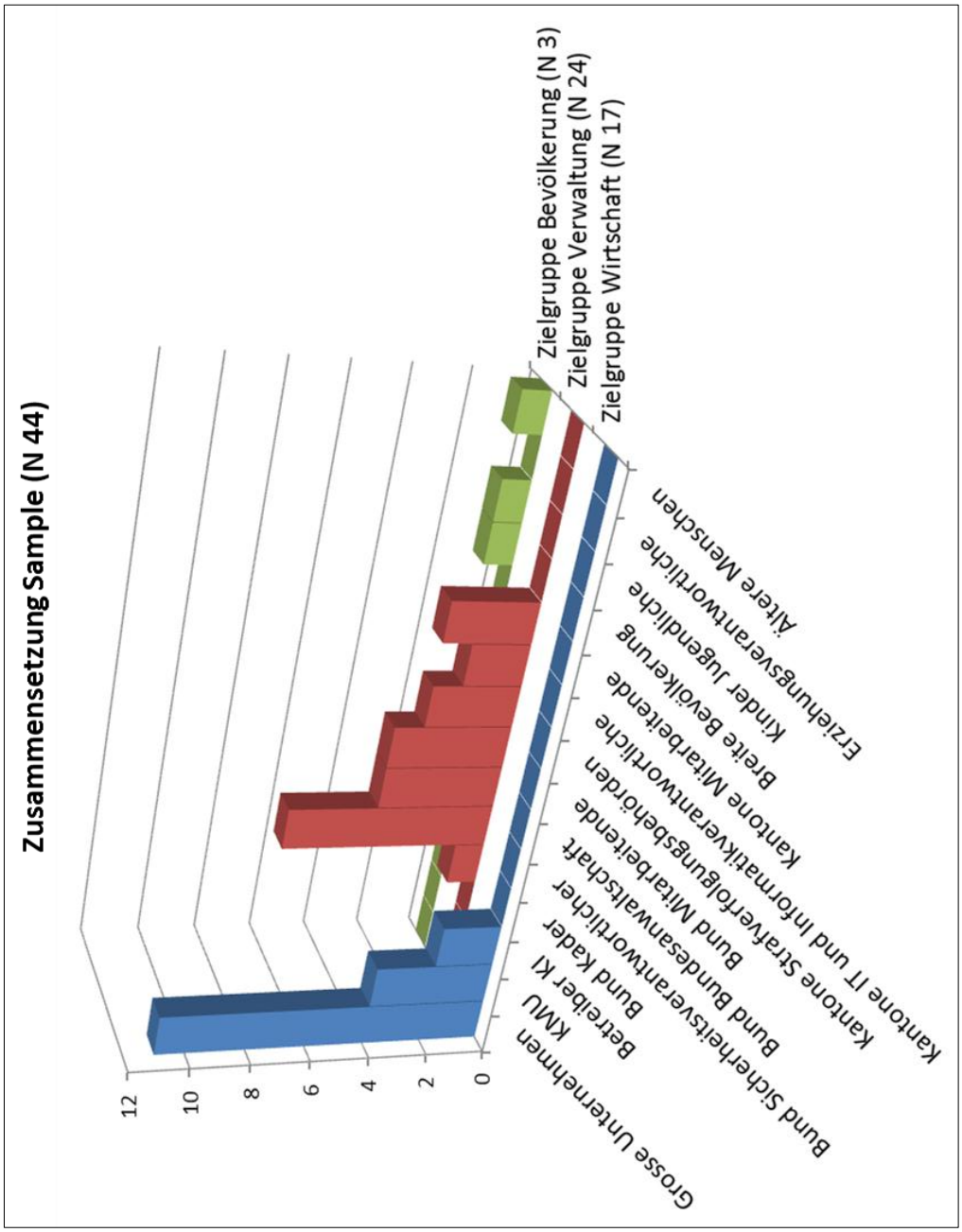


Abbildung 2: Zusammensetzung Sample.

5.1. Zielgruppe Wirtschaft

Um der heterogen und umfangreichen Stichprobe Wirtschaft Rechnung zu tragen, wurde für diese Zielgruppe die Befragung in drei Untergruppen aufgeteilt: Grosse Unternehmen, KMU und Betreiber kritischer Infrastrukturen (KI-Betreiber)[4]. Ihr Bedrohungspotential und der sich daraus ergebende Schutzbedarf ist ebenso verschiedenartig wie auch die personellen und finanziellen Möglichkeiten, sich mit den notwendigen Kompetenzen gegen Cyber-Risiken abzusichern. Ein grosses Unternehmen hat möglicherweise eine andere Angriffsfläche, aber auch andere Schutzmöglichkeiten (Ressourcen) als ein KMU.

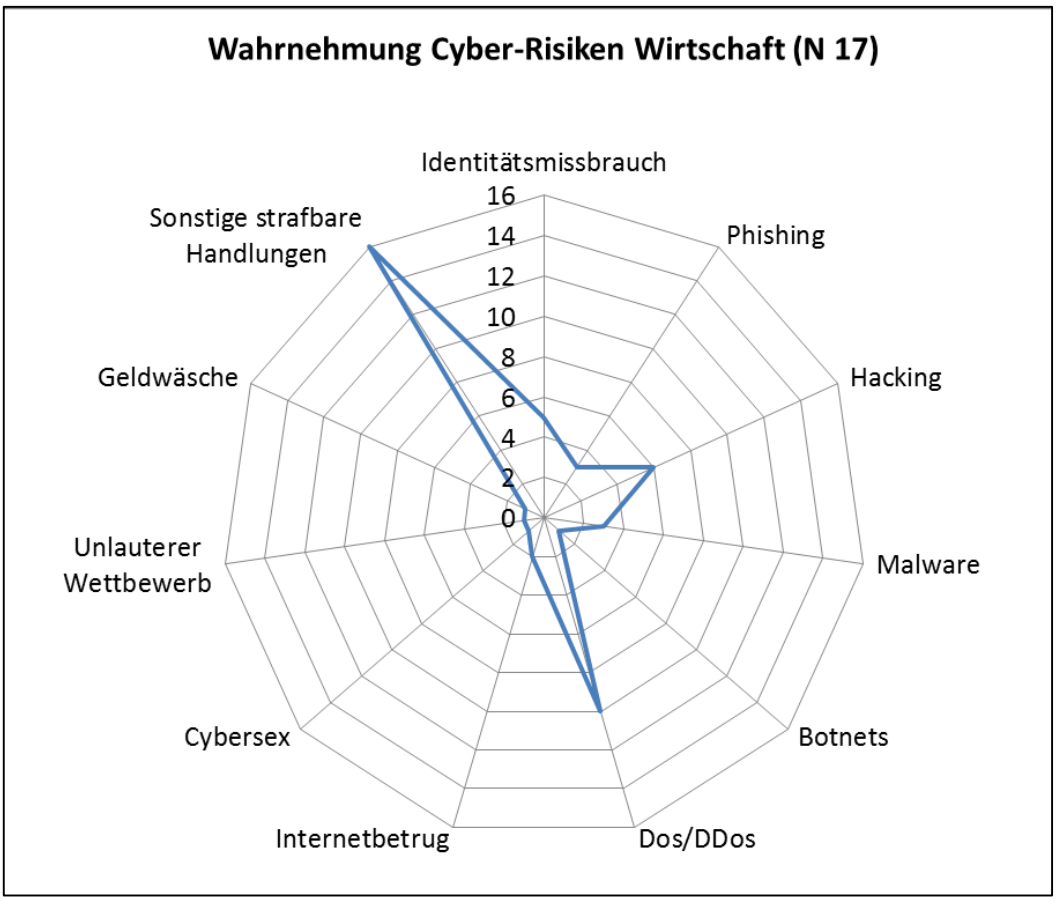


Abbildung 3: Wahrnehmung CR Cluster Wirtschaft.

Abbildung 3 verdeutlicht die Einbettung in die von KOBIK (2014) definierten Formen der Internetkriminalität[5]. Auffällig ist die starke Ausprägung im Cluster „sons-

[4] Kritische Infrastrukturen stellen die Verfügbarkeit von essenziellen Gütern und Dienstleistungen, wie etwa Energie, Kommunikation oder Verkehr, sicher. Grossflächige Ausfälle wirken sich schwerwiegend auf die Bevölkerung und die Wirtschaft aus. Ebenso beeinträchtigen sie die Sicherheit und das Wohlergehen des Staates. (vgl. Nationale Strategie zum Schutz Kritischer Infrastruktur, Bern, 2012)

[5] Spasojevic, M. Formen der Internetkriminalität, Eidgenössisches Justiz- und Polizeidepartement, Bern, 2014

tige strafbare Handlungen". Diese Ausprägung wird im Folgenden noch genauer dargestellt und untersucht werden.

Aufgrund der Vielzahl an Nennungen wird an dieser Stelle empfohlen über eine Neuformulierung der Überbegriffe, resp. der Formen nachzudenken. Eine klare Zuordnung ist oftmals nur schwer durchführbar, da eine Vielzahl an Straftatbeständen einen anderen bedingt. Beispielsweise *Hacking* als Mittel für ein *unbefugtes Eindringen in ein Datenverarbeitungssystem*.

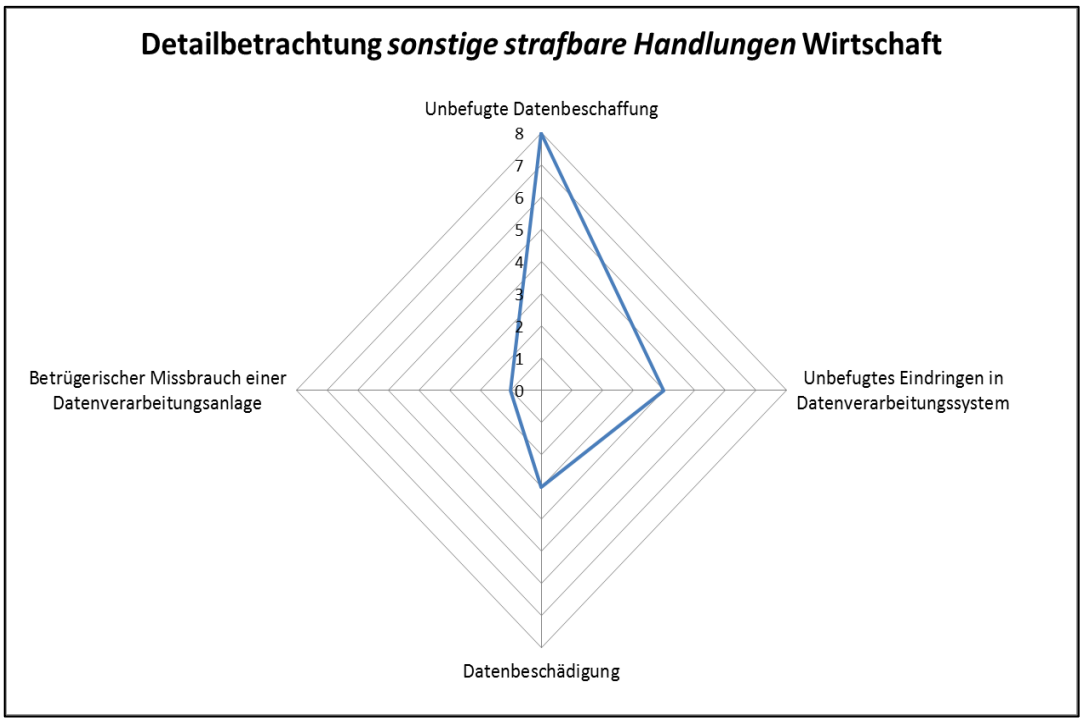


Abbildung 4: Detail strafbare Handlungen Wirtschaft.

Abbildung 4 verdeutlicht die wahrgenommenen Cyber-Risiken in der Tiefe. Eine detailliertere Betrachtung hat sich als sinnvoll erwiesen, da 16 Nennungen direkt diesem Bereich zugeordnet werden konnten. Das grösste wahrgenommene Risiko wurde von den Expertinnen und Experten des Samples Wirtschaft in der potentiellen Datenbeschaffung durch Unbefugte gesehen (z.B. Spionage).[6] Die Art und Weise der unbefugten Datenbeschaffung kann beispielsweise durch Hacking, Phishing etc. als auch durch internen Datenverlust subsumiert werden.

Die Expertengespräche haben zusammengefasst zu den im Folgenden dargestellten Ergebnissen geführt.

[6] Sonstige strafbare Handlungen vgl. (Spasojevic, M., 2014). Tatbestand Pornografie wurde wegen fehlender Relevanz gestrichen. Tatbestand Cybersex subsumiert bspw. potentielle Angriffsfläche durch kompromittierendes Bildmaterial oder den Browser als Einfallstor für Viren etc.

5.1.1. Grosse Unternehmen

Ein grosses Unternehmen beschäftigt 250 oder mehr Vollzeitäquivalente (Bundesamt für Statistik BFS).

Art der wahrgenommenen Cyber-Risiken:

Grosse Unternehmen sind je nach ihrer wirtschaftlichen Ausrichtung verschieden stark von Cyber-Risiken betroffen. Die relevantesten Risiken sind: (Kunden-) Datenverlust; Datendiebstahl für den Weiterverkauf oder für Wirtschaftsspionage; Manipulationen (intern und extern); Cyber-Attacken durch Hacker (insbes. Phishing, Viren, DDos).

Notwendige Fähigkeiten zur Wahrnehmung/Beurteilung und Bearbeitung von Cyber-Risiken:

- Technisches Wissen in Kombination mit vernetztem und unternehmerischem Denken, auch für die effektive Kommunikation der Sicherheits-Belange an die Geschäftsleitung.
- CEO: Unternehmen so organisieren, dass die Sicherheitsbelange integral angegangen und in die Geschäftsprozesse eingebaut werden (z.B. via CSO)
- Externe Leistungserbringer: Zertifizierung (ISACA und ISO 2700x-Serie).

Angebotslücken:

- Angebote richten sich primär an IT-Fachspezialisten. Die Kompetenzbildung nach einem interdisziplinären Ansatz fehlt, so z.B. zur Schulung von mit Compliance und Datenschutz oder Kommunikation befassten Mitarbeitenden.
- Es fehlen Ausbildungsmöglichkeiten für das Profil des Vermittlers zwischen der Technik und dem Business (oft C-Level), damit die Sicherheit den Business-Prozess unterstützt.

5.1.2. KMU

Ein KMU beschäftigt bis zu 249 Vollzeitäquivalente (Bundesamt für Statistik BFS).

Art der wahrgenommenen Cyber-Risiken:

KMU sind je nach ihrer marktwirtschaftlichen Ausrichtung sehr bis kaum von Cyber-Risiken betroffen. Unterschieden werden unternehmensinterne und -externe Risiken. Die relevantesten Risiken sind: Wirtschaftsspionage; Cyber-Attacken auf die Infrastruktur (DDos u.a.) und Datendiebstahl, welche bis auf DDos Attacken hauptsächlich im Bereich der sonstigen strafbaren Handlungen anzusiedeln sind.

Notwendige Fähigkeiten zur Wahrnehmung/Beurteilung und Bearbeitung von Cyber-Risiken:

- Hohe Risikoaversion, adäquate Risiko- und Vorfalleinschätzung, Aktivierung geeigneter Schutzmassnahmen, Anfordern von Unterstützung durch externe Expertinnen und Experten (bei Bedarf), nicht-technikaffinen Vorgesetzten die Betriebsrisiken verständlich machen.
- Externe Leistungserbringer: Zertifizierung (ISACA, ISO 2700x-Serie, BSI-Standards).

Angebotslücken:

- Angebote für den adäquaten Umgang mit persönlichen Daten an der Schnittstelle zwischen Privat- und Berufsleben sind kaum vorhanden: Guidelines wären wünschenswert.
- Kompetenzbildungsangebote eingebettet in Wettbewerbe wären wünschenswert und fehlen weitgehend.

5.1.3. Betreiber kritischer Infrastrukturen (KI–Betreiber)

Diese Zielgruppe umfasst die KI-Betreiber der Teilsektoren der Privatwirtschaft mit sehr grosser Kritikalität.

Art der wahrgenommenen Cyber-Risiken:

Jede Organisation muss sich in ihrem Normalbetrieb gegen das Grundrauschen der Cyber-Risiken schützen, so gegen Störungen durch Unfälle oder Naturkatastrophen und ungezielter Angriffe. Von grosser Wichtigkeit für KI-Betreiber ist aber der Schutz vor gezielten Angriffen auf die Verfügbarkeit und Integrität von IKT-Diensten. Die primären Risiken sind: Erpressung (DDos-Attacken, Drohungen mit Daten- oder Systemmanipulation, insbesondere bei Steuerungssystemen), Datenabfluss (Spionage, Suche nach Schwachstellen durch regierungsähnliche Organisationen, Innentäter-Problematik) und Manipulation/Sabotage (von KI-Systemen, inkl. Steuerungssystemen – aber auch Angriffe auf schlecht geschützte Umsysteme).

Notwendige Fähigkeiten zur Wahrnehmung/Beurteilung und Bearbeitung von Cyber-Risiken:

- Risiken und die Security ganzheitlich zu erfassen und sich nicht auf technische Massnahmen an einzelnen Systemen oder Prozessen zu beschränken.
- Durchsetzung der Zugangsberechtigungen in der Organisation durch Etablierung der Prozesse und des Wissens rund um die Informationssicherheit/den Informationsschutz.

- Analytische Fähigkeiten zur Identifikation des Schutzbedarfs.
- Schutz vor Cyber-Attacken: Detektion (Monitoring), Reaktion (Incident Handling), Notfallplanung (v.a. im Bereich Datenfluss) und Prävention (inkl. Pflegen einer Fehler- und Austauschkultur, auch in subsidiärer Zusammenarbeit mit privaten und staatlichen Organisationen).
- CERTs: Perspektivenwechsel hin zur Sicht des Angreifers, Konzept und Design von Hardware-Komponenten und ihren Sicherheitsimplikationen, von Betriebssystemen, von Anwendungssoftware, Design und Analyse von Netzwerkprotokollen, Kryptologie, Reverse Engineering von Hardware und Software (inkl. Malware), Entwicklung von Sicherheitstools, digitale Forensik, Incident Management, Vulnerability Discovery und Management.

Angebotslücken:

- In der Schweiz sind kaum Kompetenzbildungsangebote für die Schulung der CERT-Fähigkeiten vorhanden.

5.2. Zielgruppe Verwaltung

Staatliche Behörden und Verwaltungen aller Ebenen sind ebenfalls potentielle Ziele von Cyber-Angriffen, welche ihre Funktion als Legislative, Exekutive oder Judikative beeinträchtigen. Zudem sind sie auch Betreiber und Nutzer von kritischen Infrastrukturen, die es zu schützen gilt. Entsprechend wurde die Zielgruppe aufgeteilt in Bund und Kantone und dann in verschiedene Rollen oder Aufgabengebiete.

Die Ergebnisse der Expertengespräche sind zusammengefasst in Abbildung 5 dargestellt.

Die Wahrnehmung der Cyber-Risiken auf Seiten der Verwaltung zeigt ein ähnliches Bild wie bei den Befragten der Zielgruppe Wirtschaft. Je nach Verantwortungsbereich und Position ist die Wahrnehmung der Cyber-Risiken verschieden. Detailliertere Beschreibungen finden sich in den Zusammenfassungen der einzelnen Zielgruppen. Das hohe Mass an sonstigen strafbaren Handlungen wird auch in diesem Fall detaillierter aufgezeichnet.

Abbildung 6 zeigt die hohe Wahrnehmung der Befragten gegenüber potentiellen Cyber-Risiken wie unbefugter Datenbeschaffung und unbefugtes Eindringen in Datenverarbeitungssysteme.

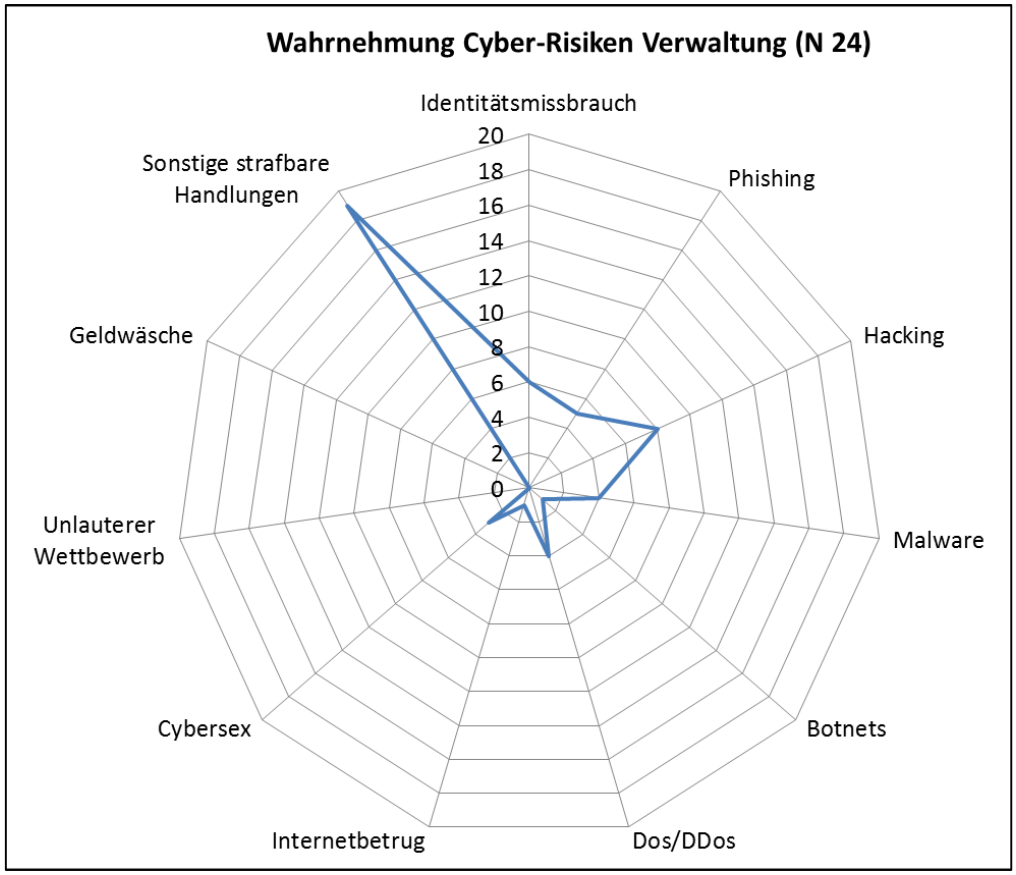


Abbildung 5: Wahrnehmung CR Cluster Verwaltung.

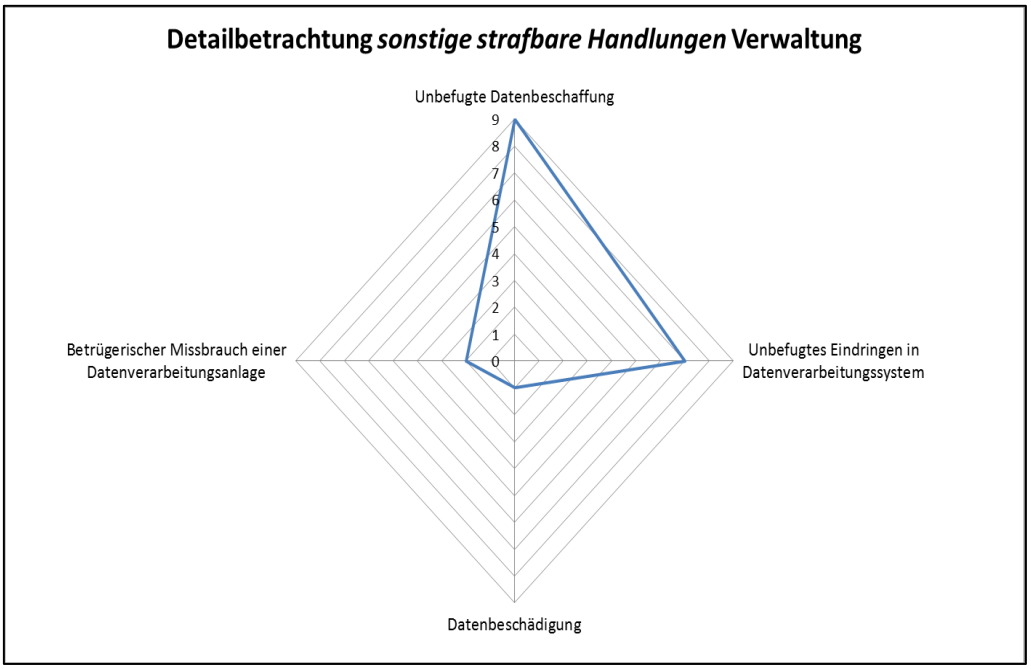


Abbildung 6: Detail strafbare Handlung Verwaltung.

5.2.1. Bund: Kader

Art der wahrgenommenen Cyber-Risiken:

Kader sind für das Geschäft verantwortlich und tragen deshalb die (Rest-)Risiken – von den finanziellen bis hin zu den operativen Risiken. Ein grosser Teil der operativen Risiken beinhaltet aufgrund der starken Vernetzung der Prozesse auch das Cyber-Risiko.

Notwendige Fähigkeiten zur Wahrnehmung/Beurteilung und Bearbeitung von Cyber-Risiken:

- Die Relevanz von Risiken für das Geschäft einzuschätzen; Sicherheit in die Geschäftsprozesse einbauen, um diese effizienter zu gestalten; mit den Instrumenten zur Risikosteuerung arbeiten (Risikomanagement ist Chefsache).

Angebotslücken:

- Systematische Schulungen für mittleres Kader. E-Learning zu Informationssicherheit ist in Planung.

5.2.2. Bund: Sicherheitsverantwortliche

Die Sicherheitsverantwortlichen im Bund umfassen Informatiksicherheitsbeauftragte (ISBD/ISBO), Datenschutzbeauftragte, Informationsschutzbeauftragte, Objektsicherheitsbeauftragte, technische Analytiker und Sicherheits-Engineers des CSIRTS und weitere mit der Sicherheit/Risiken von Prozessen befasste Personen.

Art der wahrgenommenen Cyber-Risiken:

Gezielte Angriffe auf die IKT-Infrastruktur durch Angreifer, auch solchen mit hohen Budgets (Regierungsorganisationen, Kriminelle) zur Schaffung von Datenzugang für Spionage; Datenverlust; Innentäter-Problematik in Bezug auf Datenabfluss; kommerzielles Interesse an Daten für den Weiterverkauf; Angriffe auf die Verfügbarkeit und Integrität von IKT-Diensten der Bundesverwaltung; Erpressung durch Hacker; Datenschutz- und Persönlichkeitsverletzungen.

Notwendige Fähigkeiten zur Wahrnehmung/Beurteilung und Bearbeitung von Cyber-Risiken:

- Abläufe und kritische Geschäftsprozesse im Bund verstehen.
- Mut, den Entscheidungsträgern Risiken aufzuzeigen.
- Technisches, organisatorisches wie auch Management-Fachwissen zu IT-Security und Datenschutz.

- Erarbeitung der Dokumentationen zum Schutz personenbezogener Daten für verwaltungsrelevante Prozesse.
- Zusammenarbeit und Informationsaustausch mit anderen relevanten Akteuren wie MELANI, CSIRT BIT, ISBO/ISBD.
- Verständnis der Gefahren im Cyberraum strategisch-konzeptuell und nicht nur technisch.
- CSIRT: Praktische Erfahrung im Bereich System Engineering und Betrieb sowie im Netzwerkbereich, Kenntnis im Bereich der Log-Analyse, Intrusion Detection and Prevention, Malware-Analyse, IT Forensics auf gängigen Plattformen, Web Application Security, Firewalls, Mobile Security, Cloud Security, u.a.
- Externe Leistungserbringer: Zertifizierung von Produkten und Betrieb.

Angebotslücken:

- Vergleichbare Angebote zu den SANS-Kursen in der Schweiz.
- Ausbildungen für Brückenbauerfunktionen zwischen IKT-Fachbereichen und Entscheidungsträgern des Managements zur Vermittlung der Sicherheitsanforderungen (inkl. Restrisiko).
- Kurse für die Erweiterung des Blickfelds von IT-Risiken auf den Schutz kritischer Infrastrukturen in der Schweiz („grosses Bild").
- Mehrtägige Job-Rotationen für einen Einblick in andere Bundesstellen (z.B. Rochade zwischen ISBOs).

5.2.3. Bund: Bundesanwaltschaft

Art der wahrgenommenen Cyber-Risiken:

Gezielte Angriffe zur Informationsbeschaffung im Zusammenhang mit laufenden Verfahren, Innentäter-Problematik in Bezug auf Datenabfluss; Aneignung sensibler Daten; Problematik des Persönlichkeitsrechts bekannter Personen. Nichtbefolgen oder zu wenig Beachtung von Direktiven und Guidelines.

Notwendige Fähigkeiten zur Wahrnehmung/Beurteilung und Bearbeitung von Cyber-Risiken:

- *Bereich Strafverfolgung*:
  Erfahrung und Ausbildungsbereitschaft, technische Affinität sowie forensisches und juristisches Wissen.
- *Bereich Informationssicherheit*:
  Erkennen von Risiken und Einschätzungen der Relevanz von Vorfällen; Governance-Prozesse etablieren und diese bewusst leben; Technisches, organisatorisches wie auch Management-Fachwissen zu IT-Security und Da-

tenschutz; Zusammenarbeit und Informationsaustausch (Vernetzung) mit Partnern.

Angebotslücken:

- Ausbildung von einem Doppelprofil das Forensik und Jura kombiniert bspw. „Jurist und Cyber-Ermittler", Sensibilisierung für dieses Thema.

5.2.4. Bund: Mitarbeitende

Art der wahrgenommenen Cyber-Risiken:

Ungezielte Angriffe von aussen; gezielte Angriffe via Social Engineering; Überforderung durch technische Komplexität.

Notwendige Fähigkeiten zur Wahrnehmung/Beurteilung und Bearbeitung von Cyber-Risiken:

- Grundschutzmassnahmen adäquat umsetzen.
- Informationsschutz-Vorgaben einhalten (so auch zum Umgang mit elektronischen Informationen).

Angebotslücken:

- Amtsinterne, regelmässig wiederkehrende Ausbildungen in den Ämtern zur Informationssicherheit (ev. Organisation via EPA).

5.2.5. Kantone: Strafverfolgungsbehörden

Art der wahrgenommenen Cyber-Risiken:

Gezielte Angriffe zur Informationsbeschaffung von Personendaten, insbesondere aus kantonalen Fahndungsdatenbanken. Informationsbeschaffung und Manipulation von laufenden Ermittlungen. Unsicherheitsfaktor einer sicheren Datenübermittlung.

Notwendige Fähigkeiten zur Wahrnehmung/Beurteilung und Bearbeitung von Cyber-Risiken:

- technische Grundkompetenzen, Bereitschaft zum Selbststudium, interkantonale Zusammenarbeit, internationale Vernetzung.
- Grundsätzliche Wahrnehmung / Awareness des Problems ist erforderlich

Angebotslücken:

- Ausbildung einer Kombination von Forensik und Jura
- Weiterbildung der Justiz in der Schweiz
- Nachdiplomstudium für Polizeikräfte, das in die Tiefe geht
- Sensibilisierung für diesen Themenkreis

5.2.6. Kantone: IT- und Informatiksicherheitsverantwortliche

Art der wahrgenommenen Cyber-Risiken:

Gezielte Angriffe via Internet auf Fachapplikationen (z.B. Steuerportal, guichet virtuel); Datendiebstahl; Phishing; Wartung der IKT-Mittel; menschliche Fehlmanipulationen sowie nicht erkannte Angriffe und ihre Folgen.

Notwendige Fähigkeiten zur Wahrnehmung/Beurteilung und Bearbeitung von Cyber-Risiken:

- Kombiniertes Wissen von Technik und Management, Kenntnisse der rechtlichen Rahmenbedingungen, Kommunikationskompetenz und Überzeugungskraft.
- Profundes Wissen über die Geschäftsprozesse der kantonalen Verwaltung und über ihre Infrastrukturen, langjährige Erfahrung im Netzwerkbetrieb, System-Monitoring, gute Einschätzung der Vorfallrelevanz, forensische Fähigkeiten.
- Enge Zusammenarbeit mit IT-Sicherheitsverantwortlichen anderer Kantone und mit MELANI.
- Externe Leistungserbringer: Zertifizierung (ISO 2700x-Serie).

Angebotslücken:

- Keine Nennungen.

5.2.7. Kantone: Mitarbeitende

Art der wahrgenommenen Cyber-Risiken:

Unbefugter Zugang auf vertrauliche Daten durch nicht berechtigte Personen (via Social Engineering oder Phishing); Datenmanipulationen; Verlust der Verfügbarkeit des internen Netzes.

Notwendige Fähigkeiten zur Wahrnehmung/Beurteilung und Bearbeitung von Cyber-Risiken:

- Mitarbeiter- und aufgabenspezifische Fähigkeiten sind gefragt. Je mehr Kompetenzen ein Mitarbeitender hat, je mehr Mail-Kontakt nach aussen besteht, desto häufiger ist dies mit dem Zugriff auf kritische Applikationen verbunden.
- Grundawareness auf der ganzen Breite ist erforderlich.

Angebotslücken:

- Es fehlen Angebote, die auf das jeweilige Umfeld/den jeweiligen Bedarf des Mitarbeitenden zugeschnitten sind.

- Schulung von Gerichtspräsidenten
- Schulung von HR-Abteilungen (sind oft ein Einfallstor)

5.3. Zielgruppe Bevölkerung

Cyber-Risiken betreffen auch die Bevölkerung mit allen individuellen Nutzern privater und beruflicher Informations- und Kommunikationssysteme sowie kritischer Infrastrukturen. Eine wirksame Strategie gegen Cyber-Risiken muss auch dem individuellen Verhalten und dessen Risiken Rechnung tragen. Denn auch in der Bevölkerung gilt: Wissen schafft Handlungssicherheit im Umgang mit Cyber-Risiken und kann vor bösen Überraschungen schützen.

Die Ergebnisse der Expertengespräche sind zusammengefasst in Abbildung 7 dargestellt.

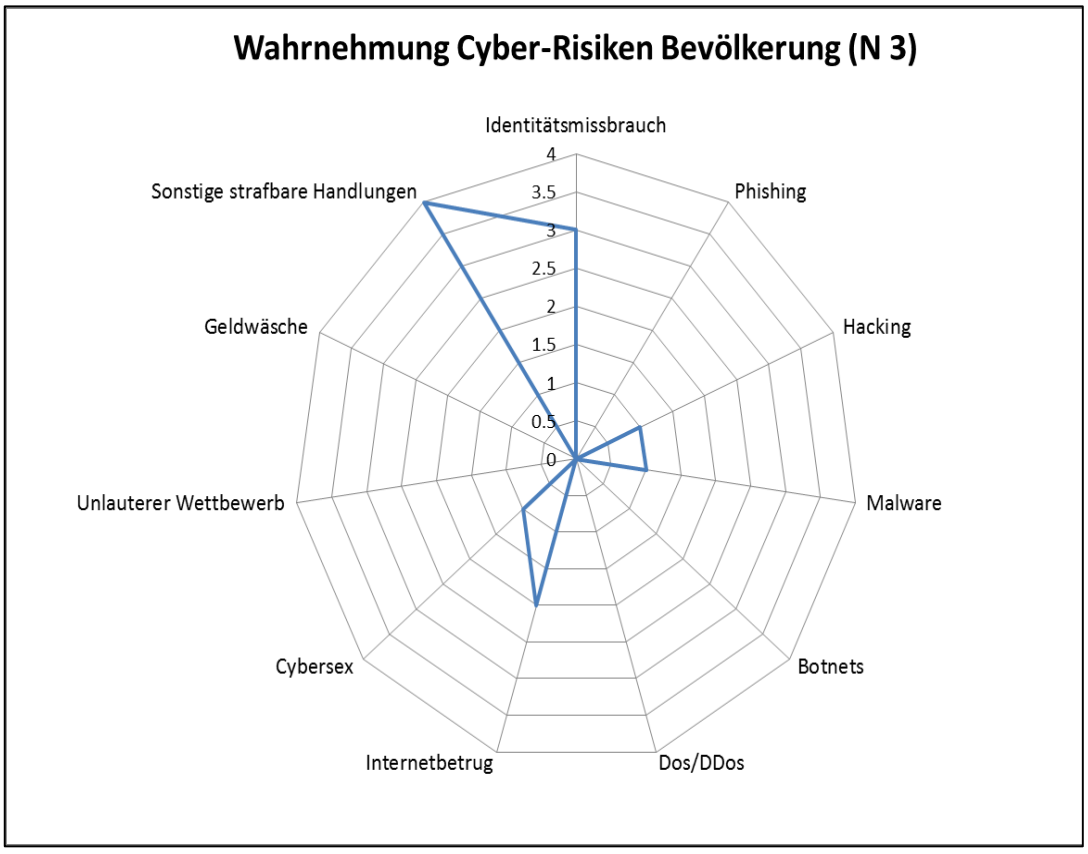


Abbildung 7: Wahrnehmung CR Cluster Bevölkerung.

5.3.1. Breite Bevölkerung

Die Zielgruppe der breiten Bevölkerung umfasst Menschen in der Schweiz jeder Nationalität, jedes Alters und mit jeder Tätigkeit.

Art der wahrgenommenen Cyber-Risiken:

Betrug, Abzocke, Phishing, Identitätsdiebstahl, Grenzüberschreitung von der legalen zur illegalen Pornografie, Romance Scam (Heiratsschwindel online), Cyberstalking, Sextorsion (professionelle Erpressung mit Nacktbildern im Internet).

Notwendige Fähigkeiten zur Wahrnehmung/Beurteilung und Bearbeitung von Cyber-Risiken:

- Basiswissen zum Funktionieren des Internets und E-Mails und des Missbrauchspotentials (z.B. Frage der Anonymität, Möglichkeiten zum Verändern von Fotos, Sicherheit von https://, etc.). Wissen zu Phishing, Cookies, Regeln für sicheres Chatten (z.B. Wahl des Nicknames) und für das Verwenden persönlicher Daten und zum „digitalen Fussabdruck" der Daten-Gesamtheit, Wissen zur Strafbarkeit von sexueller Belästigung und anderen Bedrohungen im Internet.

Angebotslücken:

- Keine Angebotslücken genannt.

5.3.2. Kinder und Jugendliche

Art der wahrgenommenen Cyber-Risiken:

Sexuelle Belästigung (Grooming), Pornografie (Jugendschutz), Sexting, Cybermobbing, Sextorsion durch Bekannte (Erpressung mit Nacktbildern im Internet). Zudem aber auch, wie bei der breiten Bevölkerung: Betrug, Abzocke, Phishing und Identitätsdiebstahl.

Notwendige Fähigkeiten zur Wahrnehmung/Beurteilung und Bearbeitung von Cyber-Risiken:

- Schutz persönlicher Daten; Kenntnis der Organisationen und Personen, die Hilfe anbieten.

Angebotslücken:

- Material zur Sensibilisierung kleinerer Kinder (3-9 Jährige) für die ersten Schritte im Netz. Ideal wäre Material analog zur Verkehrserziehung.

- Informationsmaterialien für Kinder und Jugendliche in sonderpädagogischen Kinder- und Jugendinstitutionen, weil sie über die Regelschule nicht erreicht werden.

5.3.3. Erziehungs- und Bildungsverantwortliche

Eltern, Lehrpersonen, Lehrmeister, Jugendarbeiter und weitere Personen sind als Erziehungs- und Bildungsverantwortliche für Kinder und Jugendliche auch für die Kompetenzvermittlung im Umgang mit Cyber-Risiken zuständig. Die Sensibilisierung und Schulung von Erziehungs- und Bildungsverantwortlichen ist mindestens genauso wichtig, wie die von Kindern und Jugendlichen.

Aufgrund des Bedarfs richtet sich heute eine grosse Zahl von Kompetenzbildungsangeboten an diese Zielgruppen (vgl. www.jugendundmedien.ch). Die Initiative zur Sensibilisierung von Eltern geht dabei in der Regel von einzelnen Schulen aus und ist nicht systematisch. Der Kompetenzbildungsbedarf der Lehrpersonen wird zudem weiter zunehmen, weil die neuen sprachregionalen Lehrpläne eine Verankerung von Medienerziehung (oder allenfalls auch Computer-Programmieren) im Schulunterricht vorsehen.

Art der wahrgenommenen Cyber-Risiken:

(vgl. Abschnitt Kinder und Jugendliche)

Notwendige Fähigkeiten zur Wahrnehmung/Beurteilung und Bearbeitung von Cyber-Risiken:

- Sensibilisierung von Kindern und Jugendlichen, Vermitteln von Wissen zu Spuren im Internet und spezifischen Schutzvorkehrungen gegen Cyber-Risiken, Hilfestellung bei Bedrohung und Übergriffen. Regulierung des Medienkonsums von Kindern.

Angebotslücken:

- Während es für Lehrpersonen viele öffentliche und private Angebote gibt (die Kantone sind hier zuständig), sind die Angebote im Bereich der Elternarbeit weit weniger entwickelt. Hier fehlt weitgehend das Schulungsmaterial für Eltern in Migrationssprachen und bildungsferne Eltern.
- Informationsmaterial für Jugendliche, die via Schulen und weitere öffentliche Angebote schwer erreichbar sind, z.B. weil sie in einer sozialpädagogischen Einrichtung sind.
- Es fehlen für den Bereich der Kinder- und Jugendinstitutionen Konzepte und Leitlinien mit fachlich fundierten, auf die spezifische Situation des (sozialpädagogischen) Kontextes zugeschnittenen Informationen. Auch fehlen

Grundlagen für Leitungspersonen und Sozialpädagogen/innen, die in der stationären und teilstationären Kinder- und Jugendhilfe arbeiten.

- Angebote zum Thema Internetpornografie für Kinder und Jugendliche, aber auch für Eltern und Erziehungsberechtigte. Hier sind insbesondere die rechtlichen Grenzen des jugendlichen Pornokonsums zu wenig bekannt.

5.3.4. Ältere Menschen

Zu beachten ist, dass sich das 4. Lebensalter (80+) noch kaum im Internet bewegt; die Angaben unten beziehen sich auf die sog. „Silver Surfer" (50+).

Art der wahrgenommenen Cyber-Risiken:

Betrug, Abzocke, Phishing; Identitätsdiebstahl, illegale Pornografie, Romance Scam (Heiratsschwindel online), Cyberstalking, Sextorsion (professionelle Erpressung mit Nacktbildern im Internet). Generell sind ältere Personen aber nicht eine spezielle Zielgruppe für Cyber-Attacken. Sie sind jedoch eventuell eher bereit, auf Aufforderung hin persönliche Daten bekannt zu geben oder vertragliche Verpflichtungen einzugehen.

Notwendige Fähigkeiten zur Wahrnehmung/Beurteilung und Bearbeitung von Cyber-Risiken:

- Grundkenntnisse zu Cyber-Risiken und deren Folgen, technisches Wissen über Sicherheitseinstellungen der genutzten Endgeräte, Wissen um Verhaltensregeln im Problemfall.

Angebotslücken:

- Zusammenstellung von Informationen (z.B. Broschüre) spezifisch für die Zielgruppe ältere Menschen rund um die Sicherheit im Internet.

6. Zusammenfassung Angebotslücken

Die durch die Experteninterviews identifizierten Angebotslücken sind in Abbildung 8 dargestellt. Dabei ist bemerkenswert, dass offensichtlich ein Angebotsdefizit im Bereich „Awareness & Culture" existiert. Die Angebotslücken „Technische Sanktionen", „In-house Kompetenzen" und „Ressourcen" wurden von den Expertinnen und Experten vorwiegend innerbetrieblich gesehen und beziehen sich so nicht auf Angebotslücken die durch Angebote des freien Markts gedeckt werden müssten.

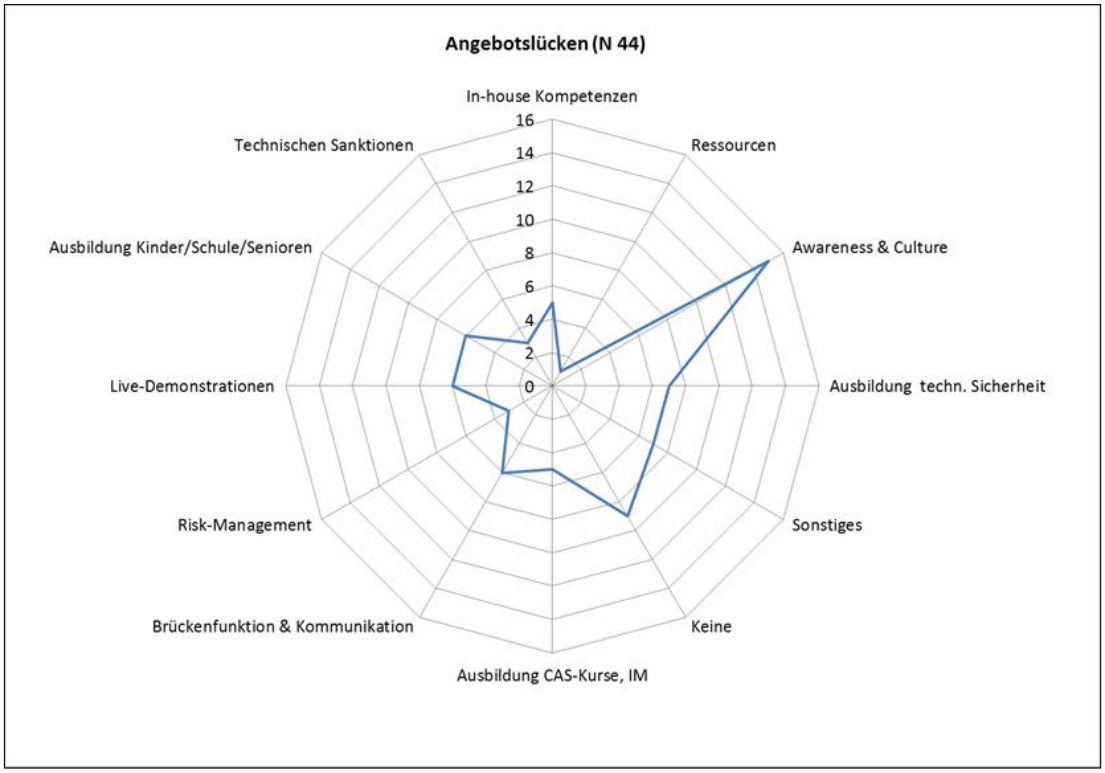


Abbildung 8: Identifizierte Angebotslücken.

In einer zweiten Betrachtungsrunde wurden die in Abbildung 8 dargestellten Angebotslücken auf Grund der in den Interviews gemachten Angaben genauer gefasst und nach folgenden Kriterien kategorisiert (vergl. Abbildung 9):

- Innerbetrieblich
- Ausbildung Kultur & Kommunikation
- Ausbildung Technik
- Ausbildung Allgemein
- Keine wahrgenommenen Angebotslücken
- Diverses
- Keine Angaben

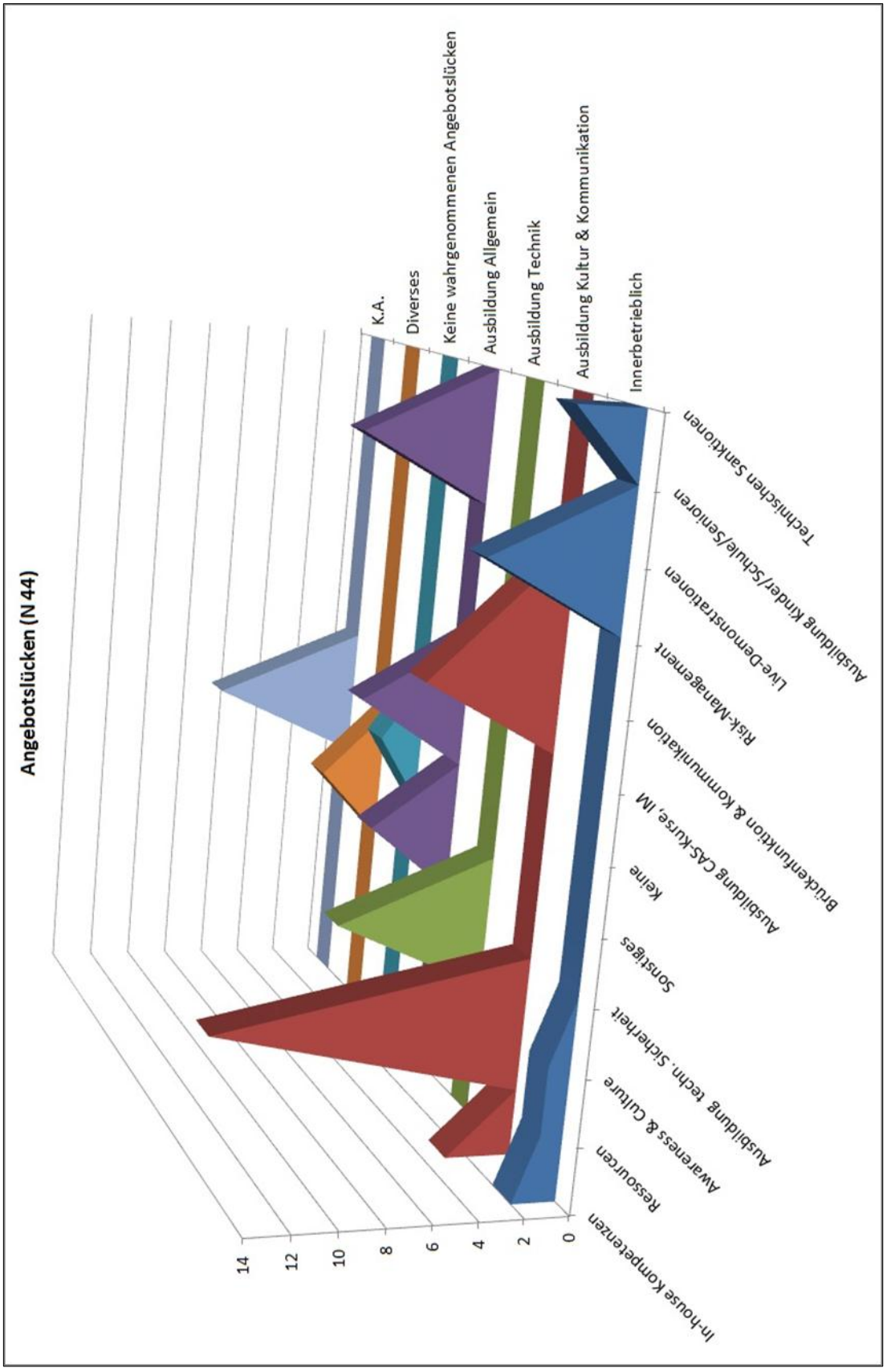


Abbildung 9: Identifizierte Angebotslücken nach Kategorien.

Diese Betrachtungsweise lässt erkennen, dass die Oberkategorie Ausbildung mit gut 70% der Nennungen ein massives Defizit darstellt. Allerdings muss auch anmerkt werden, dass rund 18% der Nennungen Diverse bzw. keine Angaben gemacht haben.

Abbildung 9 stellt die von den Expertinnen und Experten identifizierten Angebotslücken zusammenfassend dar. Es werden Kompetenzen und kategorisierte Angebotsdefizite in einer Darstellung beschrieben, die Ziffern entsprechen der Zuordnung der jeweiligen Antworten.

Die grössten Angebotslücken können in der Beziehung zwischen dem Angebotsdefizit „Ausbildung Kultur & Kommunikation" und den Kompetenzen „Awareness & Culture" sowie der „Brückenbaufunktion" und „Risk-Management" subsumiert werden. Angebotsdefizite „Innerbetrieblich" sowie in der „Ausbildung Technik" spiegeln die von den Expertinnen und Experten angesprochenen Lücken in Zertifizierungen und fehlende CAS, CERT und SAS Angeboten wieder.

Da in diesen Befragungen ausgewählte, hochqualifizierte Fachleute involviert waren, müssen den Aussagen zu den Angebotslücken gewisse Bedeutung zugemessen werden. So ist bemerkenswert, dass in den Expertennennungen neben technischen Aspekten vor allem auch der Aspekt der Sicherheitskultur in den Organisationen genannt wurde. Es lässt darauf schliessen, dass gegebenenfalls das Bewusstsein für das Gefahrenpotenzial nicht durchgängig vorhanden ist und mittels einer Implementierung und der ständigen Überprüfung einer solchen Sicherheitskultur in den Organisationen gestärkt werden muss.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Informatiksteuerungsorgan des Bundes ISB
Melde- und Analysestelle Informationssicherung

Ka Schuppisser, 9. April 2014

Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken NCS

Massnahme 7: Kompetenzbildungsangebote im Umgang mit Cyber-Risiken - Gute Praktiken im Überblick

Auftrag, Vorgehen und Interviewleitfaden

Inhaltsverzeichnis

1 Auftrag und Zielsetzung

Die Strategie zum Schutz der Schweiz vor Cyber-Risiken verfolgt mit 16 Massnahmen das Ziel, die Cyber-Resilienz in der Schweiz zu erhöhen.

Um Cyber-Risiken zu erkennen und den Lebens- und Wirtschaftsraum davor zu schützen, müssen Menschen über spezifische Kenntnisse verfügen: So ist eine verstärkte Ausbildung von IKT-Sicherheitsspezialisten notwendig, um Netze zu überwachen, die Bedrohungslage zu analysieren und bei einem Vorfall entsprechend reagieren zu können. Ebenso wichtig ist die laufende Weiterbildung aller IKT-Fachkräfte in Sicherheitsbelangen. Weiter gilt es, bei den Strafverfolgungsbehörden das juristisch-technische Fachwissen im Zusammenhang mit Cyber-Delikten zu stärken. Und in der Bevölkerung wird ein solides Sicherheits-Verständnis benötigt, um sich vor Cyber-Risiken zu schützen. Der Schutz der Privatsphäre steht hier ebenso im Fokus, wie der Schutz privater IKT-Systeme, über welche andernfalls Angriffe auf kritische Infrastrukturen vorgenommen werden könnten. Mit der Massnahme 7 „Kompetenzbildungsangebote im Umgang mit Cyber-Risiken“ hat der Bundesrat der Wichtigkeit des Auf- und Ausbaus dieser Fähigkeiten Rechnung getragen.[1]

Heute gibt es bereits eine Vielzahl von Kompetenzbildungsangeboten zum Schutz vor Cyber-Risiken: Kampagnen, Studiengänge, Lehrbücher, Websites und vieles mehr. Die bestehenden Kompetenzbildungsangebote sind aber einerseits noch zu wenig bekannt und andererseits ist es schwierig, darunter für die eigene Anspruchsgruppe die geeigneten Angebote von hoher Qualität auszumachen.

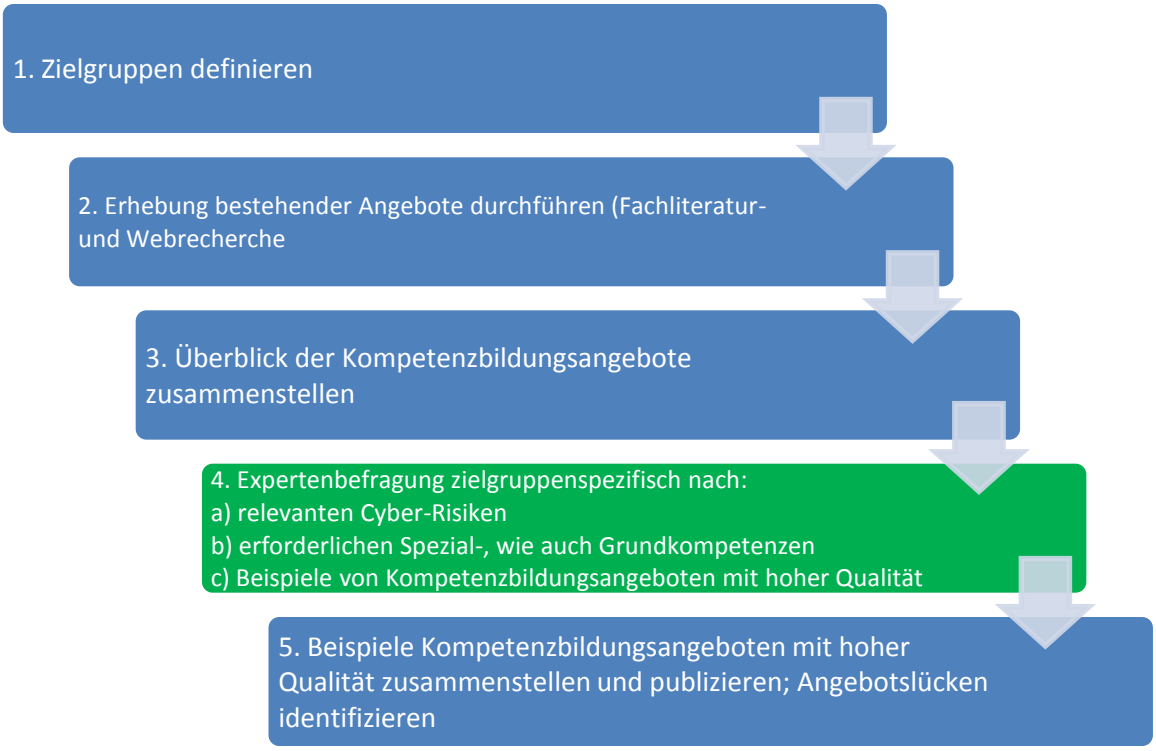
Die Massnahme 7 verfolgt deshalb das Ziel, Wirtschaft, Verwaltung und Bevölkerung bedarfsgerecht über qualitativ hochwertige Kompetenzbildungsangebote zum Umgang mit Cyber-Risiken zu informieren. Zudem sollen allfällige Angebotslücken aufgezeigt werden.

2 Methode und Vorgehen

Die notwendigen Kompetenzen im Umgang mit Cyber-Risiken sind vielgestaltig und unterscheiden sich stark aufgrund der Schutzziele und der Aufgaben und Verantwortlichkeiten der Menschen in Wirtschaft, Verwaltung und Zivilgesellschaft. Bei der Durchführung des Erhebungs-Teils der Arbeit fiel die Entscheidung deshalb auf einen zielgruppenspezifischen Ansatz mit einem qualitativen Vorgehen durch Expertenbefragungen und einer umfassenden Fachliteratur- und Internetrecherche.
Die Wahl eines qualitativen Vorgehens erlaubt es, den Erhebungsprozess sehr offen zu gestalten, was angesichts des noch wenig untersuchten Themengebietes sinnvoll erschien. Andererseits bedeutet die Wahl eines qualitativen Verfahrens auch, dass keine repräsentativen Aussagen gemacht werden können. So ist auch die Nennung der Kompetenzbildungsangebote mit hoher Qualität, welche von den Expertinnen und Experten für ihre Zielgruppe hervorgehoben werden, eine exemplarische und nicht eine abschliessende.

[1] Details des Auftrags Massnahme 7 siehe NCS-Strategie (S. 38/39) und NCS-Umsetzungsplan (S. 23): http://www.isb.admin.ch/themen/01709/

Folgende Vorgehensschritte wurden gewählt:



Grafik 1: Vorgehen Umsetzung NCS-Massnahme 7

3 Umsetzung

3.1 Zielgruppen

Die Strategie definiert ihre Zielgruppen breit und einfach: Akteure aus Wirtschaft, Verwaltung und Zivilgesellschaft sollen in der Schweiz die Cyber-Risiken minimieren können. Die Zielgruppen wurden verfeinert und folgendermassen definiert:

Zielgruppe Zivilgesellschaft
Breite Bevölkerung
Erziehungs- und Bildungsverantwortliche als Intermediäre zu Kindern und Jugendlichen (so Eltern, Lehrpersonen, Lehrmeister, u.a.)
Kinder und Jugendliche
Ältere Menschen

Zielgruppe Verwaltung
Bund: Kader
Bund: Sicherheitsverantwortliche (Botschaften, Grenzwachtkorps, Informatiksicherheitsbeauftragte, Datenschutzberater/-beauftragte, Objektsicherheitsbeauftragte, u.a.)
Bund: Bundesanwaltschaft
Bund: Mitarbeitende
Kanton: Strafverfolgungsbehörden (Kantonspolizei, Staatsanwaltschaften, Gerichte, u.a.)
Kanton/grosse Städte: IT- und Informatiksicherheits-Verantwortliche
Kanton/grosse Städte: Mitarbeitende

Zielgruppe Wirtschaft
Grosse Unternehmen
KMU: Auswahl von Branchen mit hohem Grad an Kommunikation/Interaktion
Betreiber kritischer Infrastrukturen[2]

3.2 Expertenbefragung

Für die Zielgruppen wurden Expertinnen und Experten identifiziert und gezielt auf die Cyber-Risiken einer Zielgruppe hin befragt.

Die Expertenbefragung deckt folgende Themen ab:

a) relevante Cyber-Risiken: Die Strategie definiert nicht genau, zu welchen bestehenden Cyber-Risiken die Kompetenzen gebildet werden sollen bzw. welche Angebote gesammelt werden sollen. Für jede Zielgruppe gibt es hier je nach Fokus anders gelagerte Kompetenzen im technischen, rechtlichen, organisatorischen, pädagogischen und betriebswirtschaftlichen, wie auch in weiteren Bereichen.

b) erforderliche Spezial-, wie auch Grundkompetenzen: Jede Zielgruppe benötigt gewisse grundlegende Kompetenzen (Grundkompetenzen) genauso wie spezifische Kompetenzen (Spezialkompetenzen). Bei der Expertenbefragung wird als Ergebnis die Nennung von maximal 5 Kernkompetenzen pro Zielgruppe erwartet. Diese dienen zur Reduktion des Fächers der bestehenden Kompetenzbildungsangebote, welche in einem nächsten Schritt erhoben werden.

c) bestehende best practice-Beispiele: Hier interessiert die persönliche Meinung der befragten Expertinnen und Experten, welche der bestehenden Angebote sie als best practice-Beispiele ihrer Zielgruppe weiterempfehlen würden.

d) Angebotslücken: Es ist zu erwarten, dass nicht für jede als notwendig erachtete Kompetenz einer Zielgruppen ein entsprechendes, gut zugängliches Angebot besteht. Die Expertinnen und Experten werden hier zu den Angebotslücken befragt.

Die Befragung erfolgte grösstenteils in der Form von Telefoninterviews, aber auch durch persönliche Interviews. Als Instrument diente ein Interviewleitfaden, den das „international institute of management in technology (iimt)“ der Universität Fribourg für diesen Zweck erstellt hat und der für spezifische Zielgruppen ausgebaut und angepasst wurde.

-> Der Interviewleitfaden findet sich im Anhang dieses Dokuments
(Anhang 1: Interviewleitfaden für von Cyber-Risiken direkt betroffenen Organisationen; Anhang 2: Interviewleitfaden für Vermittler von Zielgruppen, welche durch Cyber-Risiken betroffen sind).

[2] KI-Betreiber der Teilsektoren mit sehr grosser Kritikalität und Spitäler, wie auch ihre Zulieferer: Stromversorgung, Erdölversorgung, Banken, Informationstechnologien, Telekommunikation, Wasserversorgung, Schienenverkehr, Strassenverkehr. vgl. Nationale Strategie zum Schutz kritischer Infrastrukturen, BABS, 27. Juni 2012, S. 7719, http://www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/themen/ski.parsysrelated1.82246.downloadList.6453.DownloadFile.tmp/natstratski2012d.pdf.

Anhang 1:
Interviewleitfaden für von Cyber-Risiken direkt betroffene Organisationen

1. Relevante Cyber-Risiken in Ihrem Bereich:

1 a. Welche Cyber-Risiken sehen Sie für Ihre Organisation?

1 b. Wie stark sind Sie im operativen Bereich Cyber-Risiken ausgesetzt?

1 c. Verfügen Sie über interne Dokumente/Leitfäden/Standards im Umgang mit Cyber-Risiken / Cyber-Attacken?
-> Wenn positive Antwort weiter bei 1d, sonst bei 1e

1 d. Verfügen Sie über eine Sicherheits-Zertifizierung? Wenn ja welche?

1.1 Cyber-Sicherheit:

1 e. Wer ist in Ihrer Organisation für den Schutz vor Cyber-Risiken verantwortlich?

1 f. Beziehung zu Geschäftspartnern/Lieferanten. Wird hier eine Sensibilisierung zu den Cyber-Risiken vorgenommen beziehungsweise machen Sie oder erhalten Sie Vorgaben?

2. Erforderliche Kompetenzen

2 a. Kennen Sie Schulungs-/Bildungsangebote zur Thematik Cyber-Risiken?
-> Nachfrage z.B. Berufsverbände, (Fach)Hochschulen etc.

2 b. Haben Sie persönlich ein Weiterbildungsangebot bez. Cyber-Risiken wahrgenommen?

2 c. Bieten Sie für ihre Mitarbeitenden Schulungen/Weiterbildungen in diesem Thema an? Wenn ja, welche (intern/extern)?

2 d. Haben Sie in Ihrer Organisation eine ICT-Sicherheitskultur etabliert oder existiert eine ICT-Sicherheitspolitik in Ihrem Unternehmen?

2 e. Welche Fähigkeiten bedarf es Ihrer Meinung nach für die Bewältigung von Cyber-Risiken?
-> Nachfrage nach Grundkompetenzen und Spezialkompetenzen

3. Best-Practice Beispiele

3 a. Kennen Sie Best-Practice Beispiele in diesem Zusammenhang?

3 b. Sind Sie auf diesbezügliche Angebotslücken gestossen?

Anhang 2:
Interviewleitfaden für Vermittler zu Zielgruppen, die von Cyber-Risiken betroffen sind

1. Relevante Cyber-Risiken in Ihrem Bereich:

1 a. Welche Cyber-Risiken sehen Sie für Ihre Zielgruppe?

1 b. Wie stark ist Ihre Zielgruppe im operativen Bereich/im täglichen Leben Cyber-Risiken ausgesetzt?

1 c. Verfügen Sie für Ihre Zielgruppe über Dokumente/Leitfäden/Standards im Umgang mit Cyber-Risiken / Cyber-Attacken?

1 d. Beziehung zu Vermittlern/Fachpersonen (z.B. Bildungsverantwortliche als Vermittler zu Jugendlichen). Wird bei den Vermittlern eine Sensibilisierung zu den Cyber-Risiken vorgenommen beziehungsweise erhalten diese Vorgaben?

2. Erforderliche Kompetenzen

2 a. Kennen Sie Schulungs-/Bildungsangebote zur Thematik Cyber-Risiken?
-> Nachfrage z.B. Berufsverbände, (Fach)Hochschulen etc.

2 b. Haben Sie persönlich ein Weiterbildungsangebot bez. Cyber-Risiken wahrgenommen?

2 c. Bieten Sie für Ihre Zielgruppe Schulungen/Weiterbildungen in diesem Thema an? Wenn ja, welche (intern/extern)?

2 d. Haben Sie für Ihre Zielgruppe Regeln für eine ICT-Sicherheitskultur etabliert?

2 e. Welche Fähigkeiten bedarf Ihre Zielgruppe Ihrer Meinung nach für die Bewältigung von Cyber-Risiken?
-> Nachfrage nach Grundkompetenzen und Spezialkompetenzen

3. Best-Practice Beispiele

3 a. Kennen Sie Best-Practice Beispiele in diesem Zusammenhang?

3 b. Sind Sie auf diesbezügliche Angebotslücken gestossen?

Anhang 3 – Weiterführende Literatur

Im Folgenden sind aus der Vielzahl der vorhandenen Beiträge zum Themenkreis einige beachtenswerte Referenzen zusammengestellt (Stand April 2014). Diese wurden unter dem Gesichtspunkt ausgewählt, dass erfolgversprechendes Cyber-Risiko Management mehr bedeutet, als die Implementierung einer technischen Applikation.

[CARD2011] A. Cárdenas, S. Amin, Z. Lin, Y. Huang, C. Huang, S. Sastry: Attacks Against Process Control Systems: Risk Assessment, Detection, and Response. Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security (ASIACCS '11), Hong Kong, 2011.
http://dl.acm.org/citation.cfm?id=1966959

[ENISA2012a] European Network and Information Security Agency: National Cyber Security Strategies - Practical Guide on Development and Execution. ENISA, Heraklion, 2012.
http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide

[ENISA2012b] European Network and Information Security Agency: National Cyber Security Strategies - Setting the course for national efforts to strengthen security in cyberspace. ENISA, Heraklion, 2012.
http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide

[GOOD2013] C. Goodwin, J. Nicholas: Developing a National Strategy for Cyber-security. Microsoft Corp., Redmond, 2013.
http://www.google.ch/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CD4QFjAB&url=http%3A%2F%2Fdownload.microsoft.com%2Fdownload%2FB%2FF%2F0%2FBF05DA49-7127-4C05-BFE8-0063DAB88F72%2FDeveloping_a_National_Strategy_for_Cybersecurity.pdf&ei=lRsPU477F6aNywOt2oHYBA&usg=AFQjCNHXi7y5Mp25n9vcjl0asq4exuVLAg&bvm=bv.61965928,d.bGQ

[ITU2012] International Telecommunications Unit: The ITU National Cybersecurity Strategy Guide. ITU, Geneva, 2012. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

[JULI2012] K. Julisch: Understanding and overcoming cyber security anti-patterns. Journal on Computer Networks, Vol. 57, 2013, pp. 2206 – 2211. http://www.sciencedirect.com/science/article/pii/S1389128613000388

[KOUN2010] J. Kouns, D. Minoli: Information Technology Risk Management in Enterprise Environments – A Review of Industry Practices. John Wiley & Sons, Hoboken, 2010. http://eu.wiley.com/WileyCDA/WileyTitle/productCd-0471762547.html

[KRIT2010] E. Kritzinger, S. von Solms: Cyber security for home users: A new way of protection through awareness enforcement. Journal of Computers & Security, Volume 29, Issue 8, 2010, pp. 840–847 http://www.sciencedirect.com/science/article/pii/S0167404810000775

[LECL2013] J. LeClair, S. Abraham, L.Shih: An Interdisciplinary Approach to Educating an Effective Cyber Security Workforce. Proceedings of the InfoSecCD '13: Information Security Curriculum Development Conference, Kennesaw, 2013. http://dl.acm.org/citation.cfm?id=2528923

[LUII2013] E. Luiijf, K. Besseling, P. De Graaf: Nineteen national cyber security strategies. International Journal of Critical Infrastructures, Volume 9, Issue 1, pp. 3-31, 2013. http://www.inderscience.com/info/inarticle.php?artid=51608

[NICH2011] A. Nicholson, S. Webber, S. Dyer, T. Patel, H. Janicke: SCADA security in the light of Cyber-Warfare. Journal of Computers and Security, Volume 31, 2012, pp. 418 – 436. http://www.sciencedirect.com/science/article/pii/S0167404812000429

[NCSC2013] National Cyber Security Centre: Cyber Security Assessment Nether-lands. National Cyber Security Centre, The Hague, 2013. https://www.google.ch/search?q=National+Cyber+Security+Centre:+Cyber+Security+Assessment+Nether-lands&ie=utf-8&oe=utf-8&rls=org.mozilla:en-US:official&client=firefox-a&gfe_rd=ctrl&ei=gxcPU9ncMabD8gf0yYHgCA&gws_rd=cr#q=National+Cyber+Security+Centre:+Cyber+Security+Assessment+Netherlands&rls=org.mozilla:en-US:official&spell=1

[NRECA2011] National Rural Electric Cooperative Association: Guide to Develop-ing a Cyber Security and Risk Mitigation Plan. Dulles, 2011. https://www.smartgrid.gov/sites/default/files/doc/files/CyberSecurityGuideforanElectricCooperativeV11-2%5B1%5D.pdf

[PFLE2012] S. Pfleeger, D. Caputo: Leveraging Behavioral Science to Mitigate Cyber Security Risk. Journal of Computers and Security, Volume 31, 2012, pp. 597–611. http://www.sciencedirect.com/science/article/pii/S0167404811001659

[SOLM2013] R. von Solms, J. van Niekerk: From information security to cyber security. Journal of Computers and Security, Vol. 38, 2013, pp. 97 – 102. http://ac.els-cdn.com/S0167404813000801/1-s2.0-S0167404813000801-main.pdf?_tid=35497348-9fa0-11e3-b1c7-00000aacb362&acdnat=1393499798_b90774ced2f9d1c1df8bed2ceba725f4

[WANG2013] W. Wang, Z. Lu: Cyber security in the Smart Grid: Survey and chal-lenges. Journal of Computer Networks, Vol. 57, 2013, pp. 1344 – 1371. http://www.sciencedirect.com/science/article/pii/S1389128613000042