BEST AT Roadmap

BEST AT
Vertrauen rechtfertigen:
sichere Systeme

Walter Hötzendorfer - Universität Wien
Mario Meir Huber - IDC Austria
Rupert Lemmel-Seedorf – OCG
Romana Riegler - Research Institute
Erich Schweighofer - Universität Wien
Simon Tjoa - FH St. Pölten
Christof Tschohl - Research Institute

Wien, November 2015

bmvit
Bundesministerium für Verkehr, Innovation und Technologie

Projektkoordinator:

IDC Austria

Projektpartner:

Universität Wien, FH St. Pölten, Research Institute, Österreichische Computergesellschaft

Die Studie ist im Zeitraum von 2014 – 2015 im Rahmen des Projektes BEST AT entstanden. Das Projekt wurde gefördert im Rahmen des Programms „IKT der Zukunft“ durch das Bundesministerium für Verkehr, Innovation und Technologie (BMVIT), abgewickelt durch die Österreichische Forschungsförderungsgesellschaft mbH (FFG).

Executive Summary

Digital information, information systems, and related applications now influence privacy, society, and the economy more than ever before. Information and communication technologies (ICT) are found in smart homes, automotive engineering, cities of the future, industrial production lines, and agriculture. New business models, fast innovation cycles, and technologies including cloud computing, big data, and the Internet of Things, as well as changing user behavior due to social networks and mobile devices, bring new challenges for ICT security. Malware, access to sensitive information, and highly specialized cyberattacks are only some of the dangers we face. For these reasons, security and safety, reliability, and the legal security of systems have become key subjects for research and development (R&D).

To cope with security challenges and requirements, the "BEST-AT" study is developing a comprehensive technology roadmap for Austria. It formulates strong research questions and recommends future R&D projects to achieve the best possible ICT security. The design, development, and demonstration of emerging technologies following the concepts of "security by design" and "secure engineering" are high priorities. Research is required not only to prevent danger as part of a long-term security strategy, but to react to threats in case of emergency in a fast and efficient way. Another suggested focus of research is data security. The protection of privacy and digital identity should take safety, security, reliability, legality, and user friendliness into account. A third area of research should focus on the motives of cybercriminals, such as lucrative models of cybercrime, to better understand attackers and to be able to set appropriate countermeasures. The development and control of clear legal frameworks, security standards, and reference models complements the above-mentioned research areas. Ultimately, knowledge transfer is a key asset, since no adequate protection can be achieved without knowledge of potential hazards, safety awareness, or the acceptance of security solutions by ICT users.

Kurzzusammenfassung

Informationssysteme, digitalisierte Informationen und damit verbundene Anwendungen beeinflussen unsere Privatsphäre, Gesellschaft und Wirtschaft mehr denn je. Informations- und Kommunikationstechnologien (IKT) halten Einzug in Smart Homes, in die Fahrzeugtechnik, in die Stadt der Zukunft, in industrielle Fertigungsanlagen und in die Landwirtschaft. Neue Geschäftsmodelle, rasche Innovationszyklen und Technologien wie Cloud Computing, Big Data und Internet of Things sowie die Veränderung des Nutzerinnenverhaltens durch soziale Netzwerke und mobile Geräte bringen aber auch neue Herausforderungen an die Informationssicherheit mit sich. Schadprogramme, Zugriffe auf sensitive Informationen, bis hin zu gezielten und hochspezialisierten Cyberangriffen stellen nur einige der Bedrohungen dar, wodurch Angriffs- (security) und Betriebssicherheit (safety), Zuverlässigkeit sowie rechtliche Sicherheit von Systemen zu zentralen Gegenständen für Forschung und Entwicklung (F&E) werden.

Um Sicherheitsanforderungen gerecht zu werden, wird im Rahmen der Studie „BEST-AT“ eine umfassende Technologie-Roadmap erarbeitet. Die Studie liefert konkrete Forschungsfragen und Empfehlungen für zukünftige F&E-Vorhaben in Österreich zur Erreichung einer bestmöglichen IKT-Sicherheit. Neben der Konzeption, Entwicklung und Demonstration neuer Technologien im Sinne von Security by Design und Secure Engineering wird angeregt, in einem weiteren Forschungsschwerpunkt den Fokus auf die Datensicherheit zu legen. Der Schutz der Privatsphäre und der digitalen Identität bei der Nutzung innovativer, datengetriebener Technologien soll unter Berücksichtigung von Sicherheit, Zuverlässigkeit, Rechtmäßigkeit und NutzerInnenfreundlichkeit erfolgen. Gefördert werden sollen sowohl Projekte zur Prävention von Gefahren als Teil einer langfristigen Sicherheitsstrategie, als auch Projekte zur raschen und effizienten Reaktion auf Bedrohungen im Notfall. Ein dritter Forschungsschwerpunkt soll die Motive Cyberkrimineller und allen voran ökonomische Modelle des zum Teil lukrativen Geschäftsfeldes „Cyberkriminalität“ näher beleuchten, um AngreiferInnen besser verstehen und geeignete Gegenmaßnahmen setzen zu können. Die Entwicklung von rechtlichen Rahmenbedingungen, Sicherheitsstandards, Referenzmodellen und Verfahren zur Überprüfung deren Einhaltung ist eine unumgängliche Ergänzung zu den genannten Forschungsschwerpunkten. Abschließend wird dem Bereich Usable Security und der Wissensvermittlung eine hohe Priorität zugesprochen, da ohne Know-how über mögliche Gefahren, ohne Sicherheitsbewusstsein und ohne Akzeptanz von Sicherheitslösungen von Seiten der NutzerInnen kein ausreichender Schutz erreicht werden kann.

Inhalt

1 Einführung

Informationssysteme, digitalisierte Informationen und damit verbundene Anwendungen beeinflussen unsere Privatsphäre, Gesellschaft und Wirtschaft mehr denn je. Die Allgegenwärtigkeit von Informationstechnologie hat zahlreiche neue Einsatzmöglichkeiten geschaffen die vor 20 Jahren nicht denkbar gewesen wären. Den Stellenwert der IT kann man sehr gut an der Entwicklung von IT-Unternehmen am Aktienmarkt demonstrieren. Dieser zeigt, dass Unternehmen wie Facebook, Google, Amazon, IBM, Microsoft und Apple einen höheren Firmenwert als produzierende Unternehmen in anderen Sektoren wie General Motors, Caterpillar, Lockheed Martin oder McDonalds besitzen.

Einhergehend mit der zunehmenden Durchdringung der IT hat die Abhängigkeit von Informationsinfrastrukturen in den letzten zehn Jahren stark zugenommen und damit die Bedeutung der Informationstechnologie für die Volkswirtschaft. Zusätzlich bringen neue Geschäftsmodelle (z.B.: Cloud) rasche Innovationszyklen und Technologien (z.B.: Big Data, Mobile Computing) sowie die Veränderung des Benutzerverhaltens (z.B.: soziale Netzwerke, Video on demand) neue Herausforderungen für die Sicherheit von Informations- und Kommunikationstechnologien (IKT).

Schwerpunkt der Studie ist die Erstellung einer Technologie-Roadmap, welche für bevorstehende Ausschreibungen im österreichischen Förderprogramm „IKT der Zukunft“ mit dem Ausschreibungsschwerpunkt „Vertrauen rechtfertigen: Sichere Systeme“ eine zusätzliche Informationsbasis liefert. Analog zu dem Ausschreibungsschwerpunkt fokussiert diese Studie daher auf die folgenden drei Bereiche:

- Sicherheit
- Zuverlässigkeit
- Datenschutz und Datensicherheit.

Ausgehend von der Bedrohungslandschaft sowie von neuen technologischen Innovationen werden innerhalb dieser Studie Forschungsaspekte und rechtliche Rahmenbedingungen für verschiedene Bereiche (d.h. übergreifende Aspekte, Hardware/physische Assets, Betriebssysteme, Netzwerke, Anwendungen, Informationen[1]) identifiziert.

[1] abgeleitet vom IT Grundschutz des Deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI).

1.1 Methodik

Für die Studie wurde seitens des Projektteams ein mehrstufiges Vorgehensmodell gewählt. In einem ersten Schritt wurde eine umfangreiche Literaturrecherche durchgeführt. Hierbei wurden Quellen aus Wissenschaft, Wirtschaft und Politik herangezogen. Für den Bereich der Emerging Technologies und technologischen Großtrends wurden internationale Technologie-Roadmaps, wissenschaftliche Publikationen sowie Informationen über existierende Ausschreibungen der Europäischen Union und Materialien der IDC herangezogen.

Die dadurch gewonnenen Erkenntnisse bildeten die Basis für einen Workshop, welcher das Ziel verfolgte, Technologietrends und deren Auswirkung auf die technischen, rechtlichen und gesellschaftlichen Sicherheitsaspekte zu diskutieren. Zu diesem Zweck wurden in etwa 40 ExpertInnen aus dem IT-Security-Umfeld herangezogen. TeilnehmerInnen des Workshops waren ExpertInnen aus IT-Geschäftsführung, IT-Projekt- und Servicemanagement, Technik und Beratung aus KMUs und größeren IT-Unternehmen. Ebenso vertreten waren InformationssicherheitsberaterInnen der öffentlichen Verwaltung und VertreterInnen aus der angewandten Forschung. Geographisch kamen die TeilnehmerInnen aus Österreich und der Slowakei. In einer ersten Diskussion zu technischen Aspekten wurden *Bedrohungen und Trends* im Bereich sichere Systeme und Emerging Technologies identifiziert und diskutiert. Diese Ergebnisse sind in Kapitel 2 und 3 dieser Studie eingeflossen. Eine zweite Diskussion beschäftigte sich damit, relevante Forschungsgebiete zu identifizieren, zu priorisieren und die Wichtigkeit der Forschungsgebiete für die Emerging Technologies einzuschätzen. Die Ergebnisse der zweiten Diskussionsrunde lieferten einen wesentlichen Input für die Kapitel 4, 5 und 6 dieser Studie sowie Kapitel 7 – Roadmap.

In der nächsten Phase wurde eine Umfrage mit der Zivilgesellschaft durchgeführt. Hierbei wurden 163 Personen über gesellschaftliche Aspekte von IKT-Sicherheit befragt. Parallel dazu wurden an die 13 qualitative Interviews mit IKT-ExpertInnen aus Wirtschaft und Wissenschaft durchgeführt. Das Ziel der ExpertInneninterviews war es, die bis dato gewonnenen Erkenntnisse zu validieren.

Im vorletzten Schritt wurden die gewonnenen Informationen vom Projektteam ausgewertet und weiterverarbeitet. Daten und Informationen aus all diesen Quellen sind in die einzelnen Kapitel dieser Studie und in Folge in die Ausarbeitung der auf Kapitel 2-6 aufbauenden Roadmap (Kapitel 7) eingeflossen. Der abschließende Schritt stellte die Validierung der Ergebnisse dar, welche durch ausgewählte ExpertInnen und dem Projektteam sichergestellt wurde.

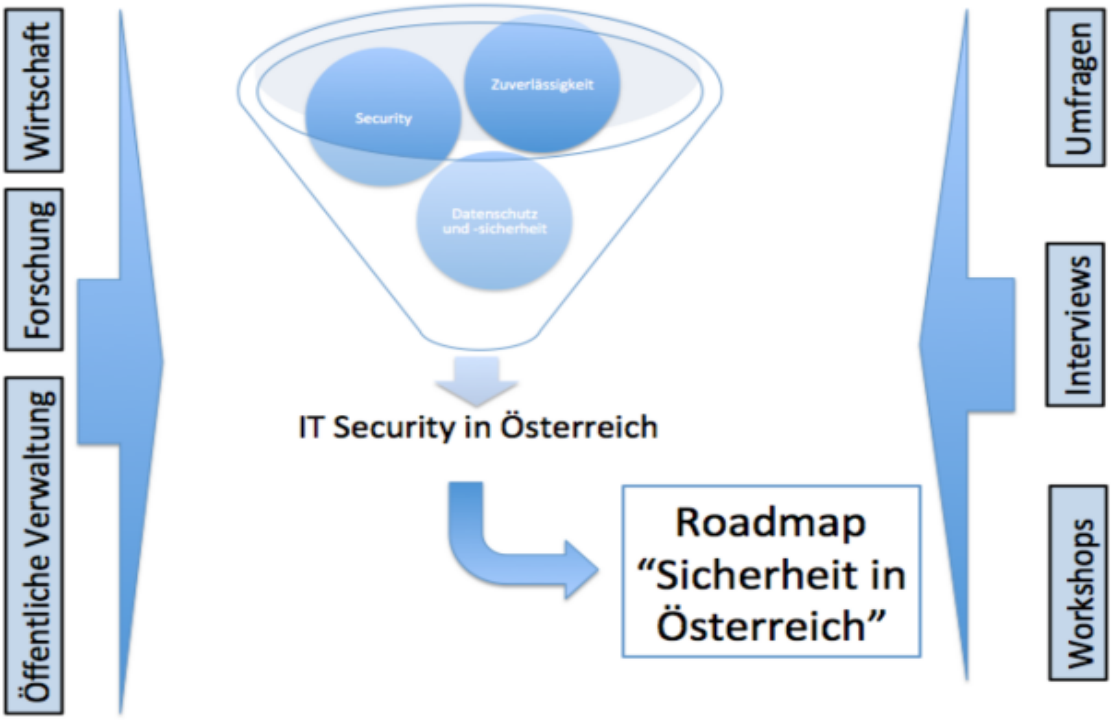


Abbildung 1: Schematische Darstellung der Vorgehensweise

1.2 Aufbau

Der Studienbericht gliedert sich in mehrere Bereiche: im ersten Teil werden aktuelle Fragen hinsichtlich IKT-Sicherheit und Vertrauen beantwortet. Hierbei geht es um Technologien und Entwicklungen, welche in den letzten Jahren bereits vermehrt zu Problemen geführt haben und daher einer verstärkten Aufmerksamkeit bedürfen (Kapitel 2 und 3).

Im zweiten Teil werden wirtschaftlich getriebene Großtrends und Emerging Technologies wie Big Data, Cloud Computing, Social Media, Mobile Devices, etc. vorgestellt. Diese haben eine kurzfristige, mittelfristige bzw. langfristige Relevanz. Sie sind bereits am Markt vertreten, oder es zeichnet sich ab, dass sie in den kommenden Jahren an Bedeutung erlangen werden (Kapitel 4). Kapitel 5 hebt aktuelle und zukünftige Forschungsfelder in den Bereichen Sicherheit, Zuverlässigkeit sowie Datenschutz und Datensicherheit hervor.

In Kapitel 6 liefert der Report Vorschläge für Leuchtturmprojekte im Bereich Sicherheitsforschung entlang der gesamten Wertschöpfungskette. Abschließend fließen die Ergebnisse in Kapitel 7 in eine Technologieroadmap für den Sicherheitsbereich ein.

2 Aktuelle Herausforderungen in der Informationssicherheit

Ziel dieses Kapitels ist die Beschreibung der Herausforderungen und allgemeiner Themenbereiche, welche anhand der Literaturrecherche identifiziert wurden. In einer kürzlich in Österreich, Deutschland und der Schweiz durchgeführten Befragung[2] wurde festgestellt, dass Informationssicherheit für 75% der Unternehmen einen wichtigen bzw. sehr wichtigen Stellenwert hat. Die Gründe hierfür sind die hohe Abhängigkeit (89% stark oder sehr stark abhängig), Gesetze und Branchenrichtlinien sowie der Schutz von Ruf und Marke. Die Wichtigkeit des Themas wird von der Tatsache unterstrichen, dass fast 90% der Befragten angaben, einen Informationssicherheitsvorfall in ihrem Unternehmen gehabt zu haben. Abbildung 2 zeigt die länderspezifische Risikowahrnehmung der befragten TeilnehmerInnen. Ein interessantes Ergebnis ist die hohe Risikowahrnehmung im Bereich zielgerichteter, komplexer und persistenter Angriffe (APT), welche bereits 30% der Befragten als Bedrohung wahrnehmen.

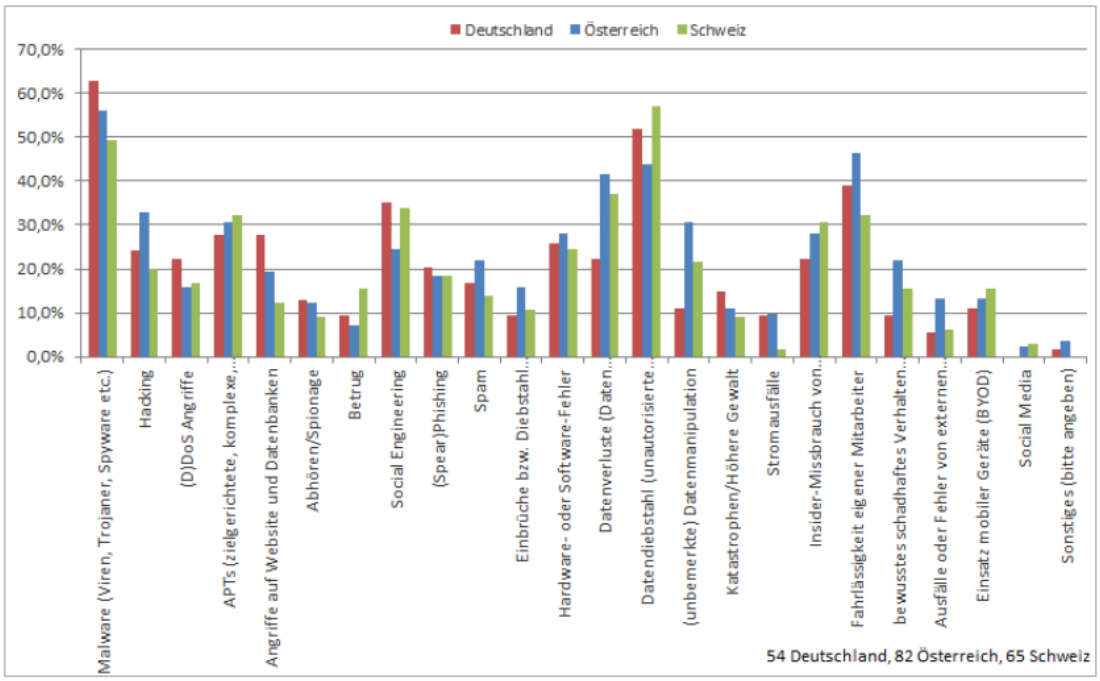


Abbildung 2: Hauptrisiken und Bedrohungen

Weitere Ergebnisse der Studie zeigten, dass Unternehmen zunehmend mobile Geräte (ca. 85%) in Kombination mit Bring Your Own Device (50%) einsetzen und eine Vielzahl von

[2] Vgl. Reisinger, 2015.

Unternehmen Bedarf an der Absicherung von ausgelagerter IT bzw. Cloud Computing Nutzung haben.

In einer weiteren Studie identifizierte das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI)[3,4] welche Herausforderungen sich in der Gegenwart und nahen Zukunft in der Cybersicherheit ergeben. Als Angriffsgruppen erkannte das BSI[5] Cyberkriminelle, Nachrichtendienste, Hacktivisten, Cyberaktivisten und Innentäter. Im Folgenden werden die derzeit gefährlichsten Bedrohungen kurz beschrieben:

SPAM bezeichnet das Versenden von unerwünschten Nachrichten. Abhängig von der Intention des Versenders/der Versenderin können SPAM neben harmlosen Werbeinhalten auch Anhänge mit Schadprogrammen, Links zu Pishingseiten oder zu Webseiten mit Drive-by-Downloads enthalten. Zum Versand der Nachrichten werden meist kompromittierte Rechner eingesetzt.[6]

Schadprogramme kommen in zahlreichen Variationen (z.B.: Viren, Würmer, Trojanische Pferde, Rootkits, Bots) vor. Aktuellen Schätzungen zufolge übersteigt PC-basierte Schadsoftware die 250 Millionen Marke. Auch mobile Plattformen werden immer häufiger Opfer von bösartiger und unerwünschter Software.[7]

Unter **Drive-by-Exploits** versteht man die automatisierte Ausnutzung von Schwachstellen durch den Besuch von präparierten Websites ohne Interaktion des Benutzers[8,9]. Meist kommen bei Drive-by-Exploits sogenannte **Exploit-Kits** zum Einsatz, welche versuchen, Schadprogramme zu installieren. Auch für gezielte Angriffe, auch **Watering-Hole-Angriff** genannt, werden Drive-by-Exploits eingesetzt[10,11].

Als **Botnetz** wird ein Netz an Rechnern bezeichnet, welches über eine Schadsoftware von einem Botnetzbetreiber gesteuert wird. Das Einsatzgebiet von Botnetzwerken ist vielfältig. So spielen sie unter anderem eine wichtige Rolle bei der Durchführung von Distributed-Denial-of-Service-Angriffen, SPAM & Phishing Versand, Informationsdiebstahl oder Online-Banking-Betrug.[12]

[3] Bundesamt für Sicherheit in der Informationssicherheit, 2013.
[4] Bundesamt für Sicherheit in der Informationssicherheit, 2014.
[5] Bundesamt für Sicherheit in der Informationssicherheit, 2014, S. 23ff.
[6] Bundesamt für Sicherheit in der Informationssicherheit, 2014, S. 15.
[7] Bundesamt für Sicherheit in der Informationssicherheit, 2014, S. 16.
[8] Bundesamt für Sicherheit in der Informationssicherheit, 2014, S. 17.
[9] Bundesamt für Sicherheit in der Informationssicherheit, o.J.
[10] Bundesamt für Sicherheit in der Informationssicherheit, 2014, S. 17.
[11] Will Gragido, 2012.
[12] Bundesamt für Sicherheit in der Informationssicherheit, 2014, S. 18.

Social Engineering versucht gezielt menschliche Schwächen auszunutzen, um Zugriff auf sensitive Informationen zu erhalten, oder Personen zu bestimmten Handlungen zu verleiten.[13]

Die unberechtigte Nutzung von personenbezogenen Daten (z.B.: Kreditkartennummern) durch Dritte wird als **Identitätsdiebstahl** bezeichnet. Identitätsdiebstahl wird meist durch Social Engineering, Schadprogramme oder Datenabfluss nach Hacking einer Webseite durchgeführt und zielt oftmals auf finanzielle Vorteile oder vertrauliche Informationen ab.[14]

Denial-of-Service-Angriffe verfolgen das Ziel, einen Dienst oder ein System für berechtigte BenutzerInnen nicht mehr nutzbar zu machen. Wird der Angriff von mehreren Systemen verteilt durchgeführt, spricht man von sogenannten Distributed-Denail-of-Service-Attacken (DDoS).[15]

Advanced Persistent Threats bezeichnen gezielte, hochspezialisierte Cyberangriffe, bei denen der AngreiferInnen versucht, persistent Zugriff zu einem Opfernetzwerk zu bekommen.[16]

Nach Informationen des BSI stellen auch **nachrichtendienstliche Cyberangriffe** eine ernsthafte Bedrohung dar. Genauere Analysen ergaben vier Angriffsvektoren. Diese sind: strategische Aufklärung, individuelle Angriffe, Beeinflussung von Standards und Implementierungen sowie gezielte Manipulation von IT-Equipment.[17]

Zu einem ähnlichen Bild (siehe Tabelle 1) kommt auch der Bedrohungsreport 2014 der europäischen Netzwerk- und Informationssicherheitsagentur (ENISA)[18], welcher die häufigsten Bedrohungen zusammenfasst und aufstrebende technologische Bereiche (z.B.: Cyber-physische Systeme, Internet der Dinge, Mobile Computing) abbildet. Dabei analysiert der Report über 400 verschiedene Quellen und zeigt alle Bedrohungen entlang des Angriffsworkflows/-lebenszyklus.

[13] Bundesamt für Sicherheit in der Informationssicherheit, 2014, S. 19.
[14] Bundesamt für Sicherheit in der Informationssicherheit, 2014, S. 20.
[15] Bundesamt für Sicherheit in der Informationssicherheit, 2014, S. 20.
[16] Bundesamt für Sicherheit in der Informationssicherheit, 2014, S. 21.
[17] Bundesamt für Sicherheit in der Informationssicherheit, 2014, S. 22.
[18] Louis Marinos, 2014.

Empfehlung:

Aufgrund der vorherrschenden Bedrohungslage wird empfohlen, Projekte zu fördern, welche die in Kapitel 2 angeführten Bedrohungen adressieren. Themen umfassen organisatorische und technische Lösungen, welche zur Bekämpfung von Schadprogrammerkennung führen, die digitale Identität schützen sowie der geänderten Bedrohungslage durch gezielte, hochspezialisierte Cyberangriffe entgegenwirken.

Eine genauere Auflistung möglicher Forschungsgebiete ist in Kapitel 5 ersichtlich.

Neben der steigenden Professionalität von AngreiferInnen und ihren Attacken, identifizierte Ernst & Young in ihrem Global Information Security Survey fünf Faktoren, welche es Organisationen zunehmend erschweren Cybersicherheit zu gewährleisten[19]. Diese sind:

- **Ständige Veränderung:** Unternehmen müssen immer schneller reagieren. Neue Produkte, Fusionen sowie die Einführung neuer Technologien nehmen zu und haben Einfluss auf die Cybersicherheit.
- **Mobilität und Consumerization:** Die Kontrolle der Informationstechnologie gerät immer näher an den/die BenutzerIn und entfernt sich damit von der Organisation.
- **Ökosystem:** Digitale Vernetzung nimmt eine immer höhere Bedeutung ein und vergrößert damit die Wahrscheinlichkeit, Opfer von cyberkriminellen Handlungen im privaten und beruflichen Umfeld zu werden.
- **Cloud:** Cloud-basierte Dienste und externe Datenverwaltung durch Dritte führen zu Risiken, die vorher in dieser Form nicht existierten.
- **Infrastruktur:** Viele geschlossene betriebliche Systeme bekommen zunehmend IP-Adressen und erhöhen damit die Angriffsfläche für Cyberangriffe.

[19] Paul van Kessel and Ken Allan, 2014, S.2.

	Top Threats	Current Trends	Top Threats in Emerging Areas						
			Cyber Physical Systems, CIP Systems	Mobile Computing	Cloud Computing	Trust Infrastructure	Big Data	Internet of Things	Network Virtualization
1	Malicious code: Worms/Trojans	↑	↑	↑	↑	↑		↑	↑
2	Web-based attacks	↑	↑	↑	↑	→		↑	
3	Web application attacks/Injection attacks	↑	↑	↑	↑	↑		↑	↑
4	Botnets	↓		↑	↑				
5	Denial of service	↑	↑		→	→		↑	↑
6	SPAM	↓	↑						
7	Phishing	↑		↑		↑	↑	↑	↑
8	Exploit kits	↓		↑		↑		↑	
9	Data breaches	↑			↑		↑		↑
10	Physical damage/theft/loss	↑	↑	↑		↑	↑	↑	↑
11	Insider threat	→	↑		↑		↑	↑	↑
12	Information leakage	↑	↑	↑	↑	↑	↑	↑	↑
13	Identity theft/fraud	↑	↑	↑	↑	↑	↑	↑	↑
14	Cyber espionage	↑	↑		↑	↑	↑		↑
15	Ransomware/ Rogueware/ Scareware	↓		↑					

Tabelle 1: ENISA Threat Landscape –Threats and Emerging Trends

↑ Increasing → Stable ↓ Declining

Empfehlung:

Um die Motivation hinter Angriffen besser zu verstehen, ist es wichtig, die ökonomischen Modelle von Cyberkriminalität näher zu beleuchten. Daher sollten interdisziplinäre Projekte gefördert werden, welche Know-how der Sicherheit, Wirtschaft und Kriminologie verbinden.

Neben der Ursachenforschung für Cyberkriminalität sollte in Projekte investiert werden, welche sich mit mobilen, eingebetteten Geräten sowie mit der Sicherheit von Cloudsystemen befassen. Auch Projekte, welche der Sicherheitsanalyse und Risikoeinschätzung komplexer Systeme gelten, sollten gefördert werden, um auf zukünftige Herausforderungen (z.B.: Industrie 4.0) reagieren zu können.

Ein weiterer wichtiger Punkt, welcher durch Forschungsschwerpunkte abgedeckt werden sollte, ist das Thema Usable Security, da ohne Akzeptanz von Sicherheitslösungen kein ausreichender Schutz erreicht werden kann.

Eine genauere Auflistung möglicher Forschungsgebiete ist in Kapitel 5 ersichtlich.

Nachfolgend werden kurz Initiativen rund um Forschungsstrategien und -roadmaps näher vorgestellt. Führende Forscher Europas identifizierten im Rahmen des SysSec Network of Excellence Projekts die Bedrohungen der nächsten Jahre sowie die Herausforderungen, die sich daraus ergeben und fassten die Ergebnisse in ihrer Publikation *„The Red Book“* zusammen.[20] In ihrem Bericht identifizieren die Forscher elf Bedrohungen, welche im Folgenden kurz beschrieben werden:

Um die **Privatsphäre und Anonymität**[21] zu schützen, ist neben technischen Ansätzen und Lösungen auch gesetzliche Unterstützung unerlässlich. Der Bereich der technischen Herausforderungen kann in die folgenden Kategorien unterteilt werden:

- Vorbeugung (Prevention): Entwicklung und Demonstration von Technologien, welche die geforderte Funktionalität mit dem Minimum an Informationen erfüllen.
- Überwachung (Monitoring): Überwachen von Informationsverlust auf allen Ebenen (z.B.: durch honey-profiles).
- Löschung (Deletion): Entwicklung von Ansätzen, um selektive Löschung der eigenen persönlichen Daten durchzuführen (Recht auf Vergessen).
- Anonymisierung (Anonymization): Entwicklung von Anonymisierungsansätzen, um Daten verlässlich zu anonymisieren und in anonymisierter Form zu teilen.

[20] Markatos et al., 2013.

[21] Markatos et al., 2013, S. 21-25.

Mögliche Forschungsgebiete in diesem Bereich umfassen die Entwicklung von honey-profiles bzw. die Erforschung neuer Ansätze und Technologien zum Schutz der Privatsphäre.

Empfehlung:

Technische, organisatorische und rechtliche Projekte, welche dem Schutz der Privatsphäre dienen, sollten gefördert werden. Durch die Ergebnisse der Projekte sollen Möglichkeiten geschaffen werden, aufkommende Technologien unter Berücksichtigung der Privatsphäre nutzbar zu machen (z.B.: Big Data Analysen unter Einhaltung der Privatsphäre).

Eine genauere Auflistung möglicher Forschungsgebiete ist in Kapitel 5 ersichtlich.

Die Hauptquelle für Sicherheitsverletzungen von Informationssystemen stellen **Softwareschwachstellen**[22] dar. Daher ist die Entwicklung von Ansätzen und Techniken zur Härtung (Hardening) von Software und zur Schadensminderung von Auswirkungen, welche beim Ausnutzen von Softwareschwachstellen entstehen, essentiell, um effektiven und effizienten Schutz gegen aktuelle und zukünftige Bedrohungen zu gewährleisten.

Mögliche Forschungsgebiete umfassen beispielsweise die Weiterentwicklung von Schutzmechanismen im Bereich Speicherverletzungen (memory corruption).

Empfehlung:

Es wird empfohlen, Projekte, welche die sichere Entwicklung von Software fördern bzw. das Aufdecken von Schwachstellen ermöglichen, zu fördern. Ein wichtiger Bereich ist dabei die Unterstützung von Sicherheitsframeworks und sicheren Entwicklungswerkzeugen.

Eine genauere Auflistung möglicher Forschungsgebiete ist in Kapitel 5 ersichtlich.

Soziale Netzwerke[23] verzeichnen steigende Beliebtheit. Die Flut an Information, welche generiert wird, erschwert es, bösartige Inhalte in Echtzeit zu erkennen und betrügerische Quellen zu identifizieren. Eine weitere Herausforderung stellt der Schutz der Privatsphäre dar.

Mögliche Forschungsprojekte im Bereich sozialer Netzwerke umfassen beispielsweise Fragestellungen rund um den Wahrheitsgehalt von Informationen in sozialen Netzwerken, das Auffinden von böswilligen/betrügerischen Identitäten und die Verarbeitung von Informationen verschiedener Quellen in Echtzeit.

[22] Markatos et al., 2013, S. 27-33.

[23] Markatos et al., 2013, S. 35-40.

Empfehlung:

Durch soziale Netze können zahlreiche Informationen über die NutzerInnen abgeleitet werden. Daher sollen Projekte geschaffen werden, welche die Privatsphäre schützen und Angriffe wie Phishing, Betrug, Cyberstalking etc. durch Verarbeitung von Informationen in Echtzeit erkennen.

Eine genauere Auflistung möglicher Forschungsgebiete ist in Kapitel 5 ersichtlich.

Durch den Einfluss, den **kritische Infrastrukturen**[24] auf unsere Gesellschaft und Wirtschaft haben, ist die Sicherheit von cyber-physischen Systemen ein besonders wichtiger Bereich der Informationssicherheit. Jedoch ist es schwierig realistische Testplattformen (Simulatoren, Testbeds) zu bekommen, um Gegenmaßnahmen unter wirklichkeitsnahen Gegebenheiten zu testen. Mögliche Felder für Forschungsaktivitäten in diesem Bereich umfassen das Design und den Betrieb eines Honeypot ICS (industrielles Steuerungssystems) um Daten für weiterführende Experimente zu bekommen, die Evaluierung von derzeitigen Modellierungs- und Simulationstools sowie neue Ansätze zur Informationskorrelation und Rekonstruktion von Angriffsszenarien.

Empfehlung:

Aufgrund der starken Auswirkungen, welche beim Ausfall kritischer Infrastrukturen auftreten können, ist Forschung im Bereich kritischer Informationsinfrastrukturen besonders wichtig. Neben Ansätzen und Werkzeugen zur Analyse von Angriffen und Ansätzen zur Bewertung von Ausfällen auf die nationale kritische Infrastrukturlandschaft sollen Schutzmechanismen für Betriebssysteme und Applikationen (z.B. auf Netzwerkebene oder durch gehärtete Betriebssysteme), welche oftmals nicht (zeitnah) aktualisiert werden können, geschaffen werden. Eine genauere Auflistung möglicher Forschungsgebiete ist in Kapitel 5 ersichtlich.

Mit zunehmender Personalisierung von Dienstleistungen werden **Authentifizierung und Autorisierung**[25] immer wichtiger. Eine der größten Herausforderungen ist die Balance zwischen Sicherheit und Benutzerfreundlichkeit sowie die starke Verknüpfung von Diensten. Als mögliche Forschungsfelder in diesem Bereich werden neue Verfahren, welche Sicherheit und Benutzerfreundlichkeit vereinen bzw. neue Verfahren zur Authentifizierung für neue Eingabegeräte angesehen.

[24] Markatos et al., 2013, S. 41-49.

[25] Markatos et al., 2013, S. 51-58.

Empfehlung:

Projekte zur Entwicklung alternativer Authentifizierungsmechanismen mit hoher Benutzerfreundlichkeit und Akzeptanz sollen gefördert werden. Eine genauere Auflistung möglicher Forschungsgebiete ist in Kapitel 5 ersichtlich.

Obwohl die **Sicherheit mobiler Endgeräte**[26] auf ähnlichen Verfahren wie sie bei traditionellen Informationssystemen vorkommen aufbauen kann, gibt es einige Eigenschaften, die spezifische Herausforderungen darstellen. Ein interessantes Langzeitforschungsprojekt wäre die Erforschung skalierbarer Technologien für die effiziente Überwachung und Analyse von sicherheitsrelevanten Ereignissen, welche das Potenzial haben, mobile Endgeräte zu kompromittieren. Weitere mögliche Forschungsprojekte umfassen hardwareunterstützte Virtualisierungslösungen oder die Erkennung von bösartigem Verhalten durch die Analyse des Netzwerkstroms auf der Netzbetreiberseite.

Empfehlung:

Forschung im Bereich eingebetteter Systeme und mobiler Endgeräte soll gefördert werden.

Eine genauere Auflistung möglicher Forschungsgebiete ist in Kapitel 5 ersichtlich.

Bestehende alte Systeme (**Legacy Systems**[27]) stellen oftmals eine große Herausforderung für die Informationssicherheit dar. Dynamische, statische und hybride Codeanalyseverfahren stellen eine Möglichkeit dar, Schwachstellen aufzudecken. Die Schwierigkeit liegt vor allem darin, gute Erkennungsraten bei gleichzeitig geringen Ergebnissen zu erzeugen.

Empfehlung:

Wie schon bei den kritischen Infrastrukturen erwähnt, stellen alte, nicht aktualisierte Systeme für Informationsinfrastrukturen eine große Bedrohung dar. Es wird daher empfohlen, Forschungsprojekte zu fördern, welche sich damit beschäftigen, Legacy Systeme zu schützen und/oder Zero-Day-Exploits entgegenzuwirken.

Eine genauere Auflistung möglicher Forschungsgebiete ist in Kapitel 5 ersichtlich.

[26] Markatos et al., 2013, S. 59-65.

[27] Markatos et al., 2013, S. 67-71.

Die immer stärkere Durchdringung der Informationstechnologie, die steigende Anzahl an Systemen und deren komplexe Vernetzungen machen es notwendig, benutzerfreundliche Sicherheitslösungen (**Usable Security**[28]) zu entwerfen. Zu diesem Zweck werden als Forschungsaktivitäten unter anderem die Untersuchung und Analyse vorhandener Lösungen oder der Entwurf von Security Design Prinzipien vorgeschlagen.

Botnetzwerke[29] sind für eine Vielzahl von Bedrohungen im Internet verantwortlich. Mögliche Forschungsgebiete sind die Erforschung neuer Ansätze um Botnetze zu bekämpfen. Ein weiterer interessanter Aspekt bei der Bekämpfung ist die Schaffung der gesetzlichen Rahmenbedingungen, um die Bekämpfung zu erleichtern.

Die immer ausgeklügelter werdende **Schadsoftware (Malware)**[30] führt dazu, dass signaturbasierte Verfahren nicht mehr ausreichen, um adäquaten Schutz zu gewährleisten. Verhaltensbasierte Verfahren zur Laufzeit und verhaltensbasierte Heuristiken sind ein vielversprechender Schritt in die richtige Richtung, sind jedoch meist aufgrund höherer Fehlerraten und Fehlalarme nicht standardmäßig aktiviert. Weitere Forschungsaktivitäten, um automatisiert neue Schadsoftware zu erkennen, sind notwendig. Herausforderungen stellen dabei unter anderem die Vielzahl an täglichen neuen Samples sowie die Komplexität der Analyse neuer Schadsoftware dar.

Um effektiven Schutz vor **Social Engineering und Phishing**[31] zu bieten, ist ein interdisziplinärer Ansatz erforderlich. Zum einen müssen effektive Wege geschaffen werden, BenutzerInnen über diese Art der Angriffe aufzuklären, zum anderen müssen Technologien geschaffen werden, Phishing automatisch zu identifizieren.

Als *Grand Challenges* identifizieren die Forscher folgende Herausforderungen[32]:

- Kein Gerät sollte kompromittierbar sein: Entwicklung geeigneter Hardware und Software, die es AngreiferInnen unmöglich macht, ein System zu kompromittieren.
- BenutzerInnen sollte Kontrolle über ihre Daten gegeben werden: Bereitstellen von Mechanismen, sodass BenutzerInnen:
    - wissen, welche Daten (z.B.: Text, Cookies) erstellt werden;
    - wissen, welche Daten Dritten zur Verfügung gestellt werden;
    - die Fähigkeiten besitzen, Bekanntgabe mancher Daten zu verweigern;
    - die Fähigkeiten besitzen, ihre eigenen Daten zu löschen;

[28] Markatos et al., 2013, S. 73-79.
[29] Markatos et al., 2013, S. 81-86.
[30] Markatos et al., 2013, S. 87-92.
[31] Markatos et al., 2013, S. 93-101.
[32] Markatos et al., 2013, S. 103f.

    - die Fähigkeiten besitzen, mithilfe rechtlicher Rahmenbedingungen das Löschen von eigenen Daten bei vorigen EmpfängerInnen durchzusetzen.
- Private Momente in öffentlichen Plätzen: Ermöglichung von privater Kommunikation in öffentlichen Orten des Cyberspaces.
- Entwicklung von compromise-tolerant systems: Bereitstellen von angemessenen Sicherheitslevels, sogar wenn manche Komponenten des Systems kompromittiert sind.

Die niederländische Cybersicherheitsforschungsagenda[33] fokussiert auf folgende sieben Forschungsthemen:

Identität, Privatsphäre und Vertrauen: Das Verwalten von digitalen Identitäten, der Schutz der Privatsphäre sowie das Aufrechterhalten von Vertrauen sind Eckpfeiler des zukünftigen Internets. Forschungsgebiete in diesem Bereich umfassen unter anderem kryptographische Lösungen, um die Privatsphäre zu schützen oder Identitätsmanagement zu verbessern.

Schadsoftware (malware): Schadsoftware ist die Voraussetzung für eine Vielzahl von Angriffen und wird daher auch in Zukunft eine große Rolle spielen. Identifizierte Forschungsvorhaben in diesem Bereich umfassen Malwareprävention, -analyse, -erkennung sowie Incident Response und Reverse Engineering.

Forensik: Das Ziel digitaler Forensik ist die fachgerechte Identifikation, Sicherstellung, Analyse und Präsentation digitaler Beweismittel/Medien. Als wichtiges Forschungsgebiet der Zukunft wurde unter anderem Live-Forensik identifiziert.

Daten- und Policymanagement: Der Bereich des Datenmanagements beschäftigt sich mit zunehmend höheren Anforderungen, die für digitale Datenhaltung in kritischen Bereichen bestehen (z.B.: Aufbewahrung von Gesundheitsdaten über 70 Jahre).

Cyberkriminalität und Schattenwirtschaft: Um Cyberkriminalität besser verstehen zu können, ist es unabdingbar, die wirtschaftlichen Rahmenbedingungen hinter Cyberkriminalität besser zu verstehen.

Risikomanagement, Wirtschaft und Regulierung: Für die immer komplexer werdenden Fragestellungen ist es wichtig, die Ökonomie von Sicherheit besser zu verstehen und Ansätze des Risikomanagements weiter zu verbessern.

Sicheres Design, Tooling und Engineering: Viele Anwendungen heutzutage sind nicht unter dem Gesichtspunkt Sicherheit entwickelt worden. Privacy-by-Design und Security-by-Design sollten so früh wie möglich in den Softwarelebenszyklus eingebaut werden.

[33] Bos et al., 2014.

Empfehlung:

Es wird empfohlen, bei Projekten mit Informationstechnologiebezug schon bei der Antragsstellung auf Konzepte hinsichtlich Security/Privacy-by-Design zu achten. Dadurch wird gewährleistet, dass Sicherheit nicht im Nachhinein unzureichend „hinzugebaut“ wird.

Des Weiteren sollten Projekte der digitalen Forensik gefördert werden, um Ursachen von Zwischenfällen besser analysieren zu können, neue Technologien forensisch analysierbar zu machen und die Aufklärung von cyberkriminellen Straftaten zu verbessern.

Eine genauere Auflistung möglicher Forschungsgebiete ist in Kapitel 5 ersichtlich.

In der Vorgängerpublikation[34] *National Cyber Security Research Agenda II* identifizierten die Autoren neben relevanten Forschungsgebieten und beteiligten Forschungsdisziplinen auch konkrete Forschungsfragestellungen für die Bereiche. Die finnische Forschungsagenda[35] zum Thema Cybersicherheit verfolgt in ihrer Vision 2019 drei große Ziele:

- Proaktiv auf Sicherheit ausgerichtete Systeme erforschen;
- Neue und effektive Werkzeuge erforschen und entwickeln, um selbstheilende Systeme zu schaffen, welche den neuen dynamischen Risikolandschaften gerecht werden;
- Das Sicherheitsbewusstsein der Bevölkerung und Vertrauen stärken.

Die Hauptforschungsgebiete[36] wurden in folgende Bereiche gegliedert:

- **Sicherheitstechnologie** umfasst die Schwerpunkte Schutz der Netzwerkinfrastruktur (Securing new network infrastructures), Sicherheit der Plattformen eingebetteter, mobiler und allgegenwärtiger Systeme (embedded, mobile and ubiquitous platform security) sowie Benutzerauthentifizierung/-autorisierung und den Schutz der Privatsphäre (Identification and privacy protection).
- Der Bereich **Sicherheitsmanagement und Governance** befasst sich mit menschlichen und organisatorischen Aspekten der Informationssicherheit und konzentriert sich auf die Bereiche Sicherheitsrichtlinienerstellung und -implementierung (Security policy development and implementation) sowie Investitionen und Anreize für Informationssicherheit (information security investment, incentives, and trade-offs).
- **Situationseinschätzung** hat das Ziel, das Cyberumfeld näher zu verstehen, um bessere Entscheidungen treffen zu können. Wichtige Aspekte in diesem Bereich

[34] Bos, et al., 2013.

[35] Ahokangas, et al., 2014.

[36] Ahokangas et al., 2014, S. 28-41.

umfassen Überwachung (observations), Analyse (analysis) sowie die geeignete Visualisierung (visualization).

- **Resilienz** beschreibt die Widerstandsfähigkeit und stellt einen wichtigen Faktor im Schutz von Informationsinfrastrukturen dar. Schwerpunkte in diesem Bereich umfassen aktive und passive Schutzmechanismen, welche Angriffe verhindern oder auf diese reagieren (active and passive countermeasures), Schutz gegen unerwünschte Inhalte (unwanted content), verbesserte Widerstandsfähigkeit der Informationstechnologie im industriellen Umfeld (improved resiliency of industrial control systems) sowie selbstschützende und selbstheilende Systeme (self-protection and -healing).

Empfehlung:

Es wird empfohlen, Projekte zu fördern, welche die Widerstandsfähigkeit erhöhen. Auch Projekte, welche sich damit beschäftigen, wie Anreize für BenutzerInnen und Unternehmen geschaffen werden können um in Sicherheit zu investieren, sollten durchgeführt werden.

Das CAMINO Projekt[37] identifizierte in seinem zweiten Arbeitspaket wichtige zukünftige Fähigkeiten und Forschungsgebiete. Beispiele für identifizierte Forschungsgebiete umfassen unter anderem die Entschlüsselung von Botnet Command and Control Server, Big Data für Cybersicherheitsanalysen, automatische und selbstlernende Applikationen, um Denial-of-Service-Attacken abzuwehren, neue Methoden für Authentifizierung und Autorisierung, und Erkennung und Schutz gegen Insiderbedrohungen.

In ihrem Bericht[38] Project 2020 zeigen die International Cyber Security Protection Alliance (ICSPA) und das Europäische Polizeiamt EUROPOL EC^3 mögliche Bedrohungen und Cyberkriminalitätsszenarien der Zukunft auf. Dabei werden die Technologieabhängigkeit und die ökonomischen Aspekte von Cyberkriminalität durch plakative Szenarien dargestellt.

[37] Vgl. Pilar Torres, 2014.

[38] International Cyber Security Protection Alliance, 2013.

3 Rechtliche und gesellschaftliche Herausforderungen

Jede Innovation hat letztlich Auswirkungen auf unsere Gesellschaft und somit eine gesellschaftliche und rechtliche Dimension. Daraus folgt:

1. Forschung auf dem Gebiet der IKT sollte stets mit einer Behandlung ihrer rechtlichen und gesellschaftlichen Aspekte einhergehen.
2. Alle in dieser Studie identifizierten Technologien und Trends haben eine rechtliche und gesellschaftliche Dimension.

Dieses Kapitel setzt sich daher mit wesentlichen rechtlichen und gesellschaftlichen Fragestellungen im Zusammenhang mit den in dieser Studie behandelten Themen auseinander. Empfehlungen, die sich aus der rechtlichen und gesellschaftlichen Dimension ergeben, finden sich einerseits bereits in diesem Kapitel und andererseits bei den jeweiligen Forschungsfeldern in Kapitel 5.

Die rechtlichen Herausforderungen im Zusammenhang mit dieser Studie können in zwei Gruppen eingeteilt werden: Die erste Gruppe bilden rechtliche Herausforderungen, die *rechtlich* zu lösen sind. Das sind Angelegenheiten, bei denen in der Praxis die rechtliche Ausgestaltung (Verträge, AGB etc.) besonders zu beachten ist, oder (neue) Phänomene, deren rechtliche Dimension und Einordnung in die Rechtsordnung noch nicht ausreichend untersucht wurde. Diesen Herausforderungen ist mit der Behandlung der sich daraus ergebenden rechtswissenschaftlichen Forschungsfragen und letztlich mit adäquater Rechtsberatung in der Praxis zu begegnen.

Die zweite Gruppe bilden rechtliche Herausforderungen, die *technisch* zu lösen sind. Zum Schutz der BürgerInnen reglementiert die Rechtsordnung den Einsatz bestimmter Technologien.[39] Dies erfolgt meist aus guten Gründen, die z.T. nachfolgend erläutert werden. Das Bestehen solcher (grund-)rechtlicher Schranken kann daher nicht grundsätzlich als „rechtlicher Anpassungsbedarf“ interpretiert werden. Vielmehr besteht die Herausforderung darin, technische Lösungen zu entwickeln, welche das Potenzial neuer Technologien innerhalb dieser notwendigen rechtlichen Schranken ausschöpfen. Rechtsvorschriften, die auf den ersten Blick möglicherweise als „Fortschrittsbremse“ wahrgenommen werden, können so zum Antrieb für die Entwicklung innovativer Lösungen werden und damit als Innovationsmotor wirken.[40] Das Stimmungsbild aus der (nicht repräsentativen) Umfrage in Kapitel 3.5 unterstützt

[39] Man denke z.B. an die Kernenergie.

[40] Die Erfüllung von datenschutzrechtlichen Anforderungen kann z.B. zur Entwicklung neuer Lösungen in der IT-Sicherheit führen, wie etwa die Projekte im Programm IKT der Zukunft zeigen.

diese These, wenn zum Beispiel rund 95% der Befragten der Ansicht bzw. „eher“ der Ansicht sind, dass der Datenschutz schon in der Konzeption einer Technologie grundlegend sichergestellt werden soll. Aus dieser Gruppe der rechtlichen Herausforderungen ergeben sich daher nicht rechtliche, sondern technische Forschungsfragen.

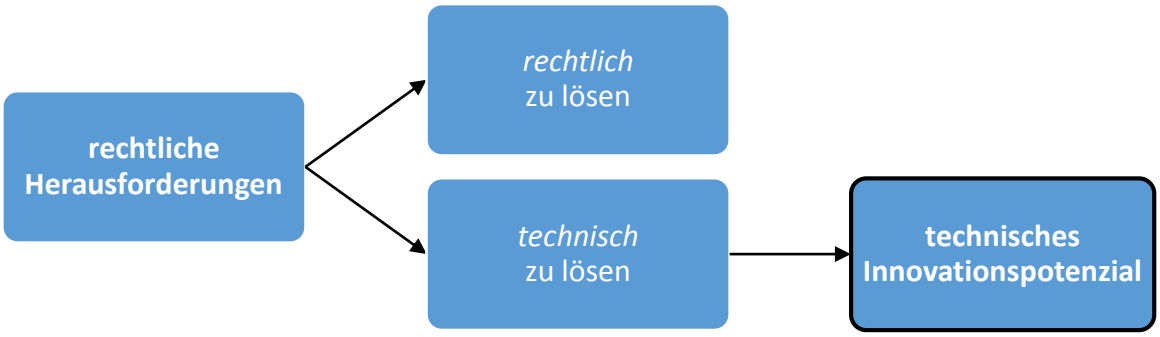


Abbildung 3: Illustration der zwei Gruppen von rechtlichen Herausforderungen. Jene die technisch zu lösen sind, können als Innovationsmotor wirken.

3.1 Datenschutz

Das gesellschaftliche Bewusstsein für Datenschutz wächst. Es ist anzunehmen, dass sich guter Datenschutz in Zukunft auch verstärkt zum Verkaufsargument entwickeln wird, mit dem europäische und insbesondere österreichische Produkte und Dienstleistungen punkten können. Die Bedenken, die die Snowden-Enthüllungen bei europäischen Unternehmen hinsichtlich der Verwendung US-amerikanischer IT- und insbesondere Cloud-Dienstleistungen ausgelöst haben, deuten in diese Richtung.[41] In der intensiven Debatte um den Entwurf der Datenschutzgrundverordnung (DSGVO)[42] geht es viel weniger um neue Prinzipien als um den Wandel des Datenschutzrechts vom „weichen Recht“ mit geringen Strafen zu einem „harten Recht“ mit empfindlichen Strafen. Die Existenz eines Unternehmens wird in der Wissens- und Netzwerkgesellschaft auch davon abhängen, wie es seinen Datenbedarf grundrechtskonform organisieren kann. Im Lichte der jüngsten Entscheidung des EuGH *Schrems*[43] zeigt sich, dass Höchstgerichte ihre Kompetenzen zum Schutz der Grundrechte auch gegen allgemeine wirtschaftliche Interessen wahrnehmen. Für Unternehmen bedeutet dies aber auch, dass wesentlich mehr in den Datenschutz und die IT-Sicherheit investiert werden muss.

[41] Vgl. Weiss, 2014.
[42] Näheres zur Datenschutzgrundverordnung siehe in Abschnitt 3.1.6.
[43] Näheres zu dieser Entscheidung und weiteren hier relevanten Entscheidungen siehe in Abschnitt 3.1.7.

3.1.1 Einleitung

Datenschutz ist ein Grundrecht[44]; näher determiniert durch die Datenschutzbestimmungen. Das Grundrecht auf Datenschutz gilt jedoch nicht absolut, sondern unter Vorbehalt von insbes. zwei Eingriffstatbeständen: Gesetz (öffentliches Interesse) und Einwilligung des Betroffenen.

Die Umsetzung dieses Grundrechts ist von den technischen Lösungen der Datenverarbeitung abhängig. In unserer technologischen Welt ist Datenschutz nur dann effizient, zweckmäßig und wirksam wenn die technischen Entwicklungen datenschutzfreundlich gestaltet sind.

Datenschutz wird sehr oft auch als bürokratischer Aufwand gesehen, wenn man die vielen Zustimmungserfordernisse, Vertragsklauseln, Genehmigungserfordernisse, etc. ansieht. Im Hinblick auf die nunmehr notwendige Datenschutz-Compliance muss eine effiziente Datenschutzorganisation auch nachgewiesen werden.

Datenschutz soll allerdings die technologische Entwicklung nicht behindern. Es bedarf daher der Erforschung datenschutzfreundlicher Lösungen auf allen Innovationsgebieten, auf denen die Verarbeitung von personenbezogenen Daten eine Rolle spielt. Dies erfordert die Zusammenarbeit von TechnikerInnen, JuristInnen und ggf. Domain-ExpertInnen auf dem jeweiligen Gebiet. Folgende Konzepte und Paradigmen wurden in diesem Kontext entwickelt bzw. entwickeln sich derzeit:

- Privacy Enhancing Technologies: Der Begriff der Privacy Enhancing Technologies (PETs) existiert bereits seit den 1990er-Jahren und kann definiert werden als „ein kohärentes System von IKT-Maßnahmen zum Schutz der Privatsphäre durch Eliminierung oder Verminderung personenbezogener Daten oder durch Vermeidung einer unnötigen und/oder unerwünschten Verarbeitung von personenbezogenen Daten ohne Verlust der Funktionalität des betreffenden Informationssystems.“[45] In der Praxis sind PETs weit verbreitet, jedoch überwiegend als eigenständige Technologien – meist Datensicherheitstechnologien – die als Komponente eines Informationssystems genutzt werden (z.B. Transport Layer Security in Webanwendungen), nicht jedoch als Konzept, das den Schutz der Privatsphäre im Gesamtsystem betrachtet.

- Privacy Impact Assessment: Wird als eigenes Forschungsfeld in Kapitel 5 dargestellt.

- Privacy by Design: Wird als eigenes Forschungsfeld in Kapitel 5 dargestellt.

[44] Insbesondere Art 8 EMRK, Art 7 und 8 GRC und § 1 DSG.

[45] Mitteilung der Kommission an das Europäische Parlament und den Rat über die Verbesserung des Datenschutzes durch Technologien zum Schutz der Privatsphäre, KOM(2007) 228 endgültig, 2.5.2007.

- Privacy by Default: Wird gemeinsam mit Privacy by Design in Kapitel 5 dargestellt.
- Datenschutz-Zertifizierung (z.B. EuroPrise): Darauf wird weiter unten in Abschnitt 3.2.2 näher eingegangen.

Diese Konzepte klingen oft nach Schlagworten, deren konkrete Verwirklichung fern erscheint. Darin liegt aber die Herausforderung der Forschung im Bereich Datenschutz und IT-Sicherheit in den nächsten Jahren: aus den bisherigen Beispielen und Umsetzungsansätzen eine zweckmäßige Datenschutz-Compliance sicherzustellen.

3.1.2 Technische Perspektive: Digitalisierung, Informationsanhäufung, Big Data & Suchmaschinen

Ein wesentliches Merkmal der Wissens- und Netzwerkgesellschaft besteht darin, dass die Menge an Daten, Informationen und Wissen überproportional zunimmt; insbesondere quantitativ, aber auch qualitativ. Die Einschränkungen des analogen Mediums Papier hinsichtlich Speicherkapazität und Durchsuchbarkeit werden durch das digitale Medium obsolet. Die Digitalisierung bringt wesentliche Veränderungen in der Handhabung von Daten. Durch die sehr geringen Kosten für Speicherplatz und die leicht mögliche Portierung der jeweiligen Datensammlungen werden immer mehr Daten gespeichert und auch dauerhaft aufbewahrt. Schon diese Informationsanhäufung stimmt bedenklich („Zentrifugalkraft der Datenanhäufung“). Aus Sicht des Datenschutzes ist die strukturierte Sammlung von Daten sowie deren Durchsuchbarkeit und damit Verknüpfung der Daten entscheidend. Die digitale Speicherung und heutige Suchmaschinen machen es erforderlich, dass jede Datensammlung, auch das Internet, den Kriterien des Datenschutzes entsprechen muss. Suchmaschinen erfordern keine strukturierte Aufbereitung der Daten, schaffen eine sehr effiziente Indizierung und bewegen sich in Richtung einer semantischen Suche. Dazu kommen die Methoden der Datenanalyse (Big Data). Es gibt daher enorm viele Daten, diese können auch nach beliebigen Kriterien durchsucht werden und sind zunehmend Objekt intensiver Datenanalyse. Hinzu kommt, dass viel zu wenige Daten gelöscht werden.

Aus technischer Sicht besteht aus ganz verständlichen Gründen eine Tendenz dazu, Daten nicht zu löschen, sondern auch dann weiterhin zu speichern, wenn es keinen konkret definierbaren Zweck mehr gibt, für den die Daten noch benötigt werden. Zum einen verursacht das Löschen vorhandener Daten in der Regel einen höheren Aufwand als das weitere Speichern, da die Kosten für Speicherplatz heute sehr gering sind. Das Speichern ist gewissermaßen der Grundzustand, das Löschen wäre ein aktiver Vorgang, der Aufwand verursacht. Zum anderen ist es ein zutiefst menschliches Verhalten, etwas aufzubewahren, was man zwar gegenwärtig nicht mehr braucht, aber vielleicht in Zukunft.

Die Rolle des Datenschutzes ist es, in Bezug auf personenbezogene Daten dieser Tendenz zum Schutz der Betroffenen nicht nur entgegenzuwirken, sondern ein modernes Datenschutzmanagement zu unterstützen. Der datenschutzrechtliche Zweckbindungsgrundsatz und generell das Prinzip der Datenminimierung sehen vor, dass Daten nur gespeichert werden dürfen, wenn sie für den jeweiligen (zulässigen) Zweck tatsächlich benötigt werden.[46] Im Folgenden werden diese und weitere Datenschutzgrundsätze und ihre Bedeutung erläutert.

3.1.3 Datenschutzgrundsätze

In der mehr als vierzigjährigen Geschichte des europäischen Datenschutzrechts haben sich Grundprinzipien herausgebildet, die in den meisten Datenschutzordnungen in Europa und darüber hinaus in der einen oder anderen Weise ihren Niederschlag finden. Die wichtigsten dieser Grundsätze können wie folgt zusammengefasst werden:

- **Fairness und Rechtmäßigkeit**[47]: Personenbezogene Daten dürfen nur nach Treu und Glauben und auf rechtmäßige Weise verarbeitet werden.

- **Zweckbindung**[48]: Personenbezogene Daten dürfen nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden.

- **Verhältnismäßigkeit/Wesentlichkeit**[49]: Personenbezogene Daten dürfen nur verarbeitet werden, wenn sie für den Zweck der Datenanwendung wesentlich sind und dürfen darüber nicht hinausgehen. Ein Eingriff in die „informationelle Selbstbestimmung“[50] muss verhältnismäßig sein, das heißt bei Interessenskollisionen muss eine faire und sachliche Abwägungsentscheidung getroffen werden.

- **Zeitliche Begrenzung**[51]: Daten dürfen nicht länger, als es für die Realisierung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist, in

[46] Dabei soll Datenschutz nicht die Geschichtsschreibung verhindern: Auch mediale Berichterstattung und Archivierung sind selbstverständlich legitime Zwecke der Datenverarbeitung (vgl. insbes. auch das Medienprivileg des § 48 DSG).

[47] Art 6 lit a DSRL, Art 5 lit a Datenschutzkonvention, Art 7 OECD-Richtlinien.

[48] Art 6 lit b DSRL, Art 5 lit b, Art. 9 OECD-Richtlinien, ISO/IEC 29100 (5.3, 5.4).

[49] Art 6 lit c DSRL, Art 5 lit c Datenschutzkonvention.

[50] Dieser Terminus stammt aus der deutschen Grundrechtsjudikatur des Bundesverfassungsgerichts und wird neuerdings vom Österreichischen Verfassungsgerichsthof (VfGH) synonym für das „Datenschutzgrundrecht“ verwendet, siehe VfGH, Erkenntnis vom 27.6.2014, G 47/2012 u.a. zur Aufhebung der „Vorratsdatenspeicherung“.

[51] Art 6 lit e DSRL, Art 5 lit e Datenschutzkonvention, ISO/IEC 29100 (5.6).

personenbezogener Form aufbewahrt werden, die die Identifizierung der betroffenen Personen ermöglicht.

- **Datenminimierung**[52]: Dieses Prinzip liegt bereits den Grundsätzen Zweckbindung, Verhältnismäßigkeit/Wesentlichkeit und Datenlöschung zugrunde, geht aber darüber hinaus. Es schließt z.B. auch mit ein, dass die Zahl jener Personen, die (Zugriff auf) personenbezogene Daten erhalten, so gering wie möglich sein soll.

- **Datenqualität**[53]: Personenbezogene Daten dürfen nur so verwendet werden, dass sie im Hinblick auf den Verwendungszweck im Ergebnis sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht sind.

- **Datensicherheit**[54]: Personenbezogene Daten müssen durch angemessene Sicherheitsvorkehrungen gegen Risiken wie Verlust sowie Zugang, Zerstörung, Nutzung, Veränderung oder Offenlegung der Daten durch Unbefugte geschützt werden.

3.1.4 Datenschutz und Datensicherheit – Abgrenzung und Gemeinsamkeiten

Informationssicherheit[55] ist – im Unterschied zur Funktionssicherheit (engl. safety), im Sinne einer Übereinstimmung der Ist-Funktionalität mit der Soll-Funktionalität[56] – die Sicherheit eines IT-Systems vor Bedrohungen von außerhalb des Systems, insbesondere vor einem/r äußeren AngreiferIn.[57] Informationssicherheit bedeutet die Sicherstellung der drei klassischen Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit. In diesem Zusammenhang spielt es keine Rolle, ob die Informationen personenbezogen oder nur sachbezogen sind, Informationssicherheit umfasst jede Art und Qualität von Informationen. Insofern ist Datenschutz eine Teilmenge von Informationssicherheit.

Datenschutz geht aber über Informationssicherheit hinaus, wenn es um den Schutz der Betroffenen vor einer missbräuchlichen Verwendung („Missbrauch“) ihrer personenbezogenen Daten geht. Jedem Individuum steht das Grundrecht zu, über die individuellen Informationen grundsätzlich selbst zu bestimmen („Recht auf informationelle Selbstbestimmung“[58]). Die deutsche Grundrechte-Judikatur hat ergänzend ein neues

52 ISO/IEC 29100 (5.5).

53 Art 6 lit d DSRL, Art 5 lit d Datenschutzkonvention, Art 8 OECD-Richtlinien, ISO/IEC 29100 (5.9).

54 Art 17 DSRL, Art 7 Datenschutzkonvention, Art 11 OECD-Richtlinien, ISO/IEC 29100 (5.11).

55 Datensicherheit und Informationssicherheit werden im Folgenden vereinfachend synonym verwendet.

56 Vgl. Eckert, 2013, S. 6 f.

57 Vgl. Eckert, 2013, S. 6 f.

58 Das Grundrecht auf informationelle Selbstbestimmung wurde vom deutschen Bundesverfassungsgericht (BVerfG) aus dem Art 1, 2 GG (deutsches Grundgesetz) heraus entwickelt und ist heute ein anerkanntes

Grundrecht „auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“[59] entwickelt. Dieses Recht schützt die Betroffenen vor Zugriffen auf Computer, Netzwerke und vergleichbare Systeme, wenn diese Zugriffe das Persönlichkeitsrecht gefährden. Anders als die „informationelle Selbstbestimmung“ setzt dieses Grundrecht jedenfalls nicht voraus, dass die Verarbeitung personenbezogener Daten betroffen ist. Eine Gefährdung von Persönlichkeitsrechten durch missbräuchliche Zugriffe auf ein Computersystem kann sich auch ohne Verarbeitung personenbezogener Daten leicht ergeben, beispielsweise durch die Zerstörung von digital gespeicherten (nicht personenbezogenen) wertvollen Arbeitsergebnissen auf einem Computersystem. Diese Judikatur zeigt, dass Datenschutz im Bereich des IT-Rechts zwar ein wichtiger Bereich ist, damit aber nicht alle Schutzbedürfnisse erfasst werden können.

Somit ergibt sich folgende Beziehung zwischen Datenschutz und Datensicherheit: Datenschutz geht über Datensicherheit hinaus, weil er auch den rechtmäßigen DateninhaberInnen oder befugten Dritten (insbes. Sicherheitsbehörden) bestimmte Datenverwendungen verbietet.

Besonders anschaulich ist dies im Alltag eines betrieblichen IT-Systems. Ein/e IT-AdministratorIn eines Unternehmens hat notwendiger- und zulässigerweise zunächst einmal uneingeschränkte Kontrolle über das betriebliche IT-System und alle darin verarbeiteten Daten. Diese Kontrolle muss ein/e Admin haben, damit die Sicherheit und Integrität der eigenen Datenverarbeitung gewährleistet werden kann. Gleichzeitig ist auch in der Rolle des/r IT-Admin niemand berechtigt, jede beliebige Auswertung im Hinblick auf die Arbeitsleistung/Anwesenheitszeit etc. der MitarbeiterInnen aus der großen praktisch verfügbaren Menge an Rohdaten zu ziehen – dazu gibt es Regeln, Grenzen, Mitbestimmungsrechte usw. Datenschutz setzt also auch normative Beschränkungen für jene, die grundsätzlich zulässigerweise die umfassende Kontrolle über das IT-System ausüben.

Datensicherheit geht über den Datenschutz hinaus, weil sie

a) nicht nur personenbezogene Daten schützt und
b) nicht nur der Vertraulichkeit der Daten dient.

Die Zielsetzungen von Datenschutz und Datensicherheit decken sich daher vielfach, insbesondere betreffend die Vertraulichkeit. Datensicherheit ist eines der wesentlichen Mittel zur Umsetzung des Datenschutzes, was sich z.B. auch in § 14 DSG niederschlägt. Umgekehrt kann der Datenschutz in Form des Datenschutz-Grundprinzips der Datenminimierung auch einen positiven Effekt auf die Datensicherheit haben, denn ein System, das insgesamt weniger

Grundrecht. Siehe dazu das legendäre „Volkszählungsurteil“, BVerfGE 65,1 vom 15. Dezember 1983; z.T. synonym mit dem „Grundrecht auf Datenschutz“ verwendet.

[59] BVerfG Urteil vom 27. Februar 2008, 1 BvR 370/07.

Daten verarbeitet, ist tendenziell auch weniger attraktiv für AngreiferInnen, die darauf abzielen, möglichst viele Daten zu erbeuten.[60]

Datenschutz und Datensicherheit können einander in bestimmten Konstellationen aber auch entgegenstehen. Ein Beispiel ist das Logging und die Analyse des Netzwerkverkehrs in einem Unternehmen für Zwecke der Datensicherheit, was zugleich einen Eingriff in das Grundrecht auf Datenschutz der betroffenen MitarbeiterInnen darstellt.

Auch folgender Zusammenhang zwischen Datenschutz und Datensicherheit ist zu beachten:

Absolute Datensicherheit ist nicht möglich. „Breach is always possible“: Die Möglichkeit, dass AngreiferInnen in ein System eindringen und Zugriff auf die darin befindlichen Daten erlangen, ist immer vorhanden und immer zu berücksichtigen. Wenn zuvor mehr Wert auf den Datenschutz gelegt wird, ist im Fall eines erfolgreichen Angriffs der Schaden geringer. Insbesondere das datenschutzrechtliche Grundprinzip der Datensparsamkeit/ Datenminimierung ist hier relevant: Werden weniger – nämlich nur die für den jeweiligen Zweck nötigsten – Daten verarbeitet, können auch weniger Daten gestohlen werden. Und noch ein zweiter Effekt tritt dann ein: Ein System, das weniger Daten verarbeitet, ist – wie bereits angesprochen – auch weniger attraktiv für AngreiferInnen, die darauf abzielen, möglichst viele Daten zu erbeuten.[61]

Eine wesentliche Gemeinsamkeit besteht schließlich in der Systematik dynamischer zyklischer Prozesse (Plan-Do-Check-Act, „PDCA Zyklus“), die zuallererst Organisation und Management betreffen – die Rolle der IT besteht hier vor allem darin, die Entscheidungen des Managements auch zuverlässig abzusichern, die unmittelbare Verantwortung liegt aber jedenfalls beim Management.

3.1.5 Die Bedeutung des Datenschutzes ist hoch und nimmt weiter zu

Zweifellos ist das Bedürfnis zur Geheimhaltung bestimmter personenbezogener Informationen von Person zu Person sehr unterschiedlich. Viele Menschen teilen auf Facebook sehr freizügig einem großen Personenkreis eine Vielzahl persönlicher Details mit; für andere ginge das bereits viel zu weit. Es sollte aber nicht übersehen werden, dass es auch für die meisten „Freizügigen“ eine Sphäre des Privaten gibt und diese Gruppe im Sinne einer informationellen Selbstbestimmung selbst entscheidet, was sie mitteilt und was nicht. Facebook und ähnliche Phänomene des Web 2.0 sollten daher nicht mit einer grundsätzlichen Abnahme der Bedeutung des Datenschutzes verwechselt werden. Es ist bloß Ausdruck sich verändernder Wertungen darüber, was von der Privatsphäre erfasst sein soll und was nicht. Auch das Bild der im Zuge der Ausarbeitung dieser Studie durchgeführte Umfrage bestätigt

[60] Vgl. Cameron, 2005.

[61] Vgl. Cameron, 2005.

diesen Befund, zumal sich hier eine sehr starke Nutzung sozialer Medien zeigt, obwohl 94% der RespondentInnen solche Dienste als „eher“ bis „gar nicht vertrauenswürdig“ einstufen.[62]

Möglicherweise ist es auch Ausdruck mangelnden Bewusstseins, welche intimen Informationen mit hoher Wahrscheinlichkeit über eine Person abgeleitet werden können, wenn nur eine ausreichende Menge vermeintlich banaler und im Einzelnen unbedeutender Daten über eine Person vorliegen.[63] Dies ist eine der wesentlichen Bedrohungen, vor der Datenschutz in unserer heutigen, informationsgetriebenen Gesellschaft schützen soll. Eine konkrete Bedrohung für jede/n Einzelnen wäre etwa eine erhöhte Versicherungsprämie oder gar die Ablehnung des Vertragsabschlusses, wenn die Krankenversicherung die Möglichkeit hätte, aus personenbezogenen Daten bestimmte individuelle Risiken zu errechnen. Dies entspräche nicht mehr dem Gedanken einer Versicherung als Mittel der Risikostreuung. Hinzu kommt, dass dabei unweigerlich Fehler passieren und dass es sich „nur“ um statistische Berechnungen handelt, sodass auch bei Richtigkeit der Berechnungen die berechneten Risiken nicht für jeden einzelnen Betroffenen eintreten.

Datenschutz hat jedoch auch eine gesamtgesellschaftliche Dimension. Datenschutz und Privatsphäre sind für die Ausübung der Meinungsfreiheit, für politische Partizipationsprozesse und somit für das Funktionieren der Demokratie unerlässlich.[64] Dadurch wird deutlich, dass die Entscheidung des/der Einzelnen, den Datenschutz in Bezug auf die eigenen Daten ernst zu nehmen oder nicht, nicht nur die Interessen des jeweiligen Individuums, sondern auch gesamtgesellschaftliche Interessen betrifft. Aufgrund der demokratiepolitischen Dimension des Datenschutzes hat „kollektiver Datenschutzverzicht“ auch negative gesamtgesellschaftliche Auswirkungen. Selbst wenn man der Meinung ist, „über mich darf jeder alles wissen“, hat man daher eine Verantwortung in Sachen Datenschutz. Vergleichbar ist dies mit dem Thema Impfen: Sich gegen eine bestimmte Krankheit impfen zu lassen, verhindert nicht nur, dass man selbst nicht erkrankt (subjektives Motiv), sondern führt kollektiv auch dazu, dass die Krankheit langfristig ausstirbt, wenn sich genügend Menschen impfen lassen.

Mit zunehmenden Möglichkeiten und Tendenzen zur Erhebung und Speicherung personenbezogener Daten nimmt die Bedeutung von Datenschutz und Privatsphäre immer weiter zu. Daraus leitet sich auch ein gesellschaftlicher Auftrag ab, mittels Bildung und Aufklärung das Individuum zu stärken.

[62] Vgl. dazu Kapitel 3.5.2.

[63] In diese Richtung zeigen auch die Umfrageergebnisse, wonach zwar 65% der Befragten ausdrückliches Interesse an Datenschutz bekunden, aber dennoch „nur“ 18% sich auch gut informiert fühlen, vgl. Kapitel 3.5.4.

[64] Dies wird am einfachsten durch den Grundsatz der geheimen Wahl illustriert, geht jedoch viel weiter.

3.1.6 Aktuelle Entwicklungen in der Datenschutzgesetzgebung

Im Rahmen des seit Längerem laufenden Reformprozesses der EU zum Datenschutz veröffentlichte die EU-Kommission am 25.1.2012[65] einen Vorschlag für eine neue, EU-weit unmittelbar gültige Datenschutz-Grundverordnung (DSGVO). Mit einer Verordnung an Stelle der Richtlinie will man die ungenügende Harmonisierung des Datenschutzrechts der Mitgliedstaaten besser in Griff bekommen. Der Rat der EU sowie das Europäische Parlament haben ihre jeweiligen Positionen festgelegt. Derzeit ist der Entwurf im Trilogverfahren; mit einem in Kraft treten wird frühestens 2018 zu rechnen sein. Dieser Vorschlag hält er doch einige neue Grundsätze, die im Rahmen der Roadmap unbedingt zu berücksichtigen sind, weil diese – unabhängig vom tatsächlichen Ergebnis der Reform – jedenfalls den neuesten Stand der Erkenntnisse im Datenschutz repräsentieren.

- Artikel 17: Recht auf Vergessenwerden

Wenngleich dieser Vorschlag in der rechtspolitischen Debatte in der Folge des Vorschlags äußerst umstritten war und ist, zeigt sich doch bereits jetzt die Tendenz, das bisher bestehende „einfache“ Recht auf Löschung in diese Richtung zu erweitern. Das jüngste Beispiel dazu ist die Entscheidung des EuGH zu Google Spanien vom 13. Mai 2014.[66] Dort stellte der Gerichtshof zum Umfang der Verantwortlichkeit des Suchmaschinenbetreibers fest, dass dieser unter bestimmten Voraussetzungen verpflichtet ist, von der Ergebnisliste, die im Anschluss an eine anhand des Namens einer Person durchgeführte Suche angezeigt wird, Links zu von Dritten veröffentlichten Internetseiten mit Informationen über diese Person zu entfernen. Eine solche Verpflichtung kann ggf. auch bestehen, wenn deren Veröffentlichung dort als solche rechtmäßig ist.[67] Wenngleich dieses Urteil auch teilweise harte Kritik dahingehend erfahren hat[68], dass der Gerichtshof die Abwägung mit der entgegenstehenden Meinungs- und Informationsfreiheit nicht hinreichend berücksichtigt, zeigt das Urteil doch eine eindeutige Richtung der Rechtsentwicklung, welche den rechtspolitischen Vorschlag der EU Kommission umso relevanter erscheinen lässt.

Artikel 17 Absatz 2 DS-GV schlägt folgende Formulierung zu einem solchen „Recht auf Vergessenwerden“ vor: „Hat der in Absatz 1 genannte für die Verarbeitung Verantwortliche

[65] Vorschlag für eine „VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung). Seit Veröffentlichung dieses Vorschlags wurden und werden laufend von Parlament und Rat neue Versionen und Formulierungen diskutiert. Dieser Prozess ist jedoch noch nicht abgeschlossen. Hier wird der Text des ursprünglichen Vorschlags der Kommission behandelt (vgl. Europäisches Parlament, 2012).

[66] Urteil des Gerichtshofs der EuGH (Große Kammer) vom 13. Mai 2014 in der Rechtssache C-131/12. Siehe dazu Abschnitt 3.1.7.

[67] Gerichtshof der Europäischen Union, 2014.

[68] Vgl. Lehofer, 2014.

die personenbezogenen Daten öffentlich gemacht, unternimmt er in Bezug auf die Daten, für deren Veröffentlichung er verantwortlich zeichnet, alle vertretbaren Schritte, auch technischer Art, um Dritte, die die Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Querverweise auf diese personenbezogenen Daten oder von Kopien oder Replikationen dieser Daten verlangt. Hat der für die Verarbeitung Verantwortliche einem Dritten die Veröffentlichung personenbezogener Daten gestattet, liegt die Verantwortung dafür bei dem für die Verarbeitung Verantwortlichen."

Diesen Anforderungen werden IKT-Systeme wohl in Zukunft nur dann gerecht werden können, wenn entsprechende Sicherungen auch auf der technischen Ebene berücksichtigt werden.

- Artikel 23: Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

Diese beiden Grundsätze, besser bekannt unter den englischen Bezeichnungen „Privacy by Design" und „Privacy by Default", adressieren unmittelbar die Ebene der technischen Entwicklung und sind daher auch für diese Roadmap von besonderer Bedeutung. Ihnen ist daher unten ein eigenes Kapitel gewidmet. An dieser Stelle ist festzuhalten: Mit steigendem Datenschutzbewusstsein in der Gesellschaft besteht bereits jetzt ein sanfter Druck auf den Markt neuer IKT-Entwicklungen, Datenschutz schon möglichst in der Architektur und den Funktionen eines Systems zu berücksichtigen und so bestimmte – zuvor identifizierte – Risiken von vornherein zu vermeiden. In dem (wahrscheinlichen) Fall, dass diese Bestimmung am Ende des Reformprozesses tatsächlich in die neue Datenschutz-Grundverordnung aufgenommen wird, bestünde hierzu dann zusätzlich ein normativer Druck, der dieser Entwicklung zweifellos massiv Vorschub leisten würde. Dies wird technologische Innovationen auslösen und da Datenschutz und Informationssicherheit hierzulande bereits einen sehr hohen Stellenwert haben, hat Österreich das Potenzial, wirtschaftlich an dieser Entwicklung führend zu partizipieren und von dieser zu profitieren.

- Artikel 30: Erhöhte Anforderungen an die **Datensicherheit**

Wenngleich schon die bestehende Datenschutzrichtlinie allgemeine Pflichten zur Datensicherheit enthält, bringt der Vorschlag zur DS-GV auch hier einige Neuerungen. Umfasst ist beispielsweise eine Risikobewertung, um die Daten vor unbeabsichtigter oder widerrechtlicher Zerstörung oder vor unbeabsichtigtem Verlust sowie zur Vermeidung jedweder unrechtmäßigen Verarbeitung, insbesondere jeder unbefugten Offenlegung, Verbreitung beziehungsweise Einsichtnahme oder Veränderung zu schützen. Weiters soll die Kommission ermächtigt werden, genauere Anforderungen insbesondere des aktuellen Standes der Technik zu bestimmen.

- Artikel 31: Allgemeine Pflicht zu „**Data Breach Notification**“

Auch die nach Artikel 31 des Vorschlages zur Datenschutz-VO künftig verpflichtende Meldung von Verletzungen des Schutzes von personenbezogenen Daten („Data Breach Notification“) will die für die Verarbeitung Verantwortlichen, insbesondere auch private Unternehmen, in Zukunft stärker in die Verantwortung nehmen. In Österreich ist eine ähnliche Bestimmung bereits derzeit in Kraft.[69]

- Artikel 33: Verpflichtung zur Vornahme einer **Datenschutz-Folgeabschätzung**

Artikel 33 des VO-Vorschlags sieht eine Verpflichtung zur Vornahme einer Datenschutz-Folgeabschätzung vor. Eine solche Risiko-Analyse soll „den Rechten und den berechtigten Interessen der von der Datenverarbeitung betroffenen Personen und sonstiger Betroffener Rechnung [tragen]“.

3.1.7 Aktuelle Entwicklungen in der Datenschutzjudikatur

In diesem Abschnitt wird anhand einiger wichtiger höchstgerichtlicher Entscheidungen der letzten Zeit illustriert, dass Datenschutz als Grundrecht an Bedeutung gewinnt und die Rechtsprechung durchaus beträchtliche Wirkung in der Praxis entfalten kann. Die beiden aktuell wohl bedeutendsten Entscheidungen, in denen der Europäische Gerichtshof (EuGH) dem Grundrecht auf Datenschutz zu mehr Durchsetzung verholfen hat, sind die Entscheidung zur Vorratsdatenspeicherung und die als „Google Spain“ bekannte Entscheidung zum Recht auf Vergessenwerden.

Am 8. April 2014 hob der EuGH die Richtlinie 2006/24/EG zur Vorratsdatenspeicherung wegen Unvereinbarkeit mit den Grundrechten auf Privatsphäre und Datenschutz vollständig auf.[70] Diese Richtlinie verpflichtete Mitgliedstaaten, Gesetze zu erlassen, welche wiederum AnbieterInnen öffentlicher Kommunikationsdienste und die BetreiberInnen öffentlicher Kommunikationsnetze in der gesamten EU verpflichten, die Zugangs- und Verkehrsdaten sämtlicher NutzerInnen für einen Zeitraum von mindestens sechs Monaten bis zu zwei Jahren auf Vorrat zu speichern, unabhängig davon, ob die NutzerInnen selbst ein verdächtiges Verhalten gesetzt haben oder die AnbieterInnen die Daten für betriebliche Zwecke (insbesondere Rechnungslegung) selbst noch benötigen. Der österreichische Verfassungsgerichtshof hat infolge des EuGH-Urteils die innerstaatliche Umsetzung dieser Richtlinie im Wesentlichen mit denselben Argumenten im Juni 2014 ebenfalls mit sofortiger Wirkung als verfassungswidrig aufgehoben.[71]

[69] § 24 Abs 2a DSG.

[70] Urteil des EuGH in den verbundenen Rechtssachen C-293/12 und C-594/12.

[71] Urteil des Verfassungsgerichtshofs, 27.6. 2014, G 47/2012-49, G 59/2012-38, G 62/2012-46, G 70/2012-40, G 71/2012-36.

Die oben in Abschnitt 3.1.6 im Zusammenhang mit dem Recht auf Vergessenwerden behandelte Entscheidung „Google Spain“[72] ist vor allem deshalb so bedeutend, weil der EuGH spanisches bzw. europäisches Datenschutzrecht auf eine Datenverarbeitung anwendete, die nicht von der spanischen Google-Niederlassung vorgenommen wird, sondern nur deren Tätigkeit als Vertriebsniederlassung zuzuordnen ist.

In der jüngsten und vielleicht bedeutendsten hier zu nennende Entscheidung des EuGH[73], die auf ein Verfahren des österreichischen Juristen und Aktivisten Max Schrems gegen Facebook Irland zurückgeht, wurde die sogenannte Safe-Harbor-Entscheidung der Europäischen Kommission für ungültig erklärt, weil diese pauschal die Übertragung personenbezogener Daten von EU-BürgerInnen an US-Unternehmen erlaubte, wo diese Daten den von Edward Snowden enthüllten Überwachungsbefugnissen der US-Behörden unterliegen. Der EuGH setzte sich damit zum ersten Mal mit dieser Praxis der Massenüberwachung auseinander und erklärte diese für mit europäischen Grundrechten unvereinbar. Er definierte damit Anforderungen, die ein Verhandlungsergebnis zwischen der EU und der USA betreffend eine Nachfolgeregelung von Safe Harbor zwingend erfüllen muss, und erhöhte damit den Druck auf diese Verhandlungen. Die Auswirkungen der Entscheidung könnten somit enorm sein. Kurzfristig können wohl meist andere Rechtsgrundlagen für den Transfer personenbezogener Daten zu US-Unternehmen, insbesondere auch von europäischen Tochtergesellschaften von US-Konzernen zu ihren Konzernmüttern in den USA, gefunden werden.

Eine weitere sehr bedeutende Entscheidung des EuGH[74] aus dem Jahr 2014, die Netzsperren zur Durchsetzung von Urheberrecht grundsätzlich für zulässig erklärte, hat ebenfalls sehr viel mit Datenschutz zu tun, wenn auch erst auf den zweiten Blick. Der EuGH entschied, dass Internet-Zugangsprovider dazu verpflichtet werden können, den Zugang zu Websites zu sperren, die überwiegend urheberrechtlich geschütztes Material anbieten, ohne dazu berechtigt zu sein. Das Problem dabei ist, dass es mehrere Methoden gibt, dies umzusetzen und die effektivste davon, Deep Packet Inspection (DPI), eine massive Überwachung des Internetverkehrs der NutzerInnen bedeuten würde. Der EuGH hat offen gelassen, mit welcher Methode die Sperren umzusetzen sind. Die Methode DPI nimmt eine Analyse des gesamten Netzwerkverkehrs auf der Ebene von IP-Paketen vor, analysiert dabei sowohl Inhaltsdaten als auch Verkehrsdaten und speichert diese zu diesem Zweck zum Teil auch (zumindest für kurze Zeit). Demgegenüber steht das Argument, dass ein effektives Netzwerkmanagement nur durch DPI möglich sei. Dem lässt sich entgegenhalten, dass insbesondere die Version 6 des

[72] Urteil des EuGH (Große Kammer) vom 13. Mai 2014 in der Rechtssache C-131/12, Google Spain SL und Google Inc. gegen Agencia Española de Protección de Datos (AEPD) und Mario Costeja González.

[73] Urteil des EuGH (Große Kammer) vom 6. Oktober 2015 in der Rechtssache C-362/14, Maximillian Schrems gegen Data Protection Commissioner.

[74] Urteil des EuGH vom 27. März 2014 in der Rechtssache C-314/12.

Internetprotokolls (IPv6) wesentlich erweiterte Möglichkeiten zum Netzwerkmanagement bietet, die zugleich zweifellos einen geringeren Eingriff in die Vertraulichkeit des Datenverkehrs darstellen.

Das Thema „Internetsperren“ hat jedenfalls eine weitreichende Dimension für die gesamte Gesellschaft. Die Interessen betreffen den Schutz geistigen Eigentums, die wirtschaftlichen Investitionen und die Wertschöpfung aus der Internet-Infrastruktur, die Informations- und Medienfreiheit und den Datenschutz. Dabei hat die Gesellschaft bisher auch international einige wesentliche gesellschaftspolitische Grundsatzfragen noch nicht geklärt, was insbesondere die Debatte zur „Netzneutralität“ zeigt. Dringender Forschungsbedarf liegt daher vor allem bei interdisziplinären Ansätzen, die nach konkreten Lösungen für komplexe und kollidierende Interessenslagen im Spannungsverhältnis zwischen Netzfreiheit und Marktinteressen suchen.

3.1.8 Forschungspolitische Herausforderungen im Datenschutz und der Informationssicherheit

Die Umsetzung der Regeln für den Datenschutz und der Informationssicherheit bedarf einer juristischen wie technologischen Anwendungsforschung. Die Bedeutung des Wissens als wesentliche Produktionsressource und nicht mehr eines nur unterstützenden Faktors bedingt eine wesentliche Änderung in der Compliance. Es genügt nicht mehr, vereinzelte Datenanwendungen datenschutzgerecht zu gestalten; vielmehr muss der gesamte Datenfluss einer Organisation den Kriterien des Datenschutzes und der Informationssicherheit entsprechen. Das Recht gibt hier nur den Rahmen vor; es bedarf der angewandten Forschung, die Regeln wenn notwendig zu verfeinern bzw. eine praktikable Anwendungspraxis zu finden.

Wesentliche Themen sind: Identitätsmanagement, sichere Netzwerke, Verschlüsselung, Pseudoanonymisierung, Anonymisierung, Privacy Impact Assessment, Privacy by Design, Privacy by Default etc. Hierbei geht es in erster Linie darum, eine zweckmäßige Umsetzungspraxis des rechtlichen Regelungsumfelds zu finden. In einigen Fällen wird es auch nötig sein, ergänzende rechtliche Regelungen zu erlassen. Als Beispiel seien hier detailliert e-Health, Active & Assisted Living (AAL) oder Arbeitnehmerdatenschutz angeführt.

Dass sich im Rahmen der Umfrage 44% der Befragten wünschen, dass WissenschaftlerInnen und TechnikerInnen stärker über mögliche negative Folgen ihrer Entwicklungen nachdenken[75], zeigt jedenfalls, dass nicht nur die Praxis sondern schon die Forschung präventiv mehr Verantwortung übernehmen sollte.

[75] Siehe Kapitel 3.5.5.

3.1.9 e-Health und Active & Assisted Living (AAL)

Das besondere Merkmal des e-Health-Bereichs liegt in der Tatsache begründet, dass bei jeder Datenverarbeitung grundsätzlich „sensible Daten“ (vgl. die Legaldefinition in § 4 Z 2 DSG) betroffen sind, weil alle im Gesundheitswesen verarbeiten personenbezogenen Daten potentiell Aufschluss über die Gesundheit eines Menschen geben. In Bezug auf IT-Sicherheit ist damit zwar der höchste Sorgfaltsmaßstab gefordert. Wie auch in anderen Bereichen gilt es, eine angemessene Balance von Sicherheit, Compliance und Nutzerfreundlichkeit zu erreichen – wofür natürlich die Besonderheiten der Anwendungsebene e-Health auch in der korrespondierenden IKT-Entwicklung zu berücksichtigen sind. Es geht hier vor allem darum, im Sinne eines „Design Thinking“[76] in jeder Phase der Entwicklung – und besonders schon in der vorgelagerten oder begleitenden Forschung – alle Ebenen in Einklang zu bringen. Der Orientierungsrahmen besteht dabei in den Zielsetzungen in Kombination mit einem definierten prozessorientierten, dynamischen, über den gesamten Entwicklungs- und Lebenszyklus bestehenden Zugang.[77] Ein gutes Beispiel dafür liefert das Projekt „Antilope“, das teilweise mit Mitteln der EU-Kommission im „ICT Policy Support Programme (ICT PSP)“ gefördert wurde und sich auf die Interoperabilität im e-Health Bereich insbesondere in Europa konzentriert.[78]

Dringender Bedarf an Forschung und Entwicklung ist sowohl in technologischer als auch rechtlicher Hinsicht zur Absicherung der Zweckbindung bei der Verarbeitung gesundheitsbezogener Daten festzustellen. Hierzu ist auf die Ausführungen zu „Privacy by Design“ (Kapitel 5.17) und zur Nachvollziehbarkeit der Datenverarbeitung (Kapitel 5.18) zu verweisen. Welche Daten für welche Zwecke durch welche Stellen in welcher Weise verarbeitet und genutzt werden sollen und in welchem Ausmaß hierbei legitime öffentliche Interessen allenfalls auch Einschränkungen privater Interessen zu rechtfertigen vermögen, ist vor allem angesichts der Möglichkeiten durch Big Data (siehe Kapitel 4.1) bei weitem noch nicht hinreichend ausdiskutiert und erforscht.

Eine etwas weiter differenzierte Sicht erfordert Active & Assisted Living (AAL). Dies steht für technische Systeme, die Menschen mit gesundheitsbezogenen Einschränkungen bei der Bewältigung des Lebensalltags in der eigenen Wohnumgebung unterstützen. Dieses durch Technologie „co-betreute“ Wohnen, gelangt schon jetzt und in absehbarer Zeit verstärkt in der Betreuung älterer Menschen zur Anwendung. Letztlich geht es darum, ab wann der Einsatz

[76] Vgl. Design Thinking, 2015.

[77] Vgl. dazu den in Kapitel 3.1.4 beschriebenen „Plan – Do – Check – Act“ (PDCA) Zyklus im Informationssicherheitsmanagement.

[78] Vgl. Antilope Projekt Webseite.

von Technologie zur Betreuung hilfsbedürftiger Menschen die Grenzen der Menschenwürde berührt oder vielleicht sogar überschreitet. Die Grund- und Menschenrechte können hierbei als Orientierungsnormen nützliche Anhaltspunkte bieten. Gerade die Aspekte der Zuverlässigkeit (Safety, siehe dazu Kapitel 3.1.4) spielen hier eine noch stärkere Rolle als allgemein schon im gesamten Bereich e-Health.

Empfehlung:

Die FFG möge Projekte fördern, welche die besonderen Bedürfnisse des Gesundheitswesens nach sicheren und vertrauensvollen IKT-Lösungen bei der Forschung und Entwicklung von Informations- und Kommunikationstechnologien fokussieren. Besonders förderungswürdig sind Forschungsansätze im Sinne von „Privacy by Design“ mit der Zielsetzung einer angemessenen Balance aus Sicherheit, Zuverlässigkeit, Rechtmäßigkeit und NutzerInnenfreundlichkeit. Im Fokus sollen Projekte stehen, die primär die „IKT-Seite“ von e-Health und Active & Assisted Living (AAL) erforschen, wobei die verbundenen Anwendungsebenen angemessene Berücksichtigung finden sollen.

3.1.10 Die arbeitsrechtliche Dimension des Datenschutzes

Das österreichische Arbeitsrecht bestimmt, dass Kontrollmaßnahmen und technische Systeme zur Kontrolle der ArbeitnehmerInnen, welche „die Menschenwürde berühren“[79], nur mit Zustimmung des Betriebsrates zulässig und Gegenstand einer erzwingbaren Betriebsvereinbarung sein sollen – dies ist etwa bei Zutrittskontrollsystemen oder Videoüberwachung der Fall. Es gilt, die Balance zu finden, weil betriebliche Informations- und Datensicherheit bis zu einem gewissen Grad eine Überwachung der IT-Nutzung im Unternehmen erfordern und daher mit den Interessen der ArbeitnehmerInnen kollidieren.

Beachtenswert ist hierzu ein in Österreich in der Literatur entwickeltes[80], maßhaltendes System der „abgestuften Kontrollverdichtung“, das im Wesentlichen im BeamtInnendienstrecht[81] seit mehreren Jahren gesetzlich geregelt ist und sich auch als Modell für den privaten Bereich eignet. In diesem Modell werden drei Stufen unterschieden:

- Stufe 1: Maschinelle Überwachung zur Gewährleistung der Systemfunktionalität
- Stufe 2: Signifikante Abweichungen von der "normalen" IT-Nutzung
- Stufe 3: Zugriff auf Kommunikationsdaten bei Verdacht auf Rechtsverletzung

[79] § 96 Abs. 1 Z 3 Arbeitsverfassungsgesetz (ArbVG) idF BGBl. I Nr. 71/2013.

[80] Kotschy und Reimer, 2004.

[81] Verordnung der Bundesregierung über die private Nutzung der Informations- und Kommunikationstechnik-Infrastruktur des Bundes durch Bedienstete des Bundes (IKT-Nutzungsverordnung – IKT-NV).

Der entscheidende Ansatzpunkt für die Beurteilung der Zulässigkeit oder Unzulässigkeit einer Datenverwendung ist in erster Linie – wie schon oben erwähnt – der Zweck, zu dem diese durchgeführt wird. Auf Stufe eins steht daher die maschinelle Überwachung der Gewährleistung der Systemfunktionalität. Die Systemüberwachung soll mit möglichst wenig menschlicher Kenntnisnahme von IT-Gebrauchsdaten erfolgen. Dem Zweck „Gewährleistung der Systemfunktionalität" sind beispielsweise alle Maßnahmen zur Abwehr von Viren und sonstigen Attacken Unbefugter erfasst.[82]

In jeder der drei Kontrollstufen sind der für Grundrechtseingriffe maßgebliche Grundsatz der Verhältnismäßigkeit und das Gebot der Anwendung des jeweils gelindesten Mittels zu beachten. Die Einsicht in Kommunikationsinhalte als Kontrollmaßnahme sollte daher auf die absolut notwendigen Fälle beschränkt werden. Die Befassung von Vorgesetzen der ArbeitnehmerInnen sollte jeweils erst erfolgen, wenn der Kontakt der SystemadministratorInnen mit den betreffenden ArbeitnehmerInnen keine befriedigende Erklärung für die Abweichung im IT-Ressourcenverbrauch oder hinsichtlich des Verdachtsfalles ergeben hat. Über festgestellte, aber bereits im Gespräch mit den Betroffenen zufriedenstellend aufgeklärte Kontrollanlassfälle sollte Verschwiegenheitspflicht der SystemadministratorInnen bestehen.[83]

Empfehlung:

Die FFG möge Projekte fördern, deren Zielsetzung darin besteht, die Verhältnismäßigkeit betrieblicher Kontrollmaßnahmen zum Schutz der betrieblichen IT-Sicherheit gegenüber dem Recht der ArbeitnehmerInnen auf Schutz personenbezogener Daten (ArbeitnehmerInnendatenschutz) zu wahren. Zu bevorzugen sind dabei interdisziplinäre Forschungsansätze aus Recht und Technologie. Insbesondere in Hinblick auf weit verbreitete betriebliche IT-Systeme und Muster-Datenanwendungen, die unternehmens- und branchenübergreifend gleichartige Interessenskonflikte zeigen, ist die Erforschung und Entwicklung von Standardverfahren und -systemen für maßhaltende Überwachung sowohl für die Ebene der IT-Administration als auch der Unternehmensorganisation ein wesentliches Ziel. Die genannten, aus der österreichischen Rechtsordnung abgeleiteten, Prinzipien erscheinen bereits gut etabliert, ihre Umsetzung in die Praxis ist jedoch noch wenig behandelt und es bedarf daher anwendungsorientierter Forschung wie ein solches „Privacy Preserving Monitoring" in Einklang mit der österreichischen Rechtslage umgesetzt werden kann.

[82] Fercher, 2009, 9f.

[83] Kotschy und Reimer, 2014.

3.1.11 Bring Your Own Device (BYOD)

Eng verbunden mit dem Thema ArbeitnehmerInnendatenschutz ist das zunehmend verbreitete Phänomen, dass MitarbeiterInnen in einem Unternehmen ihre eigenen elektronischen Geräte (vor allem Smartphone, Tablet und Notebook) für betriebliche Zwecke verwenden wollen/sollen und diese daher mehr oder weniger intensiv in die betriebliche IT-Infrastruktur eingebunden werden. Diese Entwicklung wird auch im deutschsprachigen Raum mit der englischen Formulierung „Bring Your Own Device“ (BYOD) bezeichnet.

Die Nutzung privater Endgeräte im Rahmen einer betrieblichen IT-Infrastruktur bringt zunächst zusätzliche Risiken für die IT-Sicherheit mit sich. Damit die ArbeitgeberInnen tatsächlich die Kontrolle über ihre IT-Systeme behalten, wird häufig ein gewisses Maß an Kontrolle in Bezug auf die privaten, betrieblich integrierten Endgeräte erforderlich. In diesem Zusammenhang stellen sich vordringlich die Fragen des ArbeitnehmerInnendatenschutzes umso mehr, als hier potenziell der Kernbereich privater Lebensführung der MitarbeiterInnen berührt ist. Über den Datenschutz hinaus erfordert BYOD auch die Beachtung anderer Rechtsfragen, etwa zur Gestaltung im Arbeitsvertrag bzw. in einer Betriebsvereinbarung oder Organisationsrichtlinie, die Regelung der Vergütung, die Regelung des Zugriffes durch die ArbeitgeberInnen auf betriebliche Daten auf einem privaten Endgerät, die Regelung der zeitlichen Nutzung, Regelungen zur Wartung und Verwendung des Gerätes, Regelungen des Umganges bei Beschädigung oder Verlust des Gerätes (mitsamt Daten), das Lizenzmanagement (Urheberrecht), den Einsatz von Mobile Device Management Software und schließlich auch steuerrechtliche Überlegungen.

Empfehlung:

Die FFG möge Forschungsvorhaben fördern, die sich mit der österreichischen Rechtslage betreffend die Integration privater Endgeräte in eine betriebliche IT-Infrastruktur beschäftigen. Besonders forciert werden sollten die Auswirkungen rechtlicher Vorgaben auf Technologieentscheidungen sowie vice versa der Einfluss von Technologieentscheidungen auf die zulässige Rechtsgestaltung. Interessant sind dabei Projekte, welche Fragen adressieren, die sich unternehmens- und branchenübergreifend im Zusammenhang mit BYOD stellen.

3.1.12 Rechtsdurchsetzung

Während bestehende Datenschutzbestimmungen aufgrund ihrer Technologieneutralität nach wie vor besser auf aktuelle technologische Entwicklungen anwendbar sind, als vielfach angenommen wird, ist der primäre Grund für unzureichende Datenschutzsituation im Internet,

insbesondere im Zusammenhang mit den dort dominierenden US-Unternehmen, die mangelnde Durchsetzung des Datenschutzrechts.

Eines der prominentesten Beispiele dafür – unter unzähligen alltäglichen Beispielen – ist der Wiener Datenschutzaktivist Max Schrems[84], der Facebook zahlreiche Verstöße gegen geltendes Datenschutzrecht nachweisen konnte. Seine bereits vor mehreren Jahren bei der zuständigen irischen Datenschutzbehörde eingebrachten Beschwerden gegen diese klaren und klar belegten Rechtsverstöße hatten für Facebook bisher keine juristischen Konsequenzen und dauern größtenteils weiter an.

Das Problem liegt wesentlich darin begründet, dass im internationalen Rechtsverkehr und vor allem in Bezug auf internationale Rechtshilfe häufig keine effektiven Durchsetzungsmechanismen bestehen. Darüber hinaus besteht auch innerhalb der EU das Problem, dass die nationalen Datenschutzbehörden – oft aufgrund mangelhafter Ressourcenausstattung – nicht in der Lage sind, Datenschutzvorschriften effektiv durchzusetzen[85].

Empfehlung:

Die FFG möge Forschungsvorhaben fördern, die sich spezifisch mit den Gründen der unzureichenden Rechtsdurchsetzung im Datenschutzrecht beschäftigen und Lösungen zur Verbesserung dieser Situation erarbeiten. Dies ist auch für die österreichische IKT-Branche von hoher Bedeutung, denn die geschilderte mangelnde Rechtsdurchsetzung auf internationaler Ebene führt zu einem Wettbewerbsnachteil österreichischer Unternehmen, die sich an das österreichische Datenschutzrecht halten müssen.

3.2 IT-Sicherheitsrecht

Dieser Abschnitt beantwortet die Frage, welche rechtlichen Rahmenbedingungen für die Informationssicherheit bestehen und in absehbarer Zukunft bestehen werden.

3.2.1 Allgemeines

Zu nennen sind dabei zunächst die im Zusammenhang der Verarbeitung personenbezogener Daten bestehenden, bereits erwähnten Datensicherheitsbestimmungen, die sich aus dem Datenschutzrecht ergeben, in Österreich aus § 14 DSG.

[84] Vgl. Europe vs. Facebook Webseite, wo auch die von ihm angestrengten Verfahren ausführlich dokumentiert sind.

[85] Siehe dazu die Vergleichsstudie der European Union Agency for Fundamental Rights (FRA), 2014.

Demzufolge hat jede Organisationseinheit eines datenschutzrechtlichen Auftraggebers oder Dienstleisters "Maßnahmen zur Gewährleistung der Datensicherheit zu treffen. Dabei ist je nach der Art der verwendeten Daten, nach Umfang und Zweck der Verwendung, unter Bedachtnahme des Stands der technischen Möglichkeiten und in Bezug auf die wirtschaftliche Vertretbarkeit sicherzustellen, dass die Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind, dass ihre Verwendung ordnungsgemäß erfolgt und dass die Daten Unbefugten nicht zugänglich sind."[86] Aus den Vorgaben des § 14 DSG lassen sich folgende Prinzipien ableiten:[87]

- Kompetenzklarheitsprinzip: Klare und eindeutige Aufbauorganisation und Festlegung der Aufgaben und Befugnisse
- Auftragsprinzip: Klare interne Richtlinien für den Umgang mit Daten
- Belehrungspflichtprinzip: Information und Schulung der MitarbeiterInnen
- Zutrittsbeschränkungsprinzip: Zutritt nur für Berechtigte
- Zugriffsbeschränkungsprinzip: Zugriff nur durch Berechtigte
- Betriebsbeschränkungsprinzip: Verhindern unbefugter Inbetriebnahme
- Protokollprinzip: Protokollierung von Änderungen, Abfragen und Übermittlungen
- Dokumentationsprinzip: Dokumentation der ergriffenen Maßnahmen

Weitere rechtliche Vorgaben für die Informationssicherheit ergeben sich aus allgemeinen Bestimmungen, die unten behandelt werden. Im Strafrecht gibt es Delikte, die Eingriffe in Datenverarbeitungssysteme und in Datensicherheitsmaßnahmen sanktionieren. Diese werden ebenfalls unten näher behandelt.

Auf EU-Ebene wird derzeit eine Richtlinie zur Netzwerk- und Informationssicherheit („Cybersecurity-Richtlinie“/„NIS-Richtlinie“) verhandelt.[88] Ziel der Richtlinie ist es, die Sicherheit jener Infrastruktur und Systeme zu erhöhen, von deren Funktionieren unsere Gesellschaft und Wirtschaft abhängen. Dies soll durch bessere Vorbereitung und bessere Kooperation erreicht werden und durch die Verpflichtung der BetreiberInnen kritischer Infrastrukturen, wie z.B. Energie und Verkehr, der AnbieterInnen wichtiger Dienste der Informationsgesellschaft sowie der öffentlichen Verwaltung Sicherheitsrisiken angemessen zu managen und sicherheitskritische Vorfälle an die nationalen Behörden zu melden. Der Richtlinienentwurf sieht unter anderem die folgenden Maßnahmen vor:[89]

[86] § 14 Abs.1 DSG 2000.
[87] Vgl. Dohr et al., 2013.
[88] Europäische Kommission, 2013.
[89] Vgl. Rack, 2013.

- Jeder Mitgliedstaat erstellt eine Netzwerk- und Informationssicherheitsstrategie.
- Jeder Mitgliedstaat richtet eine zuständige Behörde für Cybersicherheit ein, die ein *Computer Emergency Response Team* (CERT) unterhält. CERTs sollen für die Bewältigung von Sicherheitsvorfällen und Risiken nach einem konkret festgelegten Ablauf zuständig sein.
- BetreiberInnen kritischer Infrastrukturen unterliegen einer Meldepflicht für bestimmte Sicherheitsvorfälle.
- Jeder Mitgliedstaat hat eine nationale NIS-Strategie anzunehmen, welche die strategischen Ziele und konkreten politischen und Regulierungsmaßnahmen enthält, mit denen eine hohe Netzwerk- und Informationssicherheit (NIS) erreicht und aufrechterhalten werden soll. Die nationale NIS-Strategie umfasst auch einen nationalen NIS-Kooperationsplan.
- Jeder Mitgliedstaat muss zumindest eine für die NIS zuständige nationale zivile Behörde benennen, deren Aufgabe in der Überwachung der Anwendung der Richtlinie auf nationaler Ebene und im Beitrag zu ihrer einheitlichen Anwendung in der Union liegt.
- MarktteilnehmerInnen[90] haben größere IT-Sicherheitsvorfälle an die Behörde zu melden. Solche Vorfälle können auch öffentlich bekannt gemacht werden, wenn die Bekanntmachung des Sicherheitsvorfalls im öffentlichen Interesse liegt. Die Behörde kann sicherstellen, dass die MarktteilnehmerInnen ihren Verpflichtungen hinsichtlich der Sicherheitsanforderungen und der Meldung von Sicherheitsvorfällen nachkommen, und verbindliche Anweisungen erteilen.
- Die zuständige Behörde, die Kommission und die ENISA bilden ein Kooperationsnetz für die Zusammenarbeit bei der Bewältigung von Sicherheitsrisiken und -vorfällen.
- Darüber hinaus bestimmt die NIS-Richtlinie, dass die MarktteilnehmerInnen zur Sicherheit der Netze und Informationssysteme Sicherheitsanforderungen zu erfüllen haben, und zwar haben sie geeignete und verhältnismäßige technische und organisatorische Maßnahmen zu ergreifen, um die Risiken für die Sicherheit der Netze und Informationssysteme, die ihnen unterstehen und die sie für ihre Tätigkeiten nutzen, zu erkennen und konkret zu bewältigen.

3.2.2 Standards und Zertifizierungen rechtlich betrachtet

In internationalen Standards zur Datensicherheit sind vor allem organisatorische Maßnahmen beschrieben, verknüpft mit abstrakten und technikneutralen Vorschlägen zur technischen

[90] Gemäß Artikel 3 Abs. 8 lit. a sind dies "Anbieter von Diensten der Informationsgesellschaft" sowie gemäß Artikel 3 Abs. 8 lit. b, geändert durch die legislative Entschließung des Europäischen Parlaments vom 13. März 2014, "Betreiber von Infrastrukturen, die für die Aufrechterhaltung zentraler wirtschaftlicher und gesellschaftlicher Tätigkeiten in den Bereichen Energie, Verkehr, Banken, Finanzmarktinfrastrukturen, Internet-Knoten, Lebensmittelversorgungskette und Gesundheit unerlässlich sind; vgl. Europäische Kommission, 2013.

Umsetzung. Die maßgeblichen internationalen Standards zur Informationssicherheit nach ISO/IEC 27000 sind rechtlich unverbindlich und ihre vollständige Implementierung erfordert einen hohen wirtschaftlichen Aufwand, weshalb nur eine geringe Zahl österreichischer Unternehmen zertifiziert ist. Diese Standards aus juristischer Sicht als verbindlichen Sorgfaltsmaßstab heranzuziehen wäre überschießend und für kleinere Unternehmen wirtschaftlich unverhältnismäßig. Umgekehrt ist eine ISO-27000-Zertifizierung allein juristisch noch kein „Persilschein“, wenngleich eine hinreichende strukturelle Sorgfalt bei der Datenverarbeitung dadurch indiziert ist. Diese Standards beziehen sich nämlich nicht auf bestimmte Anwendungen oder Risiken, sondern beschreiben vielmehr abstrakt die innerbetrieblichen Prozesse, um Informationssicherheit allgemein zu gewährleisten. Die Risikoanalyse, die Prioritätensetzung und die konkrete technische Umsetzung bleiben den Unternehmen überlassen.

Aus rechtlicher Sicht ist daher interessant, die Schnittmenge aus internationalen Standards wie ISO/IEC 27000 und den Datensicherheitsanforderungen aus dem Datenschutzrecht zu bestimmen:

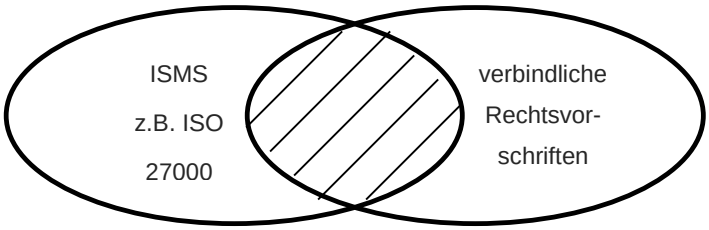


Abbildung 4: Schnittmenge zwischen internationalen Standards wie ISO/IEC 27000 und Recht

Die in der Abbildung schematisch dargestellte Schnittmenge zwischen unverbindlichen Industriestandards und verbindlichen Rechtsvorschriften könnte vor allem für kleinere und mittlere Unternehmen (KMU) sehr hilfreich sein, um auch ohne enorm aufwändigen Zertifizierungsprozess die Prioritäten für ein (eigenes) Informationssicherheitsmanagementsystem (ISMS) richtig zu setzen.

In Österreich wurde im Hinblick auf die Problematik des hohen Aufwands von Zertifizierungen bereits wichtige Arbeit geleistet, konkret durch das „Österreichische Informationssicherheitshandbuch“[91], welches stark an die ISO-27000-Reihe anknüpft, die Themen demgegenüber jedoch in etwas komprimierter Form auf insgesamt 730 Seiten darstellt. Gleichwohl ist dadurch das Problem des – für KMU zu großen – Aufwandes nicht gelöst. Kompaktere Darstellungen speziell für KMU wie beispielsweise das „IT-

[91] Chief Information Office - Stabsstelle IKT-Strategie des Bundes, 2013.

Sicherheitshandbuch für KMU“[92] der Wirtschaftskammer Österreich (WKO) sind zwar in dieser Hinsicht praktisch sehr nützlich, bieten aber keine Möglichkeit einer der Organisationsgröße angemessenen Zertifizierung.

Auch zum spezifischeren Bereich Datenschutz existiert bereits ein grundsätzlich europaweit anerkannter Standard für eine Datenschutz-Zertifizierung mit dem „EuroPrise“-Datenschutzsiegel[93]. Angeboten werden Zertifizierungen für HerstellerInnen und HändlerInnen von IT-Produkten und IT-basierten Diensten. Wenngleich die Zertifizierung nur für ein spezifisches Segment verfügbar ist und nur auf konkrete Produkte oder Dienste anwendbar ist, ist das „EuroPrise“-Siegel doch ein Leuchtturmprojekt, das auch unter österreichischer Forschungsbeteiligung entwickelt wurde.[94]

Der Vorschlag der EU-Kommission für eine neue „Datenschutz-Grundverordnung“ (siehe Kapitel 3.1.6) enthält in Artikel 39 Absatz 1 eine programmatische Bestimmung zum Thema Datenschutz-Zertifizierung: „Die Mitgliedstaaten und die Kommission fördern insbesondere auf europäischer Ebene die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -zeichen, anhand deren betroffene Personen rasch das von für die Verarbeitung Verantwortlichen oder von AuftragsverarbeiterInnen gewährleistete Datenschutzniveau in Erfahrung bringen können. Die datenschutzspezifischen Zertifizierungsverfahren dienen der ordnungsgemäßen Anwendung dieser Verordnung und tragen den Besonderheiten der einzelnen Sektoren und Verarbeitungsprozesse Rechnung.“

Allgemeine Vorgaben betreffend die Unternehmens-IT und somit auch die IT-Sicherheit im Unternehmen ergeben sich aus den Grundsätzen ordnungsmäßiger Buchführung des Unternehmensrechts. Für die breite Masse der Unternehmen ist dies der primäre und zumeist einzige Anlass für Prüfungen (Audit) der Unternehmens-IT. Das wichtigste Ziel dieser Prüfungen der IT-Systeme eines Unternehmens besteht in der Beurteilung der Verlässlichkeit der mit diesen Systemen erstellten Rechnungsabschlüsse; ausdrücklich ist jedoch ein weiteres Ziel auch die Beurteilung, ob sich aus den IT-Risiken des geprüften Unternehmens eine Gefährdung für dessen Fortbestand oder Entwicklung ergeben kann.[95] Die Informationssicherheit steht dabei in der Praxis jedoch nicht im Vordergrund.

Angesichts eines steigenden Risikos für „Cyber-Attacken“ quer durch alle Branchen stehen immer mehr Unternehmen vor der Frage, welcher konkrete Sorgfaltsmaßstab zur IT-Daten-

[92] Wirtschaftskammer Österreich, 2011.

[93] EuroPriSe Webseite.

[94] Einer der Partner war das Institut für Technikfolgenabschätzung der Österreichischen Akademie der Wissenschaften.

[95] Fachgutachten der Kammer der Wirtschaftstreuhänder über Abschlussprüfung bei Einsatz von Informationstechnik vom 20. Oktober 2004 (siehe Kammer der Wirtschaftstreuhänder, 2014, S. 3 und S. 7 ff.) und Fachgutachten der Kammer der Wirtschaftstreuhänder (2011) über die Ordnungsmäßigkeit von IT-Buchführungen.

und Informationssicherheit nun gefordert ist, um eine Haftung zu vermeiden, falls ein Schaden in dieser Hinsicht eintritt. Sowohl das Datenschutzrecht als auch die (wenigen) gesetzlichen Vorgaben zur IT-Sicherheit sowie die (teilweise oben beschriebenen) Standards und Normen geben keine konkreten Hinweise für bestimmte technologische Standards sondern sind bewusst technologieneutral. Solche Normen stellen grundsätzlich die Zielsetzung und die Leitprinzipien auf und beschreiben die Methodik, die Indikatoren, die Prozesse usw. Diese Normen sollen den AnwenderInnen helfen, die richtigen Fragen zu stellen und ihre eigenen Prozesse unter Kontrolle zu haben. Für die Informationssicherheit ist gewissermaßen „der Weg das Ziel“. Der Kern eines Informations-Sicherheits-Management-Systems (ISMS) besteht nämlich darin, Informationssicherheitsmanagement als dynamischen Prozess zu verstehen (Plan-Do-Check-Act-Zyklus) und Mechanismen auf organisatorischer und zugleich technischer Ebene zu schaffen, die mit Routinen und den richtigen Indikatoren zu einer hohen Informationssicherheit führen. Der jeweils konkrete Schutzzweck – oder anders betrachtet das jeweils konkrete Risiko, dem ein ISMS zu begegnen hat – ist aber entscheidend dafür, in welcher Sicherheitsklasse eine Information ein bestimmtes (mehr oder weniger hohes) Schutzniveau findet. Der globale Grundsatz ist, dass jede Information innerhalb eines abgeschlossenen Informationssystems vertraulich, integer und verfügbar ist. Welche Informationen nach außen gehen, und wer innerhalb des Systems über welche Informationen verfügt, soll eine bewusste Entscheidung der für das Informationssystem Verantwortlichen sein. Daher ist das Thema sehr stark ein organisatorisches. Damit korrespondiert, dass eine große Zahl von Cyberattacken mit der Methode des „Social Engineering“ arbeitet und z.T. die mangelnde Vorsicht der NutzerInnen für das Schrittweise erschließen von Sicherheitslücken nützt.

Leider besteht aktuell eine große Rechtsunsicherheit im Hinblick auf Haftungsfragen aus Verletzungen der Daten- und Informationssicherheit. Der Klärungsbedarf wird umso dringender, je mehr Komponenten in Wohnungen und Häusern und industriellen Fertigungsanlagen potenziell über das Internet erreichbar und damit angreifbar sind (Internet der Dinge). Die Judikatur zu solchen Fragen ist auch international noch spärlich. Ein interessanter juristischer Ansatz zur wissenschaftlichen Erschließung offener Fragen könnte hierzu sein, Anleihen aus der Judikatur zu anderen Regelungsbereichen zu nehmen, die mit ähnlichen Problemlagen wie das IT-Sicherheitsrecht konfrontiert sind. Hierzu könnte sich etwa das Umweltrecht eignen (Stichwort Umweltverträglichkeitsprüfung), interessant wäre aber wohl auch die Analyse von Finanz-Anlegerprozessen. Ähnlich wie im Internet gibt es nämlich auch auf den Finanzmärkten eine große Zahl an nicht oder nur schwer vorhersehbaren und beherrschbaren Risiken. Zugleich gibt es eine große Zahl von vorhersehbaren und auch beherrschbaren Risiken, bei deren Realisierung auch eine Haftung regelmäßig greift. Die

wesentliche Anforderung an die Sorgfaltspflicht besteht vor allem darin, zu erkennen, welche vorhersehbaren Risiken bestehen und wie diesen begegnet wird. Ein großes Interesse an einer möglichst umfassenden Klärung vieler noch offener Fragen sollten vor allem auch Versicherungsunternehmen haben, die immer häufiger direkt oder indirekt auch für Schäden aus dem Bereich der IT-Sicherheit haften.

Empfehlung:

Die FFG möge Projekte fördern, deren Zielsetzung die Entwicklung neuer, der österreichischen Rechtslage entsprechender Informationssicherheitsstandards sowie Datenschutz-Zertifizierungen für ganze Organisationen – nicht nur für spezifische Produkte und Dienstleistungen – ist. Forciert werden sollte gezielt die Entwicklung von Standards für den KMU-Bereich, für den eine Zertifizierung nach etablierten Standards zur Informationssicherheit regelmäßig zu aufwendig ist. Interdisziplinäre Forschungsansätze aus Recht und Technologie sollten auch der Systematik von Zertifizierungen selbst entsprechende Aufmerksamkeit widmen, also insbesondere der Akkreditierung von Zertifizierung-Stellen und AuditorInnen.

3.3 Weitere Themen aus rechtlicher Perspektive

3.3.1 Cybercrime

Im engeren Sinn bedeutet Cybercrime (auf Deutsch: Computerkriminalität oder Internetkriminalität) jedes unbefugte Eindringen in ein Computersystem sowie jedes unbefugte Abfangen oder Manipulieren von Daten oder Programmen. Im Kern geht es also um rechtswidrige Handlungen, deren Ziel eine Attacke auf das Computersystem selbst ist. Der Großteil der Tatbestände, welche in der „Cybercrime-Konvention“ des Europarats[96] normiert sind, bezeichnet eben solche Vorgänge. Synonym für diese Kategorie steht auch der Begriff „Hacking“, wenngleich dieser in seiner ursprünglichen Bedeutung nicht nur Handlungen in unredlicher Absicht erfasst. Das Ziel solcher Angriffe ist typischerweise das Verschaffen von (personenbezogenen oder systembezogenen) Daten sowie die Übernahme der Kontrolle über ein Computersystem, um dadurch weiteren Schaden anzurichten. Darüber hinaus erfasst die Cybercrime-Konvention auch Fälle des computerbezogenen Betrugs, also jedes Eingeben, Verändern, Löschen oder Unterdrücken von Computerdaten sowie jedes Eingreifen in den Betrieb eines Computersystems, in der betrügerischen oder unredlichen Absicht, sich oder einem anderen unbefugt einen wirtschaftlichen Vorteil zu verschaffen. In

[96] Council of Europe, 2013; nach dem Ort der Unterzeichnung auch „Budapest-Konvention“ genannt.

der Praxis handelt es sich dabei häufig um Angriffe, bei denen zunächst durch das Einschleusen einer Schadsoftware („Malware“) die Kontrolle über Komponenten eines Systems, z.B. über E-Mail-Programme, übernommen wird, um in der Folge unter einer falschen Identität (Identitätsdiebstal) Täuschungshandlungen zu setzen und die Opfer so zu einer Vermögensverschiebung zu veranlassen. Stetig wachsende Verbreitung findet aus dieser Kategorie auch der Einsatz von „Ransomware“. Dabei werden durch eine Schadsoftware Prozesse (z.B. eine Internetsitzung) oder das ganze Computersystem blockiert und die NutzerInnen werden via Anzeige am Monitor aufgefordert, einen bestimmten Geldbetrag zu zahlen, um die Sperre wieder aufzuheben. Typischerweise werden in diesem Zusammenhang auch staatliche Hoheitszeichen missbraucht, die erpresserische Aufforderung wird etwa als Einschreiten des Bundeskriminalamts getarnt und dem Opfer wird suggeriert, er habe sich selbst rechtswidrig Verhalten und könne sich nun „freikaufen“. Besonderes Schadenspotenzial besteht bei direkten Attacken auf Computersysteme dann, wenn besonders weit verbreitete Technologien kompromittiert sind[97] oder ein Angriff auf Dienste an neuralgischen Punkten in verbreiteten IT-Sicherheitskonzepten erfolgreich war. Wenn etwa große ZertifizierungsdiensteanbieterInnen (ZDA, englisch Certification Authorities oder kurz CA) oder die BetreiberInnen eines nationalen „Domain Name Service“ (DNS)[98] betroffen sind, steigert sich die Dimension der Gefährdung weil dadurch kritische Infrastrukturen betroffen sind.

Schließlich erfasst der Begriff Cybercrime im weiteren Sinn auch Delikte, die grundsätzlich auch „offline“ begangen werden können, bei denen jedoch regelmäßig das Internet gezielt als Tatmittel genutzt wird. Die Cybercrime-Konvention zählt aus dieser Kategorie ausdrücklich „Straftaten mit Bezug zu Kinderpornographie“ (Art 9) sowie „Straftaten in Zusammenhang mit Verletzungen des Urheberrechts und verwandter Schutzrechte“ (Art 10) auf. Dazu gehören aber auch die meisten Tathandlungen, die mit dem Schlagwort „Phishing“ (von „Password fishing“) bezeichnet werden. „Phishing“ erfolgt häufig ohne unmittelbare Einwirkung auf das Computersystem des (potenziellen) Opfers, typischerweise handelt es sich einfach nur um unerwünschte E-Mails („Spam“), die einen irreführenden Umstand mehr oder weniger glaubwürdig behaupten und damit die NutzerInnen veranlassen sollen, persönliche Daten und Passwörter preiszugeben (häufig die Zugangsdaten zum Onlinebanking-System mittels einer diesem nachgebildeten Eingabemaske). Die meisten „Phishing“-Angriffe sind zunächst weniger technologiebezogen, sondern viel mehr ein Versuch, einer psychologischen

[97] Siehe z.B. den 2014 publik gewordenen „Heartbleed“-Bug, eine Sicherheitslücke in der weit verbreiteten Open-Source-Bibliothek „OpenSSL“, die eine Vielzahl vertraulicher Systeme, insb. auch Onlinebanking-Systeme, gefährdet hat.

[98] Ein DNS sorgt für die Übersetzung von menschenlesbaren Internetadressen (www.xyz.com) in maschinenlesbare Adressen.

Manipulation („social engineering“) zur Preisgabe vertraulicher Informationen. Allerdings ist dies zumeist nur einer von vielen Schritten im Rahmen eines komplexen Betrugsschemas. Der größte Teil dieser Art „Spam“ wird über sogenannte „Botnets“ (siehe Begriffserklärungen Kapitel 2) verbreitet, womit wieder ein unmittelbarer Zusammenhang mit den Phänomenen des Cybercrime im engeren Sinn besteht. Der absolut überwiegende Teil aller Cybercrime-Attacken wird über solche „Botnets“ durchgeführt, womit als Spur am „Cyber-Tatort“ dann auch meistens die Internet-Zugangskennung (IP-Adresse) eines fernkontrollierten Rechners aufscheint, hinter der sich die tatsächlichen AngreiferInnen effektiv verstecken können.

Von den Erscheinungsformen des Cybercrime abzugrenzen sind jene Handlungen, bei denen Informations- und Kommunikationstechnologie schlicht zur Verabredung von Verbrechen in der „realen Welt“ genutzt werden. Im Rahmen von Ermittlungen gegen klassische Delikte wird daher immer häufiger auf IKT-Verbindungs- und -Zugangsdaten zurückgegriffen, um damit mutmaßliche TäterInnen zu identifizieren. Während bei echten Cybercrime-Delikten solche „Auskünfte über Daten einer Nachrichtenübermittlung“[99] nicht selten zu Beginn der einzige Ermittlungsansatz sind, handelt es sich im Bereich der klassischen Kriminalitätsbekämpfung regelmäßig um ein zusätzliches Instrument, welches die Ermittlungen erleichtern soll. In diesem Sinne war auch die EU-Richtlinie 2006/24/EG zur „Vorratsdatenspeicherung“ zu verstehen, welche der Gerichtshof der Europäischen Union (EuGH) am 8. April 2014 vollständig aufgehoben hat, weil sie mit der EU-Grundrechte-Charta unvereinbar war.[100] Aktuell kommt nun die öffentliche politische Debatte in Gang. Es geht darum, ob eine Lücke in der Verbrechensbekämpfung entstanden ist und welche (mit den Grundrechten zu vereinbarende) Ermittlungsinstrumente die Strafverfolgung im Hinblick auf IKT benötigt. Außer Zweifel steht jedenfalls, dass IKT-AnbieterInnen wie schon vor der Umsetzung der Vorratsdatenspeicherung weiterhin zulässigerweise Zugangs- und Verbindungsdaten für betriebliche Zwecke (insbesondere zur Rechnungslegung, aber auch für technische Zwecke) speichern[101] und diese Daten den Strafverfolgungs- und Sicherheitsbehörden auf Basis bestehender Rechtsgrundlagen[102] auch weiterhin zur Verfügung stehen.

Im Hinblick auf Maßnahmen zur Verhütung von Cybercrime lassen sich zwei wesentliche Ebenen identifizieren: Erstens lässt sich der überwiegende Teil durch entsprechendes Bewusstsein und Vorsicht auf Seiten der NutzerInnen relativ einfach vermeiden. Die meisten aller Angriffe sind auch technisch nur deshalb möglich, weil Dateianhänge oder Internetressourcen von unbekannten und nicht vertrauenswürdigen Quellen fahrlässig

[99] Vgl. § 134 ff Strafprozessordnung (StPO).

[100] Urteil des EuGH in den verbundenen Rechtssachen C-293/12 und C-594/12. Siehe dazu Abschnitt 3.1.7.

[101] Im Bereich der Mobil- und Festnetztelefonie im Regelfall zumindest für einen Zeitraum von drei Monaten.

[102] Siehe insbesondere §§ 134 ff StPO sowie § 53 Abs 3a und Abs 3b Sicherheitspolizeigesetz (SPG).

geöffnet werden, wodurch die initiale Schadsoftware überhaupt erst in das Computersystem gelangen und dort weiteren Schaden anrichten kann. Auch der Einsatz von handelsüblicher Virenschutz-Software und von „Firewalls“ vermag bereits einen großen Teil der Bedrohungen abzuwehren, wenn diese regelmäßig aktuell gehalten werden. Schließlich könnte eine ganz allgemeine Anhebung des Bildungsniveaus und der Medienkompetenz in der Bevölkerung weitgehend davor schützen, dass die Menschen allzu leichtgläubig auf (teilweise durchaus plumpe) Betrugsversuche („Phishing“) hereinfallen und geschädigt werden. Schulungsmaßnahmen zu Informations- und Datensicherheit sind daher sowohl im rein privaten als auch beruflichen/betrieblichen Zusammenhang ein sehr wesentliches Element des Informationssicherheitsmanagements. In dieser Hinsicht sind auf Seiten der NutzerInnen noch starke Informationsdefizite auszumachen, wie auch die Umfrageergebnisse bestätigen, wo nur 18% der NutzerInnen sich hinreichend informiert fühlen, obwohl 65% angeben, an Fragen des Datenschutzes tatsächlich interessiert zu sein.[103]

Die zweite Ebene betrifft die IT-Sicherheit im technischen Sinn. Die Verbesserung von Sicherheitsarchitekturen und konkreten Hard- und Softwarekomponenten zur technischen Informationssicherheit steht in einem ständigen Wettlauf mit der Entwicklung im Bereich der Schadsoftware. Sowohl in der kommerziellen als auch nicht kommerziellen Softwareentwicklung ist die ständige Suche nach Sicherheitslücken auf HerstellerInnen- wie auf AngreiferInnenseite eine ständige Begleiterin. Von entscheidender Bedeutung ist daher auch, Informationssicherheit als dynamischen Prozess zu begreifen, einmalige Maßnahmen sind mittelfristig selten hinreichend. Insofern ist hier auf die allgemeinen Aspekte der technischen Informationssicherheit zu verweisen.

Empfehlung:

Die FFG möge Projekte fördern, deren Zielsetzung die Stärkung des Risikobewusstseins sowie der digitalen Medienkompetenz auf Seiten der NutzerInnen von IKT-Systemen ist. Besonders zu fokussieren sind technologieimmanente Ansätze, welche den NutzerInnen schon aus der Systemkonzeption heraus bestimmte, besonders häufige Risikofaktoren bewusst machen und diese zum sicherheitsbewussten Handeln anleiten. Ein Beispiel hierfür sind etablierte Systeme für Passwortrichtlinien zur automatisiert begleiteten Wahl starker Passwörter.

[103] Vgl. Kapitel 3.5.4.

3.3.2 Hilfe, Selbsthilfe und Gefahrenabwehr durch Sicherheitsbehörden

Eine Gefährdung der IT-Sicherheit durch einen Einfluss von außen kann zwar denkmöglich auch ohne vorsätzliche Attacken von außen durch verschiedene Umstände entstehen, typischerweise hängt die Bedrohungslage jedoch mit mindestens einem vorsätzlichen Angriff zusammen. Daher ist auch die Frage naheliegend, ob und in welchem Umfang den österreichischen Sicherheitsbehörden und den Strafverfolgungsbehörden Befugnisse zur Abwehr und/oder zur Aufklärung solcher Angriffe zur Verfügung stehen, was im Folgenden beleuchtet wird.

Gefahrenabwehr nach dem Sicherheitspolizeigesetz

Für ein Unternehmen praktisch interessant ist u.U. die Frage, wann ein bestimmtes Cyber-Bedrohungsszenario ein Einschalten und Einschreiten der Polizei rechtfertigt. Für die Beurteilung dieser Frage ist vor allem zu untersuchen, ob durch die angenommenen Sachverhalte die Handlungs- und Eingriffsbefugnisse nach dem Sicherheitspolizeigesetz (SPG) aktiviert werden. Im Zentrum steht hierbei die Qualifikation eines Sachverhalts als „gefährlicher Angriff“ im Sinne des § 16 Abs. 2 und 3 SPG. Ein „gefährlicher Angriff“ ist unter anderem „die Bedrohung eines Rechtsgutes durch die rechtswidrige Verwirklichung des Tatbestandes einer gerichtlich strafbaren Handlung, die vorsätzlich begangen und nicht bloß auf Begehren eines Beteiligten verfolgt wird, sofern es sich um einen Straftatbestand (Z1) nach dem Strafgesetzbuch (StGB) handelt. Eine praktisch wichtige Erweiterung dazu normiert § 16 Abs. 3 SPG: „Ein gefährlicher Angriff ist auch ein Verhalten, das darauf abzielt und geeignet ist, eine solche Bedrohung (Abs. 2) vorzubereiten, sofern dieses Verhalten in engem zeitlichen Zusammenhang mit der angestrebten Tatbestandsverwirklichung gesetzt wird.“ Gerade bei typischen „Cybercrime“-Attacken sind ex ante häufig zunächst nur solche Vorbereitungshandlungen erkennbar, während die vollständige Verwirklichung eines Delikts nach dem StGB (dazu sogleich) oft erst sichtbar wird, wenn es bereits zu spät ist. In dieser Hinsicht ist die Ausdehnung des Begriffs des „gefährlichen Angriffs“ auf zeitnahe Vorbereitungshandlungen enorm wichtig, damit die Polizei rechtzeitig auch mit entsprechenden Befugnissen reagieren darf.

Die Kernfrage ist also letztlich, ob die Verwirklichung eines materiellen Straftatbestands des StGB bevorsteht und dieser Straftatbestand nicht als sog. „Privatanklagedelikt“ normiert ist, weil solche schon nach § 16 Abs. 2 SPG vom Begriff des „gefährlichen Angriffs“ ausgenommen sind. Die in Frage kommenden Straftatbestände sind vor allem die „Cybercrime“-Tatbestände des StGB, konkret sind dies: § 118a („Widerrechtlicher Zugriff auf ein Computersystem“), § 119 („Verletzung des Telekommunikationsgeheimnisses“), § 119a („Missbräuchliches Abfangen von Daten“), § 126a („Datenbeschädigung“), § 126b („Störung der Funktionsfähigkeit eines Computersystems“), § 126c („Missbrauch von

Computerprogrammen oder Zugangsdaten“), § 148a („Betrügerischer Datenverarbeitungsmissbrauch“) sowie § 225a („Datenfälschung“).

Selbsthilfe und Notwehr

Neben der Zulässigkeit des Einschreitens der Sicherheitsbehörden stellen sich auch die Frage der Zulässigkeit der eigenmächtigen Abwehr eines Cyber-Angriffs und die Frage, wie weit diese gehen darf. Dies wird unter dem Schlagwort „Offensive Security“ diskutiert. Notwehr ist grundsätzlich nach § 3 Strafgesetzbuch (StGB) zulässig und bedeutet, „wer sich nur der Verteidigung bedient, die notwendig ist, um einen gegenwärtigen oder unmittelbar drohenden rechtswidrigen Angriff auf Leben, Gesundheit, körperliche Unversehrtheit, Freiheit oder Vermögen[104] von sich oder einem anderen abzuwehren“, handelt nicht rechtswidrig. Die Handlung ist nach der folgenden Einschränkung in § 3 Abs 1 zweiter Satz StGB jedoch nicht gerechtfertigt, „wenn es offensichtlich ist, dass dem Angegriffenen bloß ein geringer Nachteil droht und die Verteidigung, insbesondere wegen der Schwere der zur Abwehr nötigen Beeinträchtigung des Angreifers, unangemessen ist“. Es ist also eine gewisse Verhältnismäßigkeit zu wahren, wobei das Gesetz hier zur Abwehr rechtswidriger Angriffe durchaus großzügig zugunsten dessen ist, der den Angriff abwehrt. Die Anforderungen an die Verhältnismäßigkeit der Mittel sind für private RechtsträgerInnen geringer als für Sicherheitsbehörden (Polizei). Nicht relevant ist zunächst auch die Verhältnismäßigkeit der betroffenen Rechtsgüter – außer es besteht ein offensichtliches krasses Missverhältnis (Grenze des „Notwehrexzesses“). Zulässig ist das gelindeste Mittel, das den Angriff zuverlässig abwehrt. Dabei ist z.B. offline-gehen, nur um sich einer Attacke zu entziehen, jedenfalls kein gebotenes gelinderes Mittel, d.h. der/die Angegriffene ist zu einem solchen bloß defensiven Verhalten nicht gezwungen, sondern ist zu einer aktiven Abwehr befugt.

Übertragen auf die IT-Welt ist jedenfalls technisch vorstellbar, dass eine Cyber-Attacke durch einen „Gegenangriff“ auf das System, von dem die Bedrohung ausgeht, abgewehrt wird. Sofern dabei nicht ein grobes Missverhältnis zwischen der abzuwehrenden Bedrohung und dem bei den AngreiferInnen durch die Notwehrmaßname entstehender Schaden besteht, wird eine solche „Cyber-Notwehr“ auch rechtlich zulässig sein. Vorsicht ist geboten, wenn das Bedrohungsbild noch eher abstrakt ist und ein „verdächtiges Angreifersystem“ gewissermaßen präventiv durch Cyberattacken unschädlich gemacht werden soll. Wichtig ist somit die Abgrenzung, ob bereits eine gegenwärtige oder unmittelbar drohende Gefahr besteht. Besondere Problematik dabei ist auch der Eingriff in Rechtsgüter Dritter, z.B. wenn der Angriff typischerweise von einem „Botnet“ ausgeht und sich der „Gegenangriff“ auf Computersysteme bezieht, die gar nicht im Eigentum der AngreiferInnen/TäterInnen stehen.

[104] Sog. „notwehrfähige Rechtsgüter“.

Ein solcher Eingriff in Rechte Dritter kann grundsätzlich nicht durch Notwehr gerechtfertigt sein, u.U. kann dies aber durch rechtfertigenden Notstand entschuldigt sein.

3.3.3 Digitale Forensik

Eine Studie zur digitalen Forensik in Österreich, durchgeführt von SBA Research im Rahmen der KIRAS-Sicherheitsforschung,[105] kam aus juristischer Sicht zu dem Ergebnis, dass die Beweiswürdigung hinsichtlich der Echtheit elektronischer Dokumente an sich sehr schwierig ist, in der gerichtlichen Praxis jedoch keine großen Probleme bereitet, weil diese Aufgabe faktisch an Sachverständige ausgelagert wird. Auf diese Weise begegnet man pragmatisch dem Problem, dass die Einbeziehung von Daten in elektronischer Form in den Prozess rechtlich nicht vorgesehen ist. Langfristig sollten jedoch Möglichkeiten einer solchen Einbeziehung entwickelt werden, da die Bedeutung digitaler Forensik weiter zunehmen wird.

Zur Frage der Rechtmäßigkeit des Sammelns von Beweismitteln ist auf die Ausführungen zum ArbeitnehmerInnendatenschutz zu verweisen. Siehe auch die grundsätzlichen Ausführungen zur digitalen Forensik in Kapitel 2.

3.3.4 Identitätsmanagement

Die derzeitige Situation betreffend elektronische Identitäten im Internet ist aus gesellschaftlicher und rechtlicher Sicht aus folgenden Gründen unzureichend und gefährlich:[106]

- Mangelnde Sicherheit: Die gängige Authentifizierung mittels Passwörtern tendiert in der Masse zur Unsicherheit, weil Passwörter häufig auf dem authentifizierenden Server unsicher gespeichert werden und von den NutzerInnen vielfach entweder unsichere Passwörter oder für mehrere unabhängige Anwendungsfälle identische Passwörter verwendet werden.
- Mangelnder Datenschutz: Bei jedem Service Provider muss ein eigenes BenutzerInnenkonto angelegt werden, wobei häufig mehr als nur die jeweils zwecknotwendigen Daten angegeben werden müssen. Die NutzerInnen verlieren den Überblick darüber, wer welche ihrer Daten hat, und diese Daten werden von den Service Providern potenziell missbraucht. Problematisch ist dies vor allem aufgrund der mangelnden Durchsetzbarkeit bestehender Datenschutzbestimmungen.
- Mangelnde Anonymität/Pseudonymität: Für viele Anwendungsfälle ist die Offenlegung der Identität der Betroffenen nicht erforderlich. So erfolgt der Kauf von Waren in Ladengeschäften in der Regel anonym. Oft reicht Pseudonymität aus, die es

[105] KIRAS Projekt; AFOR, 2012.

[106] Vgl. Schweighofer und Hötzendorfer, 2012, S. 429-438.

ermöglicht, dass die Identität nur im Fehlerfall aufgedeckt wird oder es interessieren nur bestimmte generische Eigenschaften (z.B. männlicher Hietzinger, 45-55 Jahre, mittleres Einkommen). Im Geschäftsverkehr im Internet sind sehr viele Vorgänge identifizierend und eine solche (partielle) Geheimhaltung der Identität bei gleichzeitiger Gewährleistung der Rechtssicherheit ist meist nicht möglich.

- Mangelnde Transparenz und Kontrolle: Das Schicksal einmal dem Service Provider übergebener Daten ist für die NutzerInnen nicht mehr nachvollziehbar und kontrollierbar.
- Mangelnde Nachweisbarkeit: Der qualifizierte Nachweis der Identität und einzelner Attribute ist häufig nicht möglich und somit können bestimmte Transaktionen, wie etwa die Eröffnung eines Bankkontos via Internet nicht durchgeführt werden.
- Mangelnder Komfort: Die Authentifizierung vor der Nutzung jedes einzelnen Service ist aufwändig, ebenso wie das sichere Verwalten der verschiedenen Passwörter. Ein weiteres Problem ist, dass die bei den verschiedenen Service Providern gespeicherten Nutzerdaten veralten. Dies sowie der Verwaltungsaufwand sind die wesentlichen Komfortnachteile aufseiten des Service Providers.

Die Lösung dieser Probleme ist daher eine der wesentlichen IT-Herausforderungen unserer Zeit.

Für Schneier[107] lassen sich alle drei Schutzziele der Informationssicherheit auf Zugriffskontrolle (Authentifizierung) reduzieren: Autorisierte Individuen sollen machen können (hierzu ist auch die Verfügbarkeit erforderlich), wozu sie autorisiert sind, und andere Individuen nicht. Näheres zum Identitätsmanagement siehe im entsprechenden Forschungsfeld in Kapitel 5.

3.4 Vertrauen: sozialwissenschaftliche Perspektiven

Die vorliegende IKT-Roadmap stellt eine Zukunftsvision unserer Gesellschaft dar: Welche Schlüsseltechnologien, welche Risiken, Probleme und Chancen sie als relevant identifiziert und welche nicht, ist Ausdruck bestimmter Vorstellungen von (nicht-) wünschenswerten Entwicklungen und der erste Schritt zu ihrer Verwirklichung.

Der technowissenschaftliche Fortschritt wirft mitunter kontroverse ethisch-moralische Fragen auf oder birgt komplexe und langfristige soziale, wirtschaftliche und ökologische Risiken, die in der Bevölkerung mitunter zu Misstrauen, Skepsis und Ablehnung führen. In den letzten Jahren und Jahrzehnten wurde daher die Forderung nach stärkerer demokratischer

[107] Schneier, 2000, S. 122.

Legitimation von Wissenschaft und Technik laut. Immer wieder wird auch eine stärkere Verantwortungsübernahme durch die WissenschaftlerInnen selbst bzw. ihre Auseinandersetzung mit den Folgen ihrer Forschungs- und Entwicklungsarbeit gefordert.

Dass auch die Nutzung von IKT nicht frei von Kontroversen ist, zeigt in aktuell der holprige Start des eHealth-Pilotprojektes ELGA (*Elektronische Gesundheitsakte*), das zwischen Gesundheitsministerium, Sozialversicherungsträgern, PatientInnenvertreterInnen und ÄrztInnenkammer noch immer umstritten ist. Ende Juni 2014 betrug der Stand der aktiven Abmeldungen potenzieller PatientInnen rund 165.000. Auch die zentrale Speicherung von SchülerInnen-Daten im Zuge des Projektes *Sokrates* wurde in den Medien kritisch diskutiert, nicht zuletzt aufgrund eines Datenlecks des BIFIE, das erst wenige Monate zuvor publik wurde. Neuen und erweiterten Formen der IKT-Nutzung, insbesondere im Bereich sensibler personenbezogener Daten (hier: Gesundheit, schulische Leistungen etc.) wird also immer wieder mit Misstrauen begegnet. Beispiele wie diese zeigen, dass es wichtig ist, alle relevanten Stakeholder und Interessensgruppen rechtzeitig „mit ins Boot zu holen“ und ihre Sorgen, Anliegen und Wünsche adäquat zu berücksichtigen, um „sozial robuste“ Innovation zu schaffen.

Aus sozialwissenschaftlicher Sicht stehen bei der Erstellung der IKT-Roadmap daher zwei Ziele im Vordergrund:

1 Der Prozess der Entwicklung der Roadmap selbst soll einen Aushandlungsprozess darstellen, der die Sichtweisen, Anliegen und Sorgen aller relevanten Stakeholder (aus Forschung, Wirtschaft und Zivilgesellschaft) berücksichtigt. Die Pluralität gesellschaftlicher Meinungen, Wünsche und Vorstellungen wird auf methodologisch fundierte Weise abgebildet und dadurch die Legitimität der Roadmap gewährleistet.
2 Im Zuge der Erstellung der Roadmap sollen Empfehlungen bzw. Vorschläge erarbeitet werden, wie die Forschungsförderung Rahmenbedingungen schaffen kann, die die Reflexion von ForscherInnen über (positive, negative, diskussionswürdige) Auswirkungen ihrer F&E-Tätigkeiten anregen. Künftig könnte etwa die Abschätzung von Technikfolgen durch ProjektnehmerInnen als ein Evaluationskriterium von Projektanträgen an die FFG etabliert werden. Die Dynamik von Forschung und Entwicklung soll dadurch nicht gebremst werden, im Gegenteil: Die Berücksichtigung sozialer, gesellschaftlicher, rechtlicher Herausforderungen kann an sich zu innovativen Lösungen führen. Es geht darum, Anreize für (sozial, wirtschaftlich, ökologisch) verantwortungsvolle und nachhaltige Forschung zu setzen.

3.4.1 Wieso ist die „soziale Robustheit“ von Technik und Wissenschaft wichtig?

Im österreichischen ebenso wie im europäischen politischen Diskurs wird technologischer Fortschritt vor allem als Frage des wirtschaftlichen Wachstums, der erfolgreichen Wettbewerbs- und Standortpolitik gerahmt. Der Zustimmung der Bevölkerung zu bzw. ihrem Vertrauen in wissenschaftliche und technologische Entwicklungen wird dabei große Bedeutung beigemessen. In Österreich zeigten sich die Folgen fehlender gesellschaftlicher Akzeptanz vielleicht am deutlichsten an der 1978 durch eine Volksabstimmung erzwungenen Nicht-Inbetriebnahme des (bereits fertiggestellten) AKW Zwentendorf.

Die Auffassungen darüber, *wie* die offensichtlich notwendige Zustimmung und das Vertrauen der Bevölkerung gewonnen werden können, klaffen jedoch mitunter weit auseinander. Die Wissenschafts- und Technologieforschung unterscheidet im Hinblick auf die Kommunikation zwischen Wissenschaft und Öffentlichkeit grundsätzlich zwei Paradigmen: das ältere Defizit- und das neuere Dialogmodell. Beide enthalten unterschiedliche Annahmen über „die Wissenschaft“, „die Öffentlichkeit“, ihre jeweiligen Rollen sowie ihr Verhältnis zueinander.

Das so genannte „Defizitmodell“ geht in idealtypischer Form von einem Informations-, möglicherweise auch einem Defizit an Interesse aufseiten der Bevölkerung aus, das zu Misstrauen und Skepsis gegenüber Wissenschaft und Technik führt. Deren Produkte werden hingegen als a priori positiv gesehen. Es gilt daher, die Bevölkerung über den „Segen“ der Wissenschaft und Technik auf ausreichende, verständliche und interessante (z.B. Infotainment) Weise aufzuklären. Es handelt sich um ein lineares „Sender-Empfänger-Modell“, sprich: eine zu optimierende kommunikative Einbahnstraße von der Wissenschaft zur Öffentlichkeit, welcher im Rahmen verschiedener Studien[108] erschreckende Ahnungslosigkeit in wissenschaftlich-technischen Fragen attestiert wird. Sind die Missverständnisse und Informationslücken jedoch erst einmal ausgeräumt, schwinden auch Ablehnung und Angst, und die „LaiInnen“ können von den positiven Methoden und Produkten der Wissenschaft überzeugt werden. Nicht zuletzt erlauben diesem Modell zufolge überhaupt erst fundierte Sachkenntnisse das Mitdiskutieren und -entscheiden der BürgerInnen z.B. im Rahmen eines Referendums über die Nutzung einer bestimmten Technologie.

[108] Beispiele hierfür sind die seit Jahrzehnten regelmäßig durchgeführte Studie “Science and Engineering Indicators“ *der US National Science Foundation* sowie die Eurobarometer-Umfragen zum Thema Wissenschaft und Technologie (Europäische Kommission 2005 und 2010). Relevanz, Formulierung und Antwortmöglichkeiten der gestellten Fragen bzw. Statements, die von den Befragten als „richtig“ oder „falsch“ zu klassifizieren sind, wurden jedoch teils stark kritisiert, ebenso wie ihre fehlende kontextuelle Einbettung (Lévy-Leblond, 1992). Abgefragt wird das „wissenschaftliche Verständnis“ der RespondentInnen mit Items wie „Das Zentrum der Erde ist sehr heiß“ (84 % der befragten US-Amerikaner antworteten 2012 mit „ja“), „Dreht sich die Erde um die Sonne oder die Sonne um die Erde?“ (74% der RespondentInnen tippten auf ersteres) und „Das Universum begann mit einer riesigen Explosion“ (nur 39% stimmten dieser Aussage zu) (National Science Board, 2014).

Die Annahmen dieses Modells, das am prominentesten in einem Dokument der britischen *Royal Society*[109] vertreten wird, wurden jedoch bald stark kritisiert und teils auch empirisch widerlegt[110]. Nicht die „uninformierte Bevölkerung“ sei das Problem, so die KritikerInnen, sondern vielmehr eine ignorante und verantwortungslose Wissenschaft, die ohne Rücksicht auf gesellschaftliche Sorgen, Werte und Bedürfnisse riskante technologische Entwicklungen vorantreibe. Der französische Physiker und Wissenschaftsphilosoph Jean-Marc Lévy-Leblond spricht von einem Paradoxon: Während den „LaiInnen“ wissenschaftliches Fachwissen abverlangt werde, bevor sie bei technischen, medizinischen, militärischen etc. Problemen mitdiskutieren dürften, würden von WissenschaftlerInnen und IngenieurInnen (die in Zeiten hochgradiger Spezialisierung ja selbst gerade *keine* universellen ExpertInnen, sondern in fast jedem Teilgebiet – außer ihrem eigenen – LaiInnen sind) keine vergleichbaren sozialen und politischen Kenntnisse verlangt. Diese wären jedoch notwendig, um die Art und Folgen der eigenen Arbeit bzw. Entdeckungen verstehen zu können[111]. Lévy-Leblond fragt somit, fast schon provokant: “What is more dangerous (in the short *and* in the long run): to have scientists doing nuclear or biomedical research without a clear idea about its possible social and economic impact, or to have the public refusing the risk of this impact without a good grasp of the fundamentals of the sciences involved?”[112]

3.4.2 Der „participatory turn“: aktive Einbindung der „BürgerInnen“

In Folge dieser Diskussion wurden die bisher vor allem durch ExpertInnen auf technokratischem Weg durchgeführten Technikfolgenabschätzungen durch partizipative Formen ergänzt, die seit dem so genannten „participatory turn“ der 1990er Jahre[113] – zumindest rhetorisch – zum Mainstream gehören. Es wurden seither zahlreiche Verfahren zur „BürgerInnenbeteiligung“ entwickelt, u.a. die in Dänemark entstandene *Consensus Conference*, der *Round Table* (siehe weiter unten) und zahlreiche weitere Formen. Die Verfahren unterscheiden sich hinsichtlich ihrer Dauer, Zielsetzung (offene Diskussion oder konsensueller „Abschlussbericht“), der beteiligten Personen („DurchschnittsbürgerInnen“ oder „VertreterInnen von Interessensgruppen“, siehe dazu auch die Ausführungen weiter unten), und nicht zuletzt hinsichtlich ihrer praktischen Anbindung an die Politik, was die tatsächliche Berücksichtigung bzw. Verwertung der Ergebnisse beeinflusst.

[109] The Royal Society, 1985.

[110] "[E]in Mehr an Information [führt] keineswegs automatisch zu größerem Vertrauen in die Wissenschaft […]. Vielmehr werden bestehende Werturteile durch die Informationsvermittlung oftmals eher bestätigt als verändert" (Irwin, 1995, zitiert nach Fochler und Müller, 2006, S. 5).

[111] Lévy-Leblond, 1992, 20.

[112] ibid.

[113] Jasanoff, 2003.

Seit Jahren besteht großes Interesse an der methodologischen Standardisierung von partizipativen Verfahren und deren Evaluation im Sinne von „Best Practice“-Vorgaben. Ob dies gelingen kann, wird jedoch mitunter bezweifelt[114], da die Anforderungen an und Rahmenbedingungen für partizipative Verfahren je nach Land teils sehr unterschiedlich ausgeprägt sind[115]. Das „Transferieren“ genormter Methoden von einem nationalen Kontext in einen anderen, ohne Berücksichtigung verschiedener politischer Kulturen und Rahmenbedingungen, sehen Felt und Fochler[116] daher als kaum erfolgversprechend.

Griessler[117] etwa beschreibt die Zivilgesellschaft in Österreich als schwach, die Möglichkeiten für direkte Demokratie als sehr beschränkt. Abgesehen vom allgemeinen Wahlrecht und der verpflichtenden Mitgliedschaft in Interessensvertretungen („Sozialpartner“: Arbeiterkammer, Wirtschaftskammer etc.) bestehe kaum Einbindung von BürgerInnen in den politischen Prozess. Dieser so genannte Neo-Korporatismus (d.h. Beteiligung von etablierten, organisierten Interessensvertretungen an politischen Entscheidungen) könne laut Degelsegger und Torgersen[118] vor dem Hintergrund eines jahrhundertealten paternalistischen Verhältnisses von Staat und Öffentlichkeit verstanden werden. Dieses reicht zurück bis ins 18. Jahrhundert, in die Anfangszeit österreichischer staatlicher Bürokratie. Bis heute wirke laut Degelsegger und Torgersen[119] der damals herrschende „aufgeklärte Absolutismus“ nach, der zwar „alles für das Volk, aber nichts durch das Volk“ umsetzen will. Lenkung und Information der unmündigen Masse zu ihrem besten Wohl[120]: Eine Strategie, die geradezu archetypisch dem Defizitmodell der Wissenschaftskommunikation entspricht.

Tatsächlich blieb noch bis in die 2000er Jahre hinein in österreichischen Politikdokumenten und Publikationen zum Thema Wissenschaft und Technologie dieses „traditionelle Defizit-Modell […] tief verankert“, wenngleich man sich immer wieder um eine „Dialog“-Rhetorik bemüht – die allerdings noch lange keinen ergebnisoffenen Dialog auf Augenhöhe meint[121].

Für den österreichischen Kontext ist somit deutlicher Aufholbedarf feststellbar, was die Einbindung der Öffentlichkeit in richtungsweisende Entscheidungen über die Entwicklung bzw. den Einsatz bestimmter Technologien betrifft.

[114] Felt und Fochler, 2008, S. 5.

[115] Für einen diesbezüglichen Vergleich zwischen der Schweiz und Österreich siehe Griessler, 2012.

[116] Felt und Fochler, 2008.

[117] Griessler, 2012, 74.

[118] Degelsegger und Torgersen, 2011.

[119] Ibid.

[120] „[P]olicy-makers aim to inform a public supposedly unaware of its own best interests, while they fear obstructive mobilization against their own, in their view, essential function to drive forward objectively necessary, sensible and useful policy projects, balancing powerful interests'' (Degelsegger und Torgersen, 2011, S. 392).

[121] Fochler und Müller, 2006, 16.

3.4.3 Governance von Wissenschaft und Technik – wer trägt die Verantwortung?

Unbestreitbar ist, dass technologische Entwicklungen durch ganz bestimmte normative Visionen der Gesellschaft angetrieben werden (*Ko-Produktion* von Wissenschaft und Gesellschaft[122]). Diese Vorstellungen und die ihnen zugrundeliegenden Prämissen über die Gesellschaft bleiben jedoch meist implizit. Ihnen wird daher mitunter vorgeworfen, nicht ausreichend gesellschaftlich ausverhandelt zu werden und somit nicht demokratisch legitimiert zu sein[123]. Tatsächlich stellt sich die Frage, wer die AkteurInnen im Feld der Governance von Wissenschaft und Technologie überhaupt sind und wie bzw. wie stark sie Einfluss auf die Steuerung von Technologie und Wissenschaft nehmen (können).

Anhand der begleitenden Untersuchung eines *Round Tables*[124] zum Thema Genomforschung zeigen Felt und Fochler, dass österreichische BürgerInnen die Governance von Wissenschaft (insbesondere in Hinblick auf deren langfristige soziale Folgen) als chaotisch und undurchsichtig wahrnehmen. Der Staat wird als machtloser Akteur in einem Netz verschiedener Player gesehen, die ihre jeweiligen Eigeninteressen verfolgen[125]. Die teilnehmenden GenomforscherInnen pochten ihrerseits zwar auf Selbstregulation der Wissenschaft (z.B. durch Einhaltung ihres „Forschungsethos“) als effektivste[126] Möglichkeit der Steuerung, gleichzeitig beriefen sie sich aber auch auf ihre Tätigkeit in der vermeintlich neutralen „Grundlagenforschung“, um jegliche Verantwortung für mögliche längerfristige soziale Folgen (im konkreten Beispielfall durch die Entwicklung einer „Anti-Fett-Pille“) zu negieren.

Wie, durch wen bzw. ob überhaupt eine politische Lenkung des Systems „Wissenschaft“ im Sinne (gesamt-)gesellschaftlicher Interessen stattfindet, ist also aus Sicht der BürgerInnen in der Studie von Felt und Fochler[127] unklar bzw. höchst zweifelhaft; keiner der beteiligten

[122] Jasanoff, 2006.

[123] "[T]echnological developments are driven by particular visions for society that are normative. Because these visions (and the latent premises that underpin them) are implicit and not negotiated by society, they are, in effect, undemocratic." (Russell, Vanclay & Aslin 2010, 109); siehe auch Levy-Leblond, 1992, 20.

[124] Es handelt sich um ein Design, welches von der Schweizer Organisation Science et Cité übernommen und adaptiert wurde. Eine Gruppe von (hier: 14) BürgerInnen und WissenschaftlerInnen beschäftigt sich im Zuge mehrerer Diskussionen über einen längeren Zeitraum mit einem bestimmten Thema. Der Ablauf ist kaum vorherbestimmt, sondern kann von den TeilnehmerInnen selbst entwickelt werden. Es wird kein vordefinierter Output (z.B. Konsenspapier) erwartet. Die insgesamt sechs „Round Table“-Sitzungen in der Studie von Felt und Fochler dauerten jeweils einen ganzen Tag und fanden in einem Zeitraum von acht Monaten statt (Felt und Fochler, 2010, 7f.).

[125] Felt und Fochler, 2010, 15.

[126] "[G]overnment was seen [by participants, Anm.] as a weak actor in the governance of science. Especially scientists repeatedly underlined the state’s limited ability to govern science in comparison to the self governance capacity of science. A first reason they gave for this was that governmental regulation would always be lagging behind science in its ability to recognise and address any dangerous developments within science." (Felt und Fochler, 2010, 12).

[127] Felt und Fochler, 2010.

AkteurInnen scheint Verantwortung für den Prozess als Ganzes zu tragen. Diese Situation wird von den BürgerInnen als potenziell bedrohlich wahrgenommen.[128]

Eine zentrale „Stellschraube" der Governance von Wissenschaft und Technologie ist freilich die Lenkung von Forschungsfinanzierung. Welche Themen bzw. Projekte mit öffentlichen Geldern gefördert werden sollen ist gleichzeitig Steuerungsinstrument und verdichtete Manifestation von (im besten Fall) gesellschaftlich geteilten Zukunftsvisionen. Die Einbindung von BürgerInnen, Stakeholdern, kurz: allen, die an der Mitgestaltung der Zukunft von Technik und Gesellschaft interessiert sind, sollte gerade an diesem Punkt ansetzen. Je weiter „Upstream" die Beteiligung stattfindet, d.h. je früher im Entwicklungsprozess und somit *vor* der Schaffung vollendeter Tatsachen[129], desto größer ist der tatsächliche Gestaltungsspielraum und desto weniger kann dem Prozess ein „Demokratiedefizit" vorgeworfen werden.

Einbindung der Öffentlichkeit bedeutet dabei *nicht*, dass nur möglichst „unbedarfte" DurchschnittsbürgerInnen[130] teilnehmen dürfen, um die Meinung der Bevölkerung „repräsentativ" abzubilden. Auch die Einbindung von AktivistInnen, organisierten Interessensgruppen, Personen bzw. Vereinigungen, die aus irgendeinem Grund bereits ein starkes (kollektives) Interesse und Engagement für dieses Thema mitbringen, ist laut Wehling legitim, sinnvoll oder sogar notwendig; kurz: „interessenorientierte zivilgesellschaftliche Einmischung [spielt] eine wichtige Rolle bei der polyzentrischen Governance von Wissenschaft und Technik"[131]. Ganz grundsätzlich ist zu vermeiden, eine kleine, ausgewählte Gruppe von BürgerInnen als die „exklusive Repräsentanz" und „Stimme" der gesamten Bevölkerung zu verstehen.

Auch der große Einfluss von Normierungs- und Verwaltungsorganisationen auf die Gestaltung von Technologien darf nicht unterschätzt werden – und auch hier gibt es Bestrebungen für mehr Transparenz und Demokratie. Ein aktuelles Beispiel stellt der Versuch der „Demokratisierung" der Internet Corporation for Assigned Names and Numbers (ICANN), die wichtige Kontroll- und Verwaltungsfunktionen für das Internet (u.a. globale Zuteilung von IP-

[128] [The citizens'] central concern was the limited role of the state in governing the consequences of the knowledge produced in science. They saw no possibility to influence either the production of scientific knowledge or its inscription in society. In the course of this argument reference was made to assumed properties of scientific knowledge itself, and patterns of its societal uptake: knowledge was conceptualised as fluid, moving rapidly and hence as very likely to be taken up by other actors even if its development would be discontinued at a specific location. The uptake of scientific and technological knowledge was seen as a process, which is too complex and dynamic to be steered by government. […] Many citizens saw government as well as science as actors among many in an opaque and de-centralised network of governance. […] [T]hey assumed that these actors were mainly concerned with following their own interests, and neither able nor especially interested to govern the development of the system as a whole in a direction that would reflect broader public interests. Thus the situation was perceived as somehow chaotic and potentially threatening" (Felt und Fochler, 2010, 13).

[129] Felt, Fochler und Müller, 2006, S. 106.

[130] „hitherto uninformed, disinterested, unorganized, and therefore supposedly 'unbiased' individual citizens"; Wehling, 2012, S. 45.

[131] Wehling, 2012, S. 43f.

Adressen und Top Level Domains wie .com) wahrnimmt, dar. Dass die Organisation bisher im direkten Einflussbereich der US-Regierung stand, sorgte jahrelang für Kritik. Im März 2014 erklärte das Handelsministerium, dass ICANN jedoch fortan einem „multinationalen und aus diversen Bereichen zusammengesetzten Gremium unterstehen solle“. Aus diesem Zweck seien „Regierungen, Privatsektor, Zivilgesellschaft und andere Internet-Gesellschaften aus aller Welt [eingeladen], an der Gestaltung der neuen Strukturen teilzunehmen“.[132]

Doch auch weiter „Downstream“ ist die Beteiligung von ExpertInnen (z.B. SozialwissenschaftlerInnen) wichtig, um die gesellschaftliche Aufnahme einer Technologie, mögliche Verwendungsmöglichkeiten und deren soziale Folgen abzuschätzen (etwa im Rahmen „sozialwissenschaftlicher Begleitforschung“). Dadurch wird im besten Fall eine öffentliche Diskussion darüber angestoßen, welche Entwicklungen wünschenswert sind, welche nicht oder wo gegebenenfalls rechtliche Regulationen sinnvoll erscheinen. Bis dato fehlen jedoch Wegweiser, wann, wie, in welcher Form und welchem Umfang solche begleitenden Abschätzungen Teil von natur- oder ingenieurswissenschaftlichen Projekten sein sollen. In dieser Hinsicht soll die Roadmap mögliche Ansatzpunkte bieten.

Zwar ist festzuhalten, dass IKT *an sich* – im Gegensatz zu anderen Technologien, die „klassische Streitpunkte“ sind – meist weder eine potenzielle Verletzung ethisch-moralischer Grundüberzeugungen darstellen (wie etwa embryonale Stammzellenforschung), noch mit völlig unvermeidbaren Risiken bzw. Nachteilen behaftet sind, die bei der Nutzung der Technologie unweigerlich auftreten *müssen* (wie etwa die Notwendigkeit der Endlagerung von nuklearen Brennstäben, die ökologischen und geologischen Folgen von Schiefergas-Fracking etc.)[133]. Die gravierendsten „Schattenseiten“ von IKT liegen bis jetzt vor allem in der Möglichkeit der Verletzung bzw. Einschränkung von Persönlichkeitsrechten und Freiheiten (etwa Privatsphäre, Meinungsfreiheit, Versammlungsfreiheit) durch tatsächliche oder vermutete Überwachung sowie unzureichenden Datenschutz. Diesen Risiken kann, abgesehen von entsprechenden rechtlichen Rahmensetzungen und deren wirksamer Durchsetzung, auch durch bewusste technische Vorkehrungen („Privacy-by-Design“) zumindest teilweise entgegengewirkt werden. Vermeintlich „subtilere“ soziale oder psychische Auswirkungen von IKT, z.B. durch die allgegenwärtige Verfügbarkeit des Internets, die ständige Erreichbarkeit durch Mobiltelefone, den sich ändernden Umgang mit Wissen/Information durch nahezu unlimitierte elektronische Datenspeicherkapazitäten, die Veränderung sozialer Beziehungen durch die Teilnahme an digitalen sozialen Netzwerken etc., kommen vergleichsweise seltener zur Sprache, sollten aber stärker in den Fokus der

[132] Henkel, 2014.

[133] Eine Ausnahme sind Fragen aus dem Bereich der lernfähigen Maschinen bzw. „künstlichen Intelligenz“, Semantic Web etc. Diese werfen teils sehr wohl grundlegende ethische Fragen oder die Notwendigkeit der Auseinandersetzung mit schwer abschätzbaren Risiken auf.

Aufmerksamkeit rücken – nicht zuletzt auch bei den EntwicklerInnen selbst: „[I]f science is to meaningfully contribute to the growing debates on innovation governance, it will have to adopt a more integrated vision of science's role in society. For the single scientist, this may imply more actively taking the hybrid role of the scientist/citizen concerned about the impacts of scientific knowledge beyond the narrow short-term risks of his or her own work."[134]

Empfehlung:

Forschungsprojekte im Technologiebereich sollten verpflichtend eine Komponente zur Technikfolgenabschätzung enthalten, die schon im Förderantrag zu beschreiben ist. Wenn aufgrund der Natur des Forschungsvorhabens eine solche Komponente nicht sinnvoll erscheint, sollten die FörderungswerberInnen die Gründe dafür beschreiben. Falls das Forschungsvorhaben potenziell Auswirkungen auf größere Teile der Zivilgesellschaft hat, sollte idealerweise methodisch auch eine Inklusion von RepräsentantInnen der betroffenen Gruppen angestrebt werden.

Empfehlung:

Nützlich sind grundsätzlich Checklisten für die Technikfolgenabschätzung, die entweder Bestandteil eines Projektes in Bezug auf eine bestimmte Entwicklung sein könnten oder, bei entsprechend hoher Komplexität, im Rahmen eines eigenen Projekts entwickelt werden könnten.

Darüber hinaus ist es empfehlenswert, abseits von Technologieprojekten spezifisch sozialwissenschaftliche Forschung zur Auswirkung bestimmter neuer Technologien (z.B. Big Data, Smart Cities etc.) auf die Gesellschaft und die Menschen zu fördern.

Beispielprojekte hierzu sind etwa die Studie des ITA zu „Geodaten-Nutzung bei mobilen Geräten"[135] oder das EU FP7 Projekt „surprise"[136] zum Verhältnis von Sicherheit und Privatsphäre, an dem auch das Institut für Rechts- und Kriminalsoziologie (IRKS) beteiligt war. Mit den genannten und weiteren Forschungseinrichtungen besteht in Österreich in diesem Bereich bereits eine gewisse Stärke, deren weitere Förderung im Hinblick auf die oben beschriebenen Herausforderungen anzuraten ist.

[134] Felt und Fochler, 2010, S. 17.
[135] Rothmann et al., 2012.
[136] Surprise Projektwebseite.

3.5 Ergebnisse der Umfrage

Die Umfrage „Vertrauen in Informations- und Kommunikationstechnologien“ wurde im Rahmen des Projekts BEST AT zur vorliegenden Roadmap-Studie von 03.11. bis 21.11.2014 mithilfe eines Online-Fragebogens durchgeführt. Der Aufruf zur Teilnahme erfolgte über die elektronischen Nachrichten- bzw. „Social Media“ Verteiler der Österreichischen Computer Gesellschaft (OCG), des Arbeitskreises Vorratsdatenspeicherung (AK Vorrat), der Arbeiterkammer (AK) sowie durch Verbreitung über private Kanäle im Netzwerk der Studienautoren. Da die Teilnahme auf Selbstrekrutierung beruhte, erheben die Ergebnisse der Umfrage keinen Anspruch auf Repräsentativität in Hinblick auf die österreichische Gesamtbevölkerung. Das Ziel war vielmehr, ein Stimmungsbild (auch und gerade unter zivilgesellschaftlich engagierten bzw. interessierten AkteurInnen) einzufangen.

Insgesamt schlossen 163 Personen den Online-Fragebogen ab. An den Verteilungen von Merkmalen wie Geschlecht oder höchstem Bildungsabschluss zeigt sich, dass die Stichprobe kein Abbild der österreichischen Gesamtbevölkerung darstellt. Männer sind mit 58% deutlich überrepräsentiert, ebenso Personen mit akademischem Abschluss (50%) bzw. Matura (33%) als höchstem Bildungsabschluss. Das Durchschnittsalter der RespondentInnen liegt mit 40,5 Jahren (arithmetisches Mittel) jedoch relativ in der Nähe des Durchschnittsalters der österreichischen Gesamtbevölkerung von 42 Jahren[137], wobei die Spannweite in der Stichprobe von 18 bis 77 Jahren reicht.

3.5.1 Nutzungsintensität von IKT

Die erste Frage, „Welche der folgenden Dienste nutzen Sie?", umfasste insgesamt zwölf Items mit Antwortmöglichkeiten von 1 („seltener als 1x pro Monat“) bis 5 („mehrmals täglich“). Wenig überraschend werden Internet-Suchdienste, Mobiltelefonie und E-Mail am häufigsten genutzt – von rund 80% der RespondentInnen mehrmals täglich. Ebenfalls häufig genutzt werden „andere Dienste zur Übermittlung von Nachrichten über das Internet (z.B. WhatsApp)“, soziale Netzwerke und bargeldlose Bezahlung im Geschäft.

Der Mittelwert über alle zwölf Items, also die insgesamte „Nutzungsintensität“ beträgt bei den Frauen durchschnittlich 2,97, bei den Männern 3,06 (Skalenmittelwert). Zwischen den Geschlechtern kann somit kein relevanter Unterschied festgestellt werden.

Zwischen Alter und Nutzungsintensität liegt hingegen ein negativer Zusammenhang vor. Der Korrelations-Koeffizient nach Pearson (*r*) liegt bei -0,32 (schwacher bis mittlerer Zusammenhang), d.h. je höher das Lebensalter, desto niedriger die Nutzungsintensität von IKT. Da es sich nicht um eine repräsentative Stichprobe handelt, beschränken sich sämtliche

[137] Statistik Austria, 2014.

Aussagen auf den untersuchten TeilnehmerInnenkreis und die Angabe von Signifikanzniveaus entfällt.

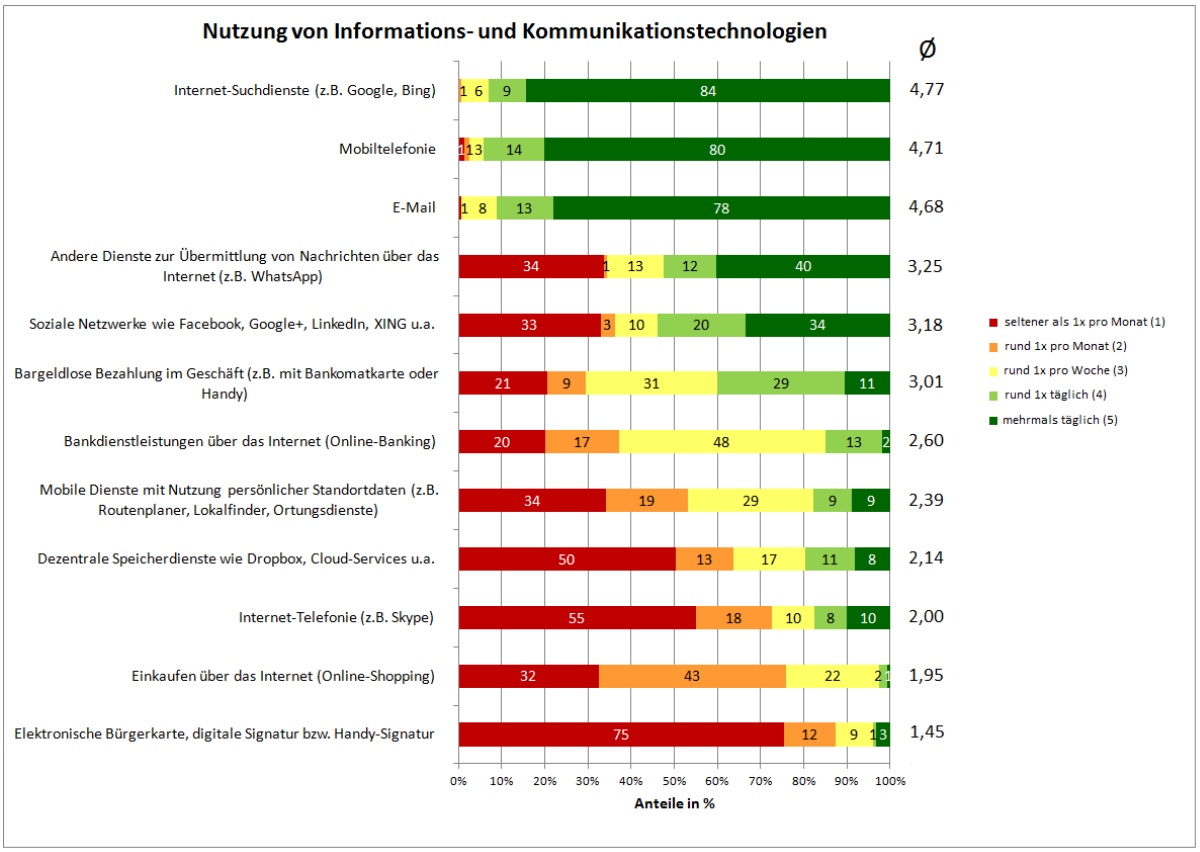


Abbildung 5: Nutzung von Informations- und Kommunikationstechnologien in Österreich

3.5.2 Vertrauen in IKT

Der zweite Fragenkomplex beschäftigte sich mit Vertrauen in einer Reihe verschiedener Informations- und Kommunikationstechnologien bzw. -dienste. Sie konnten jeweils mit einem Wert von 1 (gar nicht vertrauenswürdig) bis 4 (sehr vertrauenswürdig) beurteilt werden.

Unter den genannten Technologien bzw. Services genießen Online-Banking, die elektronische Bürgerkarte und andere digitale Signaturen sowie bargeldlose Bezahlung im Geschäft das größte Vertrauen. Diese werden von 87%, 72% bzw. 81% der RespondentInnen als „sehr“ oder „eher vertrauenswürdig“ eingestuft.

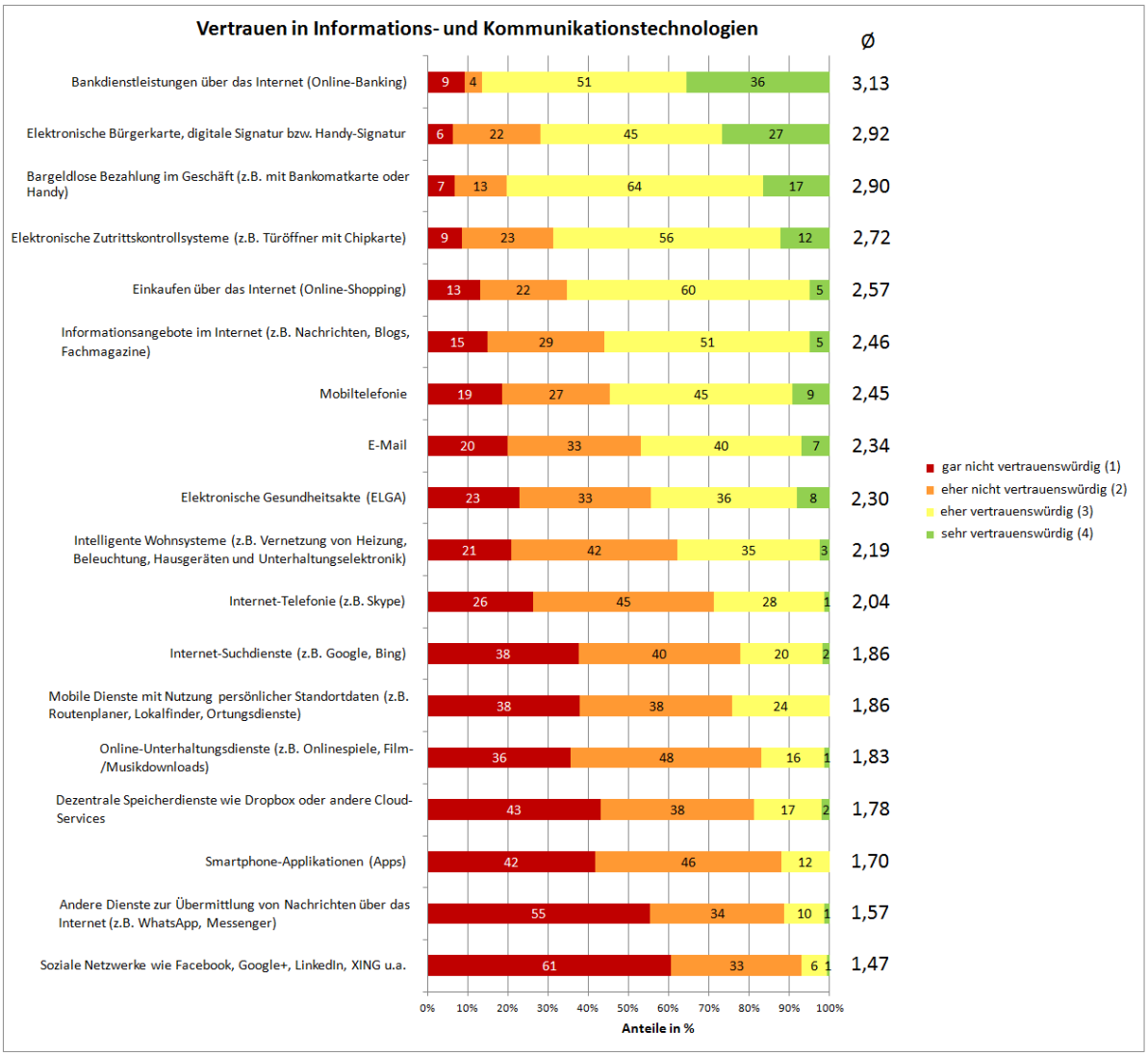


Abbildung 6: Vertrauen in Informations- und Kommunikationstechnologien

Die Mittelwerte etlicher Dienste liegen jedoch unter zwei und somit im „eher“ bis „gar nicht vertrauenswürdigen“ Bereich: Internet-Suchdienste, Standortdaten nutzende Dienste, Online-Unterhaltungsdienste, Speicherdienste wie Dropbox, Smartphone-Apps, Dienste zur Online-Nachrichtenübermittlung sowie soziale Netzwerke.

Die drei letztgenannten bilden dabei die Schlusslichter; sie werden von 88, 89 bzw. 94% der RespondentInnen als „eher“ bis „gar nicht vertrauenswürdig“ wahrgenommen. Interessant ist, dass die RespondentInnen somit gerade den häufig genutzten sozialen Netzwerken und Online-Messengerdiensten besonders misstrauisch gegenüberstehen. Diese werden offensichtlich *trotz* fehlender Vertrauenswürdigkeit genutzt.

Um dies genauer zu beleuchten, soll festgestellt werden, ob bzw. welcher Zusammenhang zwischen den Skalenmittelwerten „Nutzungsintensität“ (die Skala besteht aus allen in

Abbildung 5 angeführten Variablen) und „Vertrauen in IKT“ (aus allen in Abbildung 6 angeführten Variablen) besteht.

Zu diesem Zweck werden zwei lineare Regressionsmodelle berechnet. Modell 1, eine bivariate lineare Regression der Variable „Nutzungsintensität“ auf „Vertrauen in IKT“, weist einen niedrigen r^2-Wert von 0,04 auf (und „erklärt“ somit nur 4% der Varianz der Nutzungsintensität).

Es zeigt sich ein leichter positiver Zusammenhang: Ein Punkt mehr auf der vierstufigen Vertrauensskala führt zu einem 0,26 Punkte (β) höheren Wert bei der fünfstufigen Nutzungsintensität. Der p-Wert[138] von 0,025 wäre signifikant auf einem Niveau von $p < 0,05$, wenn es sich um eine repräsentative Stichprobe handeln würde. Die Konstante[139] liegt bei 2,46.

Nimmt man Alter als Kontrollvariable hinzu (Modell 2), erhöht sich r^2 auf rund 0,14. Die Konstante steigt nunmehr auf rund 3, und der β-Koeffizient von Vertrauen sinkt auf rund 0,24. Sein p-Wert würde nunmehr 0,030 betragen. Ein zusätzliches Lebensjahr führt in diesem Modell zu einer Abnahme der Nutzungsintensität um rund 0,012 Punkte (p-Wert: <0,001).

Zusammenfassend lässt sich festhalten, dass für den untersuchten TeilnehmerInnenkreis ein sehr geringer positiver Zusammenhang zwischen „Vertrauen“ und „Nutzungsintensität“ vorliegt, der auch bestehen bleibt, wenn man auf die Variable Alter kontrolliert (wie bereits festgestellt, macht das Geschlecht keinen nennenswerten Unterschied). Ob es sich dabei tatsächlich um eine kausale Beziehung handelt, und wenn ja, in welche Richtung diese verläuft (stärkere Nutzung durch höheres Vertrauen, oder stärkeres Vertrauen durch häufigere Nutzung) kann durch die Regression jedoch nicht beantwortet werden.

3.5.3 Datenschutz als (Grund-)Recht

Ein Variablenblock beschäftigte sich mit den Einstellungen zum Thema Datenschutz als (Grund-)Recht und dem Umgang der Politik mit diesem Thema.

48% sind der Meinung, dass das Thema „Internetsicherheit“ von der Politik nicht ausreichend ernst genommen wird, und weitere 28% stimmen „eher“ zu. Neun von zehn Befragten stimmen der Aussage „Der Schutz persönlicher Daten wird immer stärker ausgehöhlt“ (eher) zu.

Auch der Wunsch nach „Privacy by Design“ kommt stark zum Ausdruck: Rund 95% sind der Ansicht bzw. „eher“ der Ansicht, dass der Datenschutz schon in der Konzeption einer Technologie grundlegend sichergestellt werden soll.

[138] p-Wert: Wahrscheinlichkeit, ein solches Stichprobenergebnis bei Gültigkeit der Nullhypothese (hier: kein Zusammenhang zwischen Nutzungsintensität und Vertrauen) zu erhalten.

[139] Konstante: Geschätzter Wert der abhängigen Variablen, falls der Wert der unabhängigen Variable 0 ist.

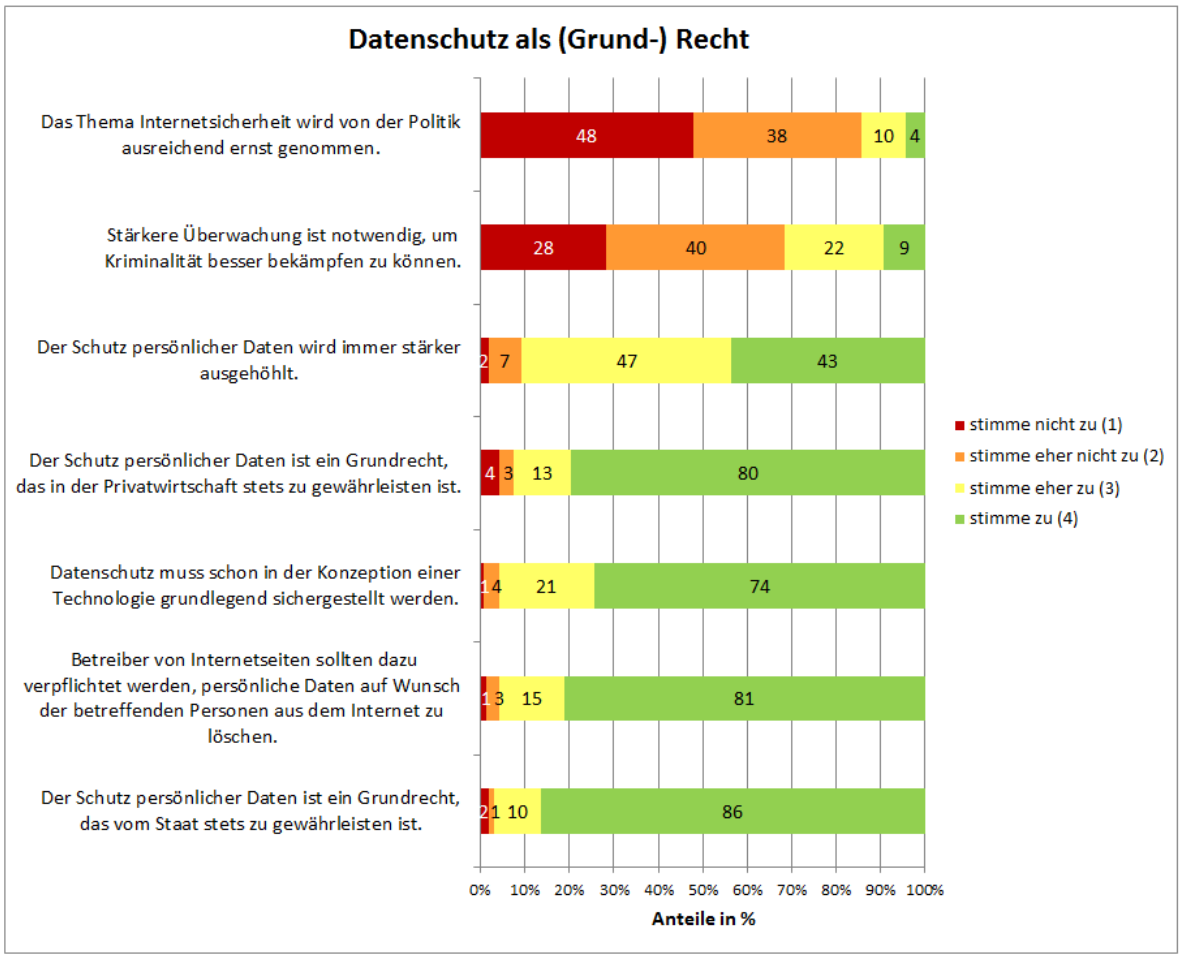


Abbildung 7: Datenschutz als (Grund-) Recht

3.5.4 Datenschutzbewusstsein im Alltag

Das Interesse am Thema Datenschutz ist hoch: 65% der Befragten geben an, sich dafür zu interessieren und 25% haben auch beruflich mit dem Thema Datenschutz zu tun. Diese hohen Werte sind vermutlich nicht zuletzt auf die Verbreitung der Umfrage durch die E-Mail-Verteiler von *OCG* und *AK Vorrat* zurückzuführen.

Interessant ist, dass sich trotzdem „nur“ 18% auch gut informiert fühlen. Es besteht also eine gewisse Diskrepanz zwischen bekundetem Interesse an Datenschutzthemen und der Einschätzung des eigenen Kenntnisstandes.

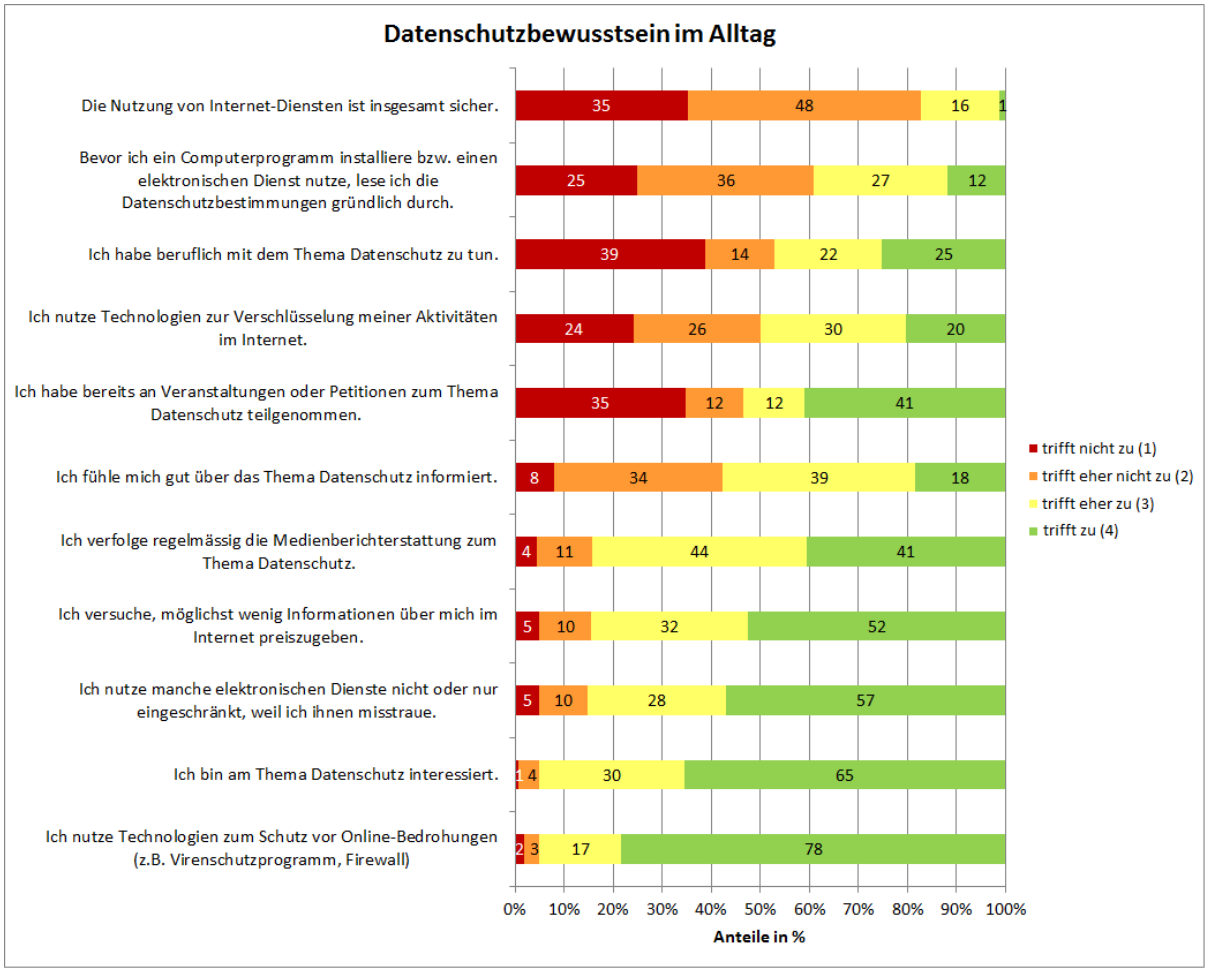


Abbildung 8: Datenschutzbewusstsein im Alltag

Interessant sind auch die Ergebnisse der beiden Fragen zum Thema „Vermeidungsverhalten“: Jeweils über die Hälfte der Befragten gibt an, manche elektronischen Dienste aus Misstrauen nicht oder nur eingeschränkt zu nutzen, sowie möglichst wenig Informationen über sich im Internet preiszugeben. Auf weitere 28 bis 32% trifft diese Aussage „eher“ zu. Dies korrespondiert mit der sehr geringen Zustimmung zur Aussage, dass die Nutzung von Internetdiensten „insgesamt sicher“ sei, sowie dem auf S. 66 beschriebenen Regressionsmodell, das einen schwach positiven Zusammenhang zwischen Vertrauen und Nutzungsintensität findet.

Der durchschnittliche Skalenmittelwert[140] „Datenschutzbewusstsein im Alltag“ beträgt bei Frauen 2,86, bei Männern 3,02.

[140] Die Skala „Datenschutzbewusstsein im Alltag“ besteht aus allen in Abbildung 8 angeführten Variablen außer „Die Nutzung von Internet-Diensten ist insgesamt sicher“, da es sich dabei inhaltlich weniger um die Beschreibung eigener Verhaltensweise handelt. Das Maß der internen Konsistenz der Skala, Cronbach's Alpha, kann durch den Ausschluss dieses Items von 0,621 auf 0,672 gesteigert werden.

3.5.5 Einstellungen zu Wissenschaft und Technologieentwicklung

Die Aussage, dass neue Technologien das Leben einfacher und komfortabler machen, spiegelt die Meinung eines großen Teils der Befragten wider. Insgesamt 87% stimmen hier zu bzw. eher zu. Gleichzeitig sind jedoch „nur“ 52% (eher) der Ansicht, dass neue Technologien die Gesellschaft zum Positiven verändern. Die Zunahme an Komfort geht also scheinbar mit gefühlten Nachteilen einher, die den „Saldo“ neuer Technologien (im Sinne ihrer Gesamtwirkung auf die Gesellschaft) in den Augen der Befragten trüben.

44% der Befragten wünschen sich, dass WissenschaftlerInnen und TechnikerInnen stärker über mögliche negative Folgen ihrer Entwicklungen nachdenken. Die Meinung, dass WissenschaftlerInnen und TechnikerInnen für entsprechende negative Folgen auch verantwortlich sind, vertreten nur noch 12% voll und ganz. Der Aussage, dass Technologie und Wissenschaft durch zu starke Regulation bereits in ihren Möglichkeiten eingeschränkt sind, stimmen 8% der Befragten zu.

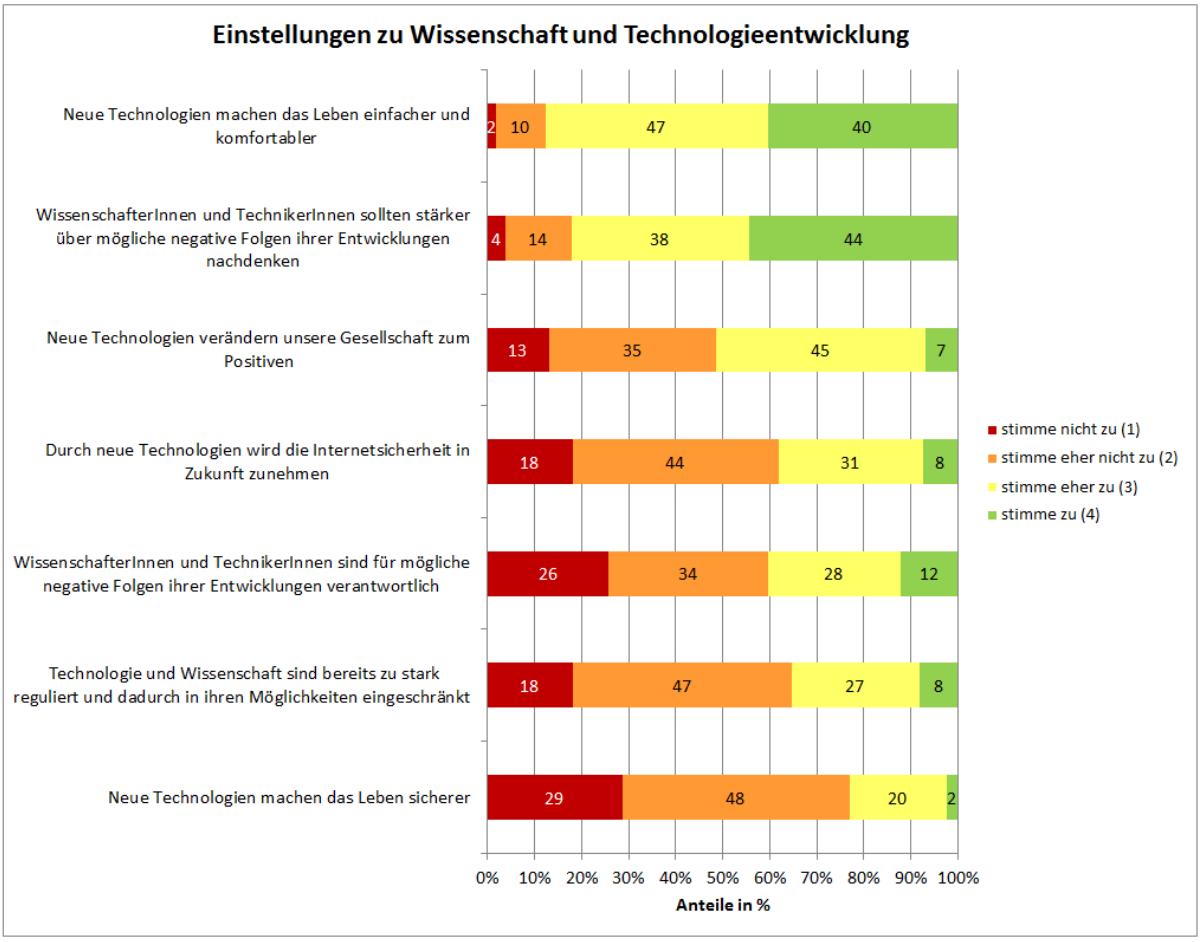


Abbildung 9: Einstellungen zu Wissenschaft und Technologieentwicklung

4 Emerging Technologies

In diesem Kapitel werden aufkommende Technologien in Österreich sowie ihre Potentiale zum Schutz von Informationen beschrieben. Aufgrund der zahlreichen und schnellen Entwicklungen der Informationstechnologie umfasst dieses Kapitel vorwiegend jene Themenfelder, welche in den ExpertInneninterviews sowie in der Recherche priorisiert wurden. Die Auswahl der Emerging Technologies basiert also auf den Angaben österreichischer ExpertInnen aus Wissenschaft und Wirtschaft und eigenen Recherchen. Ergänzt werden die Emerging Technologies in diesem Kapitel durch Leuchtturmprojekte in Kapitel 6. Zum besseren Verständnis werden die Themenbereiche mit Beispielanwendungen der jüngsten Vergangenheit bzw. prognostizierte Entwicklungsszenarien angereichert. Eine Zuordnung der Emerging Technologies zu den in Kapitel 5 beschriebenen Forschungsfeldern erfolgt in Kapitel 7 – Roadmap.

„*Eine neue Technologie führt meist zu einer neuen Sicherheitsproblematik*."

(Zitat aus den Interviews)

Einleitend stellen wir den österreichischen Markt für neue Technologien dar. Das folgende Diagramm zeigt die Bereitschaft der NutzerInnen neue Technologien zu erwerben (purchasing appetite) und die Chancen (opportunity) für IT-Service Provider und ihre angebotenen Services. Die Größe der Kreise illustriert die aktuelle Marktreife der verschiedenen Technologien in Österreich. Demnach haben Big Data Analysen, Internet of Things, Predictive Analysis und Mobilitätslösungen die höchste Marktreife und Spracherkennung die geringste. Die Kauflust ist in Österreich am Größten im Bereich Big Data Analyse, Predictive Analysis und Mobilität; bei diesen Technologien wurden auch die größten Chancen für IT-Service Provider festgestellt. Eine geringe Kauflust sowie weniger Chancen für Service Provider ist bei Spracherkennungs-Technologien und Business Intelligence[141] Lösungen festzustellen. [142] Die neuen Technologien (Emerging Technologies) werden in den folgenden Unterkapiteln näher erläutert.

[141] Sammelbegriff für den IT-gestützten Zugriff auf Informationen, sowie die IT-gestützte Analyse und Aufbereitung dieser Informationen. Siehe Springer Gabler Verlag, Stichwort: Business Intelligence.

[142] Vgl. IDC, 2015a.

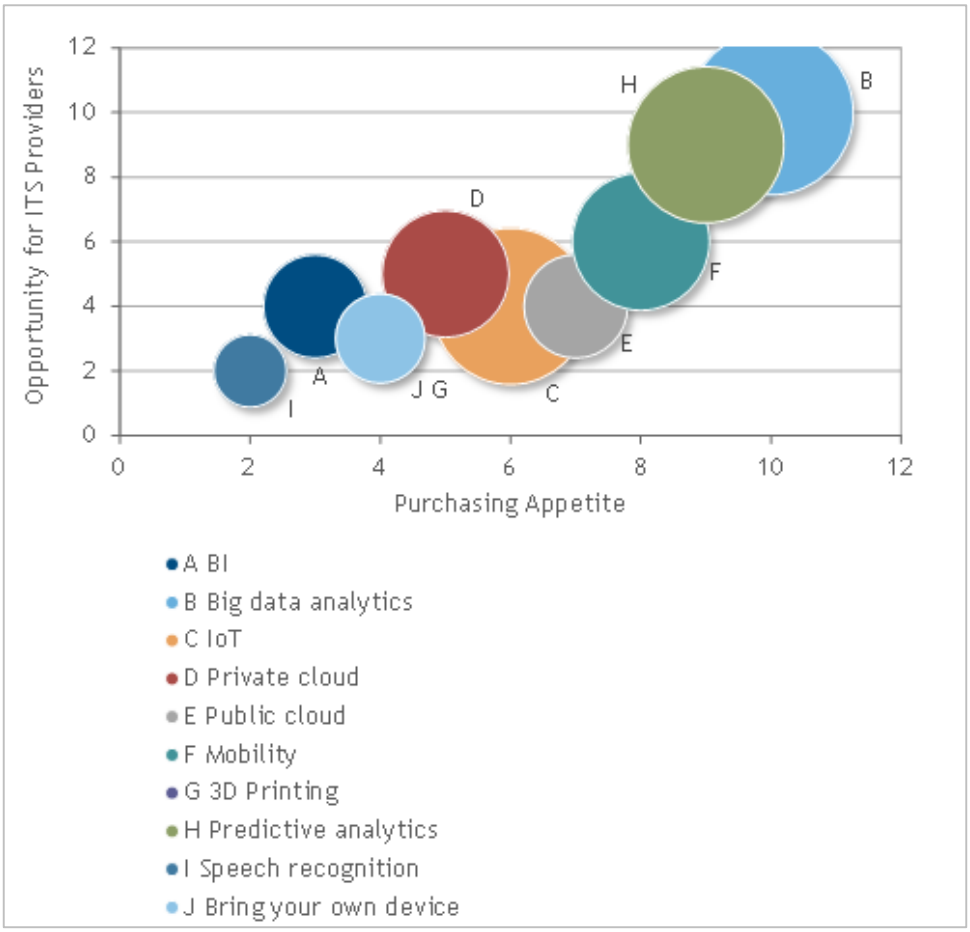


Abbildung 10: Chancen für Emerging Technologies in Österreich 2014 (IDC, 2015)

Interessant sind zudem ein Blick auf den Security Software Markt und ein Ländervergleich (siehe Abbildung 11). Herausforderungen in der Informationssicherheit und Cyber-Gefahren machen das Thema sichere Systeme in Österreich zu einem viel diskutierten von TechnologieführerInnen aus Wirtschaft und Forschung. Im Fokus stehen consumer-driven technologies, also vom Konsumenten getriebene Technologien wie cloud und mobile computing. Laut einer IDC Studie hat Österreich einen Anteil am westeuropäischen Security Software Markt von 1,9% im Jahr 2013. Für 2018 wird in etwa dieselbe Zahl prognostiziert. Den weitaus größten Anteil am westeuropäische Security Software Markt 2013 hat Großbritannien (26,8%), gefolgt von Deutschland (19,1%) und Frankreich (12,2%).[143]

[143] IDC, 2015b.

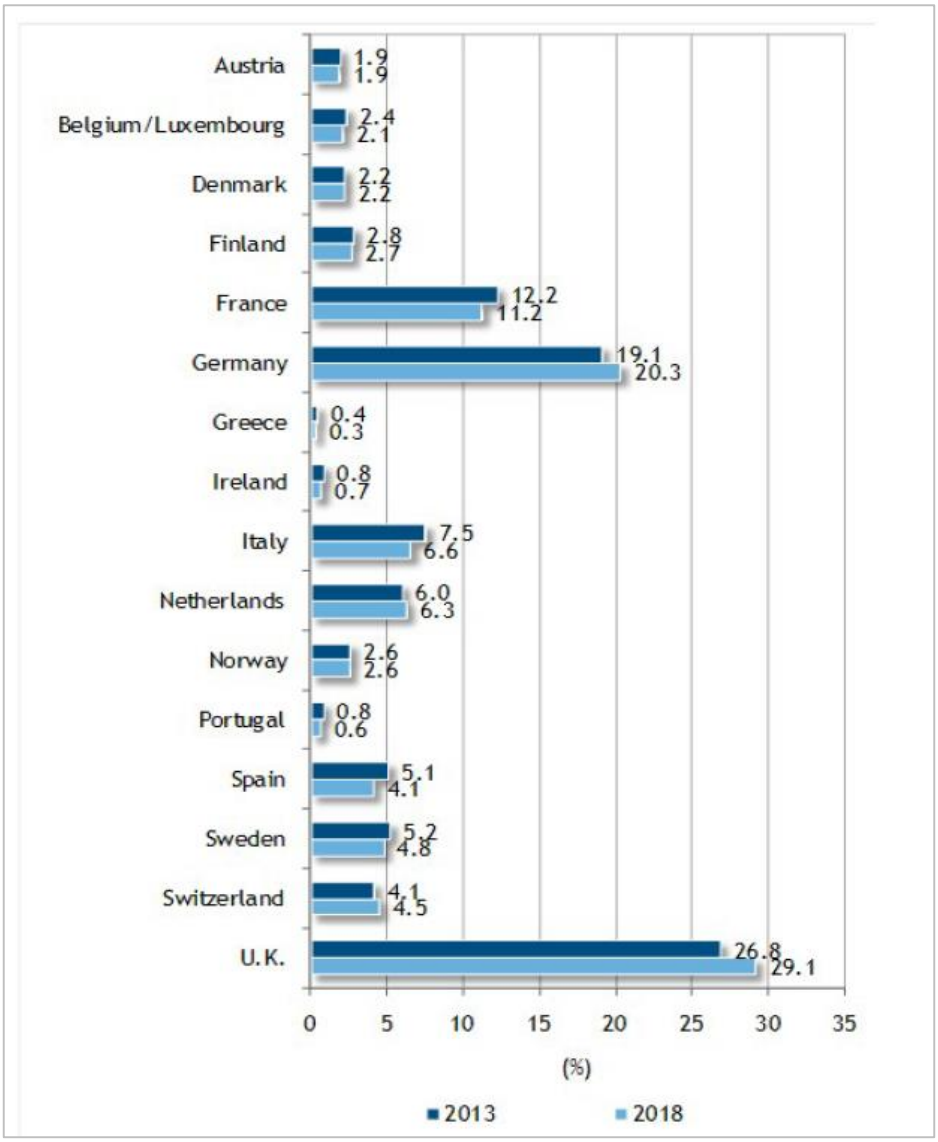


Abbildung 11: Security Software Anteil nach Ländern (Westeuropa) 2013 und 2018 (IDC, 2014a)

Generell ist anzumerken, dass die österreichische Wirtschaft aufgrund der Krise der vergangenen Jahre eine nur schwache Leistung zeigte, was sich auch auf den IT-Service Markt ausgewirkt hat. Für die kommenden Jahre ist aber mit einem verstärkten Aufschwung zu rechnen.[144]

4.1 Big Data

4.1.1 Beschreibung

IDC beschreibt Big Data Technologien als „a new generation of technologies and architectures designed to economically extract value from very large volumes of a wide variety of data by

[144] IDC, 2014a, S. 35.

enabling high velocity capture, discovery, and/or analysis“.[145] In Verbindung mit Big Data werden oft die vier Vs genannt – diese sind durch folgende Eigenschaften charakterisiert:

- Volume: Die generierte Datenmenge ist in den letzten Jahren enorm gestiegen.
- Velocity: Analyse von immer mehr Daten in immer kürzeren Zeitfenstern.
- Variety: Enorme Vielfalt an Datenformaten (Arbitrary > Relational > Freitext).
- Value: Generierung von Mehrwert aus Daten. Hier stellt sich die Frage, wie man die Potenziale nutzen kann.[146]

ExpertInnen sind sich einig, dass sich das Datenvolumen in den nächsten zehn Jahren weltweit dramatisch erhöhen wird. Schon heute verarbeitet Wal Mart mehr als eine Million Kundentransaktionen pro Stunde, Facebook über 900 Millionen Objekte pro Tag[147] und Google 3.5 Milliarden Suchanfragen pro Tag.[148]

Die zur Verfügung stehende Datenmenge in den unterschiedlichsten Unternehmen wächst kontinuierlich. Prognosen sprechen von einem durchschnittlichen Wachstum von 33,5% in Umsatzzahlen in den nächsten vier Jahren, wobei der Big Data Markt in Österreich von 22 Millionen Euro im Jahr 2013 auf 73 Millionen Euro im Jahr 2017 anwachsen wird.[149]

IDC hat 2014 unter fast 150 österreichischen CIO und IT-Managern eine Online-Umfrage durchgeführt, die den Status quo von Big Data in österreichischen Unternehmen erfasst und analysiert. 47% der befragten Unternehmen geben an, dass der Einsatz von Big Data Lösungen im Unternehmen ernsthaft diskutiert wird. Der Anteil jener Unternehmen, für die Big Data kein Thema ist, ist von 62% im Vorjahr auf 39% gesunken. Vergleicht man 2013 mit dem Vorjahr, so stellt man fest, dass die Anzahl der Unternehmen, welche nicht an Big Data denken, stark zurückgegangen ist. Dies entspricht in etwa dem internationalen Trend, wobei IDC Research indiziert, dass in anderen Ländern (Deutschland, USA, CEMA Region) dieser Trend noch wesentlich stärker ist als hierzulande.

Der Einsatz von Big Data Technologien hat zahlreiche Geschäftsbereiche und Geschäftsmodelle in fast allen Branchen maßgeblich verändert. Erfolgreiche Beispiele der jüngsten Vergangenheit umfassen unter anderem die Betrugsbekämpfung bei Finanzdienstleistern, die Prozessanalyse und vorausschauende Wartung bei Fertigungs- und Produktionsbetrieben oder die Analyse von Gesundheitsdaten zur Verbesserung von Behandlungsmöglichkeiten.[150] So verarbeitet Visa mehr als 35 Milliarden Transaktionen pro

[145] Nadkarni und Vesset, 2015.
[146] Wolschmann, 2014.
[147] SAS Institute Inc., 2012.
[148] Internet Live Stats, vom 22.11.2014.
[149] Köhler und Meir-Huber, 2014.
[150] Kearney, 2013.

Jahr[151] und korreliert dabei mehr als 500 verschiedene Variablen bei jeder Zahlung[152]. Das Betrugsvolumen, welches durch den Einsatz der Big Data Modelle erkannt wird, schätzt VISA auf ca. 2 Milliarden US Dollar.[153] Der Fortschritt von Big Data Analysen im Bereich der vorausschauenden Wartung ermöglichte Rolls Royce die Vorhersagen von Motorausfällen in der Flugindustrie und führte damit zu einem neuen, geänderten Geschäftsmodell, indem das Unternehmen seine Produkte vermietet und die Verantwortung für Reparatur, Wartung und Austausch übernimmt.[154]

4.1.2 Herausforderungen für Sicherheit und Zuverlässigkeit

Die Cloud Security Alliance[155] identifizierte in ihrem Bericht über Herausforderungen im Zusammenhang von Big Data und Sicherheit sowie Privatsphäre die folgenden zehn Punkte:

- Sichere und zuverlässige Berechnungen in verteilten Programmierframeworks (z.B.: Hadoop)
- Absicherung von NoSQL Datenbanken
- Absicherung von Data Storage und Transaction Logs
- Inputvalidierung von Endpoints
- Echtzeit Sicherheits- und Complianceüberwachung
- Skalierbare und zusammenführbare Data Mining und Analytics Ansätze, welche die Privatsphäre schützen/bewahren
- Kryptographisch abgesicherte Zugriffskontrolle und sichere Kommunikation
- Granulare Zugriffskontrolle
- Granulare Audits
- Datenherkunft

Hemmfaktoren bestehen in Österreich vor allem aufgrund der Novität der Technologie. Viele Unternehmen hierzulande haben Angst vor der Komplexität der Anwendungen und fürchten, dass das interne Know-how nicht ausreicht. Trotz oder wegen des Einsatzes von Cloud-Anwendungen für Big Data sind Hemmfaktoren für Skalierung und Bereitstellung stark zurückgegangen, wobei die Angst hinsichtlich der Sicherheit der Daten gestiegen ist. Für 46% der befragten Unternehmen in Österreich sind der Aufbau des Know-hows und das Verstehen der Prozesse jene Bereiche, in denen der größte Handlungsbedarf besteht. Dahinter folgt mit 21% der Aufbau der IT-Umgebung für entsprechende Datenspeicherung und Analyse und mit 13% die Auswahl der richtigen Software. 22% der befragten Unternehmen geben an, nicht zu

[151] Massachusetts Institute of Technology Projektwebseite.
[152] Strassmann, 2013.
[153] Rosenbush, 2013.
[154] Goodwin, 2013.
[155] Cloud Security Alliance, 2012.

wissen, welches Datenvolumen im Unternehmen gespeichert wird. Fast 50% der RespondentInnen fallen in den Bereich 50-500 TB, nur 4% speichern ein Volumen von über einem Petabyte. Aktuell befindet sich Big Data in Österreich in einem initialen Stadium. Die Einsatzentscheidung ist oftmals schon gefallen, es mangelt NutzerInnen jedoch noch am Know-how bzgl. Anbieter, Verfahren und Werkzeugen.

4.1.3 Herausforderungen aus rechtlicher Sicht

Big Data birgt einen großen Nutzen, ist aber bei Wahrung digitaler (Grund- und Menschen-) Rechte nur umsetzbar, wenn die Herausforderung der unkontrollierbaren Wissenssammlung in Händen weniger Stakeholder gelöst werden kann. Dabei steht das überkommene Datenschutzverständnis auf dem Prüfstand, weil manche Voraussetzungen angesichts „Big Data“ völlig neu gedacht werden müssen. Vor allem das Kriterium der "Bestimmbarkeit der Person" als Anknüpfungspunkt für die Schutzwürdigkeit von Daten steht vor einem völlig neuen Paradigma. Anonyme, öffentlich zugängliche Daten können durch komplexe Verknüpfungen mit großen Datenbeständen plötzlich personenbezogene Informationen offenbaren. Bei der Veröffentlichung der anonymen Datenbestände wird typischerweise nicht bedacht, was die Daten bei entsprechender Verknüpfung offenbaren. Für Datensubjekte wird es immer schwieriger einzuschätzen, ob Daten wirklich anonym sind oder eben durch „Big Data Methoden“, also insbesondere zu Verknüpfung mit anderen, großen Datenbeständen, doch wieder auf die Person rückführbar werden, obwohl die ursprünglichen Referenzdaten isoliert betrachtet durchaus anonym sind. Der Abgrenzungsfrage, wann personenbezogene Daten vorliegen, kommt datenschutzrechtlich eine hohe Bedeutung zu, weil (in Österreich ausdrücklich nach der Verfassungsbestimmung des § 1 Absatz 1 Datenschutzgesetz (DSG 2000) Daten ohne Personenbezug gar nicht in den Schutzbereich des Grundrechts und damit des DSG 2000 fallen.

Eine riesige, diverse und teilweise sogar unstrukturierte Anhäufung von Daten war noch vor wenigen Jahren – geradezu im paradoxen Gegenteil zu heute – beinahe ein sicheres „Datenversteck“, weil die Kapazitäten einfach nicht vorhanden waren, aus einem solchen „Datenhaufen“ (freie Übersetzung von „Big Data“) zuverlässige und relevante Informationen zu ziehen. Die Kapazitäten und zugleich die Verbreitung nützlicher Tools haben aber dazu geführt, dass derzeit in der Praxis eine stetige Entwicklung von (einfachsten) „Data Mining“ Methoden bis zu hoch komplexen „echten“ Big Data Systemen stattfindet und den freien Markt erschließt. Dadurch steht bald und z.T. schon jetzt jedermann die Möglichkeit und Technologie zur Verfügung, um über komplexe Informationsgewinnungsinstrumente aus riesigen verteilten Datenmengen Antworten auf – praktisch beliebige – Fragen zu generieren. Diese Antworten können sich auch auf natürliche oder juristische Personen beziehen. Die Integrität dieser Antworten, die Qualität und Vollständigkeit der Informationen, sind primär durch die

Algorithmen und deren Umsetzung bedingt. Die Auswirkung für die von einer „Analyse“ betroffene Person oder Sache hängt wiederum primär davon ab, in welcher Umgebung und zu welchem Zweck die Anwendung betrieben wird, und welches Vertrauen die AnwenderInnen in die Antwort haben. Mit anderen Worten stellt sich die Frage, inwiefern den maschinengenerierten Antworten als Ergebnis einer „Big Data Analyse“ Autorität verliehen wird und ob die Ergebnisse allenfalls noch in Zweifel gezogen werden. Diese Ebene ist nicht primär eine technologische sondern eine soziologische und letztlich auch rechtliche Dimension des Phänomens.

Die Forschung und Entwicklung sollte dringend erschließen, was der moderne Trend "privacy by design" bedeutet und welche Möglichkeiten und Grenzen er im Hinblick auf die Risiken von Big Data bietet. Voraussetzung ist in jedem Fall eine interdisziplinäre Sicht- und Herangehensweise, sowohl für die Entwicklung von Big Data Anwendungen als auch für die Entwicklung der rechtlichen und gesellschaftlichen Rahmenbedingungen, in denen – bestenfalls tatsächlich auf der Technologie-Ebene wirksame – Risikominimierung beim Design von Big Data Anwendungen integriert werden kann. Big Data wirft folgende grundrechtliche Probleme auf:

- Liegt eine ausreichende Menge an Daten betreffend eine Person vor, sind diese immer auf die konkrete Person rückführbar (Beispiel: Bewegungsdaten/Smartphone).
- Wenn diese in ausreichender Menge vorhanden sind, können aus vermeintlich banalen, unbedeutenden Daten über eine Person sehr intime Informationen abgeleitet werden, die mit hoher Wahrscheinlichkeit auf die Person zutreffen. Aus im Einzelnen tatsächlich „unbedeutenden“, also isoliert gesehen anonymen Daten, die man daher im Einzelfall meist gewillt ist preiszugegeben, kann so in Summe möglicherweise sogar ein präzises Persönlichkeitsprofil erstellt werden.

Bereits die Idee hinter Big Data, das „Herausholen“ von Informationen aus Daten, die für andere und häufig für verschiedene Zwecke gesammelt wurden, widerspricht dem datenschutzrechtlichen Zweckbindungsgrundsatz.

Big Data eignet sich sehr gut um Prognosen zu erstellen. Es liegt in der Natur der Statistik, dass diese Prognosen, auch wenn sie fehlerfrei erstellt wurden und sehr präzise sind, nicht auf jeden einzelnen Betroffenen zutreffen. Werden Entscheidungen auf solche Prognosen gestützt, kommt es für Einzelne zu ungerechtfertigten Konsequenzen. Extrembeispiel: Jemand soll bestraft werden, wenn er eine Straftat begangen hat, nicht aber schon deshalb Nachteile erleiden, weil eine hohe Wahrscheinlichkeit besteht, dass er eine Straftat begehen wird. Hinzu kommt, dass Software stets fehlerbehaftet ist, sodass es unweigerlich auch aus diesem Grund für Einzelne zu ungerechtfertigten Konsequenzen kommt.

Sofern Big Data Analysen personenbezogene Daten zum Gegenstand haben und als Ergebnis schließlich neue personenbezogene Informationen hervorbringen, ist diese Verarbeitung als originärer Eingriff in das Datenschutzgrundrecht der Betroffenen zu sehen und bedarf einer entsprechenden Rechtfertigung. Das betrifft vor allem Konstellationen, bei denen personenbezogene Daten ursprünglich für einen bestimmten Zweck erhoben wurden, welcher durch eine weiterführende Big Data Analyse erweitert wird. Die Judikatur behandelt eine Widmungsänderung als Sonderfall der Übermittlung[156] von Daten. Es ist also zu beachten, dass durch Informationsgewinnung via Big Data Analyse nicht die Zweckbindung einer Datenverarbeitung unterlaufen wird. Eine weitere datenschutzrechtliche Herausforderung zu Big Data besteht im Anspruch auf Richtigkeit personenbezogener Daten. Das betrifft vor allem die Fälle, in denen das Ergebnis einer Analyse in Prognosen oder Wahrscheinlichkeiten zu einer bestimmten Person besteht. Inwiefern dann ein Problem der Richtigkeit und Zuverlässigkeit bestehen mag, hängt wesentlich vom Zweck der Analyse und damit von sich aus den Informationen ergebenden Konsequenzen für die Person ab.[157]

4.1.4 Chancen

ExpertInnen[158,159] gehen davon aus, dass die derzeitigen, oftmals statischen Sicherheitslösungen für die sich rasch ändernde Bedrohungslandschaft in Zukunft nicht mehr effektiv genug sein werden um Angriffe zu erkennen und zu verhindern. Um innovativen und gezielten Attacken entgegenzuwirken, prognostiziert IDC[160], dass neuartige Intelligence-Ansätze an Bedeutung gewinnen werden um Systemeinbrüche und Datenabflüsse zeitnah zu erkennen und dadurch die Schäden zu minieren. Damit einhergehend wird das aufgezeichnete Datenvolumen sicherheitsrelevanter Informationen die heutigen Dimensionen um ein vielfaches übertreffen.[161] Curry et al.[162] gehen davon aus, dass in den nächsten zwei Jahren Big Data Analysen großen Veränderungen in zahlreiche Bereichen (z.B.: SIEM[163], GRC[164], Identitätsmanagement, Netzwerküberwachung, etc.) der Informationssicherheit auslösen wird.

[156] § 4 Z 12 DSG: „Übermitteln von Daten: die Weitergabe von Daten an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister, insbesondere auch das Veröffentlichen von Daten; darüber hinaus auch die Verwendung von Daten für ein anderes Aufgabengebiet des Auftraggebers“.

[157] Siehe zu diesem Spannungsverhältnis von Big Data zum Schutz der Privatsphäre (Tene und Polonetsky, 2012).

[158] Curry et al., 2013.

[159] Strassmann, 2013.

[160] ibid.

[161] ibid.

[162] Curry et al., 2013.

[163] Security information and event management.

[164] Governance, Risk and Compliance.

Empfehlungen:

Es wird empfohlen Projekte in den folgenden Bereichen zu fördern:

- Konzeption, Entwicklung und Anwendung von skalierbaren und zusammenführbaren Big Data und Analytics Ansätzen, welche Daten und die Privatsphäre schützen und bewahren. Erarbeitung flexiblerer Sicherheitslösungen für die sich rasch ändernde Bedrohungslandschaft um Systemeinbrüche, Datenabflüsse und Angriffe zu erkennen und dadurch die Schäden zu minimieren (neuartige Intelligence-Ansätze). Angesprochen sind dabei v.a. die Forschungsfelder Usable Security, Security Engineering, Identitätsmanagement und Verschlüsselungstechnologien, Pseudonymisierung/ Anonymisierung, Privacy Impact Assessment.
- Wissensvermittlung und Aufzeigen von gelungenen Anwendungen, denn die noch relative Neuartigkeit und Komplexität der Technologie sind Hemmfaktoren für die praktische Anwendung. Know-how Generierung und Vermittlung bzgl. Anbieter, Verfahren und Werkzeuge durch innovative Lehrkonzepte.
- Forschung und Entwicklung sollte dringend erschließen, was der moderne Trend "privacy by design" bedeutet und welche Möglichkeiten und Grenzen er im Hinblick auf die Risiken von Big Data bietet.
- Voraussetzung ist in jedem Fall eine interdisziplinäre Sicht- und Herangehensweise, sowohl für die Entwicklung von Big Data Anwendungen, als auch für die Entwicklung der rechtlichen und gesellschaftlichen Rahmenbedingungen, in denen – bestenfalls tatsächlich auf der Technologie-Ebene wirksame – Risikominimierung beim Design von Big Data Anwendungen integriert werden kann.

4.2 Cloud Computing

4.2.1 Beschreibung

Unter Cloud Computing versteht man das Speichern von Daten in einem entfernten Rechenzentrum sowie die Ausführung von Programmen, die nicht lokal installiert sind, sondern online genutzt werden. IDC identifiziert die folgenden Schlüsselmerkmale von Cloud Services: geteilt (shared), Lösungspaket (solution packaged), Selbstbedienung (self service), elastisch in Bezug auf Ressourcen und Preis (elastic resource scaling and use based pricing) und das Vorhandensein von Service-Schnittstellen/APIs[165]. Cloud Computing ist seit dem Jahr 2010 in Österreich relativ stark präsent. Hierbei handelt es sich um einen Paradigmenwechsel

[165] IDC, 2015c.

in der IT. Was früher noch besitzt wurde (z.B. Rechenzentren im Besitz des Unternehmens) wird heute nur gemietet. Führend in der Cloud sind vor allem Amerikanische Hersteller, was Fragen hinsichtlich der rechtlichen Lage aufwirft. V.a. im Jahr 2014 erlangte die Cloud beachtliche Aufmerksamkeit und es zeigte sich ein positiveres Image der Cloud am Österreichischen Markt als in den Jahren zuvor. Außerdem ist eine stetige Zunahme der Ausgaben im Bereich Cloud Services in den kommenden Jahren zu erwarten. Jedoch sind Bedenken im Bereich Datenschutz und Datensicherheit immer noch die größten Hürden für die Nutzung der Cloud in Österreich[166].

4.2.2 Herausforderungen für Sicherheit und Zuverlässigkeit

Häufige Probleme hinsichtlich der Zuverlässigkeit von verteilten Systemen ergeben sich aus den unterschiedlichsten Anwendungsfällen. Die zwei großen Problembereiche sind die Zuverlässigkeit hinsichtlich Ausfälle und die Zuverlässigkeit hinsichtlich Interoperabilität. Ausfälle von verteilten Systemen sind sehr umfangreiche Problemstellungen und liegen in der Komplexität des Systems begründet. Ein wesentlicher Vertrauenspunkt oder Misstrauenspunkt für verteilte Systeme ist die Frage hinsichtlich des Vendor-LockIns. Aktuelle Systeme in der (public) Cloud sind ungenügend für Interoperabilität gerüstet. Es gibt einige existierende Standards, doch diese werden nur unzureichend unterstützt. Hinzu kommen ein oftmals nachlässiges NutzerInnenverhalten bzw. ein fehlendes Bewusstsein hinsichtlich der Sicherheit von Systemen: „Die Cloud kann technisch sehr sicher sein, wenn der Kunde dann aber ein einfaches Passwort verwendet, können wir nicht helfen. (…) Endanwender müssen sensibilisiert werden“ (Zitat aus Experteninterview).

4.2.3 Herausforderungen aus rechtlicher Sicht

Besondere rechtliche Fragestellungen können sich vor allem dann ergeben, wenn die Verarbeitung personenbezogener Daten über „verteilte Systeme“ (Distributed Systems) erfolgt. Das Datenschutzrecht geht von der Annahme aus, dass es einen bestimmten für die Datenverarbeitung verantwortlichen „Auftraggeber“ (§ 4 Z 4 DSG) einer Datenanwendung gibt. Wenn dieser bestimmte Verarbeitungsschritte an einen Dienstleister auslagert, ist im Innenverhältnis verpflichtend eine vertragliche Vereinbarung (datenschutzrechtliche Dienstleistervereinbarung nach § 10 DSG) zur Gewähr für eine rechtmäßige und sichere Datenverwendung zu schließen. Die Hauptverantwortung bleibt aber jedenfalls beim Auftraggeber der Datenanwendung. Für den Fall, dass verschiedene Komponenten eines „Distributed System“ von verschiedenen Akteuren betrieben werden, muss beachtet werden,

[166] IDC, 2015d.

dass die Rollenverteilung und die jeweilige Verantwortung insbesondere gegenüber dem Subjekt der Datenverarbeitung eindeutig ist.

Zu beachten sind außerdem Genehmigungspflichten und rechtliche Grenzen, wenn personenbezogene Daten „in der Cloud“ außerhalb der EU verarbeitet werden sollen.

Bei der Verarbeitung personenbezogener Daten können sich im Zusammenhang mit Cloud Computing für Betroffene im Falle einer Datenschutzverletzung die (bereits in Kapitel 3 beschriebenen) Schwierigkeiten der Rechtsdurchsetzung im internationalen Rechtsverkehr realisieren.

Eine rechtliche Herausforderung besteht auf Seiten der AnwenderInnen von Cloud Computing Lösungen vor allem im Hinblick auf die Datensicherheit, wenn gegenüber Dritten (z.B. KundInnen eines Unternehmens) potentiell das Risiko einer Haftung besteht. Da die Rechtsordnung dazu nur wenig konkrete Anhaltspunkte für den rechtlich geforderten Sorgfaltsmaßstab bietet (dazu ausführlich Kapitel 3), liegt die Herausforderung auch in einer klaren Vertragsgestaltung zwischen Cloud-Anbieter und Auftraggeber.

4.2.4 Chancen

Cloud Computing bietet eine Vielzahl von wirtschaftlichen Chancen für moderne Unternehmen. Neben cloud-basierten Sicherheitsdiensten[167] wie beispielsweise in den Bereichen sichere Kommunikation, Identitäts- und Zugriffsmanagement, oder Remote Vulnerabilitymanagement können sichere Clouds Unternehmen Ausfallschutz, Fehlertoleranz, Zuverlässigkeit und Sicherheit bieten. Ein bestehender Nachteil ist, dass Cloud Computing Anbieter meist ein sehr interessantes Angriffsziel darstellen, da häufig eine Großzahl an Personen und Firmen davon betroffen sind. Mit Hilfe von Cloud Computing ist es leichter möglich, große Datenmengen zu analysieren, da Rechenleistung leicht erweiterbar ist.

Empfehlungen:

Know-how Aufbau: Es wird bereits vielfältig im Bereich von Zuverlässigkeit von verteilten Systemen geforscht. Hierbei gibt es einige Institute in Österreich, welche sich dafür qualifizieren. Es sollen daher speziell Projekte gefördert werden, welche als wesentliche Grundlage den Know-how Aufbau von Zuverlässigkeit für verteilte Systeme gewährleisten. Ein konkretes Beispiel wäre die Förderung von wissenschaftlichen MitarbeiterInnen, welche an der Zuverlässigkeit von verteilten Systemen arbeiten und eine dedizierte Library

[167] Messmer, 2013.

entwickeln. Eine Kooperation mit Unternehmen in Österreich, welche in diesem Bereich tätig sind, sollte wesentlicher Bestandteil dieser Funktion sein.

Know-how Verteilung: Das bestehende und neu zu erwerbende ExpertInnenwissen soll in Kursen und Disseminierungsworkshops für interessierte TeilnehmerInnen bereitgestellt werden. Hierbei ist eine Vernetzung mit Wirtschaft und Wissenschaft notwendig. Inhalte dieser Know-how Verteilung sollen darlegen, wie man verteilte Systeme ausfallsicher baut.

Standard-Unterstützung in Ausschreibungen: Offene, standardisierte Systeme sollen eine Unterstützung in der Systemauswahl finden, wenn es sich um offene Förderungen handelt. Dies kann entweder aktiv (Einforderung einer Beschreibung in der Einreichung) oder passiv (bessere Gewichtung von Projekten, welche auf offene, standardisierte Systeme setzen) geschehen.

Studie zu Interoperabilität und Standards: Es soll eine Studie angefertigt werden, welche die vorhandenen Standards von Systemen beleuchtet und die am internationalen und österreichischen Markt verfügbaren Standards aufzeigt. Die Studie muss auch Informationen über Schwachstellen liefern und wo weitere Akzente gesetzt werden können.

4.3 Vernetzte Gesellschaft

4.3.1 Beschreibung

Der Begriff der vernetzten Gesellschaft umfasst jene Anwendungen, die im weitesten Sinn ein soziales Netzwerk mit Mitteln der elektronischen Kommunikation schaffen. Dazu gehören insbesondere die Vorreiter der sogenannten Social Media wie YouTube, Facebook, Twitter, um nur die Bekanntesten zu nennen. Ein Problem dieses Markts ist die hohe Marktkonzentration: Sehr wenige Anbieter teilen sich den Markt. In Österreich gibt es derzeit allein an die 3,4 Mio. Facebook NutzerInnen, 140.000 Twitter NutzerInnen und 880.000 Instagram NutzerInnen (Stand: September 2015)[168]. Die Besonderheit dieser Phänomene ist, dass die NutzerInnen selbst sowohl individuell als auch kollektiv wesentliche Inhalte erzeugen. Die Verfügbarkeit dieser Medien hat zu einer Verlagerung des politischen Diskurses auf diese Medien geführt.

4.3.2 Herausforderungen für Sicherheit und Zuverlässigkeit

Neben den Vorteilen, die soziale Vernetzung auf die Mitgestaltung der Inhalte des Internets mit sich bringt, entstehen durch diese neue Art der Vernetzung und Informationsteilung neue Herausforderungen. Identitätsdiebstahl, Social Engineering und SPAM sind nur einige der Gefahren, die durch die vernetzte Gesellschaft steigen. Durch die immer höhere Bedeutung

[168] Vgl. Social Media Radar Austria Webseite.

der digitalen Identität und die starke Verbindung mit der physischen Identität spielen Cybermobbing und -stalking eine ernstzunehmende Rolle. Ein Problem dabei ist, dass einmal veröffentlichte Inhalte nur schwer aus dem Cyberspace entfernt werden können und dass im Gegensatz zum „klassischen“ Mobbing und Stalking die räumlichen Aspekte keine Rolle spielen. Eine weitere Gefahr für Jugendliche und Kinder stellt Online Grooming dar. In Österreich beschäftigen sich v.a. das Bundesministerium für Inneres (BMI) und das Bundeskriminalamt (BK) mit Kriminalität in Social Media u. a. im FFG KIRAS Projekt Social Media Crime – eine strukturierte Analyse kriminalpolizeilich relevanter Aktivitäten in sozialen Medien.

4.3.3 Herausforderungen aus rechtlicher Sicht

Soziale Netzwerke sind aus rechtlicher Sicht besonders in Bezug auf Datenschutz eine Herausforderung. Zunächst besteht die Schwierigkeit, die Anbieter solcher Dienste effektiv dazu zu bewegen, die technische Gestaltung entsprechend dem europäischen Datenschutzrecht durchzuführen („Privacy by Design“ und „Privacy by Default“, siehe Kapitel 5.17). Das wahrscheinlich noch größere Problem liegt aber in der Gefahr, dass die Anbieter sozialer Netzwerkdienste personenbezogene Daten für Zwecke missbrauchen, die nicht offen gelegt werden und zu denen die NutzerInnen daher auch keine Zustimmung geben (können). Das Beispiel der Verfahrensführung durch die Initiative „Europe vs. Facebook“ ist hierzu äußerst illustrativ (siehe dazu Kapitel 3.1.7). Dies steht in engem Zusammenhang mit den Unzulänglichkeiten der Mechanismen zur Rechtsdurchsetzung (siehe dazu Kapitel 3.1.12). Auf technischer Ebene ist hier auf die faktischen Schwierigkeiten zur Umsetzung eines „Rechts auf Vergessenwerden“ zu verweisen (siehe dazu Kapitel 3.1.6). Schließlich liegt die wohl größte Herausforderung aber auch in einem mangelnden Datenschutzbewusstsein seitens der NutzerInnen. Vielfach werden personenbezogene Daten über soziale Netzwerke durchaus unbedarft veröffentlicht, ohne sich der Konsequenzen bewusst zu sein. Die informationelle Selbstbestimmung erfordert hier ein entsprechendes Bewusstsein zur korrespondierenden Selbstverantwortung. Der Schlüssel dazu liegt zweifellos in einer Stärkung der (Medien-) Bildung quer durch die Gesellschaft.

4.3.4 Chancen

Social Networks beinhalten eine Fülle von Informationen und bieten neue Möglichkeiten der Interaktion. Security Blogs, Videos, und Gruppen vereinfachen den Austausch sicherheitsrelevanter Informationen. Auch für das Risiko-, Notfall- und Katastrophenmanagement bieten Plattformen wie Twitter Vorteile. Sie bieten Möglichkeiten Vorfälle frühzeitig zu erkennen und im Notfall in Echtzeit zu informieren, über Sachverhalte aufzuklären oder sich zu organisieren.

Empfehlung:

Die FFG sollte Projekte fördern, welche es ermöglichen, Identitätsdiebstahl zu erschweren bzw. schneller zu erkennen, die Sicherheit von sozialen Netzwerken (z.B.: durch frühzeitige Erkennung von Cyberbullying) zu fördern und die Privatsphäre zu erhalten.

4.4 Mobile Devices (Smartphone, Tablet)

4.4.1 Beschreibung

Gemäß des US-Amerikanischen National Institute of Standards and Technology (NIST)[169] ist der Begriff „mobile device“ schwer zu definieren, da die Funktionen der Geräte sich rasch verändern. Um trotz der Schwierigkeit des stetigen Wandels den Begriff zu beschreiben, identifizierte NIST Eigenschaften, welche mobile devices erfüllen. Diese sind:

- Kleiner Formfaktor
- Zumindest ein drahtloses Netzwerkinterface, z.B. WLAN, Bluetooth
- Lokal eingebauter Datenspeicher
- Betriebssystem, welches nicht ein vollwertiges Desktop oder Laptopbetriebssystem ist
- Applikationen, welche durch mehrere Quellen zur Verfügung gestellt werden können (Hersteller, Third Party, etc.)
- Digitale Kamera oder Videoaufzeichnung
- Mikrophone

Steigende NutzerInnenzahlen von Smartphone und Tablets machen diese Geräte zu einem interessanten Ziel für Cyberkriminelle.[170] Der Umstand, dass Tablets und Smartphones längst nicht mehr nur zum Anrufen, SMS-Versand oder für das Browsen im Internet verwendet werden, machen die Geräte zu einem häufigen Ziel.

Das Smartphone wird immer mehr zu einem Multifunktionsgerät, welches vielseitig in fast allen Lebensbereichen verwendet wird.[171] Während im Bereich der Arbeitswelt vor allem Dienste rund um die Kommunikation (z.B.: E-Mail, Lync), Terminverwaltung (z.B.: Kalenderfunktionen) oder Datenzugriff eine immer wichtigere Rolle spielen, wird es im privaten Bereich für noch viel mehr Einsatzzwecke verwendet. So bieten Smartphones umfangreiche Möglichkeiten zur Unterhaltung mittels Bereitstellung von Spielen, Musikplayerfunktionalitäten und sie ersetzen oftmals unterwegs Videokamera und Fotoapparat. Auch der Einsatz als Navigationsgerät ist mittlerweile bei vielen NutzerInnen nicht mehr wegzudenken. Weiters spielt es vor allem bei

[169] NIST, 2013.
[170] IDC, 2014b.
[171] Bundesamt für Sicherheit in der Informationstechnologie, 2006.

der Gruppe der Digital Natives eine immer wichtigere Rolle, z.B.: durch Messenger wie WhatsApp oder Apps zur Teilnahme an sozialen Netzwerken. Durch die starke Nutzung wird das Smartphone auch immer interessanter für die Verwendung als Zahlungsmittel.

Eine Studie von Sophos Labs[172] zeigt, dass die Auswirkungen kompromittierter Smartphones durch die vielfältigen Anwendungsmöglichkeiten sehr unterschiedlich sein können. Anwendungen sind zum Beispiel:

- Überwachenden Tätigkeiten durch Microphone, Kamera, Anruferlisten, Ort und SMS Nachrichten
- Identitätsbetrug durch Umleitung von SMS, Senden von E-Mail Nachrichten, Posten auf sozialen Netzwerken
- Datendiebstahl wie etwa von Zugangsdaten, Kontakten, Anruferlisten, Telefonnummern, gespeicherte Daten oder die International Mobile Equipment Identity Number
- Verursachung von finanziellen Schäden durch Premium SMS, TAN Diebstahl, kostenpflichtige Anrufe, Ransomware (Schadprogramm, welches ein Weiterarbeiten am Gerät verhindert bis gewissen Aktivitäten – z.B.: Überweisung von Geld – durchgeführt werden[173]).

4.4.2 Herausforderungen für Sicherheit und Zuverlässigkeit

Die Bedrohungen für Smartphones und ähnliche mobile Endgeräte sind vielfältig. In einer Untersuchung von 101 häufig verwendeten Applikationen und Spielen für iPhone und Android wurde herausgefunden, dass mehr als die Hälfte der Geräte die eindeutige Geräte ID zu anderen Unternehmen ohne Zustimmung der/des BenutzerIn übertrugen. Manche Applikationen übertrugen weit mehr persönliche Daten wie die Position, Alter und Geschlecht.[174]

Gemäß des Sophos Mobile Threat Reports[175] besitzt Österreich eine besonders hohe Threat Exposure Rate[176] (dritthöchste weltweit) im Bereich der mobilen Endgeräte. Die Sicherheit mobiler Endgeräte weist folgende Charakteristika auf, durch die sie sich von „konventioneller Computersicherheit“ unterscheidet[177]:

- Mobilität: Mobile Endgeräte werden häufig bewegt und sind daher mehr physischen Gefahren (wie etwa Diebstahl) ausgesetzt

[172] Svajcer, 2014.
[173] F-Secure Webseite.
[174] Thurm et al., 2010.
[175] Svajcer, 2014.
[176] Angriffsfläche.
[177] Mulliner, 2006.

- Personalisierung: Mobile Endgeräte werden meistens nicht von mehreren BenutzerInnen geteilt
- Verbindungsmöglichkeiten: Mobile Endgeräte weisen zahlreiche Möglichkeiten auf um sich zu Netzwerken bzw. zum Internet zu verbinden
- Technologiekonvergenz: Mobile Endgeräte kombinieren zahlreiche verschiedene Technologien (wie PDA, Musikplayer, Kamera, etc.)
- Eingeschränkte Fähigkeiten: Mobilen Endgeräten fehlen manche Eigenschaften, welche Desktopcomputer besitzen (z.B.: vollständiges Keyboard).

4.4.3 Herausforderungen aus rechtlicher Sicht

Mobile Devices sind wie soeben beschrieben auf verschiedenen technologischen Ebenen eine Herausforderung für den Schutz personenbezogener Daten, wobei dies sowohl die Hersteller der Endgeräte als auch die Anbieter von Apps betrifft. Insbesondere die Einhaltung des Zweckbindungsgrundsatzes ist letztlich auch aufgrund der Systemschwächen zur Rechtsdurchsetzung in der Praxis schwer sicherzustellen. Für die Herausforderungen im Hinblick auf IT-Sicherheitsrecht wird auf Kapitel 3.2 verwiesen. Besondere Herausforderungen – nicht nur in Bezug auf Datenschutz – ergeben sich im Zusammenhang mit dem Phänomen „Bring Your Own Device“ (BYOD, siehe dazu Kapitel 3.1.11).

4.4.4 Chancen

Mobile Geräte bieten als zusätzliche Hardware mit vielen Sensoren ideale Voraussetzungen für benutzerInnenfreundliche Mehrfaktorauthentifizierung und viele andere Sicherheitsinnovationen. Auch der Trend das Mobiltelefon als neues Zahlungsmittel zu verwenden, zeigt das Potential, welches in dieser Technologie steckt.

Empfehlung:

Aus Sicht der Informationssicherheit ergeben sich folgende Gebiete, welche im Bereich mobile Security betrachtet werden sollten:

- Schutz der Privatsphäre: Smartphones und ähnliche Geräte werden in allen Bereichen unseres Lebens verwendet. So kann das Smartphone als universaler Informationsspeicher, vielseitiges Kommunikationsmittel (Telefonie, SMS, Messenger, Social Media, etc.), Spielekonsole, Navigationsgerät, Zahlungsmittel oder Multimediagerät u.v.m. verwendet werden. In jedem der oben genannten Kontexte können eine Vielzahl an Daten gesammelt werden. Für den/die BenutzerIn ist es sehr schwierig herauszufinden, welche Daten gesammelt, verarbeitet und gespeichert werden. Daher ist es wichtig, Forschung im Bereich Schutz der Privatsphäre zu fördern.

- Sicherheit mobiler Applikationen: Da Applikationen für mobile Geräte von einer immer größeren Zahl an EntwicklerInnen geschrieben werden, ist es notwendig, Sicherheitsmechanismen zu entwickeln, welche einfach und auch von nicht SicherheitsexpertInnen übernommen werden können.
- Schutz vor Schadsoftware: Aufgrund der wertvollen Daten und der einfachen Möglichkeit durch Mehrwertnummern und Premiumdienste Gewinne zu erzielen, erlebt die Schadsoftware auf mobilen Endgeräten einen rasanten Anstieg. Drei Forschungsbereiche, die hier besonders interessant sind, umfassen: Malware, Phishing & SPAM.
- Forensik: In der Aufklärung von Tathergängen gewinnen digitale Beweise zunehmend an Wert. In diesem Zusammenhang sind auch mobile Geräte besonders wichtig.
- Usability: Der Siegeszug von Smartphones und ähnlicher Geräte ist besonders der einfachen Bedienung zu verdanken. Daher sollte Sicherheitsforschung in diesem Bereich auch ganz besonders auf diesen Aspekt eingehen.

4.5 Netzwerkvirtualisierung (Software Defined Networks)

4.5.1 Beschreibung

Software definierte Netzwerke (SDN) ermöglichen NetzadministratorInnen, das Netz einfacher zu verwalten, indem die unteren Funktionsebenen in virtuelle Services abstrahiert werden. Für den Begriff SDN existieren zahlreiche Begriffserklärungen. Die Open Networking Foundation (ONF)[178] charakterisierte SDN-Architekturen durch die folgenden Eigenschaften:

- direkte Programmierbarkeit
- Agilität
- zentrale Verwaltung
- programmgesteuert konfiguriert
- offene Standards und Herstellerunabhängigkeit.

SDN ist somit ein neues Netzwerkparadigma, welches die Netzwerkkontrollschicht von der Weiterleitungsschicht entkoppelt. SDNs werden zentral durch die Controller der Netzwerkkontrollschicht gesteuert. Netzwerkgeräte, welche durch offene Schnittstellen (z.B.: OpenFlow) programmiert werden können, werden zu einfachen Weiterleitungsgeräten (vgl. Abb. 12). [179]

[178] Open Networking Foundation, o.J.

[179] Nunes et al., 2014.

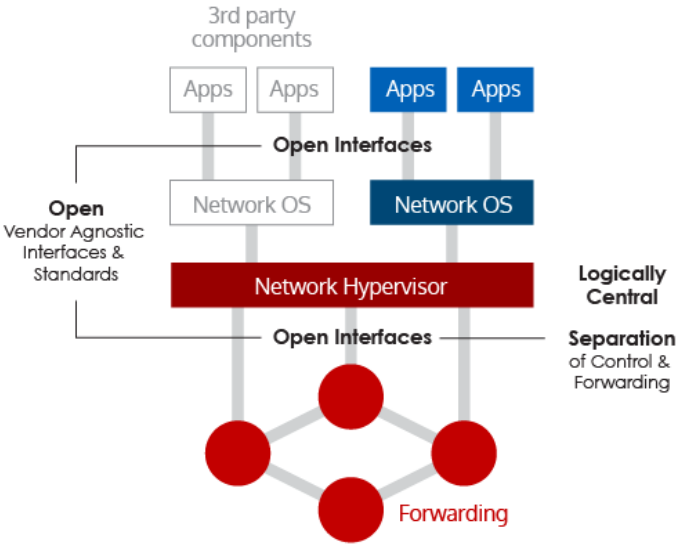


Abbildung 12: Software Defined Networks Overview[180]

4.5.2 Herausforderungen für Sicherheit und Zuverlässigkeit

Derzeit gibt es noch wenige große Installationen Software definierter Netzwerke. Durch die neuen zentralen Steuerungseinheiten, stellt sich die Frage, wie sichergestellt werden kann, dass SDN genauso sicher oder sicherer als traditionelle Netzwerke sein können. Auch die Schnittstellen zwischen Controller und Applikationen eröffnen zahlreiche Herausforderungen. Der Controller bietet zudem einen zentralen Angriffspunkt (z.B.: Denial of Service).

4.5.3 Herausforderungen aus rechtlicher Sicht

Rechtlich liegen die großen Herausforderungen hier vor allem beim Thema IT-Sicherheitsrecht und den großen bestehenden Rechtsunsicherheiten (siehe dazu Kapitel 3.2).

4.5.4 Chancen

Software definierte Netzwerke werden in Zukunft zunehmend in Unternehmensnetzwerke und im Internet verbreitet sein. Durch die Abstraktion und Virtualisierung des Netzwerks ist es möglich, neue Sicherheitslösungen zu schaffen.

Projekte in diesem Bereich umfassen unter anderem die Untersuchung der Auswirkungen auf Netzwerksicherheit aufgrund dieser neuen Technologie sowie die Erforschung und Entwicklung von Sicherheitsapplikationen (z.B.: zur Erkennung und Eindämmung von Angriffen, Integration von IDS/IPS und SDN).

[180] Open Networking Lab (ON.LAB) Webseite.

Empfehlung:

Die FFG sollte Projekte fördern, welche die sichere Verwendung dieser neuen Technologie ermöglichen. Vor allem die Entwicklung neuer sicherheitsrelevanter Applikation birgt hohes Innovationspotential.

4.6 Industrielle Steuerungsanlagen

4.6.1 Beschreibung

„Industrielles Steuerungssystem“ ist ein allgemeiner Begriff, welcher verschiedene Begriffe wie Supervisory Control and Data Acquisition Systems (SCADA), Distributed Control Systems (DCS) und andere Steuerungssysteme beinhaltet. Industrielle Steuerungssysteme werden in zahlreichen Sektoren (z.B.: Wasserversorgung, Energieversorgung, Produktion, etc.) eingesetzt.[181]

Industrial Control Systems dienen der Prozesssteuerung und Automatisierung von Industrieanlagen und nehmen in vielen Bereichen kritischer Infrastrukturen eine wichtige Rolle ein. Stuxnet, Gauss, Flame und viele andere Angriffe und Zwischenfälle in der jüngsten Vergangenheit zeigen, dass SCADA Systeme längst nicht mehr isoliert betrieben werden und dadurch eine hohe Bedrohung ausgeht.[182,183]

Die Sicherheit industrieller Kontrollsysteme wurde in der Vergangenheit durch die strikte Trennung zu anderen Netzen erreicht. Heutige SCADA Systeme sind jedoch häufig mit dem Unternehmensnetzwerk in irgendeiner Art und Weise verbunden. So stellte Sean McGurk[184] in einem Interview fest, dass seiner Erfahrung nach in hunderten Vulnerability Assessments ihm kein Fall bekannt sei, in dem gar keine Verbindung zum Unternehmensnetzwerk vorhanden ist. Im Durchschnitt würden elf Verbindungen bestehen, in Extremfällen bis zu 250.[185,186]

[181] NIST, 2011.

[182] Miller und Rowe, 2012.

[183] Bencsáth et al., 2012.

[184] ehemaliger Direktor des National Cybersecurity and Communications Integration Center (NCCIC) des Department of Homeland Security (DHS).

[185] “In our experience in conducting hundreds of vulnerability assessments in the private sector, in no case have we ever found the operations network, the SCADA system, or energy management system separated from the enterprise network. On average, we see 11 direct connections between those networks. In some extreme cases, we have identified up to 250 connections between the actual producing network and the enterprise network.” (Byres, 2013)

[186] Byres, 2013.

4.6.2 Herausforderungen für Sicherheit und Zuverlässigkeit

SCADA Systeme haben einige Merkmale, welche sie von konventionellen Computern unterscheiden, wodurch sie spezielle Herausforderungen ergeben[187]: Aufgrund der Kritikalität der Systeme müssen alle Einspielungen und Aktualisierungen umfangreich getestet und evaluiert werden. Des Weiteren ist es üblich, dass Systeme zwischen 10 und 20 Jahren zum Einsatz kommen. Sicherheit war nicht integraler Bestandteil bei der Entwicklung industrieller Kontrollsysteme.

Die NIST SP800-82 listet noch weitere Besonderheiten von industriellen Kontrollsystemen gegenüber „gewöhnlichen" Geschäftsinformationssystemen. Die nachfolgende Tabelle fasst einige der wichtigsten Unterschiede zusammen.

Kategorie	Informationstechnologie-system	Industrielles Steuerungssystem
Performance Anforderungen	• Nicht Echtzeit • Antworten müssen konsistent sein • Hoher Durchsatz ist gefordert • Hohe Verzögerungsraten und Jitter können akzeptabel sein	• Echtzeit • Antworten sind zeitkritisch • Moderater Durchsatz ist akzeptabel • Hohe Verzögerungsraten und/oder Jitter sind nicht akzeptabel
Verfügbarkeits-anforderungen	• Reaktionen, wie beispielsweise ein Neustarten eines Systems, sind akzeptabel • Verfügbarkeitsdefizite können oftmals, abhängig von den Betriebsanforderungen des Systems, toleriert werden	• Reaktionen, wie beispielsweise ein Neustarten des Systems, sind nicht akzeptable aufgrund der Prozessverfügbarkeitsanforderungen • Verfügbarkeitsanforderungen können redundante Systeme erfordern • Ausfälle müssen Tage/Wochen vorher geplant und koordiniert werden • Hohe Verfügbarkeitsanforderungen
Risiko-management Anforderungen	• Vertraulichkeit und Integrität der Daten sind oberste Priorität • Fehlertoleranz ist weniger wichtig – kurzfristige Ausfälle sind kein kritisches Risiko • Ein kritisches Risiko ist die Verzögerung des Geschäftsbetriebs	• Menschliche Sicherheit ist oberste Priorität, gefolgt von dem Schutz des Prozesses • Fehlertoleranz ist wichtig, sogar kurzfristige Ausfälle können nicht akzeptable sein • Kritische Risiken umfassen Verletzung der Complianceanforderungen, Beeinträchtigung der Umwelt, Verlust von Leben, Geräten oder Produktion
Architektur Sicherheits-fokus	• Primärer Schwerpunkt ist der Schutz von IT-Assets und Informationen, welche auf diesen Assets gespeichert und übertragen werden	• Oberstes Ziel ist der Schutz der Edge Clients (z.B.: Feldsysteme wie Prozesssteuerung) • Schutz des zentralen Servers ist auch wichtig

[187] Honeywell, 2012.

	• Zentrale Server mögen höheren Schutz erfordern	
Unerwünschte Auswirkungen	Sicherheitssysteme sind für typische IT-Systeme entwickelt	Sicherheitswerkzeuge müssen getestet werden (z.B.: offline an einem vergleichbaren industriellen Steuerungssystem) um zu gewährleisten, dass der Betrieb nicht gestört wird
Komponentenlebenszeit	Lebenszyklus von 3-5 Jahren	Lebenszyklus von 15-20 Jahren

Tabelle 2: Ausgewählte Unterschiede zwischen „normalen“ IT-Systemen und industriellen Steuerungssystemen[188]

4.6.3 Herausforderungen aus rechtlicher Sicht

In einer vom BSI durchgeführten Studie[189] wurden die Top 10 Cyberbedrohungen für Industrielle Steuerungssysteme erhoben. Dabei wurde festgestellt, dass die möglichen Auswirkungen schwerwiegende Schäden wie Produktionseinbußen, Verlust von Know-how, physische Schäden, Beeinträchtigung von Safety-Systemen sowie die Minderung von Qualität herbeiführen kann. Die folgende Tabelle listet die Top 10 Cyberbedrohungen.

No.	Bedrohung
1	Infektion mit Schadsoftware über Internet und Intranet
2	Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware
3	Social Engineering
4	Menschliches Fehlverhalten und Sabotage
5	Einbruch über Fernwartungssysteme
6	Internet-verbundene Steuerungskomponenten
7	Technisches Fehlverhalten und höhere Gewalt
8	Kompromittierung von Smartphones im Produktionsumfeld
9	Kompromittierung von Extranet- und Cloudkomponenten
10	(D)DoS Angriffe

Tabelle 3: Industrial Control System Security Top 10 Bedrohungen (BSI, 2014)

[188] Stouffer et al., 2011.

[189] Bundesamt für Sicherheit in der Informationstechnik, 2014.

4.6.4 Chancen

Vom Projektteam wurden folgende Innovationsbereiche identifiziert:

- SCADA Testbed: Da Forschungsvorhaben an industriellen Kontrollsystemen bzw. SCADA Systemen Forschungseinrichtungen oftmals nicht oder nur eingeschränkt zur Verfügung stehen, empfehlen wir als ein Leuchtturmprojekt den Aufbau eines Industrial Control System Testbeds.
- SCADA Honeypot: Um neue Gefahren analysieren zu können, ist es unabdingbar, diese zu identifizieren und zu isolieren. Honeypots stellen eine Möglichkeit dar an diese Samples zu kommen. Dafür ist es allerdings notwendig, dass die Honeypots die Funktionen kritischer SCADA Systeme realistisch abbilden.
- Ansätze zur APT (Advanced Persistent Threat) Erkennung

Empfehlung:

Die FFG sollte Projekte fördern, welche die Analyse von Risiken industrieller Steuersystemen verbessern. Mögliche Forschungsfelder in diesem Bereich umfassen Angreifermodellierung, Attack Attribution, Industrial Honey Nets sowie Verfahren zur Erkennung von Anomalien in Industriesteuerungssystemen.

4.7 Cyber-physikalische Systeme

4.7.1 Beschreibung

In der Forschungsagenda von ACATECH werden cyber-physische Systeme wie folgt beschrieben[190]: „Cyber-Physical Systems stehen für die Verbindung von physikalischer und informationstechnischer Welt. Sie entstehen durch ein komplexes Zusammenspiel

- von eingebetteten Systemen, Anwendungssystemen und Infrastrukturen – zum Beispiel Steuerungen im Fahrzeug, intelligente Kreuzungen, Verkehrsmanagementsysteme, Kommunikationsnetze und ihre Verknüpfungen mit dem Internet
- auf Basis ihrer Vernetzung und Integration
- und der Mensch-Technik-Interaktion in Anwendungs-prozessen.“

Derzeit zeichnet sich eine Entwicklung in der IT ab, welche für besondere Brisanz sorgen wird. Elemente, welche bis heute primär auf die virtuelle Welt begrenzt waren, halten immer stärkeren Einzug in die physikalische Welt. Dies bedeutet nicht nur, dass alles durch IP-

[190] Geisberger und Broy, o.J.

Adressen online ist, sondern dass digitale Baupläne sehr einfach in die Realität übertragen werden können. So hat beispielsweise die NASA einen Schraubenschlüssel im Weltraum per E-Mail versendet und in einem 3D-Drucker ausgedruckt[191]. Weitere Beispiele für den Einsatz von cyber-physikalischen Systemen finden sich in zahlreichen Branchen wie etwa in der Automobilindustrie, Energiewirtschaft oder Robotik. IT, Elektronik und das Internet brachten eine dritte Revolution und die cyber-physikalischen Systeme, die nun entwickelt werden, könnten eine vierte industrielle Revolution einleiten. Auf dieser Überlegung basiert die Bezeichnung „Industrie 4.0“.[192]

4.7.2 Herausforderungen für Sicherheit und Zuverlässigkeit

Bei cyber-physikalischen Systemen bestehen Herausforderungen für die Sicherheit, da AngreiferInnen eine breite Angriffsfläche geboten wird, wenn Gegenstände via Internet adressierbar und somit potenziell auch steuerbar sind. Aufgrund der durch die zunehmende Vernetzung komplexer werdenden Anlagen müssen die Mensch-Maschine-Schnittstellen angepasst bzw. neu gestaltet werden. Die komplexen Interaktionen von realer Anlage, steuernder und überwachender Software und den offenen, globalen Kommunikationsnetzen müssen beherrscht werden. Die bisher heterogenen Systemstrukturen müssen einander angepasst werden und müssen miteinander fehlerfrei funktionieren. Hierfür sind Referenzarchitekturen erforderlich. Die Sicherheit CPS-basierter Automatisierungslösungen muss auf dem hohen Standard der heutigen Automation gewährleistet bleiben[193].

4.7.3 Herausforderungen aus rechtlicher Sicht

Hier ist aufgrund der rechtlich sehr ähnlich gelagerten Fragestellungen auf die Ausführungen zum Thema „Internet der Dinge“ in Kapitel 4.8 zu verweisen.

4.7.4 Chancen

Chancen bestehen vor allem für Industrieunternehmen, welche durch cyber-physikalische Systeme schneller kundenspezifische Anforderungen in die Tat umsetzen können.

[191] LeTrent, 2014.

[192] Vgl. Aigner, 2013.

[193] VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik, 2013.

Empfehlung:

Die FFG sollte Projekte fördern, welche die Sicherheit und Schutz von cyber-physikalischen Systemen erhöhen. Dazu zählen beispielsweise Verfahren, welche die Einhaltung von Safetystandards während der Quellcodeerstellung, -kompilierung und -ausführung prüfen. Außerdem sollten Projekte zur Ursachenforschung von Fehlern oder Angriffen (CPS Forensics) gefördert werden.

4.8 Internet der Dinge

4.8.1 Beschreibung

IDCs Definition von “Internet der Dinge (Internet of Things IoT)” lautet: „a network of networks of uniquely identifiable endpoints (or "things") that communicate without human interaction using IP connectivity"[194]. Das Internet der Dinge bezeichnet also den Paradigmenwechsel vom Menschen, der mittels eines dafür bestimmten Geräts das Internet aktiv nutzt, hin zu Gegenständen des Alltags, die zu smarten Objekten werden und autonom mit ihrer Umwelt sowie via Internet miteinander kommunizieren und interagieren. IoT ist eng mit Big Data, Cloud, mobilen und sozialen Applikationen verknüpft und reichert diese an. Ein Teilaspekt ist dabei die Ausstattung von Gegenständen mit RFID-Tags (radio frequency identification). Das Internet der Dinge hängt mit zahlreichen anderen Trends zusammen und lässt sich von diesen nicht scharf abgrenzen. Es ist ein wesentlicher Faktor in der Entwicklung von Smart Cities und Smart Homes, etc. Ein mit dem Internet der Dinge eng verwandtes Konzept sind die cyber-physikalischen Systeme. Während diese aber grundsätzlich auch autonom bzw. in abgegrenzten Domänen, wie z.B. der industriellen Steuerung operieren, sind die Besonderheiten des Internet der Dinge seine globale Natur und die potenzielle Kommunikation eines Gegenstandes mit jedem beliebigen anderen über Domänengrenzen hinweg.

In den nächsten Jahren werden immer mehr Geräte über eine IP-Adresse verfügen. Bereits heute können Zahnbürsten, Waschmaschinen, Haushaltsgeräte und viele andere Geräteklassen miteinander und dem Web kommunizieren. Durch IoT ergeben sich viele Vorteile, jedoch gilt es auch die Sicherheitsaspekte und Datenschutzbedenken zu analysieren und auf diese einzugehen.

[194] MacGillivray et al., 2015, S. 2.

4.8.2 Herausforderungen für Sicherheit und Zuverlässigkeit

Eine besondere Herausforderung für die Privatsphäre in Zusammenhang mit dem Internet der Dinge ist, dass mit der Kommunikation der Gegenstände auch die Überwachbarkeit der Personen steigt, die diese Gegenstände mit sich führen.[195]

Wie bei den cyber-physikalischen Systemen besteht eine weitere Herausforderung für die Sicherheit in der breiten Angriffsfläche die AngreiferInnen geboten wird, wenn Gegenstände via Internet adressierbar und somit potenziell auch steuerbar sind.

4.8.3 Herausforderungen aus rechtlicher Sicht

Neben den bereits angesprochenen Risiken bestehen Herausforderungen im Hinblick auf die Privatsphäre (Datenschutz) und die Datensicherheit. Darüber hinaus ist das „Internet der Dinge“ auch im Hinblick auf die korrekte und sichere Funktionalität (im Sinne von „Safety“) und die damit verbundenen Haftungsfragen eine besondere Herausforderung, der vielfach auch mit vertraglichen Regelungen zu begegnen sein wird. Wenn die Funktionalität von Alltagsgegenständen (z.B. Zutrittssysteme, Heizungssteuerungen, usw.) auch durch Datenübertragung einem zusätzlichen Risiko ausgesetzt ist, können Schwierigkeiten im Zusammenhang mit Haftungsfragen vor allem dann auftreten, wenn mehrere Akteure (also auch Internet-Zugangsanbieter) im Zusammenspiel der Verantwortung handeln.

4.8.4 Chancen

Im Bereich „Internet der Dinge“ besteht in Österreich vor allem großes Potential durch die hier stark vertretene Industrie und Fördermöglichkeiten vor allem in den Bereichen Industrie, Governance und Gesundheitswesen. Lösungsanbieter sind v.a. mittelständische Unternehmen in Zusammenarbeit mit der Forschung[196].

Empfehlung:

Die FFG sollte Projekte fördern, welche die Analyse von Risiken durch vernetzte Objekte verbessern und sichere Lösungen entwickeln und testen. Mögliche Forschungsfelder in diesem Bereich umfassen Usable Security, Digitale Forensik, Bekämpfung von Schadsoftware und Botnetzen, Software Security Engineering und die Entwicklung sicherer Hardware und Netzwerke sowie Identitätsmanagement.

[195] Vgl. Weber, 2010.

[196] Keßler, 2013.

4.9 Augmented Reality

4.9.1 Beschreibung

Augmented Reality (AR) sind Technologien, welche die menschliche Wahrnehmung stark ausweiten. Anders formuliert AR wird definiert als eine computerunterstützte Wahrnehmung bzw. Darstellung, welche die reale Welt um virtuelle Aspekte erweitert[197]. In der Theorie gibt es AR bereits seit vielen Jahren und wurde vor allem durch das Aufkommen von Smartphones und wearable devices in den letzten Jahren verstärkt. Hierbei sind vor allem Google Glass und Occulus Rift zu erwähnen.

4.9.2 Herausforderungen für Sicherheit und Zuverlässigkeit

Augmented Reality Anwendungen sind vor allem für den Datenschutz eine große Herausforderung. Dies ergibt sich vor allem daraus, dass die Umgebung zunächst vom Gerät wahrgenommen (gefilmt) werden muss, bevor diese um virtuelle Elemente angereichert werden kann (Augmentation). Vor allem das Beispiel Google Glass zeigt, dass – bei allen Vorteilen, die solche Anwendungen bieten – gleichzeitig leicht eine Atmosphäre des gegenseitigen Misstrauens der Menschen untereinander entstehen kann, weil niemand mehr sicher ist, ob das brillentragende Gegenüber nicht die gesamte Unterhaltung und/oder Bilder, angereichert um Metadaten wie Standort, Uhrzeit und Dauer, aufzeichnet. Ein solches Misstrauen vermag die Entwicklung sozialer Beziehungen in einer Gesellschaft tiefgreifend zu prägen. Eine Augmented Reality Anwendung ist zumeist ein Begleiter auf Schritt und Tritt und betrifft nicht nur die AnwenderInnen sondern auch alle in der Umgebung in ihren schutzwürdigen Geheimhaltungsinteressen. Gleichzeitig ist die faktische Kontrolle über die Verarbeitung der beachtlichen Datensammlungen voll bei den Anbietern der Dienste konzentriert – was bei einem sehr stark auf wenige Anbieter konzentrierten Markt ein besonders hohes Risiko darstellt. Diesen Risiken wird man rechtlich durch strenge Vorschriften zu „Privacy by Design“/“Privacy by Default“ in Kombination mit regelmäßigen Kontrollen und effektiven Durchsetzungsmechanismen begegnen müssen. Die Marktentwicklung und die Risiken durch konkrete Anwendungen werden damit zusammenhängen, wie stark das Bewusstsein der Menschen gegenüber Privatsphäre und Datenschutz in einer jeweils betroffenen Zivilgesellschaft (d.h. im jeweils adressierten Markt) ausgeprägt ist.

4.9.3 Herausforderungen aus rechtlicher Sicht

Bei Augmented Reality Anwendungen spielen rechtliche Fragen im Hinblick auf die Haftung für die Richtigkeit von Echtzeitinformationen eine Rolle (z.B.: eine Augmented Reality „Brille“

[197] Springer Gabler Verlag (Hrsg.), 2015. Stichwort: Augmented Reality.

liefert falsche Informationen zu einer in Echtzeit erkannten Person zurück, woraus sich ein negativer Geschäftsverlauf ergibt). Insofern unterscheidet sich die Problemlage aber nicht wesentlich von „herkömmlichen“ Anwendungen zur (etwas komplexeren) Informationsgewinnung. Besonderheiten die sich hier gerade aus der Technologie möglicher Augmented Reality Anwendungen ergeben, hängen vom konkreten Zusammenhang ab. Wenn beispielsweise solche „Brillen“ im Rahmen von „smart mobility“-/ „smart traffic“-Konzepten sicherheitsrelevante Informationen im Straßenverkehr an die NutzerInnen zurückliefern sollen, ist das Risikopotential wesentlich höher und damit verbundene Rechtsfragen meist viel schwieriger. Im Hinblick auf das IT-Sicherheitsrecht gelten auch hier die allgemeinen Ausführungen dazu (siehe Kapitel 3.2).

4.9.4 Chancen

Vor allem die Spielebranche zeigt sich als Wegbereiter und treibende Kraft, aber es tun sich auch sehr breite Anwendungsfelder für den geschäftlichen und industriellen Bereich auf. Eine Erweiterung der realen Welt um virtuelle Aspekte durch eine computerunterstützte Wahrnehmung bzw. Darstellung ist vor allem in der Produktion, in der Stadtplanung und Architektur, im Verkehr, bei Notfalleinsätzen von Feuerwehr und Rettung, bei der Überwachung von Großveranstaltungen, im Tourismus, im Marketing und in der Wissensvermittlung, uvm. von Nutzen.

Empfehlung:

Ähnlich wie bereits bei den mobilen Geräten angemerkt, stellt allen voran der Datenschutz die große Herausforderung im Augmented Reality Bereich dar. Dem wird man mit „Privacy by Design“/“Privacy by Default“ in Kombination mit regelmäßigen Kontrollen und effektiven Durchsetzungsmechanismen begegnen müssen.

4.10 Robotik und Cybernetics

4.10.1 Beschreibung

Cybernetics (deutsch: Kybernetik) ist die Theorie der Regelung und Steuerung dynamischer Systeme[198]. Sie beschäftigt sich besonders mit der Informationsverarbeitung in dynamischen Systemen und mit deren Regelung und Steuerung. Ein Anwendungsbereich ist die Robotik. Sie befasst sich mit dem Versuch, das Konzept der Interaktion mit der physischen Welt auf Prinzipien der Informationstechnik sowie auf eine technisch machbare Kinetik zu reduzieren.

[198] Springer Gabler Verlag (Hrsg.), 2015. Stichwort: Kybernetik.

Die Robotertechnologie existiert bereits seit vielen Jahren, doch erst in den letzten Jahren dringt diese immer stärker in allgemeine Anwendungsbereiche vor. Zum Beispiel beschäftigte sich die FFG Studie Potential of Robotics for Active & Assisted Living mit der Definition des Gebiets der AAL-Robotik, die Darstellung von Stand und Herausforderungen und eine realistische Einschätzung ihres Potentials für ältere Menschen wie auch für die Wirtschaft[199].

4.10.2 Herausforderungen für Sicherheit und Zuverlässigkeit

Die Interaktion zwischen Mensch und Roboter kann zu tiefgreifenden – vor allem ethischen – Herausforderungen in Bezug auf die Würde des Menschen führen. Dies bezieht sich z.B. auf den Bereich des durch Technologie co-betreuten Lebens (Active & Assisted Living), wenn intelligenten Maschinen immer mehr Aufgaben in der Pflege vor allem älterer Menschen übertragen werden. Innerhalb der Gesellschaft muss ein Konsens gefunden werden, wo die ethischen Grenzen verlaufen, bevor diese Problemstellung durch konkrete Rechtsvorschriften erfasst und geregelt werden kann.

4.10.3 Herausforderungen aus rechtlicher Sicht

Die Ebene der Menschenrechte bietet Ansatzpunkte für bestimmte Wertungen und Grenzen, die hier gewissermaßen als „Human Dignity by Design“ einen Orientierungsraster bieten. Betrachtet man das Thema Robotik und Cybernetics rechtlich primär im Hinblick auf Produkte, die bereits auf dem Markt erhältlich sind oder kurz davor stehen, stellen sich keine besonders schwer zu lösende, komplett neuartige und rechtliche Problemstellungen. Natürlich gelten Ausführungen in Bezug auf IT-Sicherheitsrecht (siehe Kapitel 3.2) auch in diesem Zusammenhang, wenn solche Anwendungen auch über welchen Standard auch immer mit der Umgebung kommunizieren.

Abseits dieser grundrechtlichen und ethischen Aspekte sind betreffend autonome Systeme aus rechtlicher Sicht vor allem Fragen der Haftung zu lösen: Üblicherweise ist ein technisches System, von dem eine Schädigung ausgeht, seinem/seiner BetreiberIn/EigentümerIn zuzurechnen. Bei autonomen Systemen, die nach den Vorgaben des Herstellers, der sie programmiert hat, für den/die BetreiberIn/EigentümerIn ohne dessen Beteiligung handeln, ist jedoch der Hersteller stärker in die Pflicht zu nehmen. Entsprechende Haftungsregeln sind zu entwickeln, die dann auch zur Folge haben, dass für die Hersteller die Sicherheit (Safety und Security) ihrer Systeme bei deren Entwicklung noch stärker in den Fokus rückt.

[199] Payr, Werner und Werner, 2015.

4.10.4 Chancen

Es ist zu erwarten, dass die Entwicklung von Robotik und Cybernetics in den kommenden Jahren sehr schnell von statten gehen wird, was vor allem einen großen Bedarf in der Sicherheitsforschung weckt. In der Industrie, Logistik und Produktion sind Roboter längst zu einem unverzichtbaren Helfer geworden und werden schon bald auch im Alltag, im Bereich des autonomen Fahrens und der Elektromobilität, im Haushalt und der Pflege als Assistent den Menschen unterstützen. Weitere aufkommende Anwendungsfelder sind die Unterhaltungselektronik, die Sicherheitsrobotik zur Unterstützung von Rettungs- und Sicherheitskräften, oder die Agrarrobotik.

Empfehlung:

Da dieser Bereich in Zukunft sowohl den Privat- als auch Geschäftsbereich stark beeinflussen wird, empfehlen wir Projekte zu fördern, welche die Sicherheit und Safety von Robotern verbessern. Längerfristig sind Robotik und Cybernetics für die Forschungsfelder Usable Security, Secure Engineering und Entwicklung sicherer Hardware und Security by Design interessant.

4.11 Quantenrechner

4.11.1 Beschreibung

Ein Quantencomputer ist ein auf der Quantenmechanik basierender Rechner. Spezielle quantenmechanische Eigenschaften erlauben Quantencomputern im Gegensatz zu klassischen Computern parallele Rechnungen. Dadurch können extrem rechenaufwändige Verfahren möglich werden.[200] Quantenrechner existieren derzeit jedoch lediglich am Papier beziehungsweise sind jene, die existieren, zu klein und nicht skalierbar um komplexe Aufgaben zu übernehmen. Dennoch ist es relevant, hier langfristig nach Möglichkeiten zu suchen.

4.11.2 Herausforderungen für Sicherheit und Zuverlässigkeit

Durch Quantenrechner besteht die Gefahr, dass aktuelle Verschlüsselungsalgorithmen nicht mehr verwendbar sind. Die Funktionsweise von Quantenrechnern würde es erlauben, gängige Verschlüsselungstechnologien in kurzer Zeit zu entschlüsseln.

[200] Vgl. Springer Gabler Verlag (Hrsg.), 2015. Stichwort: Quantencomputer.

4.11.3 Herausforderungen aus rechtlicher Sicht

Aus rechtlicher Sicht besteht die Herausforderung vor allem in den Auswirkungen, die Quantenrechner auf den Sorgfaltsmaßstab zur Datensicherheit im Hinblick auf Verschlüsselungssysteme mit sich bringen werden. Aus einer rechtlich-systematischen Perspektive sind die Fragestellungen dazu aber grundsätzlich Bestandteil jeder sicherheitsrelevanten Technologieentwicklung, nicht nur im IKT-Bereich. Eine besondere Herausforderung könnte aber durchaus darin bestehen, dass natürlich lange Zeit nicht alle Organisationen gleichen Zugang zu dieser Technologie haben werden und damit gewissermaßen ein „Machtgefälle“ im Bereich der Informationssicherheit einhergehen könnte – man stelle sich als fiktives Beispiel vor, die ganze Welt verschlüsselt mit herkömmlichen Verfahren und nur ein bestimmter Geheimdienst eines bestimmten Landes verfügt allein über Quantencomputer-Technologie, die bisherige Verschlüsselungsverfahren möglicherweise als völlig wirkungslos desavouieren. Daraus entstehende Rechtsfragen können so die primär individualrechtliche Ebene verlassen und in die völkerrechtliche Ebene reichen.

4.11.4 Chancen

Quantenrechner sind langfristig von Relevanz, von Neuheit geprägt und vor allem Forschungsgegentand der theoretischen Informatik. Die Chance liegt darin, dass spezielle quantenmechanische Eigenschaften Quantencomputern parallele Rechnungen erlauben und so extrem rechenaufwändige Verfahren möglich werden. Wesentliche Fragen der Informatik, z.B. die Suche in extrem großen Datenbanken, könnten deutlich effizienter gelöst werden als mit klassischen Computern.

Empfehlung:

Es wird empfohlen Projekte, welche sich dem Thema Post-Quantum Kryptographie widmen, zu fördern. Es besteht in erster Linie Bedarf nach neuen Verschlüsselungskonzepten, da bereits bestehende als nicht mehr sicher zu erachten sind.

5 Forschungsfelder

In diesem Kapitel werden Forschungsfelder dargestellt, die in den kommenden Jahren als besonders relevant für die Schaffung sicherer Systeme betrachtet werden. Durch eigene Recherche, einem Workshop gemeinsam mit ExpertInnen aus Wirtschaft, Wissenschaft und Verwaltung sowie Interviews wurden relevante Forschungsgebiete gesammelt, priorisiert und die Forschungsgebiete den Emerging Technologies zugeordnet.

„Ziel ist die bessere Vernetzung der Forschung und Wirtschaft"

(Zitat aus den Interviews)

5.1 Usable Security

Beschreibung	Sicherheitsmechanismen, welche nicht benutzerInnenfreundlich sind, werden oftmals von den BenutzerInnen ausgehebelt. Bridge identifiziert fünf Kategorien, in die Forschung im Bereich benutzerInnenfreundliche Sicherheit und Privatsphäre unterteilt werden kann[201]: Usability and design studies: Diese Kategorie widmet sich der Untersuchung von Vertrauensentscheidungen („trust decisions") und Usability-Problemen von Benutzeroberflächen (z.B. PGP[202], Pishingwarnungen[203]). Security feature studies: Diese Studien beschäftigen sich mit spezifischen, technischen Sicherheits- und Privacyrisiken und deren Bekämpfung, welche keine direkte BenutzerInneninteraktion fordern (z.B.: Sicherheit von TCP/IP[204]). Trust and ethical studies: Diese Kategorie widmet sich Konzepten wie Vertrauen und Privatsphäre in einem ethischen Kontext. Security and privacy experience studies: Forschung in diesem Bereich untersucht BenutzerInnenverhalten und -bedenken zu Sicherheit und Privatsphäre (z.B. Haltung zu offenen, drahtlosen Netzwerken[205]). Modeling and guidelines: Dieses Gebiet beschäftigt sich mit der Modellierung von Trust-Interaktionen, um daraus Leitfäden und Richtlinien abzuleiten.
Derzeitige Herausforder-ungen	Whitten und Tygar[206] identifizierten fünf problematische Eigenschaften, welche darstellen, warum es schwierig ist, BenutzerInnenfreundlichkeit und Sicherheit zu koppeln: Sicherheit ist meist ein sekundäres Ziel. BenutzerInnen sind meist an der Funktionalität und nicht an der Sicherheit interessiert (unmotivated user property). Sicherheit umfasst oftmals abstrakte Regeln und ist oftmals nicht

[201] Bridge, 2009.
[202] Whitten und Tygar, 2005.
[203] Egelman et al., 2008.
[204] Vutukuru et al. 2008.
[205] Klasnja et al., 2009.
[206] Whitten und Tygar, 2005.

	intuitiv für eine Vielzahl von NutzerInnen (abstraction property). Es ist schwierig, gute Rückmeldung zum Zustand der Sicherheit zu geben, da Sicherheitskonfigurationen komplex und abhängig von den Bedürfnissen der NutzerInnen sind (lack of feedback property). Sobald ein Geheimnis einmal versehentlich ungeschützt ist, gibt es keine Sicherheit, dass es nicht schon von AngreiferInnen gelesen wurde (barn door property). AngreiferInnen müssen nur eine Schwachstelle ausnutzen (weakest link property). Daher ist es wichtig, frühzeitig die BenutzerInnenfreundlichkeit von Sicherheitsmechanismen zu integrieren, zu testen und zu verbessern.
Zeitliche Dimension	☒ Kurzfristig ☒ Mittelfristig ☒ Langfristig
Relevanz	☒ Zuverlässigkeit (Safety) ☒ Sicherheit (Security) ☐ Recht und Gesellschaft
Assoziierte Bedrohungen	BenutzerInnenfreundliche Sicherheitsmechanismen und Systeme wirken nicht direkt gegen eine Bedrohung. Allerdings helfen sie, Sicherheitsmechanismen effektiv in der Praxis umzusetzen.
Emerging Technology	Die BenutzerInnenfreundlichkeit von Sicherheit ist ein zentrales Element um effiziente und effektive Sicherheit zu gewährleisten. Usable Security ist daher in allen Bereichen wichtig, jedoch besonders dort, wo eine Vielzahl an BenutzerInnen ein System verwenden (z.B.: soziale Netzwerke, Cloudsysteme).
Forschungs-fragen	Beispielfragestellungen für diesen Bereich umfassen: Welche Usabilityprinzipien muss die Sicherheitsforschung berücksichtigen um Sicherheitsansätze, -technologien und -werkzeuge benutzerInnenfreundlich zu gestalten?[207] Wie kann die Usability bestehender Sicherheitslösungen evaluiert werden? Wie ist die Usability vorhandener Lösungen zum Schutz der Privatsphäre und Sicherheit? [208] Wie können sichere und benutzerInnenfreundliche Authentifizierungsmechanismen (Alternativen zu Passwörtern) aussehen?[209] [210] Wie können NutzerInnenvereinbarungen und Privacyagreements benutzerInnenfreundlich dargestellt werden? [211] Wie können Sicherheitseinstellungen und Privatsphäreeinstellungen standardmäßig

[207] Markatos et al., 2013, S. 77f.
[208] Ibid.
[209] ExpertInneninterviews & Workshop.
[210] Markatos et al., 2013, S. 77f.
[211] ExpertInneninterviews & Workshop.

	eingebaut werden und gleichzeitig ein hohes Maß an BenutzerInnenfreundlichkeit bieten? [212]

5.2 Risiko- und Notfallmanagement

Beschreibung	Mit zunehmender Komplexität und Vernetzung der Informationssysteme sowie der Allgegenwärtigkeit von IT steigen auch die Anforderungen an die Risikosteuerung an Unternehmen, um effektive Schutzmaßnahmen zu ergreifen. In einem immer dynamischer werdenden Geschäftsumfeld müssen traditionelle Risikomanagement- und Notfallmanagementansätze weiterentwickelt werden, um mögliche Bedrohungsszenarien besser evaluieren zu können und dynamische Risikoeinschätzungen in Echtzeit zu gewährleisten. Vorfälle der jüngsten Vergangenheit, wie beispielsweise Heartbleed[213,214] und Shellshock[215], haben eindrucksvoll demonstriert, wie schnell sich die Bedrohungslage für eine Vielzahl an Unternehmen innerhalb kürzester Zeit im Cyberumfeld ändern kann. Neben Schwachstellen, die von potenziellen AngreiferInnen genutzt werden können, sind auch unbeabsichtigte Fehlerquellen wichtig für die Ermittlung des Risikos, wie die Fehlfunktion in der Steuerung von Energienetzen in Österreich 2013 zeigte[216]. Eine Möglichkeit Risiken zu betrachten, besteht in der Verknüpfung mit Geschäftsprozessen, welche neben Information als primäre Assets eines jeden Unternehmens angesehen werden. Conforti et al. zeigen dafür mögliche Schnittstellen zwischen Prozessmanagement und Risikomanagement.[217]
Derzeitige Heraus-forderungen	Derzeitige Herausforderungen im Bereich Risikomanagement liegen in der Entwicklung neuer Verfahren, welche die immer komplexer und dynamischer werdenden Systeme, hinsichtlich ihrer Sicherheit (Safety & Security) bewerten. Um dies zu bewerkstelligen, sollte auch von neuen Technologien (wie beispielsweise Big Data/Intelligence Ansätze) Gebrauch gemacht werden, um neue sicherheitsrelevante Informationen zu generieren. Hinsichtlich der Verknüpfung auf Geschäftsprozessebene soll erforscht werden, mit welchen Verfahren betrügerische Handlungen oder Complianceverletzungen in Geschäftsprozesse aufgedeckt werden können (z.B.: Process-Mining-Verfahren) bzw. wie Sicherheits-, Risiko- und Notfallmanagement mit Geschäftsprozess-

[212] ExpertInneninterviews-
[213] CERT.at, 2014.
[214] The Heartbleed Bug Webseite.
[215] US CERT/NIST, 2014.
[216] Bundesamt für Sicherheit in der Informationssicherheit, 2014, S. 34.
[217] Conforti et al. 2011.

	/Workflowmanagement verbunden werden kann, um Geschäftsprozesse sicherer, widerstandsfähiger und robuster zu machen[218,219]. Eine weitere Herausforderung liegt in der Einschätzung neuer Risiken. Loske et al. zeigen beispielsweise, dass unrealistischer Optimismus auch bei der Einschätzung der Verwundbarkeit auch bei CloudanbieterInnen vorkommt.[220]
Zeitliche Dimension	☒ Kurzfristig ☒ Mittelfristig ☐ Langfristig
Relevanz	☒ Zuverlässigkeit (Safety) ☒ Sicherheit (Security) ☐ Recht und Gesellschaft
Assoziierte Bedrohungen	Risikomanagement versucht eine Vielzahl von Bedrohungen zu identifizieren, zu bewerten und auf ein akzeptables Maß zu verringern.
Emerging Technology	Aufkommende Technologien wirken stark auf das Risikomanagement ein, da unter Umständen neue Risikobetrachtungen angestellt werden müssen. So hat beispielsweise Cloud Computing das Risiko in vielen Unternehmen positiv oder negativ beeinflusst, auch der Trend zu umfassenden Analysemethoden (Stichwort Big Data Analytics oder Intelligence Driven Security) fordert neue, dynamischere Risikomanagementtechniken.
Forschungs-fragen	Beispielfragestellungen für diesen Bereich umfassen etwa: • Wie können Risikomanagementansätze von neuen Technologien profitieren? [221] • Wie können Risiken in einem immer komplexeren Umfeld realistisch bewertet werden? • Wie können neue und existierende Risikomanagementansätze validiert werden?[222] • Wie können quantitative Risikomethoden verbessert werden, um Informationssicherheitsrisiken messbar zu machen? [223] • Welche Methoden können verwendet werden, um Risiken besser zu beschreiben und zu bewerten? [224] • Wie können Prozesstechnologien eingesetzt werden, um Betrug aufzudecken und Risiken besser einzuschätzen? [225]

[218] Suriadi et al., 2014.
[219] Van der Aalst, 2010.
[220] Loske, 2013.
[221] ExpertInneninterviews.
[222] Wangen und Snekkenes, 2013.
[223] Ibid.
[224] Ibid.
[225] Suriadi et al., 2014.

5.3 Wirtschaftliche & kriminologische Betrachtungen

Beschreibung	Angriffe der jüngsten Vergangenheit wie der Carbanak Bankraub[226] und Trends zur Vermarktung von Angriffsdienstleistungen, wie beispielsweise „Crime/Hacking As A Service“[227], haben gezeigt, dass hinter Cyberkriminialität und -spionage klare Geschäftsmodelle stecken. Um Cyberkriminalität besser entgegenwirken zu können, ist es zunehmend wichtiger, auch die Geschäftsmodelle der Schattenwirtschaft (Underground) zu verstehen. Insbesondere um Gegenmaßnahmen zu planen und die Hintergründe / Motive sowie Fähigkeiten von AngreiferInnen besser verstehen zu können. In einem Report kommt IDC zu dem Schluss, dass KonsumentInnen 25 Milliarden US Dollar ausgeben und 1,2 Milliarden Stunden verwenden, um Sicherheitsvorfälle, welche mit Schadsoftware in Softwareraubkopien verbreitet wurde, zu lösen.[228] Eine weitere große wirtschaftliche Herausforderung stellt die Messung von Informationssicherheit dar. Obwohl größtenteils Einigkeit herrscht, dass nur gemanagt werden kann, was auch gemessen werden kann, ist die Erforschung geeigneter Sicherheitskennzahlen ein relativ neues Forschungsgebiet. Die Wichtigkeit dieses Bereichs wird auch durch das US Cyberspace Policy Review verdeutlicht, welches die Schaffung von Performance-Kennzahlen, um Cybersicherheit zu messen, als eine Toppriorität listet.[229] Die Kriminologie hat zahlreiche Theorien (z.B. Repeat Victimization Theory[230]) entwickelt, um Verhalten von Kriminellen in der physischen Welt besser zu verstehen. Aufbauend auf diesen Theorien wurde es sogar möglich, Verbrechen vorherzusagen[231,232]. Um die Ursachen, Motivationen und Zusammenhänge von cyberkriminellen Handlungen besser verstehen zu können, ist es daher notwendig, cyberkriminologische Untersuchungen in interdisziplinärer Forschung zu unterstützen. Dabei sollte auch untersucht werden, ob durch die Verwendung neuer Technologien Vorhersagen im Cyberraum zu kriminellen Handlungen ermöglicht werden können.
Derzeitige Heraus-forderungen	Wirtschaftliche Modelle von Cyberkriminalität sowie Return on Investments bestimmter Angriffe (BotnetzbetreiberInnen, APT-Angriffe der Vergangenheit, Spear Phishing, Malwareverbreitung) sollen untersucht werden, um ein detailliertes Verständnis über die Möglichkeiten von Cyberkriminellen zu erhalten. Geeignete Kennzahlen sind die Grundlage um Veränderungen in der

[226] Vgl. Felser, 2015.
[227] EUROPOL, 2014.
[228] Gantz et al., 2014.
[229] Cyberspace Policy Review, o.J.
[230] Weisel, 2005.
[231] Vgl. Predpol Webseite.
[232] Cox, 2010.

	Bedrohungslage zu erkennen und kosteneffiziente Entscheidungen in der Informationssicherheit treffen zu können. Sie helfen auch zu zeigen, dass Sicherheitsabteilungen und -technologien ihre Aufgaben das Unternehmen zu schützen und Risiken zu verringern ausreichend wahrnehmen. Durch die hohe Komplexität und die Dynamik der Technologieentwicklung und Gefährdungslage stellt die Identifikation und Interpretation von Kennzahlen eine starke Herausforderung dar.
Zeitliche Dimension	☒ Kurzfristig ☒ Mittelfristig ☐ Langfristig
Relevanz	☐ Zuverlässigkeit (Safety) ☒ Sicherheit (Security) ☒ Recht und Gesellschaft
Assoziierte Bedrohungen	Assoziierte Bedrohungen umfassen vor allem kriminelle Handlungen mit wirtschaftlichem Interesse wie beispielsweise das Betreiben von Botnetzen, die Verbreitung von Malware, der Versand von SPAM, das Anzeigen unerwünschter Inhalte oder gezielte, persistente Angriffe auf Unternehmen.
Emerging Technology	Jede aufkommende Technologie beeinflusst potenziell die Schattenwirtschaft (Underground Economy). So wurde die aufkommende Verbreitung sozialer Netzwerke für die Verteilung von Schadsoftware, zum Identitätsdiebstahl, für die Steuerung von Botnetzen oder zur Verbreitung von SPAM verwendet. Neue Anwendungsbereiche von intelligenten Geräten beeinflussen wie durch Kompromittierung ökonomische Vorteile erzielt werden können und sollten somit untersucht werden.
Forschungs-fragen	Fragestellungen in diesem Bereich umfassen: • Welche Trends (z.B. Verwendung von Bitcoins) gibt es in der Schattenwirtschaft (Underground economy)?[233] • Wie kann festgestellt werden, welcher Betrag in Sicherheit investiert werden soll?[234] • Welche Kennzahlen geben Aufschluss über die Sicherheit in einem Unternehmen?[235] • Was sind die Motive Cyberkrimineller? Wie wählen Cyberkriminelle ihre Ziele aus?

[233] Bos et al., 2013.
[234] ExpertInneninterview.
[235] Workshop.

5.4 Sicherheitsarchitekturmanagement

Beschreibung	Eine Unternehmensarchitektur beschreibt, wie Geschäft und IT im Unternehmen zusammenhängen. Typischerweise umfasst eine Unternehmensarchitektur die Ebenen Geschäftsarchitektur, Anwendungsarchitektur, technische Architektur und Informationsarchitektur.[236] Durch die Abbildung des Zusammenhangs aller Ebenen eines Unternehmens bildet die Unternehmensarchitektur eine gute Grundlage, um Sicherheit im Unternehmen zu verankern. Die Verknüpfung oder Verwendung eines Sicherheitsarchitekturansatzes ermöglicht die Steuerung der Sicherheit in komplexen Umgebungen und gewährleistet gleichzeitig den Schutz auf allen Ebenen. Ein bekannter Ansatz zur Implementierung einer Unternehmenssicherheitsarchitektur bildet der SABSA (Sherwood Applied Business Security Architecture) Ansatz. Durch die Verknüpfung der Systeme und deren Sicherheitsmaßnahmen mit der Geschäftsstrategie ist es möglich, Sicherheitsmaßnahmen zu rechtfertigen bzw. die Erfüllung der Sicherheitsanforderungen auf allen Ebenen zu überprüfen.[237]
Derzeitige Heraus-forderungen	Komplexe neue Entwicklungen, wie beispielsweise Industrie 4.0, benötigen Referenzarchitekturen und Sicherheitsprinzipien, um von Anfang an Sicherheit ganzheitlich zu adressieren. Dies trägt dazu bei, die Sicherheit und Zuverlässigkeit zu erhöhen. Des Weiteren wird durch Architekturmanagement sichergestellt, dass Schnittstellen zwischen Anwendungen effizient verwaltet werden.
Zeitliche Dimension	☐ Kurzfristig ☒ Mittelfristig ☒ Langfristig
Relevanz	☒ Zuverlässigkeit (Safety) ☒ Sicherheit (Security) ☐ Recht und Gesellschaft
Assoziierte Bedrohungen	Sicherheitsarchitekturmanagement versucht Sicherheitsmaßnahmen auf allen Ebenen zu balancieren und adressiert somit sowohl Angriffe auf Systeme als auch die Verhinderung von Fehlern (z.B. durch Aufzeigen von Zusammenhängen zwischen Applikationen).
Emerging Technology	Vor allem cyber-physischen Systeme sowie das Internet der Dinge können durch sichere Unternehmensreferenzarchitekturen in bestimmten Bereichen (z.B. Produktion – Smart Factory) profitieren.
Forschungs-fragen	Forschungsfragen in diesem Bereich umfassen:

[236] BITKOM, 2011.

[237] Sherwood, Clark, and Lynas, 2005.

	• Wie kann durch geeignete IT-Sicherheitskonzepte, -architekturen und -standards Betriebs- und Angriffssicherheit für Industrie-4.0-Anwendungsfälle gewährleistet werden?[238, 239] • Wie können Methoden des (Sicherheits-) Architekturmanagements dazu beitragen, heterogene (bestehende und intelligente, neue) Anlagen sicher zu betreiben? • Wie kann die Sicherheit von Unternehmensinformationssystemen mit Unterstützung von Sicherheitsarchitekturmanagement verbessert werden?

5.5 Wissens- und Informationsaustausch

Beschreibung	Um großflächige Angriffe abwehren zu können, ist es notwendig, Informationen über Angriffe mit anderen Organisationen effektiv und effizient zu teilen. Um dies zu ermöglichen, ist es notwendig, Ansätze, Systeme und Datenformate zu entwickeln, welche den Austausch von Angriffs- und Bedrohungssituation organisationsübergreifend ermöglichen. Neben technischen Herausforderungen, ist es auch wichtig, organisatorische und rechtliche Aspekte zum Informationsaustausch zu beleuchten sowie existierende Ansätze und Initiativen zu berücksichtigen [240,241,242]. Für die Abbildung sicherheitsrelevanten Wissens werden oftmals Sicherheits- sowie Bedrohungsmuster (security patterns, misuse patterns) verwendet. Diese Muster dienen dazu, effektive Schutzmaßnahmen bzw. Bedrohungen zu abstrahieren und so anderen zur Verfügung zu stellen.
Derzeitige Heraus-forderungen	Die Entwicklung von Mechanismen zum Wissens- und Informationsaustausch über Schwachstellen, Angriffe und Fehlerquellen in Informationssystemen stellt vielseitige Herausforderungen dar. Neben rechtlichen Herausforderungen aufgrund von gesetzlichen Bestimmungen kommen technische und organisatorische Herausforderungen zum Tragen.
Zeitliche Dimension	☒ Kurzfristig ☒ Mittelfristig ☒ Langfristig
Relevanz	☒ Zuverlässigkeit (Safety) ☒ Sicherheit (Security) ☒ Recht und Gesellschaft

[238] ExpertInneninterviews.
[239] ACATECH – Deutsche Akademie der Technikwissenschaften, 2013.
[240] Rutkowski et al., 2010.
[241] Open IOC Indicators of Compromise Webseite.
[242] MITRE, Structured Threat Information Expression Webseite.

Assoziierte Bedrohungen	Der Austausch von Informationen ist vor allem bei schwerwiegenden Angriffen (z.B. großflächigen Denial-of-Service-Angriffen, gezielten, persistenten Angriffen) oder Fehlern kritischer Infrastrukturen (z.B. Steuerungsnetze von Energiebetreibern) essentiell.
Emerging Technology	Neuartige Technologien beeinflussen dieses Forschungsgebiet durch mögliche neue Informationsartefakte, welche ausgetauscht werden, oder rechtliche Herausforderungen bei grenzüberschreitendem Informationsaustausch, wie etwa bei Cloud-Technologien.
Forschungs-fragen	Beispielhafte Forschungsfragen dieses Bereichs umfassen: • Wie können Informationen ausgetauscht werden, um ein umfassendes Lagebild komplexer, hochdynamischer Systeme zu erhalten (z.B. Smart Grids)? [243,244] • Wie können Informationen während Zwischenfällen ausgetauscht werden und gleichzeitig die Vertraulichkeit wichtiger Daten gewährleistet werden? [245]

5.6 Visualisierung / Visual Analytics

Beschreibung	Eine Vielzahl an Werkzeugen, wie beispielsweise Security Information and Event Management (SIEM) Systeme, Virenscanner und viele mehr, sammelt wertvolle, sicherheitsrelevante Informationen. Visual Analytics koppelt Techniken der Visualisierung mit analytischen Techniken wie Data-Mining. Vorteile für die Verwendung von Cybersicherheit umfassen laut Staheli et al.[246] beispielsweise die Identifikation von Mustern aus Daten, welche von Maschinen nicht erkannt werden oder die Unterstützung von SicherheitsanalystInnen, um ihre Tätigkeiten effizienter zu erledigen. Dass Visual Analytics verwendet werden kann, um immer ausgereiftere Angriffe zu erkennen und Anomalien in wachsenden Datenbeständen zu untersuchen, zeigen auch Forschungsprojekte wie VIS-Sense[247] oder VALCRI[248].
Derzeitige Heraus-forderungen	Durch die stetig wachsende Zahl an Daten besteht die Herausforderung, die geeigneten Informationen aus den vorhandenen Datenbeständen zu identifizieren, zu verknüpfen und zu visualisieren.
Zeitliche Dimension	☒ Kurzfristig ☒ Mittelfristig

[243] ExpertInneninterviews.
[244] Bos et al., 2013.
[245] ibid.
[246] Staheli et al., 2014.
[247] Vgl. VIS-Sense Webseite.
[248] Vgl. VALCRI Projektwebseite.

	☐ Langfristig
Relevanz	☒ Zuverlässigkeit (Safety) ☒ Sicherheit (Security) ☐ Recht und Gesellschaft
Assoziierte Bedrohungen	Die Visualisierung von Sicherheitsinformationen kann auf eine Vielzahl von Bedrohungen angewandt werden.
Emerging Technology	Vor allem der Bereich Big-Data-Analysetechniken beeinflusst Visual Analytics für Sicherheitszwecke. Des Weiteren stellen neue Anwendungsgebiete, wie Industrie 4.0 oder andere komplexe cyber-physische Systeme, ein interessantes Einsatzszenario für dieses Forschungsgebiet dar.
Forschungs-fragen	Forschungsfragestellungen umfassen beispielsweise: • Wie können Visual-Analytics-Techniken dabei unterstützen, ein nationales Lagebild zu erstellen? • Wie kann Visual Analytics unterstützen, Angriffe und Fehler in Informationssystemen zu erkennen bzw. zu analysieren?[249]

5.7 Bekämpfung von Schadsoftware

Beschreibung	Schadsoftware wie beispielsweise Viren, Würmer, welche Betriebssysteme oder Anwendungssoftware angreifen, stellen eine ernsthafte Bedrohung für die Sicherheit von Systemen dar und sind meist die Speerspitze vieler Attacken. Durch die Professionalisierung[250] und Kurzlebigkeit bzw. durch den gezielten Einsatz von Schadsoftware sind statische Verfahren kaum mehr effektiv, um der Bedrohung entgegenzuwirken. Mögliche Ziele von Schadsoftware umfassen unter anderem Phishing, Verbreitung von Malware, Verbreitung illegaler Inhalte und Identitätsdiebstahl.[251] Als besonders gefährdet gelten auch zunehmend mobile Systeme wie Sophos in seinem Mobile Security Threat Report 2014 herausstreicht.[252] Jüngste Analysen russischer SicherheitsexpertInnen der Firma Kaspersky bestätigen auch die Gefahr, welche von Veränderung von Hardware ausgeht. Die Erkennung und Beseitigung kompromittierter Hard- und Firmware stellt eine große Herausforderung dar, da sie schwer entfernt und entdeckt werden kann. [253] Daher ist es notwendig, neuartige Verfahren zur Erkennung Hardware-basierter Schadsoftware (z.B. Hardware Trojans) zu entwickeln.

[249] Workshop.
[250] Kaspersky, 2014.
[251] KrebsonSecurity, 2012.
[252] Vgl. Sophos, 2014.
[253] Vgl. Menn, 2015; Tehranipoor und Koushanfar, 2010.

Derzeitige Heraus-forderungen	Panda Security[254] veröffentlicht im letzten Security Report (Q3/2014), dass weltweit mehr als 22.0000 neue Malware Samples pro Tag erzeugt werden. Kaspersky geht sogar von über 31.5000 täglichen Samples aus.[255] Neben zahlreichen Verschleierungstaktiken ist ein weiteres Problem im Kampf gegen Schadsoftware, dass Schadsoftware oftmals nur für einen kurzen Zeitraum (mehrere Stunden) aktiv ist.[256]
Zeitliche Dimension	☒ Kurzfristig ☒ Mittelfristig ☒ Langfristig
Relevanz	☐ Zuverlässigkeit (Safety) ☒ Sicherheit (Security) ☐ Recht und Gesellschaft
Assoziierte Bedrohungen	Malware
Emerging Technology	Schadsoftware kann in allen Hard- und Softwarekomponenten vorkommen und stellt damit eine Bedrohung in jeder aufkommenden Technologie dar.
Forschungs-fragen	Um Schadsoftware zu bekämpfen, könnten folgende Forschungsfragen unterstützen: • Wie kann Schadsoftware frühzeitig für spezielle Anwendungen analysiert werden? • Wie können Analysetechniken verbessert werden, um schnelleres und effizienteres Schadcode Reverse Engineering zu ermöglichen? • Welche Möglichkeiten existieren, um Schadsoftwaretrends vorherzusagen? • Wie kann gezielt geschriebene Schadsoftware erkannt werden? Wie können Angriffe durch Schadsoftware zeitnah erkannt werden? • Wie können neue Verfahren, welche das Verhalten von Software prüfen, dazu dienen, nicht bekannte Schadsoftware zu identifizieren?

5.8 Bekämpfung von Botnetzen

Beschreibung	Botnetze werden häufig verwendet, um weitere Systeme zu attackieren oder unerwünschte Inhalte weiter zu verbreiten. Da sie eine wichtige Einnahmequelle für Cyberkriminelle darstellen, werden zunehmend neue Techniken und Verfahren verwendet, um ihre Widerstandsfähigkeit zu steigern. Das Ausmaß dieser Bedrohung zeigen aktuelle Zahlen des Anti-Botnet-Beratungszentrums

[254] Panda Labs, 2014.
[255] Kaspersky, 2014, S. 3.
[256] Vgl. sicherheit.info, 2009.

	Eco. Danach sind 40% aller PCs in Deutschland infiziert.[257] Der beste Weg diese mächtigen Netzwerke zu stoppen, ist die Blockierung der Kommando- und Kommunikationsstrukturen.[258]
Derzeitige Heraus-forderungen	Die Herausforderungen bei der Bekämpfung von Botnetzen stellen sich vor allem in der Unterbrechung der Command & Control Strukturen über welche die Bots neue Befehle erhalten.
Zeitliche Dimension	☒ Kurzfristig ☒ Mittelfristig ☐ Langfristig
Relevanz	☐ Zuverlässigkeit (Safety) ☒ Sicherheit (Security) ☒ Recht und Gesellschaft
Assoziierte Bedrohungen	Botnetzwerke
Emerging Technology	Botnetzwerke betreffen alle Technologien, welche über das Internet verbunden sind. Besonders gefährdet scheinen jedoch vor allem mobile Geräte[259] bzw. ungesicherte Haushaltsgeräte.[260]
Forschungs-fragen	Forschungsfragen in diesem Bereich umfassen: • Wie können neue Techniken unterstützen, um Botnetzkommandostrukturen zu infiltrieren? • Welche Ansätze können helfen, Botnetzkommunikation zu erkennen und zu analysieren (Reverse Engineering)? • Wie kann die Größe und Verteilung bestehender Botnetze besser analysiert werden? • Wie können die Auswirkungen, welche von Botnetzangriffen hervorgerufen werden können, verringert werden? • Welche rechtlichen Maßnahmen könnten die Bekämpfung von Botnetzen verbessern?

5.9 Sichere Software

Beschreibung	Das Herzstück jedes Informationssystems ist die Software, welche Services bereitstellt. Zunehmende Komplexität, Einbindung externer Bibliotheken sowie eine steigende Anzahl an EntwicklerInnen (z.B. mobiler Applikationen) ohne Sicherheitsausbildung benötigen neue Verfahren zur Unterstützung von

[257] Spiegel, 2015.
[258] Neeraj, 2013.
[259] FutureZone, 2012.
[260] Kannenberg, 2014.

	SoftwarearchitektInnen und EntwicklerInnen. Vorfälle der jüngsten Vergangenheit[261] sowie zahlreiche Publikationen[262,263] zeigen die Gefahr, welche von fehlerhafter oder schlecht geschriebener Software ausgeht. Daher ist es notwendig, Ansätze zur Verfügung zu stellen, welche die Betriebs- und Angriffssicherheit über den gesamten Lebenszyklus zur Verfügung zu stellen. Dazu zählen sowohl Techniken, um Designfehler (Flaws) als auch Progammierfehler (Bugs) aufzudecken. Zu diesem Zweck sollen Ansätze und Werkzeuge geschaffen werden, welche die Qualität und Sicherheit von Applikationen gewährleisten.
Derzeitige Heraus-forderungen	Zunehmende Komplexität, die immer stärkere Abhängigkeit der Wirtschaft und Gesellschaft von Informationsdienstleistungen sowie eine Vielzahl von SoftwareentwicklerInnen ohne Sicherheitsausbildung (vor allem im mobilen App-Bereich) erfordern neue Ansätze, um die Sicherheit von Anwendungen zu gewährleisten.
Zeitliche Dimension	☒ Kurzfristig ☒ Mittelfristig ☒ Langfristig
Relevanz	☒ Zuverlässigkeit (Safety) ☒ Sicherheit (Security) ☐ Recht und Gesellschaft
Assoziierte Bedrohungen	Unsichere Software kann zu Fehlern oder Schwachstellen für Angriffe durch AngreiferInnen oder Schadsoftware führen.
Emerging Technology	Da Software alle Bereiche umfasst, betrifft sichere Softwareentwicklung alle aufstrebenden Technologien.
Forschungs-fragen	Mögliche Forschungsfragestellungen umfassen: • Wie kann die sichere Codeentwicklung durch Entwurfsmuster, Referenzmodelle o.ä. gefördert werden? • Wie können nicht sicherheitsaffine EntwicklerInnen bei der Implementierung durch spezielle Programmierumgebungen unterstützt werden, sicheren Code zu schreiben? • Wie kann Software gegen Reverse Engineering und Raubkopien geschützt werden? • Wie können neue Plattformen den EntwicklerInnen die Sicherheit abnehmen? • Wie können neue Verfahren beim Auffinden/Erkennen von Schwachstellen unterstützen?

[261] ABC News, 2014.
[262] SANS, 2011.
[263] Huckle, 2015.

	• Wie ist es möglich, Schäden von Softwareschwachstellen einzudämmen? • Wie könnten neue Verfahren zur Adressierung von Gefahren bei Zero-Day Exploits beisteuern?

5.10 Sicherheit von Systemen in fremden Umgebungen

Beschreibung	Oftmals ist es wichtig, Systeme an Umgebungen aufzustellen, in denen die BetreiberInnen den physischen Zugriff auf das System nicht absichern können (z.B. Stromzähler, vermietete Maschine, etc.). Neue Geschäftsmodelle bei denen Geräte immer häufiger nicht mehr gekauft, sondern nur mehr geleast werden, erfordern Sicherheit in fremden, feindlichen Umgebungen (hostile environments). In diesem Fall stellt es eine besondere Herausforderung dar, das System vor unerwünschten Manipulationen zu schützen. Smart Cards und ähnliche Technologien sind bereits für diese Art von Einsatz konzipiert. Aufgrund der steigenden Anzahl an Geräten, welche durch neue Technologien in fremden Umgebungen stehen werden, ist es wichtig, Sicherheitsmechanismen in diesem Bereich zu entwickeln.
Derzeitige Heraus-forderungen	Leasinggeschäftsmodelle in zahlreichen Branchen erfordern Sicherheit auch in nicht physisch abgesicherten Systemen zu gewährleisten.
Zeitliche Dimension	☒ Kurzfristig ☒ Mittelfristig ☒ Langfristig
Relevanz	☒ Zuverlässigkeit (Safety) ☒ Sicherheit (Security) ☐ Recht und Gesellschaft
Assoziierte Bedrohungen	Durch das Aufstellen von Systemen in nicht kontrollierten Bereichen ist es möglich, Informationen zu verändern oder auszulesen. Daher sind vor allem Bedrohungen wie unerlaubtes Eindringen (Hacking) oder Datenabfluss (Data Loss) mögliche Bedrohungen.
Emerging Technology	Cyber-physische Systeme, Internet der Dinge, Robotics
Forschungs-fragen	Mögliche Forschungsfragen umfassen: • Wie können Systeme in feindlichen („hostile“) Umgebungen abgesichert werden? • Wie kann Sicherheit in Ad-hoc-Netzwerken gewährleistet werden?

5.11 Identitätsmanagement

Beschreibung	Die derzeitige Situation betreffend elektronische Identitäten im Internet ist unzureichend und unsicher: Die Vielzahl an BenutzerInnenkonten und Passwörtern überfordert die NutzerInnen und führt zur unsicheren/mehrfachen Verwendung von Passwörtern und zur Verwendung unsicherer Passwörter. Die NutzerInnen müssen i.d.R. viel mehr Daten von sich preisgeben, als für die jeweiligen Dienste notwendig wäre und die personenbezogenen Daten der NutzerInnen sind über eine unüberschaubare Zahl von DienstanbieterInnen verteilt. Der qualifizierte Nachweis der Identität und einzelner Attribute ist häufig nicht möglich und somit können bestimmte Transaktionen, wie etwa die Eröffnung eines Bankkontos via Internet, nicht durchgeführt werden. Aus den genannten Gründen ist das Thema der elektronischen Identitäten eines der weitreichendsten Probleme bei der Nutzung des Internets. Ansätze, diese Situation zu verbessern, existieren, wie z.B. die US-Initiative NSTIC[264] oder die Ergebnisse von FP7-Projekten wie etwa FutureID[265]. Basis dieser Ansätze ist das Konzept der Identity Federation, das ist die mehrfache Verwendung elektronischer Identitäten über Organisationsgrenzen hinweg. Eine Rolle spielen dabei sogenannte Identity Provider, denen sowohl von Seiten der NutzerInnen (Datenschutz) als auch von Seiten der DienstanbieterInnen (Identitätsdaten) vertraut wird. Aus verschiedenen Gründen haben sich diese Ansätze jedoch noch nicht etabliert, vermutlich primär aufgrund einer Henne-Ei-Problematik (es bestehen Netzwerkeffekte; in der Anfangsphase entsteht ein vergleichsweise hoher Aufwand, während sich der Nutzen erst bei tatsächlicher Verbreitung einstellt). Daher werden Aktivitäten empfohlen, um die praktische Umsetzung und Durchsetzung solcher Ansätze zu fördern. Während in der Geschäftswelt ein wichtiger Aspekt des Identitätsmanagement in der Beherrschung der Rollen, Rechteverwaltung der Vielzahl an Systemen sowie geeigneter Authentifizierungsmechanismen liegt, gibt es im privaten Umfeld vor allem Herausforderungen im Management von mehreren Identitäten, Stärkung von Vertrauen (z.B. durch Trust and Reputation Systeme) und sichere, benutzerfreundliche Authentifizierungssysteme.
Derzeitige Heraus-forderungen	Neue Verfahren, steigende Automatisierung und Smartness von Geräten / Maschinen sowie die zunehmende Verbindung zwischen digitaler und realer Realität stellen die Forschung in diesen Bereich vor zahlreiche Herausforderungen. Großer Bedarf hinsichtlich rechtlicher, wirtschaftlicher und gesellschaftlicher Sicht besteht an:

[264] Vgl. NIST National Strategy for Trusted Identities in Cyberspace Webseite.

[265] Vgl. FutureID Shaping the Future of Electronic Identity Webseite.

	• der wissenschaftlichen Erforschung der wirtschaftlichen Zusammenhänge in Identity-Federation-Systemen (Geschäftsmodelle etc.); • der soziologischen Erforschung des Themas aus der Perspektive der NutzerInnen und der übrigen StakeholderInnen im Hinblick auf die Einführung und Etablierung von Identity-Federation-Systemen; • der wissenschaftlichen Erforschung der rechtlichen Rahmenbedingungen von Identity-Federation-Systemen (Schwerpunkt Datenschutzrecht) und ihrer möglichst effektiven vertraglichen Gestaltung.
Zeitliche Dimension	☒ Kurzfristig ☒ Mittelfristig ☐ Langfristig
Relevanz	☐ Zuverlässigkeit (Safety) ☒ Sicherheit (Security) ☒ Recht und Gesellschaft
Assoziierte Bedrohungen	Identity Theft, Social Engineering, Advanced Persistent Threats
Emerging Technology	Cloud Computing, Internet of Things
Forschungs-fragen	Forschungsfragen umfassen: • Wie können offene und skalierbare Lösungen für Federated Identity Management aussehen?[266] • Wie kann sicheres Identitätsmanagement für Maschine-zu-Maschine/Gerät-zu-Gerät Situationen aussehen? [267] • Wie kann ein allgegenwärtiges Identitätsmanagement für Internet of Things und andere Zukunftsszenarien aussehen?[268] • Wie können neue Authentifizierungsmechanismen die Sicherheit und BenutzerInnenfreundlichkeit personenbasierter Verfahren erhöhen?[269] • Wie können neue Verfahren und Analysemethoden verwendet werden, um Rechte und Rollen besser zu definieren?

[266] Torres et al., 2014, S. 58.
[267] Torres et al., 2014, S. 71.
[268] Torres et al., 2014, S. 58.
[269] Interviews, Workshop.

5.12 Entwicklung sicherer Hardware

Beschreibung	Viele Technologien der Zukunft basieren auf der Annahme sicherer Hardware wie beispielsweise Smart Cards/Chipkarten/SIM Cards. Es ist wichtig zu verstehen, dass nur durch die Sicherstellung der gesamten Wertschöpfungskette (Hardware, Firmware, Software) gewährleistet werden kann, dass ein Gesamtsystem sicher und zuverlässig ist. Um die Sicherheit in diesem Bereich zu fördern, ist es notwendig, formale Methoden zur Sicherheitsprüfung sowie Ansätze zur Schaffung sicherer Hardware zu schaffen.
Derzeitige Heraus-forderungen	Sicherheit auf der untersten Ebene eines Systems ist unabdingbar Hardware. Eine Schwierigkeit ist, dass durch Komplexität und Kostendruck meist zahlreiche Entitäten an der Chipherstellung beteiligt sind.[270] King et al.[271] zeigen, dass nur wenige Veränderungen der Hardware notwendig sind, welche extrem schwer auffindbar sind.
Zeitliche Dimension	☒ Kurzfristig ☒ Mittelfristig ☒ Langfristig
Relevanz	☐ Zuverlässigkeit (Safety) ☒ Sicherheit (Security) ☒ Recht und Gesellschaft
Assoziierte Bedrohungen	Da Hardware von allen Informationssystemen benötigt wird, hätte Schadsoftware in Hardware weitreichende Folgen.
Emerging Technology	Alle
Forschungs-fragen	Forschungsfragen umfassen Fragestellungen wie: • Wie können Methoden zur Sicherheitsprüfung von Hardware verbessert werden? • Wie können Hochsicherheitsstandards (z.B. SIM) auf Chips transferiert werden? • Wie könnten Lightweight Kryptographieverfahren für Echtzeitsysteme mit geringen Ressourcen (Energie, Rechenleitung, Speicher) weiter verbessert werden um das Schutzniveau zu verbessern?

[270] Mitra et al., o.J.

[271] King et al., 2008.

5.13 Sichere Netzwerke

Beschreibung	Netzwerke bilden die Grundlage für die Kommunikation zwischen Systemen und sind damit ein unabdingbarer Bereich für Sicherheitsbetrachtungen. Neue Entwicklungen von Netzwerktechnologien (z.B. Software Defined Networks) führen zu neuen Chancen und Herausforderungen im Sicherheitsbereich. Auch immer größer werdende Datenmengen, welche über Netzwerke transportiert werden, der höhere Grad an Vernetzung durch neue Geräte (in Industrie und Heimanwenderbereich) sowie die starke Abhängigkeit von Kommunikationsnetzwerken machen Netzwerke zu einem interessanten Ziel für AngreiferInnen. Zusätzlich können Fehler, die von Netzwerkschutzmechanismen nicht gefiltert werden, zu weitreichenden Folgen der Betriebssicherheit (Safety) führen. Die Wichtigkeit des Schutzes von Netzwerken zeigen beispielsweise jüngste Sicherheitsuntersuchungen von Controller Area Networks in Autos[272,273].
Derzeitige Heraus-forderungen	Im Rahmen der Interviews konnten Herausforderungen in folgenden Bereichen identifiziert werden. **Sichere Netzwerkprotokolle:** Da Informationsnetzwerke die Grundlage für unsere Kommunikation bilden, ist es unerlässlich, Protokolle zu analysieren, zu verbessern sowie neue Protokolle zu entwickeln. In diesen Bereich fällt beispielsweise die Entwicklung effizienter Protokolle für die sichere Kommunikation in Controller Area Networks. **Sicherheit von Software Defined Networks / Network Function Virtualization:** Die neuen Technologien vereinfachen die Netzwerkadministration und bringen Virtualisierung im Netzwerkbereich. Durch die Entkopplung der Steuerung und Weiterleitung sind auch neue Ansätze und Anwendungen im Sicherheitsbereich zu erwarten. **Intelligence Driven Network Security[274,275]/Netzwerk Intrusion Detection/Prevention:** im Bereich der Netzwerke ergeben sich durch die stark steigende Datenflut neue Herausforderungen (stark steigendes Volumen[276]) und Chancen (mehr Daten, die für eine umfassende Analyse herangezogen werden können). **Netzwerkverkehrsanalyse / Frühwarnsysteme:** Um großflächige Angriffe frühzeitig zu erkennen und sich darauf vorzubereiten, ist es wichtig, Systeme zu schaffen, welche diese erkennen und in der Lage sind, die Informationen zielgerichtet mit potenziell betroffenen oder gefährdeten Entitäten auszutauschen.

[272] Center for Automotive Embedded System Security Webseite.
[273] Valasek und Miller, o.J.
[274] Curry et al., 2013.
[275] Hutchins et al., o.J.
[276] Cisco, 2014.

Zeitliche Dimension	☒ Kurzfristig ☒ Mittelfristig ☐ Langfristig
Relevanz	☒ Zuverlässigkeit (Safety) ☒ Sicherheit (Security) ☐ Recht und Gesellschaft
Assoziierte Bedrohungen	Durch die immer stärker werdende Vernetzung ist dieser Forschungsbereich mit zahlreichen Bedrohungen wie etwa Schadsoftware, SPAM, Denial of Service, Advanced Persistent Threats verbunden.
Emerging Technology	Da der Trend zu Vernetzung aller Geräte und Maschinen ungebrochen ist, werden zukünftige Technologien auch sehr stark von der Sicherheit der darunterliegenden Netzwerke abhängen.
Forschungs-fragen	Forschungsfragen, welche die Sicherheit von Netzwerken zu verbessern umfassen, sind unter anderem: • Wie können Informationen aus mehreren Netzwerksicherheitsanwendungen (z.B. Firewalls, Honeypots, Logs, Network Intrusion Detection Systeme, Antivirus,…) verwendet werden, um Angriffe besser vorherzusagen und zu analysieren? • Wie kann die Identifikation von Anomalien im Netzwerkstrom helfen, Angriffe bzw. erfolgreiche Einbrüche in die IT frühzeitiger zu erkennen? • Wie können langfristige, gezielte Angriffe (Advanced Persistent Threats) durch neue Netzwerk-Sicherheitstechnologien erkannt werden? • Wie kann die Sicherheit von Maschine-zu-Maschine (M2M) Kommunikation in Systemen erhöht werden? • Wie kann sichergestellt werden, dass unterschiedlichste Geräte (Kühlschrank, Waschmaschine) in einem Netzwerk der Geräte und Services (Internet of Things and Services) sicher kommunizieren? • Wie können Schutzmaßnahmen für Echtzeitsysteme der Netzwerksicherheit in Safety-kritischen (Produktionsanlagen, Car Area Network) aussehen?

5.14 Self-healing / Self-protection

Beschreibung	Um die zunehmende Automatisierung – trotz steigender Komplexität der Systeme – voranzutreiben, werden Systeme benötigt, welche in der Lage sind, Fehler selbst zu diagnostizieren und im Falle eines Fehlers oder Angriffs selbstheilende Mechanismen anzustoßen.

Derzeitige Heraus-forderungen	Eine besondere Herausforderung dabei ist die Entwicklung von Ansätzen und Werkzeugen, welche mit der dynamischen Risikolandschaft umgehen können.[277]
Zeitliche Dimension	☒ Kurzfristig ☒ Mittelfristig ☐ Langfristig
Relevanz	☒ Zuverlässigkeit (Safety) ☒ Sicherheit (Security) ☐ Recht und Gesellschaft
Assoziierte Bedrohungen	Vor allem Bedrohungen, welche die Widerstandskraft eines Systems gefährden, wie etwa Fehler (Betriebssicherheit) oder technische Angriffe durch Dritte (Angriffssicherheit) fallen in diesen Bereich.
Emerging Technology	Fortschritte in diesem Bereich hätten hohe Bedeutung für Internet of Things, cyber-physische Systeme, Embedded Systems sowie Robotics.
Forschungs-fragen	Forschungsfragen umfassen: • Wie können neue Verfahren zu Fehlererkennung die Selbstdiagnosefähigkeiten erhöhen? • Wie kann Selbstheilung von Systemen in verschiedenen Bereichen umgesetzt werden? • Wie könnte Selbstmanagement von Infrastruktur (self-learning, self-repairing) aussehen?[278]

5.15 Verschlüsselung, Pseudonymisierung, Anonymisierung

Beschreibung	Die Sicherheit digitaler Daten basiert zu einem großen Teil auf der Sicherheit von kryptographischen Verfahren. Daher ist es notwendig, die Sicherheit aktueller Verfahren laufend zu evaluieren, neue Verfahren für bestimmte Anwendungsbereiche zu entwickeln und Verfahren zur Gewährleistung der Privatsphäre zu kreieren. Datensammlung durch Unternehmen sowie soziale Netzwerke, die immer stärkere Allgegenwärtigkeit von Informationssystemen sowie Berichte über Massenüberwachung im Netz machen die Entwicklung neuer Verfahren zum Schutz der Privatsphäre notwendig.
Derzeitige Heraus-forderungen	Testen vorhandener Verschlüsselungsverfahren sowie die Entwicklung neuer Verfahren (z.B. für Echtzeitsysteme mit geringen Ressourcen) sind wichtige Forschungsfelder in diesem Bereich. Auch moderne Verschlüsselungsalgorithmen, welche auch nach Entwicklung von

[277] Ahokangas et al., 2014.

[278] Torres et al., 2014, S.45-69.

	Quantenrechnern einsetzbar wären (Postquantumkryptographie), stellen eine wichtige Herausforderung in diesem Bereich dar. Für die Sicherheit von Cloudsystemen sind Projekte wichtig, die sich mit dem Suchen und Rechnen mit verschlüsselten Werten beschäftigen. Im Bereich der Privatsphäre sind vor allem Verfahren zu Pseudonymisierung und Anonymisierung interessant, welche einerseits ein Arbeiten mit den Daten ermöglichen und anderseits die Privatsphäre von Personen bewahren.
Zeitliche Dimension	☒ Kurzfristig ☒ Mittelfristig ☒ Langfristig
Relevanz	☐ Zuverlässigkeit (Safety) ☒ Sicherheit (Security) ☒ Recht und Gesellschaft
Assoziierte Bedrohungen	Verschlüsselung ist ein zentrales Element der Informationssicherheit und daher für alle Bereiche interessant.
Emerging Technology	Dieser Bereich hat für nahezu alle Emerging Technologies Implikationen, besonders jedoch für Cloud Computing, Big Data und Quantenrechner.
Forschungs-fragen	Forschungsfragen umfassen: • Wie können Verschlüsselungsverfahren für bestimmte Anwendungsbereiche (z.B.: resource constraint devices) aussehen? • Wie kann die Sicherheit kryptographischer Verfahren trotz Quantenrechner aufrecht erhalten bleiben? • Wie könnte effiziente Verschlüsselung für Big Data aussehen? • Wie können neue Verfahren (privacy preserving) für Big Data Analysen aussehen?

5.16 Technikfolgenabschätzung und Privacy Impact Assessment

Beschreibung	Die folgende Beschreibung umfasst sowohl Technikfolgenabschätzung als auch Privacy Impact Assessment (PIA) und setzt diese beiden Begriffe zueinander in Beziehung. Impact Assessment (dt. Folgenabschätzung) ist ein etabliertes Konzept, das insbesondere in seiner Form als Technikfolgenabschätzung seit Jahrzehnten anerkannt ist. Privacy Impact Assessment (PIA) entwickelte sich nach Anfängen, die deutlich weiter zurückreichen, insbesondere in den 1990er-Jahren primär zunächst außerhalb Europas. PIA kann als Spezialfall der Technikfolgenabschätzung betrachtet werden und wird definiert als „methodology for assessing the impacts on privacy of a project, policy, programme, service, product or other initiative and, in consultation with stakeholders, for taking

	remedial actions as necessary in order to avoid or minimise negative impacts."[279] Zu betonen ist, dass „privacy" hier weit zu verstehen ist und sich auf verschiedene Aspekte der Privatsphäre bezieht, nicht nur auf Datenschutz und insbesondere nicht nur auf die Einhaltung datenschutzrechtlicher Bestimmungen. Dem gegenüber zielt der weitere Begriff der „Technikfolgenabschätzung" auf sämtliche, insbesondere nicht intendierte, negative Folgen einer Entwicklung für Einzelne oder die Gesellschaft insgesamt ab, beispielsweise im Hinblick auf andere Grundrechte als „Privacy" bzw. „Datenschutz", wie etwa die Informationsfreiheit aus sozialwissenschaftlicher Perspektive – dazu näher in Kapitel 3.4.3. Aus technischer Sicht können folgende fünf Schritte des PIA unterschieden werden:[280] 1. Identifikation und Konsultation der StakeholderInnen 2. Identifikation der Risiken (unter Berücksichtigung der Sichtweise der StakeholderInnen) 3. Identifikation von Lösungen und Formulierung von Empfehlungen 4. Umsetzung der Empfehlungen 5. Reviews, Audits und Haftungsregeln
Derzeitige Heraus-forderungen	Die Herausforderung besteht in der Umsetzung in die Praxis in Form eines praxisnahen und möglichst effizienten und effektiven Prozesses.
Zeitliche Dimension	☒ Kurzfristig ☒ Mittelfristig ☒ Langfristig
Relevanz	☐ Zuverlässigkeit (Safety) ☐ Sicherheit (Security) ☒ Recht und Gesellschaft
Assoziierte Bedrohungen	Bedrohungen der Privatsphäre und des Schutzes personenbezogener Daten.
Emerging Technology	Technikfolgenabschätzung und PIA sind für fast alle Emerging Technologies relevant, insbesondere für Big Data, Vernetzte Gesellschaft, Mobile Devices und Augmented Reality.
Forschungs-fragen	Forschungsfragen umfassen: • Wie können Technikfolgenabschätzung und PIA in die Praxis umgesetzt werden und möglichst effizient und effektiv gestaltet werden?

[279] Wrigh und De Hert, 2012, S. 5.

[280] Vgl. ENISA, 2014, S. 18.

5.17 Privacy by Design and by Default

Beschreibung	Privacy by Design bedeutet, bei der Entwicklung von Systemen den Datenschutz und den Schutz der Privatsphäre bereits von Beginn im Entwicklungsprozess zu berücksichtigen und zum integralen Bestandteil des Systems werden zu lassen. Privacy by Default bedeutet, dass die Grundeinstellungen einer Software möglichst im Sinne des Datenschutzes und des Schutzes der Privatsphäre gewählt sind und die Software nicht bloß durch „wissende“ NutzerInnen in diesem Sinne konfiguriert werden muss, sodass die datenschutzfreundlichen Einstellungen vielen DurchschnittsnutzerInnen verborgen bleiben. Das Konzept Privacy by Design wurde in den 1990er-Jahren von der früheren langjährigen Informationsfreiheits- und Datenschutzbeauftragten der kanadischen Provinz Ontario Ann Cavoukian postuliert. Eine Umsetzung des Konzepts in die Praxis und vor allem eine Methode für diese Umsetzung, die in der Softwareentwicklung und in der Entwicklung anderer technischer Systeme allgemein anwendbar wäre, fehlt jedoch nach wie vor weitgehend.[281] Zum Teil wird kritisiert, dass Privacy by Design häufig nicht verstanden wird.
Derzeitige Heraus-forderungen	Es besteht ein großer Forschungsbedarf hinsichtlich der konkreten Umsetzung des Konzepts Privacy by Design in die Praxis. Dies ist primär ein technischer Forschungsbedarf. Um sich in der Praxis durchzusetzen, muss sich das Konzept Privacy by Design aus seiner derzeitigen Domäne im Umfeld der Datenschutzforschung emanzipieren und insbesondere in der Domäne des Software Engineering etablieren.
Zeitliche Dimension	☒ Kurzfristig ☒ Mittelfristig ☐ Langfristig
Relevanz	☐ Zuverlässigkeit (Safety) ☐ Sicherheit (Security) ☒ Recht und Gesellschaft
Assoziierte Bedrohungen	Bedrohungen der Privatsphäre und des Schutzes personenbezogener Daten.
Emerging Technology	Privacy by Design and by Default sind für zahlreiche Emerging Technologies relevant, insbesondere für Vernetzte Gesellschaft, Mobile Devices und Augmented Reality.
Forschungs-fragen	Forschungsfragen umfassen: • Wie kann Privacy by Design in die Praxis umgesetzt werden?

[281] Vgl. ENISA, 2014.

	• Wie können Privacy by Design and by Default im Software Engineering etabliert werden und dort als Teil der nichtfunktionalen Anforderungen in jede Software einfließen, die personenbezogene Daten verarbeitet? • Wie muss ein Softwareentwicklungsprozess gestaltet sein, um Privacy by Design Rechnung zu tragen? • Können in der Softwareentwicklung standardisierte Prozesse eingeführt werden, deren Einhaltung durch die Beteiligten die Prinzipien Privacy by Design and by Default umsetzt, ohne dass eigene Privacy-Experten hinzugezogen werden müssen?

5.18 Nachvollziehbarkeit der Datenverarbeitung (Transparenz)

Beschreibung	Das Konzept der informationellen Selbstbestimmung erfordert die Kontrollierbarkeit der Datenverarbeitung. Die Verarbeitung personenbezogener Daten ist heute in der Regel nicht unmittelbar durch die Betroffenen kontrollierbar. Sie findet meist auf Servern von Unternehmen oder Behörden und somit im Verborgenen statt. Rechtswidrige Verwendung personenbezogener Daten ist daher oftmals den Betroffenen gar nicht bekannt. Dies ist eines der Grundprobleme in Bezug auf die Durchsetzung des Datenschutzrechts. Die Kernfrage ist: Wie kann dem Individuum zu mehr Wissen darüber verholfen werden, wer wo welche seiner personenbezogenen Daten zu welchem konkreten Zweck verarbeitet? Denn derzeit besteht das Problem, wenn man Daten an Dritte weitergibt, können diese mit den Daten faktisch machen, was sie wollen. Die Kontrolle soll in erster Linie den Betroffenen selbst möglich sein. Wenn dies nicht möglich ist, sollte die Kontrolle der Datenverarbeitung durch Dritte (z.B. Behörden) erfolgen. Letztlich geht es darum, die wesentlichen Voraussetzungen für eine effektive Rechtsdurchsetzung zu schaffen. Dies ist als eigenständiger Aspekt neben Privacy by Design zu verstehen und könnte, trotz Überschneidungen, als Transparency by Design bezeichnet werden. Adressiert sind hier vor allem technologische Ansätze zur Optimierung der Nachvollziehbarkeit und Transparenz aus Sicht der Betroffenen bei der Verarbeitung personenbezogener Daten, sowie letztlich zur Ausübung einer effektiven Kontrolle eines Individuums über dessen personenbezogene Daten. In dieser Hinsicht sei vor allem das sog. „Recht auf Vergessenwerden“ genannt, welches derzeit in der Praxis vor allem daran weitgehend scheitern würde, dass es sich rein technisch kaum durchsetzen ließe.
Derzeitige Heraus-forderungen	Es ist keine Technologie bekannt, die es dem Betroffenen ermöglicht, festzustellen, wer welche seiner personenbezogenen Daten innehat und verarbeitet, geschweige denn, diese Verarbeitung zur kontrollieren. Eine

	untrennbare technische Verknüpfung zwischen personenbezogenen Daten und der zugehörigen Person ist derzeit nicht vorstellbar.
Zeitliche Dimension	☒ Kurzfristig ☒ Mittelfristig ☐ Langfristig
Relevanz	☐ Zuverlässigkeit (Safety) ☐ Sicherheit (Security) ☒ Recht und Gesellschaft
Assoziierte Bedrohungen	Bedrohungen der Privatsphäre und des Schutzes personenbezogener Daten.
Emerging Technology	Die Nachvollziehbarkeit der Datenverarbeitung ist für zahlreiche Emerging Technologies relevant, insbesondere für Big Data, Cloud Computing und Vernetzte Gesellschaft.
Forschungs-fragen	Forschungsfragen umfassen: • Wie können Systeme der Datenverarbeitung in einer Weise transparent gestaltet werden, dass die Realisierung der jeweiligen Verantwortlichkeit faktisch ermöglicht wird? • Wie kann dem Individuum zu mehr Wissen darüber verholfen werden, wer wo welche seiner personenbezogenen Daten zu welchem konkreten Zweck verarbeitet? • Wie kann man ermöglichen, „Daten an die Leine zu legen“, auch in der Form, dass die Daten „nachhause telefonieren“, wenn sie verwendet werden, sodass Betroffene informiert werden, wenn die Daten verwendet werden, ohne dass dies deaktiviert oder umgangen werden kann? • Welche Rolle spielt das für das soziale Gefüge gesellschaftlich wichtige Vergessen und wie kann und soll es in einer Welt, die von der Erfassung und langfristigen Speicherung von immer mehr personenbezogenen Daten geprägt ist, umgesetzt werden?

5.19 Recht, Organisation und Kooperation in der Informationssicherheit

Beschreibung	Dieses Forschungsfeld betrifft Themen der Organisation von Informationssicherheit auf einer Makroebene. Die Kernfrage ist: Wie können sich die Gesellschaft, der Staat und die Wirtschaft auf allgemeine Bedrohungen der Informationssicherheit vorbereiten und angemessen auf solche reagieren? Wichtige Elemente sind Bewusstseinsbildung für Bedrohungen, die Erstellung von Notfallplänen zur Reaktion auf Angriffe und organisationsübergreifende Kooperation zur Abwehr von Bedrohungen.

	Das Recht spielt hier in zweierlei Hinsicht eine wichtige Rolle. Einerseits in Form des Informationssicherheitsrechts, einem sehr jungen Rechtsgebiet (vgl. dazu Abschnitt 3.2), das Vorgaben betreffend die genannten Aspekte macht. Beispielsweise sieht die geplante EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS-Richtlinie) die verpflichtende Einrichtung von Computer Emergency Response Teams (CERTs) sowie gewisse Meldepflichten vor. Andererseits kann das Recht auch Hürden für die Kooperation in Angelegenheiten der Informationssicherheit bedeuten, z.B. wenn aus datenschutzrechtlichen Gründen die Weitergabe von Daten über bestimmte AngreiferInnen eingeschränkt ist, die möglicherweise auch andere Organisationen (z.B. derselben Branche) bedrohen. Dieses Forschungsfeld hat auch eine technologische Komponente: Als Basis jeder Kooperation muss im Falle eines allgemeinen Angriffs eine funktionierende Kommunikationsinfrastruktur zur Verfügung stehen. Es stellt sich also z.B. die Frage, über welche Infrastruktur die Kommunikation bei der Abwehr eines Angriffs durchgeführt wird, dessen Ziel es ist, die Internetkommunikation möglichst flächendeckend lahmzulegen.
Derzeitige Heraus-forderungen	Herausforderungen bestehen in der Erstellung und Erprobung von Infrastruktur und Technologie für sichere und vertrauliche Kommunikation in Notfallszenarien, Notfallplänen für Notfallszenarien und in der Berechtigung zum Austausch sicherheitsrelevanter Informationen im Bedrohungsfall.
Zeitliche Dimension	☒ Kurzfristig ☒ Mittelfristig ☒ Langfristig
Relevanz	☒ Zuverlässigkeit (Safety) ☒ Sicherheit (Security) ☒ Recht und Gesellschaft
Assoziierte Bedrohungen	Vor allem (nachrichtendienstliche) Cyberangriffe und alle Angriffe und Bedrohungen, die sich auf kritische Infrastrukturen oder eine größere Zahl von Zielen richten, Denial of Service, Advanced Persistent Threats.
Emerging Technology	Das Forschungsfeld Recht, Organisation und Kooperation in der Informationssicherheit ist für fast alle Emerging Technologies relevant, insbesondere für Big Data, Vernetzte Gesellschaft, Mobile Devices und Augmented Reality.
Forschungs-fragen	Forschungsfragen umfassen: • Wie können sich die Gesellschaft, der Staat und die Wirtschaft auf allgemeine Bedrohungen der Informationssicherheit vorbereiten und angemessen auf solche reagieren?

	• Wie kann das Recht die Kooperation im Informationssicherheitsbereich fördern bzw. hemmen?

6 Leuchtturmprojekte

Auf Basis der Analyse allgemeiner Sicherheitssysteme und Emerging Technologies (vgl. Kapitel 4) werden Leuchtturmprojekte in den vier unterschiedlichen Domänen Wohnen, Energie, Produktion und Verkehr abgeleitet. Es werden dabei mögliche Szenarien und damit zusammenhängende Herausforderungen und Innovationspotentiale dargestellt. In Österreich wurden v.a. im Rahmen von Forschungsprojekten Pilotprojekte, Living Labs, Testregionen, Musterwohnungen, o.ä. entwickelt, die einzelne und z.T. auch schon mehrere Aspekte dieser Leuchtturmprojekte in der Praxis umsetzen und gemeinsam mit AnwenderInnen testen.

„Sicherheit im Allgemeinen wird immer ernster genommen und Unternehmen investieren gezielt in Projekte.“ (Zitat aus den Interviews)

6.1 Wohnen der Zukunft

Die Verwendung von Heimautomatisierungssystemen erfreut sich aufgrund sinkender Anschaffungskosten und möglicher Einsparungspotenziale einer zunehmenden Beliebtheit. Schätzungen prognostizieren einen rasanten Anstieg des Heimautomatisierungsmarkts von ca. 2 Milliarden weltweit 2012 auf ca. 11 Milliarden im Jahr 2017.

6.1.1 Szenario

Eine Familie verwendet ein Heimautomatisierungssystem. Dieses deckt sämtliche Elemente des täglichen Lebens ab. Das Heim ist für mehrere Generationen ausgelegt: die Großmutter wohnt ebenso im selben Haus wie die Familie mit den beiden Kindern, 7 und 10 Jahre alt.

Fährt ein Kind von der Schule nach Hause, beginnt die Hausautomatisierung die Temperatur im Zimmer des Kindes auf ein vordefiniertes Niveau zu bringen. Sobald das Kind an der Haustür angekommen ist, besteht die Möglichkeit, die Tür mit dem Smartphone zu öffnen. Um bei Verlust des Smartphones die Sicherheit der Wohnung nicht zu gefährden, verwendet die Smartphone-App biometrische Authentifizierung, welche benutzerfreundlich und sicher auch für Kinder anwendbar ist. Bei Verlust des Smartphones besteht die Möglichkeit, Zugänge zu sperren.

Die Beleuchtung im Haus wird automatisch gesteuert – es erkennt, wie hell es draußen ist und kennt die jeweiligen Jahreszeiten. Geht eine BewohnerIn nachts auf die Toilette, so dreht das System automatisch eine Flurbeleuchtung auf – diese ist weder zu hell (da sich die Augen anpassen müssen) noch zu dunkel, um Unfällen vorzubeugen.

Das System weiß auch, welche Musik eine Person hört und kann die Musik über die jeweiligen Räume des Hauses mitnehmen, wenn sich die Person bewegt. Ähnlich verhält es sich mit Telefonaten. Das System kann einen Anruf in das korrekte Zimmer durchstellen.

Vordefinierte HausbewohnerInnen können jederzeit Zugriff auf das System haben, um Alarmmeldungen zu verifizieren, Personen in das Gebäude hereinzulassen, die Temperatur zu steuern, Rollläden zu öffnen und zu schließen und auf weitere Dienste wie etwa das hauseigene Netzwerk zuzugreifen. Dies funktioniert über ein Cloud Service.

Das System kennt den Lagerstand (z.B. Kühlschrank) an verschiedenen Produkten und kann je nach Konfiguration Abfragen zu Produkten beantwortet und selbstständig Produkte bestellen. Hierfür misst es die Produkte und deren Ablaufdatum. Macht sich einer der beiden Elternteile auf den Heimweg von der Arbeit, so kann er/sie überprüfen, ob alle Zutaten für ein bestimmtes Gericht vorhanden sind bzw. sich vorschlagen lassen, welche Gerichte mit den vorhandenen Lebensmitteln gekocht werden können. Durch die Informationen über die Haltbarkeit kann der Speiseplan hinsichtlich des Ablaufdatums optimiert werden.

Für Arbeiten bzw. Unterstützung im Haushalt ist ein Haushaltsroboter verfügbar, welcher heruntergefallene Dinge aufhebt, staubsaugt, wäscht und andere Haushaltsarbeiten erledigt. Außerdem ist es möglich, über den Roboter mit anderen Personen in Kontakt zu bleiben.

Für die Großmutter der Beispielfamilie bietet das System gesundheitsrelevante Vorteile: es überprüft die Vitalfunktionen sowie den Gesundheitszustand und warnt, sobald eine Gefährdung (z.B. ein Sturz) erkannt wird. Bei Eintritt einer Gefahr benachrichtigt das System die jeweiligen Kontakte anhand des von der Familie erstellten Notfallplanes und liefert Informationen zum Zustand.

Eine zwingende Voraussetzung für die Umsetzung dieses oder ähnlicher Szenarien ist

- die Gewährleistung mobiler Sicherheit (weitreichende Steuerungsmöglichkeiten)
- die Absicherung von Heimautomatisierungssystemen (welche wahrscheinlich über eine lange Zeit nicht verändert werden und wichtige Bereiche des Lebens regeln)
- die Gewährleistung der Privatsphäre
- die Balance zwischen Sicherheit und BenutzerInnenfreundlichkeit
- die Zuverlässigkeit von Überwachungsdiensten zur Überwachung lebenswichtiger Funktionen
- Die Sicherheit und Zuverlässigkeit von Robotern

Beispiel Made in Austria

In Österreich beschäftigt sich zum Beispiel die Active & Assisted Living Testregion in Österreich (West-AAL[282]) mit Wohnen der Zukunft. Im Rahmen des Projektvorhabens „West-AAL“ werden in über 70 Testhaushalten in Tirol und Vorarlberg, IKT-gestütztes Leben und Wohnen durch Active & Assisted Living Lösungen (AAL-Lösungen) über einen längeren Zeitraum aktiv getestet. Im Fokus stehen dabei nutzenorientierte, innovative Smart Home und Smart Service Lösungen, welche auf neuesten Informationstechnologien aufbauen und im betreuten und betreubaren Wohnen sowie im allgemein häuslichen Umfeld im Sinne der BewohnerInnen und BetreiberInnen eingesetzt werden.

6.1.2 Herausforderungen

Herausforderung aus rechtlicher Sicht

Der Einsatz von Technologie im Wohnraum berührt grundsätzlich die Privatsphäre. Intelligentes Wohnen sollte daher auch bedeuten, möglichen Risiken für die grundrechtlich geschützte Privatsphäre der betroffenen Menschen schon in der Konzeption der Systeme zu begegnen („Privacy by Design“). Beim Thema „intelligentes Wohnen“ spielt Recht vor allem dann eine Rolle, wenn es um sicherheitsrelevante Komponenten geht (z.B. im Bereich „Active & Assisted Living“). Ein rechtlich fokussiertes Risk-Assessment soll auch hier früh zur Optimierung von Lösungen führen. Rechtliche Anforderungen und mögliche Haftungsrisiken sollen schon im frühesten Stadium eines Projekts berücksichtigt werden und so Vertrauen in die Lösung schaffen. Der Zugang soll dabei auch vermitteln, dass beim Einsatz von Technologie nach wie vor der Mensch und seine rechtlich geschützten Sphären im Mittelpunkt stehen. Die Würde des Menschen und der Grundsatz der Verhältnismäßigkeit sollen Grundpfeiler der Lösung zum „intelligenten Wohnen“ sein. Ausgangspunkt rechtlicher Überlegungen sind die Grund- und Menschenrechte durch deren internationale und universelle Gültigkeit schon der Konzeption nach „exportfähige“ Lösungen entwickelt werden sollen. Die feineren Ebenen des jeweils relevanten nationalen Rechts können und sollen auf Basis einer schon dem Grunde nach rechtskonform gestalteten Lösung bearbeitet werden.

6.1.3 Innovationspotential für Österreich

Schnittstellen für Smart Homes

Von zentraler Bedeutung für die Sicherheit und Zuverlässigkeit in Heimsystemen sind die jeweiligen Schnittstellen. Derzeit existiert eine hohe Anzahl an proprietärer Standards wie etwa durch Apples HomeKit oder Googles Nest. All jene Systeme sind nur wenig kompatibel

[282] West-AAL Webseite.

zueinander. Somit stellt sich gleich zu Beginn die Frage nach der jeweiligen Interoperabilität in diesem Umfeld.

Von wichtiger Bedeutung ist ebenso die Fragestellung der Sicherheit von Schnittstellen. Hierbei entsteht eine potenziell hohe Bedrohung der Sicherheit des Eigentums. Schaffen es HackerInnen, in das System einzudringen, so können sie enorm tiefe Einblicke in das Privatleben erreichen und gleichzeitig auch die Sicherheit der Personen im Haushalt gefährden. Smart Homes benötigen daher eine umfangreiche Forschung und Entwicklung im Sicherheitsbereich. Stellt ein Unternehmen sichere Systeme her, so kann dies ein bedeutender Wettbewerbsvorteil sein und sich das Unternehmen damit im internationalen Umfeld etablieren.

Eine weitere zentrale Fragestellung ist die Wartung solcher Systeme. Oftmals handelt es sich um sehr einfache, kleine Geräte, welche jedoch in großer Anzahl im Haushalt vorkommen. Daher ist die Auslieferung von Updates eine zentrale Herausforderung, bedenkt man die Tatsache, dass es bereits mit einfacheren Systemen wie etwa Smartphones schon nicht ausreichend funktioniert.

Empfehlung:

Der Bereich der Heimautomatisierung ist ohne jeden Zweifel ein wesentlicher Wachstumsmarkt für künftige IKT-Lösungen, jedoch wird er neben anderen Themen wie Industrie 4.0 und selbstfahrenden Autos noch nicht so stark beachtet. Dies bietet vor allem für einen kleinen Markt wesentliche Wachstumspotenziale, sich international in eine derzeit noch vorhandene Nische zu setzen. Alleine der Bereich der Sicherheit solcher Systeme kann bereits ein wesentlicher Wettbewerbsvorteil sein, da es vor allem um Systeme geht, welche die Privatsphäre direkt betreffen. Das Projektteam empfiehlt, gezielt diesen Bereich zu fördern und somit nachhaltiges Wachstum in einem noch sehr jungen Segment zu generieren.

Heimsicherheitssysteme

Ein Heimsystem kann auch um wesentliche Aspekte für Heimsicherheit ergänzt werden. Hierbei ist ein „intelligentes Sicherheitssystem“ notwendig.

- Das System kann zwischen HausbewohnerInnen und Fremden unterscheiden. Ebenso erkennt das System, ob ein Haustier im Haus ist.
- Kommt eine fremde Person, so kann man dem System beibringen, dass es sich hierbei um einen Gast handelt. Dieser soll klarerweise nicht überall überwacht werden und das System soll darauf reagieren können.

- Wichtig ist, dass das System keine personenbezogenen Daten weiterleitet. So kann das System gegebenenfalls erkennen, dass eine Person öfter auf die Toilette geht und könnte daraus verschiedenes ableiten.
- Ein zentraler Aspekt ist, einen hohen Grad an Sicherheit durch ein intelligentes Sicherheitssystem herzustellen, welches jedoch gleichzeitig die Privatsphäre schützt.

Empfehlung:

Ein intelligentes Sicherheitssystem hat das Potenzial für österreichische Unternehmen, eine internationale Spitzenposition zu erreichen, wenn diese das Vertrauen der jeweiligen BenutzerInnen gewinnen. Bei intelligenten Sicherheitssystemen handelt es sich um ein Nischenprodukt für IT-Security in einem modernen Umfeld, welches ein hohes Wachstumspotenzial aufweist.

Dienstleistungsbranche für Home Security

Durch eine gezielte Ausrichtung von Unternehmen auf Security im Smart Home Bereich kann eine Dienstleistungsbranche in Österreich entstehen. Diese Branche kann, wenn Sie frühzeitig entsteht, für internationale Wettbewerbsfähigkeit sorgen. Einige Unternehmen haben bereits dargelegt, wie sie international wettbewerbsfähig sind und eine zumindest europäische Marktführerschaft erreichen können.

6.2 Energie der Zukunft

6.2.1 Szenario

Energie begleitet uns täglich und unser Bedarf steigt stetig. In einem Haushalt wird zu bestimmten Zeiten viel Energie gleichzeitig benötigt, z.B. am Morgen nach dem Aufstehen für diverse Elektrogeräte, oder am Abend, nach einem Arbeitstag zum Aufladen des Elektrofahrzeugs. Während des Tages, wenn die BewohnerInnen in der Arbeit sind, verbraucht der Haushalt weniger Strom. Das Hausdach ist mit Solaranlagen ausgestattet. Der durch Photovoltaik produzierte Strom, der im Überschuss vorhanden ist, wird in das Stromnetz eingeführt und kann somit anderorts, wo er gerade gebraucht wird, genutzt werden. Energiesysteme werden sich in den nächsten Jahren sehr stark verändern. Vor allem durch den Wechsel hin zu erneuerbaren Energiequellen und der dadurch stärkeren Dezentralisierung der Energienetze entstehen neue Herausforderungen. Die zukünftige Energieversorgung wird stärker von einzelnen geleistet werden, wodurch intelligente Systeme notwendig sind. Smart Grids sind intelligente Energienetze, die alle Akteure des Energiesystems über ein Kommunikationsnetzwerk miteinander verbinden. Sie ermöglichen

es, auf Basis der Kommunikationstechnologien ein energie- und kosteneffizientes Gleichgewicht zwischen einer Vielzahl von Stromverbrauchern, Stromerzeugern und in Zukunft auch verstärkt Stromspeichern herzustellen. Dieses Gleichgewicht wird durch optimiertes Management von Energieerzeugung, Energiespeicherung, Energieverbrauch und dem Stromnetz selbst erreicht.

Beispiel Made in Austria

Verschiedene Pionier- und Modellregionen in Österreich sind dabei smarte Netzwerke zur Energieversorgung zu implementieren und zu testen[283]. Unter anderem untersucht die Forschungsgesellschaft Aspern Smart City Research im Norden von Wien das gesamte System: Gebäude, Stromnetz, Kommunikations- und Informationstechnologie sowie das Nutzungsverhalten fließen zusammen in ein großes Energieforschungsprogramm[284].

6.2.2 Herausforderungen

Eine durchgängige Kommunikationsfähigkeit vom Kraftwerk bis hin zu den VerbraucherInnen ist notwendig, um eine nachhaltige, wirtschaftliche und sichere Elektrizitätsversorgung zu gewährleisten. Einzeltechnologien für Smart Grids existieren bereits in Österreich beim Management von Stromübertragungsnetzen und bei der ferngelenkten Steuerung von großen Kraftwerken. Es gilt nun, diese Konzepte ins Stromverteilernetz einzubringen, um neue Elemente zu ergänzen und diese einzeln systematisch zu kombinieren. Dabei existieren große technische, organisatorische, wirtschaftliche und nicht zuletzt rechtliche Herausforderungen. Smart Grids – Technologien und Konzepte werden für den Einsatz in intelligenten Stromnetzen in Zukunft national und international stark an wirtschaftlicher Bedeutung gewinnen. Die Europäische Technologieplattform (ETP) Smart Grids schätzt, dass bis 2030 Investitionen in der Höhe von € 390 Mrd. in Europa, davon € 90 Mrd. in Stromübertragung und € 300 Mrd. in die Stromverteilung für die Erneuerung und Erweiterung der elektrischen Stromversorgungsinfrastruktur hin zu intelligenten Stromnetzen notwendig werden.

Herausforderung aus rechtlicher Sicht

Ein intelligentes Netz zur Elektrizitäts-Energieversorgung ist aus gesellschaftlicher und rechtlicher Sicht zweifellos eine insgesamt anzustrebende Entwicklung, zumal damit höhere Energieeffizienz und Versorgungssicherheit, eine Schonung der Umwelt und geringere

[283] Energiesysteme der Zukunft Webseite.
[284] Aspern Smart City Research Webseite.

Kosten für VerbraucherInnen verbunden sein sollen. Dennoch wird die Entwicklung in der Gesellschaft durchaus kritisch gesehen[285], aus rechtlicher Sicht betrifft die Kritik im Wesentlichen zwei Ebenen:

Erstens wird damit ein Risiko für Privatsphäre und Datenschutz gesehen. Mithilfe intelligenter Stromzähler (Smart Meters) können bei entsprechend kurzem Takt der Messungen[286] aus dem solcherart exakt erhobenen Verbrauch detaillierte Rückschlüsse auf die Lebensgewohnheiten der Menschen gezogen werden, wenn die Messung sich jeweils auf einzelne Wohneinheiten (Wohnung, Einfamilienhaus) bezieht. Würde etwa eine sekundengenaue Messung erfolgen, wäre aus den Zählerdaten ableitbar, ob jemand mit der Mikrowelle kocht, wann die Dusche benutzt wird (weil z.B. eine Heiztherme elektrisch gezündet wird) und zu welchen Zeiten Computer und Fernseher benutzt werden. In Verbindung mit Big Data ließe sich theoretisch aus diesen Daten einiges für die Erstellung eines Persönlichkeits- oder Familienprofils ableiten. In dieser Hinsicht wird entsprechende Kritik von Datenschutzorganisationen formuliert. Diese Kritik sollte aus datenschutzrechtlicher Sicht ernst genommen und ihr mit entsprechenden Schritten begegnet werden, das Schlagwort hierzu lautet einmal mehr „Privacy by Design“. Smart Meter und Smart Grids lassen sich durchaus datenschutzfreundlich umsetzen, allerdings bedarf es dazu systemimmanenter Sicherungsmechanismen und Grenzen. Um diese zu finden, bedarf es entsprechender interdisziplinärer Forschung.

Zweitens bestehen Bedenken, dass durch die IKT-Vernetzung der Energieversorgungssysteme zusätzliche Angriffsflächen für HackerInnen (im negativen Sinn des Begriffes) geschaffen werden. Das Risiko besteht darin, dass durch ferngesteuerte Angriffe via Internet die Versorgung gefährdet sein könnte, damit also kritische Infrastruktur gefährdet ist. Dies ist ebenso ernst zu nehmen, dementsprechend müssen in diesem Bereich die höchsten Anforderungen an die IKT-Sicherheitskonzepte gestellt werden. Aufgrund der Durchdringung verschiedener Technologien und damit der möglichen Kooperation verschiedener Infrastruktur-Anbietern (konkret zwischen Energieanbietern und IKT-Infrastruktur-Anbietern, soweit die Energieversorger nicht über eigene Datennetze verfügen) sind auch Haftungsfragen zu klären, die schon in der Konzeption von Systemen zu berücksichtigen sind, weil alle Beteiligten nur für jene Teile haften sollen, über die sie tatsächlich die Kontrolle haben.

[285] Siehe z.B. Zirm, 2014.

[286] Vgl. § 83 Abs. 3 Elektrizitätswirtschafts- und –organisationsgesetz 2010 (ElWOG) idF BGBl. I Nr. 174/2013, der Messungen im Takt von 15 Minuten vorsieht.

6.2.3 Innovationspotential für Österreich

Mit Smart Grids eröffnet sich somit international ein relevantes Technologiefeld, das aufgrund des bereits bestehenden Know-hows der österreichischen Energie- und Kommunikationsindustrie die Möglichkeit bietet, sich in diesem Markt frühzeitig zu etablieren und zu positionieren. Für die Forschung, Entwicklung und Realisierung der Smart Grids-Technologien bestehen in Österreich die besten Voraussetzungen, denn Österreich verfügt über eine Industrie mit hohem technologischen Know-how, anerkannten Produkten und Innovationen, aktive und einander ergänzende F&E Institutionen, innovative Stromnetzbetreiber und Energieversorger und ein unterstützendes F&E Umfeld. Bei rechtzeitiger Entwicklung der Smart Grids Technologien in Österreich ergibt sich für diverse Hersteller der „Enabling Technologies" wie zum Beispiel Leistungselektronik, Kommunikationstechnik, elektrotechnische Komponenten wie etwa Schutztechnik, die Chance, sich am stark wachsenden internationalen „Smart Grids Markt" zu positionieren und damit hochqualifizierte F&E und Produktionsarbeitsplätze zu schaffen. Zusätzlich kann eine signifikante Steigerung der Integrationsdichte von dezentralen Stromerzeugungsanlagen durch Smart Grids Regionen ermöglichen, existierende Primärenergieressourcen verstärkt zu nutzen. In der Marktüberleitung ist aber eine gemeinsame Kooperation von Industrie, Unternehmen der Energiewirtschaft und Forschungseinrichtungen, mit Unterstützung durch entsprechende nationale Rahmenbedingungen, eine unverzichtbare und entscheidende Voraussetzung. [287]

6.3 Produktion der Zukunft

6.3.1 Szenario

Ein/e BenutzerIn bestellt mit seinem/ihrem Smartphone ein hoch individualisiertes Produkt (spezielles Autoteil), welches aufgrund neuer Produktionsverfahren (Smart Factory) zum Massenproduktionspreis erzeugt werden kann. Die Bezahlung erfolgt über eine neuartige Bezahlplattform in Internet. Durch die Bestellung wird ein Smart Product angelegt, welches seine Produktionsparameter (Standorte an denen es produziert werden kann, benötigte Ressourcen, Konfiguration, etc.) kennt und über eine eindeutige Kennung jederzeit über eine Cloud-Anwendung verfolgt werden kann. Durch die ständige Kommunikation mit einem mobilen Cloud-Service, weiß das Smart Product über die Auslastungen und Möglichkeiten der Fabriken und kann so bestimmen, wo der nächste Verarbeitungsschritt stattfinden soll. Mittels autonom fahrender Kraftfahrzeuge wird das Produkt in die erste Fabrik gebracht, um die

[287] Smart Grids Austria Webseite.

ersten Verarbeitungsschritte zu beginnen. Nach der Erstellung des Produkts wird es mit Hilfe von Smart Logistiklösungen zum Kunden geliefert.

Beispiel Made in Austria

Kürzlich wurde die erste Industrie 4.0 Pilotfabrik in Österreich eröffnet. Hier sollen sich WissenschaftlerInnen und Unternehmen an die Industrie 4.0 annähern. Nach der Automatisierung der Produktionsanlagen werden diese nun über das Internet vernetzt und damit zu smarten Maschinen aufgewertet. Das hat enorme Auswirkungen auf den gesamten Produktionsprozess: angefangen bei der stärkeren Kooperation mit ZuliefererInnen und PartnerInnen über die Anzahl und Art der MitarbeiterInnen, bei den verwendeten Maschinen bis hin zu neuen Produkten und Geschäftsmodellen, die durch die Vernetzung erst entstehen. Die Modell- und Forschungsfabrik soll Unternehmen die Möglichkeit geben, neue Arten der Produktion gemeinsam mit WissenschaftlerInnen zu erforschen, zu testen und weiterzuentwickeln. Rund 20 Unternehmen sind aktuell bereits an der Pilotfabrik beteiligt.[288]

6.3.2 Herausforderungen

Aufgrund des Themas ergeben sich vor allem Herausforderungen und Fragestellungen im Bereich der mobilen Sicherheit. Damit Bestellungen und Zahlung sicher sind, muss die Sicherheit des mobilen Endgeräts sowie des Cloud/Webservices gegeben sein. Im Bereich 3D-Printing muss gewährleistet werden, dass die Anbieter des 3D-Drucks kein urheberrechtlich geschütztes Material drucken. Im Bereich Automotive Security ermöglicht die stärkere Vernetzung von Fahrzeugen mit der Verkehrsinfrastruktur beziehungsweise mit anderen Fahrzeugen die Wahl von optimalen Routen und kann Unfälle vorbeugen. Ist die sichere Kommunikation innerhalb eines Fahrzeugs bzw. zu externen Objekten nicht gewährleistet, kann dies folgenschwere Konsequenzen haben. Zur Automatisierung werden industrielle Kontrollsysteme (z.B. SCADA) benötigt. Da diese Systeme oftmals sehr lange in Verwendung sind, jedoch aus Effizienzgründen zunehmend mit dem Unternehmensnetzwerk verbunden werden, bestehen besondere Schutzanforderungen (Schutz von Legacy Komponenten, individuelle Zusammenstellungen, etc.). Um Bestellungen entgegenzunehmen und Informationen über die Industrieanalage (wie beispielsweise Auslastung, Fähigkeiten) zur Verfügung zu stellen, ist ein funktionierendes Unternehmensnetzwerk notwendig. Da alle Unternehmen zunehmend von ihrer IT abhängig sind und alle Firmen interne und sensible Daten meist in elektronischer Form ablegen, spielt der Schutz des Unternehmensnetzwerks

[288] Drucker, 2015a.

und aller sich darin befindlichen Systeme eine wichtige Rolle. Aufgrund der zunehmenden Professionalität von AngreiferInnen und der Individualisierung der Angriffsvektoren, ist es von großer Bedeutung, dynamische Verfahren zur Erkennung von Attacken einzusetzen (Stichwort: intelligence driven security, behavior based malware detection, etc.). Neben den technischen Herausforderungen Informationssicherheitssysteme zu schützen, wirkt sich die zunehmende Dynamisierung von Produktionsprozessen und deren Wertschöpfungskette auch auf organisatorische Prozesse wie Geschäftsprozesssicherheit, Governance, Compliance, Risikomanagement oder Kontinuitätsmanagement aus. Rechtliche Herausforderungen betreffen hauptsächlich Privacy, Produktsicherheitsstandards und Haftungsfragen wie zum Beispiel: Wer ist verantwortlich, wenn am Ende etwas nicht so funktioniert, wie es sollte? Eine weitere Herausforderung betrifft die Zuverlässigkeit: Wie kann sichergestellt werden, dass die jeweiligen Komponenten ideal miteinander zusammenspielen? Welche aktuellen und zukünftigen Standards und Normen hinsichtlich Schnittstellen müssen wie berücksichtigt werden?

Herausforderung aus rechtlicher Sicht

Die „intelligente Fabrik“ als Produktions- und Arbeitsstätte der (näheren) Zukunft ist geprägt durch einen hohen Grad der Vernetzung ihrer Komponenten in Verbindung mit künstlicher Intelligenz zur Optimierung aller vertikalen und horizontalen Produktionsprozesse. Sowohl Maschinen als auch Produkte bzw. deren Bestandteile sollen über Datennetzwerke, z.B. auch das Internet, selbständig miteinander kommunizieren. Logistische Prozesse sollen durch Automatisierung und Integration interner und externer PartnerInnen unmittelbar mit der Produktion verzahnt sein und dadurch den Aufwand so gering wie möglich halten. Cyber-Physical-Systems mit intelligenten Maschinen, Lagersystemen und Betriebsmitteln, die eigenständig Informationen austauschen, Aktionen auslösen und sich gegenseitig selbstständig steuern, sollen zeitkritisch eine flexible und energiesparende Produktion gewährleisten[289] (siehe Kapitel 4.7). Moderne Sensortechnologie und Vernetzung sollen auch in den Bauwerken eines Produktionsbetriebes durch künstliche Intelligenz ideale Umwelt- und Produktionsbedingungen bei möglichst kleinem Energieaufwand schaffen.

Diese Beschreibung ist keine ferne Zukunftsvision mehr. Die Basistechnologien zur Umsetzung stehen bereits zur Verfügung, hier ist vor allem die Entwicklung zum Internet der Dinge zu nennen (vgl. Kapitel 4.8). Künstliche Intelligenz und Ontologie im Internet erfreuen sich unter dem Schlagwort „semantic web“ einer stetigen Entwicklung. Nichts desto weniger erscheint das Konzept revolutionär. Nach der Mechanisierung, der Elektrifizierung und der

[289] Mehr Details bieten die Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0, Abschlussbericht (Deutsches Bundesministerium für Bildung und Forschung, 2013, 18).

Digitalisierung der Industrie ist die Vernetzung im Rahmen intelligenter automatisierter Systeme der nächste Schritt[290], der die industrielle Produktion nachhaltig verändern wird. Daher wird jedenfalls in Fachkreisen regelmäßig von der vierten industriellen Revolution gesprochen, woraus sich der – seit 2012 in Deutschland öffentlich geprägte[291] – Terminus „Industrie 4.0“ ableitet. Mit zwei bis drei Jahren Verzögerung im Vergleich zum großen nördlichen Nachbarn Deutschland[292] hat nun auch in Österreich die Politik das enorme wirtschaftliche Potenzial dieser Entwicklung erkannt und kürzlich die Pläne der Bundesregierung zur Förderung heimischer Forschungseinrichtungen und Unternehmen bei der Umstellung auf Industrie 4.0 im Ausmaß von 250 Millionen Euro in den nächsten zwei Jahren[293] vorgestellt.

Haftung und Risikoverteilung – gesetzliche und vertragliche Rechtsbeziehungen

Relevante Haftungsfragen stellen sich einerseits im Hinblick auf zwingende Rechtsvorschriften, beispielsweise im Datenschutz- oder Arbeitsrecht, andererseits im Bereich der privatautonomen Gestaltung der Vertragsbeziehungen mit KundInnen, ZulieferInnen oder DienstleisterInnen. Beide Ebenen sind für einen Industriebetrieb nicht neu und führen in aller Regel zu Strukturen, die über längere Zeit wachsen und auch die Unternehmenskultur reflektieren. Wenn nun ein Industriebetrieb den Weg beschreitet, seine Systeme in Richtung Industrie 4.0 aufzurüsten, entstehen neue Sachverhalte, die rechtlich zu erfassen sind.[294] Mögen die Rechtsfragen dabei auch weitgehend nicht völlig neu sein, so ist die deutlich gesteigerte Komplexität doch auch eine rechtliche Herausforderung.[295] Gleichzeitig ist die objektive Rechtslage (Gesetze, Verordnungen, Rechtsprechung, Verwaltungspraxis) nicht im selben Maß entwickelt wie die Technologie. Im Hinblick auf neuartige Fragen kann daher Rechtsunsicherheit bestehen, die ein Unternehmen möglichst schon im Zuge der Investitionsentscheidung erfassen, einschätzen und berücksichtigen sollte.

Zwei relevante Haftungsebenen sind grundlegend zu unterscheiden: Einerseits die Haftung für spezifische Risiken, die von einer Industrieanlage ausgehen, andererseits die Haftung für die entstandenen Produkte, die ihren Weg in den Markt finden, wobei hier auch die Problematik von Lieferausfällen miterfasst ist. In einer intelligenten Produktionsanlage werden nun zusätzliche Beteiligte und Dienste der Informations- und Kommunikationstechnologie in Prozesse eingebunden. Dadurch können neue Risikoszenarien entstehen oder bekannte

[290] Siehe Fraunhofer Austria Webseite.
[291] Vgl. Deutsche Bundesregierung, 2012, S. 52 ff.
[292] Zur Kritik an Österreich siehe z.B. Factory, 2014.
[293] Siehe Felser, 2014.
[294] Anschaulich dazu die konkreten Beispiele bei Loskyll, 2013, S. 2f.
[295] Vgl. ACATECH, 2013, S. 62.

Szenarien für den Industriebetrieb selbst weniger beherrschbar werden. Sofern diese auf der technologischen Ebene nicht vollständig vermeidbar sind – und das ist nur selten der Fall – können die verbleibenden Restrisiken durch entsprechende Vertragsgestaltung in einem überschaubaren Rahmen gehalten werden. Häufig ist die Rechtsgestaltung, z.B. durch Service Level Agreements (SLA) oder Versicherungsverträge, eng mit wirtschaftlichen Fragen verbunden. Gerade im Zusammenhang mit einer in Europa typischen verschuldensunabhängigen Produkthaftung kann die eindeutige und detaillierte Regelung von Regressansprüchen gegenüber ZuliefererInnen und DienstleisterInnen ein wesentlicher Kostenfaktor sein. Zur Veranschaulichung stelle man sich etwa ein Szenario vor, bei dem an einer bestimmten Stelle im Produktionsprozess eine Authentifizierung durch digitale Signatur erforderlich ist. Wenn die Signatursoftware, der Kartenleser und die Signaturkarte[296] von jeweils verschiedenen HerstellerInnen stammt, möglicherweise noch ein/eine außenstehende/r ZertifizierungsdienstanbieterIn (ZDA) involviert ist, entsteht bei Produktionsausfällen aufgrund einer Störung des Signaturprozesses mitunter ein Haftungsstreit zwischen fünf beteiligten Unternehmen (jeweils ein/e eigene/r AnbieterIn für Software, Kartenleser und Signaturkarte sowie ein ZDA und der Industriebetrieb selbst).

Risikoerhebung und Risikomanagement

Jedes faktische Risiko hat in der Regel eine rechtliche Dimension, weil am Ende zumeist die Frage der Haftung bzw. Gefahrtragung zu klären ist. Umgekehrt wird ein Szenario abstrakt oft überhaupt nur dann als Risiko eingestuft, wenn daran bestimmte Rechtsfolgen geknüpft sind. Im Bereich Datenschutz ist dies besonders häufig der Fall, weil der Schaden einer missbräuchlichen Datenverwendung meistens abstrakt ist und schon die Verletzung der Zweckbindung eine Haftung auslöst.[297] Das konkrete Risiko bestimmt sich in solchen Fällen durch die konkrete Strafdrohung und die Wahrscheinlichkeit, erwischt zu werden. Die Komplexität eines intelligenten Produktionssystems potenziert dieses Phänomen. Es ist daher empfehlenswert, nicht nur deren Funktionalität sondern auch die Risiken insbesondere auch aus rechtlicher Sicht zu modellieren und so schon in frühen Projektphasen die (notwendigerweise interdisziplinäre) Risikoabschätzung vor den wesentlichen Investitionsentscheidungen durchzuführen. Abhängig vom Ergebnis kann nämlich so noch rechtzeitig entschieden werden, bestimmte Risiken schon durch die einzusetzende

[296] Oder auch andere Technologien mit noch komplexeren Strukturen, z.B. via Smartphone über NFC.

[297] In ca. 3 bis 4 Jahren werden in der EU drastische Verwaltungsstrafen gegen Datenschutzverletzungen drohen. Artikel 79 des Entwurfes der EU-Kommission für eine neue „Datenschutz-Grundverordnung“ vom 25.1.2012 sieht Strafen bis zu 1 Mio. Euro oder alternativ bis zu 2% des weltweiten Jahresumsatzes vor. Diese Obergrenze wurde in den Vorschlägen des EU Parlaments noch auf 3 Mio. Euro bzw. 5% angehoben. Die Datenschutz-Grundverordnung wird dabei ohne Umsetzungsakt in allen Mitgliedstaaten unmittelbar gelten.

Technologie möglichst weitgehend zu eliminieren. „Security-/Safety-/Privacy by Design“ sind hierfür die Schlagworte.

Informationssicherheit und Datenschutz

Wesentliche Erfolgsfaktoren in den intelligenten Produktionssystemen sind die Betriebs- und Angriffssicherheit. Es geht nicht nur darum, die Gefahren für Menschen und Umgebung zu beherrschen, die von Produktionsanlagen und Produkten ausgehen. Auch die Anlagen und Produkte selbst müssen vor Missbrauch und unbefugtem Zugriff geschützt werden – insbesondere die darin enthaltenen Daten und Informationen. Integrierte Sicherheitsarchitekturen, eindeutige Identitätsnachweise und nicht zuletzt MitarbeiterInnenschulungen werden dazu unabdingbar sein.[298] Die Herausforderung liegt dabei auch in der Mittel-Zweck-Relation, weil abstrakt schwer zu beurteilen ist, welcher konkrete Sorgfaltsmaßstab hinreichend ist, um möglichen Haftungen zu entgehen. Hier ist auf die Ausführungen oben zu Informationssicherheitsrecht und Zertifizierungen zu verweisen.

Arbeitsrecht und ArbeitnehmerInnendatenschutz

Neue rechtliche Fragestellungen bringt Industrie 4.0 insbesondere in der Beziehung zwischen Unternehmen und Belegschaft mit sich. Obgleich die Auswirkungen von Industrie 4.0 für die Arbeitswelt durchwegs positiv beschrieben werden[299], entstehen doch auch spezifische Risiken. Wenn nämlich die „intelligente Fabrik“ jeden Produktionsabschnitt beliebig genau kontrollieren und steuern kann, besteht die Gefahr, dass die Überwachung auch die MitarbeiterInnen erfasst, möglicherweise lediglich als nicht intendiertes „Nebenprodukt“. Hier ist auf Kapitel 3.1.10 zur arbeitsrechtlichen Dimension des Datenschutzes zu verweisen.

Das Recht soll keinesfalls zur „Innovationsbremse“ für Industrie 4.0 werden. Vielmehr geht es darum, die rechtliche Ebene möglichst früh im Rahmen einer Investitionsstrategie einzubeziehen, insbesondere bereits im Rahmen einer Risiko- bzw. Folgeabschätzung. Im Idealfall können auf diese Weise schon die technologischen Lösungen so gestaltet werden, dass bestimmte Risiken von vornherein vermieden oder minimiert werden.

[298] Vgl. ACATECH, 2013, S., 6.

[299] Siehe die Argumente bei Spath et al., S. 52ff.

Empfehlung:

Die FFG möge Projekte fördern, deren Ziel die Entwicklung praxisorientierter Leitfäden, Checklisten und Mustervertragsklauseln für intelligente Produktionssysteme („Industrie 4.0“) ist. Insbesondere Kooperationen aus Forschung und Industrie sind geeignet, allgemeine Vorarbeit für die gesamte Branche zu leisten, die vor allem für KMUs ohne eigene Rechtsabteilung eine große Hilfestellung beim Vollzug der für Österreich zukunftssichernden vierten industriellen Revolution bedeuten könnte.

6.4 Verkehr der Zukunft

Fahrzeuge werden immer stärker autonom. Derzeit verwenden viele Autos Fahrunterstützungssysteme, doch die Entwicklung geht in Richtung eines autonomen Betriebes. In einigen Jahren wird es somit möglich sein, dass Autos gänzlich unabhängig und großflächig von unmittelbaren menschlichen Einflüssen fahren können.

6.4.1 Szenario

Eine Geschäftsreisende kommt nach einer mehrtägigen Reise in Nordeuropa am Flughafen Wien an. Dort besteigt sie kein Taxi, sondern wird vom eigenen Auto, welches einen Zugriff auf den Terminkalender hat, abgeholt. Da die Geschäftsreisende sehr lange unterwegs war, ist sie erschöpft und froh, nicht selber mit dem Auto fahren zu müssen. Sie lässt sich folglich vom Auto nach Hause fahren. Das autonome Auto kommuniziert während der Fahrt mit anderen autonomen Autos. Dies ist notwendig, damit die Fahrzeuge sich miteinander abstimmen können. Hierbei werden an Autos in der Nähe gewisse Fahrmanöver wie der Spurwechsel, die Erhöhung oder Verringerung der Geschwindigkeit und weitere wichtige Elemente gemessen. Das autonom fahrende Auto meldet die jeweiligen Daten über seinen Bestimmungsort an ein zentrales System. Dieses System dient dem Auto wiederum zur besseren Planung der Route. Damit können Staus verhindert werden, bevor diese entstehen. Merkt das System beispielsweise, dass die Auslastung an gewissen Straßen höher sein wird, so können einzelne Autos umgeleitet werden. Hierbei handelt es sich um voraussehende Algorithmen, die nicht im Hinblick auf existierende Staus arbeiten, sondern auf potenziell entstehende. Herkömmliche Taxiunternehmen haben aufgrund dieser Entwicklungen starke Einbußen. Es gibt mehrere IT-Unternehmen, welche einen Taxi-ähnlichen Service oder Carsharing-Modelle, bei denen mehrere Personen ein Fahrzeug gemeinsam nutzen, anbieten. Diese können einfach mittels eines Smartphones oder anderweitigen Geräten bestellt werden.

Beispiel Made in Austria

Österreich bekommt ab 2016 erste Teststrecken für selbstfahrende Autos. Autonome Fahrzeuge sollen etwa neue Straßenstücke vor deren Eröffnung sowie Teilabschnitte bereits erbauter Straßen nutzen können. ExpertInnen rechnen damit, dass selbstfahrende Autos in 15 bis 20 Jahren zur Marktreife gelangen. In Österreich sind Firmen der Autoindustrie aktiv an der Forschung beteiligt.[300]

6.4.2 Herausforderungen

Herausforderung aus rechtlicher Sicht

Eine Überwachung und intelligente Steuerung des Verkehrs ist ein gesellschaftlich sehr bedeutsames Ziel. Dies gilt sowohl für den Individualverkehr, als auch für BenutzerInnenströme öffentlicher Verkehrsmittel. Ebenso in den autonomen Fahrzeugen selbst werden eine Vielzahl von Sensoren Daten erheben, von denen viele einen Personenbezug aufweisen. Dies bedeutet einen Eingriff in die Privatsphäre der NutzerInnen, wie das vergleichsweise einfache Beispiel der Section Control gezeigt hat. Es ist daher genau zu prüfen, welche dieser Daten tatsächlich von wem benötigt werden (Datenminimierung, Separation of Concerns, Need-to-Know-Principle) und welche davon gespeichert werden müssen und nicht gleich nach Treffen der jeweiligen Steuerungsentscheidung wieder verworfen werden können. Ethische und gesamtgesellschaftliche Aspekte eines effizienteren aber zugleich stärker überwachten und gelenkten Verkehrs sind ebenfalls zu beachten.

Betreffend autonome Fahrzeuge sind insbesondere auch Haftungsfragen zu berücksichtigen. Wie bereits oben in Bezug auf Robotik ausgeführt, ergeben sich bei autonomen Fahrzeugen besondere Haftungsfragen, da nicht mehr der/die FahrerIn/HalterIn/EigentümerIn das Fahrzeug kontrolliert, sondern das Fahrzeug der Programmierung durch den Hersteller entsprechend agiert. Die Hersteller sind diesbezüglich in die Pflicht zu nehmen, was auch proaktiv dazu führen sollte, dass diese der Sicherheit (Safety und Security) ihrer Systeme in der Entwicklungsphase eine noch größere Bedeutung beimessen.

Neben dem Bedarf an solchen Haftungsregelungen ergibt sich aus Smart Mobility im Hinblick auf den Straßenverkehr der Zukunft ganz generell ein Bedarf für neue Verkehrsregeln. Dabei ist auch die internationale Koordination besonders zu beachten, die bei Verkehrsregeln üblich und sehr bedeutsam ist.

[300] Sulzbacher, 2015.

6.4.3 Innovationspotenziale für Österreich

In Österreich gibt es vor allem im Großraum Graz eine sehr vitale Automobilindustrie mit den Unternehmen AVL List und Magna, die ihr Innovationspotenzial entfalten können. Besonders im Security-Bereich ergeben sich nicht nur Anforderungen, sondern auch tatsächliches Potenzial für Wachstum bei vorhandenen Unternehmen und auch bei neuen Unternehmen (Start-ups).

Intelligente und Sichere Logistiklösungen

Ein wichtiger Aspekt ist das Thema „Smart Logistics“. Hierbei besteht nicht nur Innovationsbedarf in der jeweiligen Anwendung, sondern auch wesentlicher Bedarf in Bezug auf Sicherheit und Vertrauen eben jener Systeme. Grundlegende Fragen betreffen die allgemeine IT-Sicherheit, die sichere Kommunikation mit den jeweiligen Sensoren, die Absicherung der jeweiligen Schnittstellen und die Ausfallsicherheit der Systeme. Dies ergibt nicht unwesentliche Schnittmengen zu folgenden Themen der IT-Sicherheit:

- **Smart Production:** Sichere Produktionssysteme und die Integration der Kommunikation mit einer Vielzahl an Fahrzeugen, welche selbst wiederum eine hohe Anzahl an interner Sicherheit benötigen.
- **Sichere und zuverlässige Systeme**: Hierbei handelt es sich um die Frage, wie ein Steuerungssystem zuverlässig agiert und sicher ist. Da autonome Fahrzeuge in Produktionssystemen durch Smart Logistics nicht durch ein einfaches Computersystem ermöglicht werden, kommt hier voraussichtlich ein verteiltes System (Cloud) zum Einsatz. Hierbei ist die Sicherheit dieser Systeme aus unterschiedlichsten Perspektiven zu beachten. Wesentlich ist die Tatsache, dass eine zu geringe Sicherheit oder auch ein Ausfall des Systems nicht nur wirtschaftliche Folgen haben kann, sondern es auch zu folgeschweren Verkehrsunfällen kommen kann.
- **Ausfallsicherheit**: Es ist abzuklären, welche Probleme mit der Ausfallsicherheit einhergehen. Hierbei geht es nicht nur um die Frage nach den wirtschaftlichen Folgen, sondern auch nach weiteren Schäden wie im vorherigen Punkt dargestellt.

Empfehlung:

Das Projektteam empfiehlt, den Standort Österreich für intelligente Logistiklösungen fit zu machen. Das Thema IT-Security ist dank der immer stärker werdenden Digitalisierung sehr wichtig. Österreich hat eine starke Automobilindustrie und kann dadurch einen Wettbewerbsvorteil erzielen. Bereits ansässige Unternehmen können sich in deren internationalen Feld wesentlich besser aufstellen, gleichzeitig können neue Unternehmen entstehen, welche das Thema der Sicherheit dieser Lösungen adressieren. Hierbei kann eine USP rund um dieses Thema entstehen.

Personentransport 2.0

Ein Thema, welches vor allem für intelligente Städte (Smart Cities) von Interesse ist, ist der durch Digitalisierung unterstützte Personentransport. Autonome Systeme erlauben eine gänzlich neue Sicht. Personenströme können besser gemessen und damit der Verkehr optimiert werden. Dies führt nicht nur zu einer optimierten Verteilung und damit Stauvermeidung in Ballungszentren, sondern auch zu einem wesentlich effizienteren Umgang mit vorhandenen Ressourcen.

Es ergeben sich jedoch auch einige Probleme im Umgang mit Personentransport 2.0. Ebenso wie bei intelligenten Logistiklösungen kann es zu Problemen mit den jeweiligen Sensoren und deren Sicherheit kommen. Zentrale Herausforderung ist die Fragestellung, wie Sensoren für BenutzerInnen sicher gemacht werden können. Fällt ein Sensor aus oder liefert dieser korrupte Daten, hat dies wesentliche Auswirkungen auf die Zuverlässigkeit. Es kann jedoch auch vorkommen, dass Sensoren nicht aufgrund von Fehlern unzuverlässig werden, sondern dies bewusst herbeigeführt wird. Ein Beispiel ist das unzulässige Eindringen in solche Systeme.

Empfehlung:

Das Projektteam empfiehlt, analog zu Förderungen rund um intelligente Logistiklösungen auch die Erforschung und Entwicklung intelligenter Verkehrssysteme und Personentransport 2.0 zu fördern. So können neue Zulieferer für die Automobilindustrie entstehen beziehungsweise vorhandene Zulieferer einen Wettbewerbsvorteil erzielen. Das Thema Sicherheit spielt hierbei eine zentrale Rolle, da mögliche Probleme nicht nur einen wesentlichen wirtschaftlichen Schaden nach sich ziehen, sondern auch zu erheblichem Personenschaden führen können.

Stadtplanung

Durch die Integration von Sensoren ergeben sich neue Möglichkeiten hinsichtlich einer Wegeanalyse. Diese basieren auf Basis von Daten einzelner Fahrzeuge. Durch datenbezogene Systeme können Vorteile in der Stadtplanung sichergestellt werden. Dies trägt somit wesentlich zu einer intelligenteren Stadt bei. Aus Vertrauenssicht ergeben sich nicht nur Fragen rund um die sichere Kommunikation und Ablage dieser Daten, sondern auch die Frage nach dem Datenschutz.

Sicherheit in Autos

In den vorherigen Beschreibungen wurde bereits das Thema der Sicherheit innerhalb des Autos mehrfach adressiert. Hierbei sind verschiedene Elemente relevant, welche einen Wettbewerbsvorteil erbringen können. Die jeweiligen Themen, welche eine besondere Bedeutung hinsichtlich Sicherheit von autonomen Fahrzeugen genießen sind:

- **Vehicular Networks and Systems**. Hierbei geht es um die IKT-Systeme in Fahrzeugen, welche immer stärker verbaut werden. Es besteht ein nicht unwesentlicher Unterschied zur klassischen Business-IT, da nicht nur ein finanzieller Schaden sondern auch ein Personenschaden entstehen kann. Innovationsthemen entstehen rund um die Verknüpfung der jeweiligen Sensoren im Auto und wie diese sicher und zuverlässig kommunizieren können. Zentrale Ansatzpunkte sind „Vehicle to Infrastructure“, also die Kommunikation des Fahrzeuges mit Verkehrselementen wie der Straße oder Schildern sowie „Vehicle to Vehicle“, welches die Kommunikation mit anderen Fahrzeugen bestimmt.
- **Secure Interfaces**. Eine besondere Bedeutung kommt der Frage nach Schnittstellen in Autos zu. Eine nicht unwesentliche Herausforderung ist die Absicherung dieser Schnittstellen. Probleme sind oftmals, dass Sensoren eine sehr geringe Leistung aufweisen und daher oftmals unverschlüsselt senden und empfangen.
- **Patching**. Je komplexer ein Softwaresystem ist, desto häufiger entstehen auch Fehler. Diese auszubessern stellt in naher Zukunft gewisse Herausforderungen an Automobile dar.
- **BYOD im Auto**. Neue Autos unterstützen die Kommunikation mit Smartphones und anderen intelligenten Geräten über Technologien wie etwa Bluetooth. Es ist aus Sicherheitssicht zu untersuchen, wie die jeweilige Kommunikation sicher gestaltet werden kann.
- **Verbesserung der Zuverlässigkeit des Autos.** Die Zuverlässigkeit des Automobils kann durch predictive maintenance gehoben werden. Hierbei kommen Datenanalysen und Auswertungen von Sensordaten zum Einsatz. Damit ist es den Herstellern

möglich, Muster zu erkennen und die jeweiligen BesitzerInnen des Fahrzeuges über mögliche Ausfälle und Probleme zu informieren.

- **Forensik.** Auswertung von Sensoren bei z.B. Unfällen.
- **Entscheidungsmodelle für selbstfahrende Autos.** Selbstfahrende Autos reagieren selbstständig auf Gefahrensituationen. Besteht die Gefahr eines Unfalles, so kann das Fahrzeug automatisch die beste Lösung wählen. Dies kann beispielsweise ein Fahrspurwechsel sein. Hierbei bestehen jedoch sehr viele Parameter, welche zu beachten sind. Die beste Lösung für das Fahrzeug ist nicht zweifelsfrei die beste Lösung für alle Beteiligten. Die Zuverlässigkeit von solchen Fahrzeugen kann durch intelligente Entscheidungsmodelle verbessert werden.

Leuchtturmprojekt „Autonome Systeme“

Die Zuverlässigkeit von IKT-Systemen wird sich in Zukunft viel stärker auf bis dato nicht digitale Bereiche ausdehnen. Dies geht vor allem mit der immer stärker werdenden Digitalisierung einher. Dadurch wird es notwendig, Leuchtturmprojekte außerhalb eines reinen IKT-Umfeldes zu testen. Die Freigabe einer Modellregion mit den im Leuchtturmprojekt beschriebenen Parametern kann es ermöglichen, frühzeitig Erfahrung zu sammeln und Entwicklungen gezielt zu steuern.

7 Roadmap

Die Technologieroadmap zur Unterstützung der IKT-Sicherheit in Österreich leitet sich aus den vorhergehenden Kapiteln ab. In einem ersten Schritt wird den Emerging Technologies eine zeitliche Dimension zugeordnet (Kapitel 7.1). In einem zweiten Schritt wird eine Verknüpfung zwischen den Emerging Technologies und den Forschungsfeldern hergestellt und aufgezeigt, welche Forschungsfelder für welche Emerging Technologies hohe Priorität haben und vice versa (Kapitel 7.2). Diese beiden Punkte wurden anhand von eigener Recherchen, Interviews und gemeinsam mit ExpertInnen aus Wirtschaft, Wissenschaft und Verwaltung im Rahmen eines Workshops erarbeitet. In Kapitel 7.3 werden die Entwicklungspotentiale des Humankapitals in Österreich beschrieben und das abschließende Kapitel 7.4 fasst die wesentlichen Empfehlungen, die an mehreren Stellen im Bericht ausgesprochen wurden, für zukünftige Forschungsschwerpunkte- und -projekte zusammen.

„Ziel ‚Made in Austria': sichere Lösungen rund um neue Technologien bauen"

(Zitat aus den Interviews)

7.1 Zeitachse und Ziele für den österreichischen Markt

Die Emerging Technologies, welche in Kapitel 4 beschrieben sind, werden in drei Zeitdimensionen eingeteilt, die für den österreichischen Markt relevant sind. Diese sind kurzfristige Technologieinnovationen (< 2 Jahre), mittelfristige Technologieinnovationen (2-6 Jahre), langfristige Technologieinnovationen (> 6 Jahre). Tabelle 4 liefert eine Begründung für die zeitliche Einteilung der Emerging Technologies.

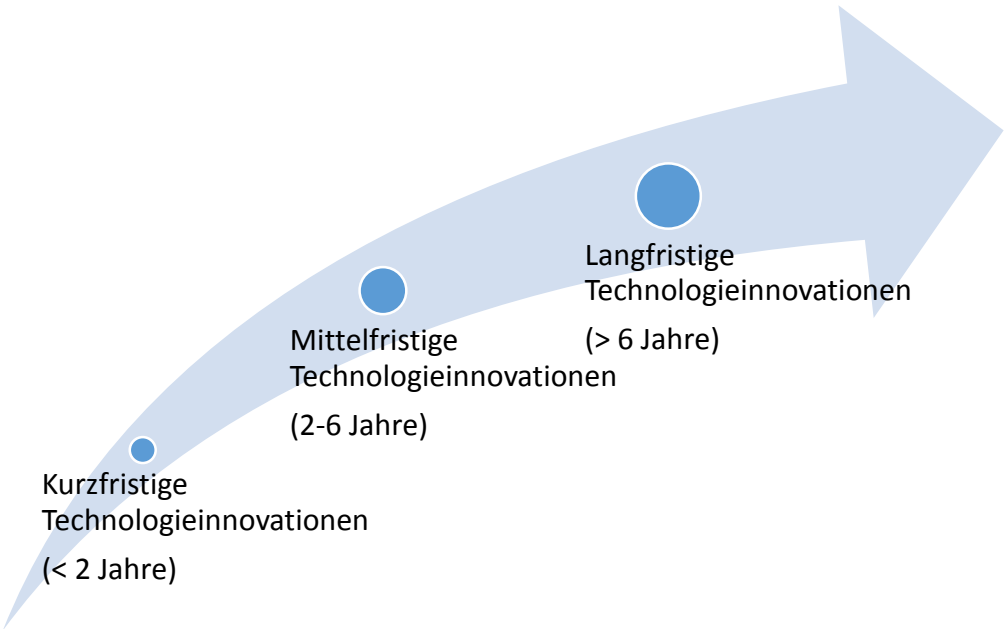


Abbildung 13: Zeitachse der Emerging Technologies

Zu den kurzfristigen Technologieinnovationen gehören Technologien, die bereits einen bedeutenden Einfluss auf die globale IKT haben. Hierzu zählen Technologien, welche starke Wachstumszahlen aufweisen und von vielen Unternehmen eingesetzt werden. Die Technologien wurden in den letzten Jahren stark in den Medien „gehypt“ oder werden es aktuell. Daher besteht hier unmittelbarer Handlungsbedarf. Zu den kurzfristigen Technologieinnovationen zählen Technologien rund um Big Data, Cloud Computing, vernetzte Gesellschaft und Mobile Devices.

Mittelfristige Technologieinnovationen sind Technologien, welche bereits vielfältig diskutiert, jedoch noch nicht im großen Stil eingesetzt werden. Hierbei ist davon auszugehen, dass diese eine wesentliche Rolle für die globale IKT in den nächsten zwei bis sechs Jahren erlangen. Zu den mittelfristigen Technologieinnovationen zählen Netzwerkvirtualisierung, cyber-physikalische Systeme, Internet der Dinge und Augmented Reality.

Als langfristige Technologieinnovationen werden Technologien angesehen, welche noch sehr weit von der tatsächlichen Umsetzung entfernt sind. Es gibt hier teilweise bedeutende Forschungsbewegungen, ein großflächiger Einsatz ist aber in den nächsten sechs Jahren nicht abzusehen. Hier besteht primär Bedarf an Grundlagenforschung hinsichtlich der sicherheitsrelevanten Aspekte. Zu den langfristigen Technologieinnovationen zählen Technologien rund um Quantenrechner, Robotics und Cybernetics (Abbildung 14).

Ebenso ergeben sich für die einzelnen Forschungsfelder verschiedene Zeithorizonte, die in Abbildung 14 dargestellt werden. Mit so gut wie allen gelisteten Forschungsfeldern wird man sich in den kommenden 1-2 Jahren beschäftigen müssen. Dies sind vorwiegend Identitätsmanagement, Usable Security, Bekämpfung von Schadsoftware, Security Engineering / Secure Coding, Privacy Impact Assessment, oder Nachvollziehbarkeit der Datenverarbeitung/Transparenz. Betroffen sind sowohl Aspekte der Informationssicherheit als auch Aspekte aus Recht und Gesellschaft, insbesondere Datenschutz.

Für die meisten Forschungsfelder wird eine kurzfristige Auseinandersetzung allerdings nicht ausreichen und sie werden für österreichische WissenschaftlerInnen und UnternehmerInnen mittelfristig, d.h. bis zu sechs Jahre, von Bedeutung sein. Einige wenige Forschungsfelder, wie etwa Sicherheitsbewusstsein & innovative Lehrkonzepte, Entwicklung sicherer Hardware, oder Security by Design werden auch langfristig, d.h. mehr als sechs Jahre österreichische ForscherInnen und UnternehmerInnen intensiv beschäftigen.

Abbildung 14: Zeithorizonte der Forschungsfelder und Emerging Technologies

Die Zuordnung der Emerging Technologies zu den jeweiligen Zeitzielen (kurz-, mittel- und langfristig) erfolgt folgendermaßen:

Technologie	Begründung
Kurzfristig	
Big Data	Laut einer Studie von IDC (2014[301]) ist davon auszugehen, dass Big Data stark an Fahrt aufnehmen wird. Es besteht großer Bedarf seitens der Wirtschaft und 47% der befragten österreichischen Unternehmen geben an, dass der Einsatz von Big-Data-Lösungen im Unternehmen ernsthaft diskutiert wird. Häufig fehlt es jedoch noch an einer Strategie für das umfassende Datenmanagement in österreichischen Unternehmen. Die zur Verfügung stehende Datenmenge in den unterschiedlichsten Unternehmen wächst kontinuierlich. Prognosen sprechen von einem durchschnittlichen Wachstum von 33,5% in Umsatzzahlen in den nächsten vier Jahren, wobei der Big Data Markt in Österreich von 22 Millionen Euro im Jahr 2013 auf 73 Millionen Euro im Jahr 2017 anwachsen wird. Der Markt für Big Data Anwendungen ist noch sehr jung und daher stark umkämpft. Aktuell befindet sich Big Data in einem initialen Stadium. Die Einsatzentscheidung ist oftmals schon gefallen, es mangelt NutzerInnen jedoch noch am Know-how in Bezug auf Anbieter, Verfahren und Werkzeuge. Ziel ist es deshalb, Unternehmen über die zur Verfügung stehenden Tools und Werkzeuge im Zusammenhang mit Big Data zu informieren. Unternehmen, die am österreichischen Markt aktiv sind, sollten jetzt stark in die Entwicklung und Vermarktung qualitativ hochwertiger Lösungen investieren. Strategie, effektives Marketing und Awareness Building können entscheidende Wettbewerbsvorteile darstellen.
Cloud Computing	Cloud Computing ist auch in Österreich bereits am Massenmarkt angekommen. Viele österreichische Unternehmen setzen bereits auf das Thema Cloud. Außerdem ist eine stetige Zunahme der Ausgaben im Bereich Cloud-Services in Österreich von 16 Mio. Euro im Jahr 2014 auf 54 Mio. Euro im Jahr 2018 zu erwarten. Kollaboration und Kommunikation stellt den häufigsten Anwendungsbereich dar.[302] In einer Befragung zum Thema Informationssicherheit gaben 21% der österreichischen befragten Unternehmen an, Cloud-Services aufgrund Sicherheitsbedenken nicht zu nutzen.[303] Ziel muss deshalb sein, Sicherheitsbedenken so weit wie möglich auszuräumen, d.h. einerseits aus technischer Sicht für sichere Systeme zu sorgen, andererseits das Bewusstsein der NutzerInnen für einen sicheren Umgang mit neuen Technologien zu schärfen.

[301] Wolschann, 2014.
[302] IDC, 2015d.
[303] Reisinger, 2015, S. 60.

Vernetzte Gesellschaft	Unter „vernetzter Gesellschaft“ wird im allgemeinen Social Media verstanden. Dieser Bereich ist seit einigen Jahren weltweit und in Österreich sehr gut vertreten. Daher ist die Relevanz als „kurzfristig“ einzuordnen. In Österreich gibt es derzeit allein an die 3,4 Mio. Facebook NutzerInnen. Twitter nutzen 140.000 Personen und Instagram 880.000 Personen, Zahlen stark steigend (Stand: September 2015)[304]. Auch wenn aktuell ein Rückgang der Cyber-Kriminalität zu verzeichnen ist, so ist im Zehn-Jahresvergleich doch ein deutlicher Trend nach oben ablesbar. Dies ist durch die zunehmende Verbreitung von Computern – speziell in Form von Smartphones und Tablets – dem Ausbau von Netzwerken und hier vor allem mobilen Breitbandverbindungen zu erklären. Da die Informations- und Kommunikationstechnologie zu einem ständigen Begleiter im Alltag geworden ist, entstehen laufend neue Kriminalitätsphänomene, wobei weiterhin von einem großen Dunkelfeld im Bereich Cybercrime auszugehen ist. Das Gefährdungs- und Schädigungspotenzial durch Cybercrime bleibt auch in Zukunft unverändert hoch.[305] Ziel ist es, das Gefährdungs- und Schädigungspotenzial zu senken.
Mobile Devices	Smartphones und Tablets sind seit mehreren Jahren am Markt und die Durchdringung des Marktes ist bereits sehr stark fortgeschritten. In einer im Jahr 2015 durchgeführten Befragung gaben 85% der Unternehmen an, bereits mobile Geräte für Geschäftstätigkeiten zu verwenden. Die Hälfte gab sogar an, „Bring your own Device (BYOD)“-Konzepte zu erlauben.[306] Dies zeigt die Notwendigkeit die Sicherheit der Daten auf mobilen Endgeräten zu erhöhen. Daher sind mobile Geräte ganz klar als „kurzfristig“ einzuordnen.
Mittelfristig	
Netzwerk-virtuali-sierung	Ein momentan einsetzender Trend ist „software defined networks“. Hierbei handelt es sich um einen Abstraktionslayer über die physische Netzwerkschicht, welcher Verbesserungen im Netzwerkverkehr zulässt. Netzwerkvirtualisierung ist noch nicht am Markt angekommen. Jüngste Statistiken zeigen aber ein sehr schnelles Wachstum und Prognosen gehen davon aus, dass auch in den nächsten Jahren mit einem starken Anstieg gerechnet werden kann.[307]
Cyber-physikalische Systeme	Cyber-physikalische Systeme erleben immer mehr Anwendungsfelder. Vor allem für geplante Aktivitäten unter dem Schlagwort Industrie 4.0 bieten diese Systeme die Basis.[308],[309] Die Kooperationen im Rahmen des Forschungsthemas Industrie 4.0 zwischen österreichischen Forschungsinstituten und Unternehmen stehen heute

[304] Social Media Radar Webseite.
[305] Bundeskriminalamt Österreich, 2014.
[306] Reisinger, 2015, S. 59f.
[307] IDC, 2014c.
[308] Heinze, 2014.
[309] Fraunhofer, Cyber-Physical Systems Webseite.

	noch am Anfang. Industrie 4.0 wird jedoch das zentrale Thema für Industrieunternehmen in den kommenden Jahren darstellen. Die Umsetzungsgeschwindigkeit von entsprechenden Initiativen in Firmen wird allerdings stark davon abhängen, inwiefern Lösungskonzepte Unternehmen bei der Bewältigung aktueller Herausforderungen, wie der Einsparung von Produktionskosten, einer stärkeren Automatisierung, dem Management der höheren Produktkomplexität und der schnelleren Reaktion auf neue Anforderungen unterstützen können.[310] Zwar gab es in den letzten Monaten zahlreiche Diskussionen zu den Chancen, die Digitalisierung und die Vernetzung von Industriebetrieben mit sich bringen, um den europäischen Produktionsstandort zu sichern. Die Technologie an sich ist jedoch noch nicht im großen Stil am österreichischen Markt angekommen und hat daher eine mittelfristige Dimension. Laut einer Gallup-Umfrage geben 47% von 200 heimischen Industriebetrieben an, bereits etwas über den Begriff und das Konzept gehört zu haben, Industrie 4.0 stößt aber nicht überall auf offene Ohren. Ein Viertel der Befragten gab an, noch weitere Informationen zu benötigen. Jedes fünfte Unternehmen glaubt, dass es sich nur um einen Hype handle, der wieder vorübergehen wird. 8% der Befragten gehen davon aus, dass das Thema Europa weniger betreffe als Asien oder die USA.[311]
Internet der Dinge	Internet der Dinge bezeichnet die Entwicklung, dass einfache oder komplexe Dinge (z.B. Kühlschränke, Heizungssteuerungen, etc.) direkt mit dem Internet verbunden sind und so vom Menschen oder anderen Maschinen angesprochen werden können. Das Phänomen wird zwar bereits stark diskutiert, hat jedoch noch keine große praktische Verbreitung gefunden. Es ist zu erwarten, dass es in den nächsten zwei bis drei Jahren sehr stark kommen wird. Auch das österreichische Computer Emergency Response Team CERT[312] weist in seinem Jahresbericht auf die rasante Entwicklung bis 2020 hin und fordert zu proaktiven Maßnahmen auf, um die Risiken dieser Entwicklung zu adressieren.
Augmented Reality	Google Glass und Oculus Rift sind bekannte Vertreter dieser Technologie. Bei beiden hat sich jedoch gezeigt, dass eine Tauglichkeit für den Massenmarkt noch nicht gegeben ist. Daher werden Augmented Reality Technologien als „mittelfristig“ eingestuft.
Langfristig	
Quanten-rechner	Quantenrechner haben das Potenzial, aktuelle Berechnungsmethoden und Verschlüsselungsalgorithmen auf den Kopf zu stellen, was zu gravierenden Problemen im Bereich der Sicherheit führen kann. Die tatsächliche Machbarkeit von

[310] IDC Event, 2015.
[311] Drucker, 2015b.
[312] CERT, 2014, S.34f.

	Quantenrechnern ist aber auch noch sehr weit entfernt, wodurch diese Kategorie als „langfristig“ einzuordnen ist.
Robotik und Cybernetics	Die Entwicklungen in der Robotik zeigen in den letzten Jahren große Fortschritte in allen Bereichen. Neben dem Industriebereich finden Roboter auch im Heimbereich / Servicebereich (z.B.: Service Roboter wie Asimo[313]) immer mehr neue Einsatzgebiete. Robotik gilt als einer der Schwerpunkte[314] von Horizon 2020, vor allem aufgrund der Möglichkeit viele Industrien (z.B.: Gesundheit, Produktion, Logistik) weiter voranzutreiben. Angesichts der umfangreichen Einsatzmöglichkeiten und langen Forschungs- und Entwicklungshorizonte von Robotik und Cybernetics, wird dieser Themenbereich der langfristigen Kategorie zugeordnet.

Tabelle 4: Zuordnung der Emerging Technologies zu den Zeitachsen

7.2 Zuordnung der Forschungsfelder zu den Emerging Technologies

Die in Kapitel 4 beschriebenen Emerging Technologies werden an dieser Stelle den jeweiligen Forschungsfeldern aus Kapitel 5 zugeordnet und priorisiert. Eine Unterteilung erfolgt in hohe Priorität (grüner Pfeil), mittlere Priorität (gelber Pfeil) und geringe Priorität (roter Pfeil) (Tabelle 5). Eine besonders hohe Priorität für alle Emerging Technologies weisen die Forschungsfelder Usable Security, Entwicklung sicherer Hardware, Bekämpfung von Schadsoftware, Security Engineering / Secure Coding, Software Security Testing and Assurance und Security by Design auf. Von hoher Priorität für die meisten (aber nicht alle) Emerging Technologies sind die Forschungsfelder Identitätsmanagement, Digitale Forensik und Self-healing/protection.

Emerging Technologies, die für eine besonders hohe Zahl an Forschungsfeldern Priorität haben, sind v.a. Cloud Computing und Internet of Things Technologien; auch von hoher Priorität für knapp die Hälfte der genannten Forschungsfelder haben die Emerging Technologies vernetzte Gesellschaft und mobile devices.

Tabelle 5 zeigt zudem die unterschiedlichen Zeithorizonte für die einzelnen Forschungsfelder heruntergebrochen auf die einzelnen Emerging Technologies. Es erfolgt eine Unterteilung der Forschungsfelder verknüpft mit den Emerging Technologies in kurzfristig (dunkelblau), mittelfristig (blau) und langfristig (hellblau).

[313] Vgl. Asimo Webseite.

[314] Vgl. European Commission, Robotics Webseite.

	Big Data	Cloud Computing	Vernetzte Gesellschaft	Mobile Devices	Netzwerkvirtualisierung	Cyber-physikalische Systeme	Internet der Dinge	Augmented Reality	Robotik und Cybernetics	Quantenrechner
Aspekte der Informationssicherheit										
Risiko- und Notfallmanagement	●	◐	●	◑	◑	◐	●	●	●	●
Sicherheitsökonomie & -kennzahlen	●	●	◑	◑	◑	◐	●	●	●	●
Sichere und widerstandsfähige Geschäftsprozesse	●	◐	●	●	●	◐	●	●	●	●
Referenzmodelle, Security & Misuse Patterns	●	◑	●	●	●	◑	●	●	●	●
Identitätsmanagement	◐	◐	◐	◑	●	◐	◐	●	●	●
Usable Security	◐	◐	◐	◐	◐	◐	◐	◐	◐	◐
Sicherheitsbewusstsein & innovative Lehrkonzepte	◑	◑	◑	◑	◑	◑	◑	◑	◑	◑
Information Sharing/Informationsaustausch	●	◐	●	●	●	◑	●	●	●	●
Visualisierung/Visual Analytics	●	◐	●	●	◐	◐	●	●	●	●
Bekämpfung von Kriminalität in Social Media	●	●	◐	◑	●	●	●	●	●	●
Gehärtete Betriebssysteme	●	●	●	◐	●	◐	◑	●	◑	●
Entwicklung sicherer Hardware	◐	◐	◐	◐	◐	◐	◐	◐	◐	◐
Bekämpfung von Schadsoftware	◐	◐	◐	◐	◐	◐	◐	◐	◐	◐
Digitale Forensik	●	◐	◐	◐	◐	◐	◐	●	◐	●
Sicherheit von Firmware u. eingebetteter Systeme	●	●	●	◐	●	◑	●	●	●	●
Intelligence Driven Network Security	●	◐	●	●	◐	●	●	●	●	●
Sichere Netzwerkprotokolle	●	◐	●	◐	◐	◐	◐	●	●	●
Netzwerkverkehrsanalyse / Frühwarnsysteme	●	◐	●	◐	◐	◐	◐	●	●	●
Software Defined Networks Security	●	◐	●	●	◐	◐	●	●	●	●
Self-healing/protection	●	◐	◐	◐	◐	◐	◐	●	●	●
Data Leakage/Loss Protection	◐	◐	◑	◐	●	●	●	●	●	●
Security Engineering / Secure Coding	◐	◐	◐	◐	◐	◐	◐	◐	◐	◐
Software Security Testing and Assurance	◐	◐	◐	◐	◐	◐	◐	◐	◐	◐
Sicherheit von Systemen in feindlichen Systemen	●	●	●	●	◐	◐	◐	●	◐	●
Bekämpfung von Botnetzen	●	◐	◐	◐	◑	◐	◐	●	●	●
Pseudonymisierung / Anonymisierung	◐	◐	●	●	●	●	●	●	●	●
Verschlüsselungstechnologien	◐	◑	●	◐	●	◐	●	◑	◐	●
Rechnen und Suchen in verschlüsselten Daten	◐	◐	●	◑	●	●	●	●	●	●
Security by Design	◐	◐	◐	◐	◐	◐	◐	◐	◐	◐

Aspekte von Recht und Gesellschaft, insbesondere Datenschutz										
Privacy Impact Assessment	↑	→	↑	↑	↓	→	→	↑	↓	→
Privacy by Design and by Default	→	→	↑	↑	↓	→	→	↑	↓	↓
Nachvollziehbarkeit der Datenverarbeitung	↑	↑	↑	→	↓	→	→	→	↓	↓
Recht, Organisation und Kooperation	↓	→	→	→	→	↑	↑	↓	→	↓
Sonstige grundrechtliche u. ethische Challenges	↑	↓	↑	→	↓	→	↑	↑	↑	↓

Legende: ↑ Hohe Priorität → Mittlere Priorität ↓ Geringe/Keine Priorität
Kurzfristig Mittelfristig Langfristig

Tabelle 5: Zuordnung der Emerging Technologies zu den Forschungsfeldern

7.3 Entwicklungspotenziale des Humankapitals

Humankapital bedeutet, dass Menschen, die in den beschriebenen Technologiebereichen arbeiten, über bestimmte Fähigkeiten und entsprechendes Wissen verfügen. Die Besonderheit der beschriebenen Technologiebereiche liegt in ihrer hohen Anforderung an Inter- und Multidisziplinarität der ExpertInnen. Eine kürzlich durchgeführte Umfrage zum Thema Informationssicherheit in Österreich zeigt, dass mangelndes Detail-/Spezialwissen ein Problem für die Aufrechterhaltung und Verbesserung in vielen Organisationen darstellt.[315] Welche Expertisen jeweils notwendig sind, zeigt sich in den inhaltlichen Beschreibungen zu den jeweiligen Bereichen. Zusammengefasst ist neben einem breitbandigen technologischen Wissen auch ein Mindestmaß an rechtlichem, wirtschaftlichen und sozialen Verständnis und Wissen erforderlich.

ExpertInnen, die bereits jetzt in solchen Schnittstellenbereichen arbeiten, z.B. Data Analysts, DatenschutzexpertInnen, etc., haben verschiedene Möglichkeiten, sich diese inter- und multidisziplinären Kompetenzen anzueignen. Der derzeit wohl häufigste Fall, ohne dies an dieser Stelle empirisch belegen zu können, ist die eigenverantwortliche und weitgehend autodidakte Initiative der Personen selbst, z.T. unterstützt durch deren ArbeitgeberInnen.

Eine vom Befund her nach wie vor aktuelle Umfrage[316] des Instituts für Bildungsforschung der Wirtschaft (ibw) aus 2012 lässt erkennen, dass diese multidisziplinären Kompetenzen, welche an zukünftige IT-Fachkräfte in der österreichischen Wirtschaft gestellt werden, von großer Bedeutung sind. Ob Datenschutz, Lizenzierung, Haftung oder Compliance, das Rechtsbewusstsein avanciert zu einer wichtigen nicht-technischen Kompetenz, so zeigen es die Ergebnisse der Befragung von 867 österreichischen Unternehmen. Das Qualifikationsbild

[315] Reisinger, 2015.

[316] ibw-Unternehmensbefragung April/Mai 2012 (n=867 vollständig ausgefüllte Fragebögen), vgl. Dornmayr, 2012.

der IT-Fachkräfte besteht jedoch nicht nur aus technischen und rechtlichen Kompetenzen. Auch betriebswirtschaftliches Know-how, sprachliche Fähigkeiten und Zuverlässigkeit sind Bestandteile des Wunschqualifikationsprofils der Wirtschaft an die Fachkräfte (Abbildung 15).

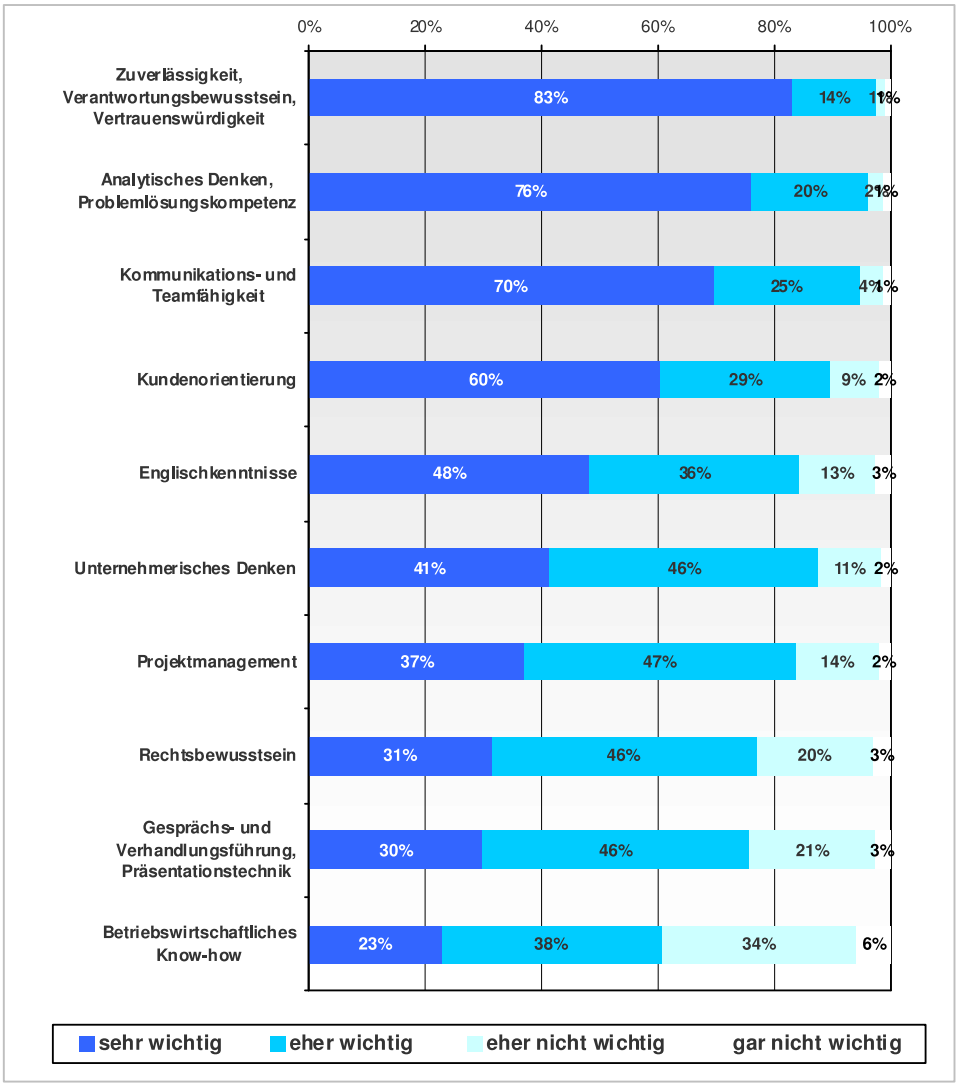


Abbildung 15: Zukünftig benötigte nicht-technische Kompetenzen von IT-Fachkräften (ibw, 2012)[317]

Aktuell gibt es in Österreich durchwegs einen Mangel an AbsolventInnen mit einschlägig technischer Spezialisierung. Die nachfolgende Statistik[318] zeigt, dass eine Mehrzahl der davon betroffenen Unternehmen das Angebot als mangelhaft ansieht. Verknüpft man nun die Aussagen dieser beiden Statistiken miteinander, so wird ersichtlich, dass ein Bedarf an Fachkräften mit multidisziplinären Kompetenzen in Österreich besteht.

[317] Dornmayr, 2012, S. 13.
[318] Dornmayr, 2012, S. 9.

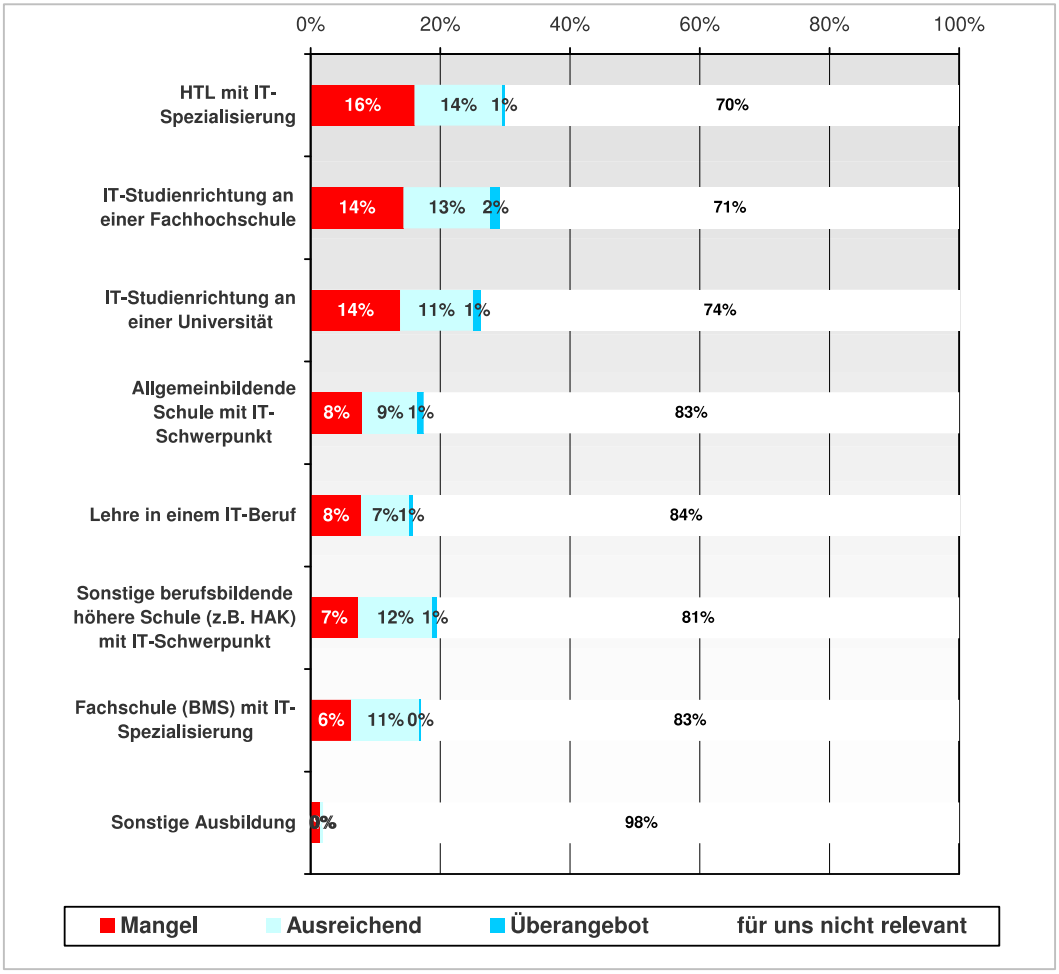


Abbildung 16: AbsolventInnen mit einschlägig technischer Spezialisierung in Österreich (ibw, 2012)

In den tertiären technischen Ausbildungszweigen ist in den letzten Jahren das Bewusstsein gestiegen, auch rechtliche und sozialwissenschaftliche Aspekte immanent zu behandeln. Dies geht jedoch i.d.R. nicht über die Vermittlung von Grundlagen hinaus. Im besten Fall werden zusätzlich fakulative Spezialvorlesungen zu solchen Schnittstellenthemen angeboten. Demgegenüber werden in allen juristischen Ausbildungszweigen – mit Ausnahme einzelner fakulativer Lehrveranstaltungen – i.d.R. keine technischen Kenntnisse vermittelt. Um das Angebot an qualifizierten AbsolventInnen zu erhöhen ist die Attraktivierung von IT-spezifischen Lehrgängen und Studien eine mögliche Lösung. Eine Erhöhung der AnfängerInnenzahlen und eine gleichzeitige Senkung der Drop-Out-Rate würden das Angebot langfristig steigern – natürlich sollte dabei nicht das Niveau der Ausbildung reduziert werden. Durch spezifische Steigerung der Attraktivität kann auch der Anteil an Frauen in der Wissenschaft gesteigert werden und somit eine größere Anzahl an Anfängerinnen und schließlich Absolventinnen erzielt werden. Mit Hilfe einer spielerischen Heranführung von Kindern und Jugendlichen an technische Problemstellungen und einer Verankerung im Lehrplan könnten die technischen Wissenschaften zusätzliche InteressentInnen gewinnen.

Bildungsangebot im Bereich der IKT-Sicherheit			
Institution	Bachelor	Master	Lehrgang
Donau-Universität Krems		St/Fv (bb)	
FH Campus Wien	St/Fv (vz,bb)	St (bb)	
FH Joanneum	Lv	St (bb)	
FH OÖ, Campus Hagenberg	St (vz)	St (vz)	Lg (bb)
FH Salzburg		Lv	
FH St. Pölten	St (vz,bb)	St (vz)	
FH Technikum Wien	St/Fv (bb)	St (bb)	
FH Wiener Neustadt			Lg (bb)
JKU Linz, FIM	Lv	St (vz)	
TU Graz, IAIK	Lv	Lv	
TU Wien, IFS, isecLab, INSO/ESSE	Lv	Lv	
Universität Innsbruck, CCS, QE		Lv	
Universität Klagenfurt, syssec	Lv	Lv	
Universität Wien, MIS	Lv	Lv	
WU Wien, NM, MIS	Lv	Lv	

Legende:

Lv	Einzelne Lehrveranstaltungen zum Thema IKT-Sicherheit werden im jeweiligen Ausbildungslevel angeboten.
St	Es gibt eine komplette Studienrichtung zur Thematik IKT-Sicherheit im jeweiligen Ausbildungslevel.
St/Fv	Es gibt eine Studienrichtung mit Fachvertiefung zur Thematik IKT-Sicherheit im jeweiligen Ausbildungslevel.
Lg	Es gibt einen kompletten Lehrgang zur Thematik IKT-Sicherheit.
bb	Die Studienrichtung bzw. der Lehrgang werden berufsbegleitend angeboten.
vz	Die Studienrichtung bzw. der Lehrgang werden als Vollzeitstudium angeboten.

Tabelle 6: Bildungsangebot im Bereich der IKT-Sicherheit in Österreich

Um die zukünftigen Anforderungen an IT-Fachkräfte zu erfüllen, bedarf es einer Neuerung in der tertiären Ausbildung. Wie oben beschrieben sind technische Kenntnisse, gepaart mit betriebswirtschaftlichen Know-how und Rechtsbewusstsein, die von der Wirtschaft gewünschten Kompetenzen einer IT-Fachkraft der Zukunft. Um diesen Anforderungen gerecht zu werden, bedarf es einer vertiefenderen Ausbildung an österreichischen Hochschulen als es bislang angeboten wurde. Als Idealfall denkbar wäre ein Studium „Informationstechnologie und Recht“, um die multidisziplinären Kompetenzen im Detail zu unterrichten. Einen Überblick über das tertiäre Bildungsangebot zur IKT-Sicherheit bietet das „A-SIT Zentrum für sichere Informationstechnologie – Austria“[319] (Tabelle 6).

[319] A-SIT, 2013. Übersicht über das Angebot an österreichischen Fachhochschulen und Universitäten. [Anmerkung: der hier dargestellte Stand erscheint nach Recherche auch für 2015 noch aktuell].

7.4 Zusammenfassung der Empfehlungen und Forschungsschwerpunkte

Die wesentlichen Herausforderungen, Ziele, Akteure und Empfehlungen, die in der Studie beschrieben sind, werden in Abbildung 17 zusammengefasst. Zu den größten Herausforderungen unserer Zeit zählt, dass Informationssysteme, digitalisierte Informationen und damit verbundene Anwendungen unsere Privatsphäre, Gesellschaft und Wirtschaft mehr denn je beeinflussen. Die Allgegenwärtigkeit von Informationstechnologie hat zahlreiche neue Einsatzmöglichkeiten geschaffen, die vor einigen Jahren noch nicht denkbar gewesen wären. Zusätzlich bringen neue Geschäftsmodelle (z.B.: Cloud) rasche Innovationszyklen und Technologien (z.B.: Big Data, Mobile Computing) sowie die Veränderung des BenutzerInnenverhaltens (z.B. soziale Netzwerke, Video on demand) neue Herausforderungen an die Informationssicherheit mit sich. Generell nimmt die digitale Vernetzung zu und somit auch die Wahrscheinlichkeit, Opfer von cyber-kriminellen Handlungen zu werden. Spam, Schadprogramme, Malware, Zugriff auf sensitive Informationen der User, Identitätsdiebstahl bis hin zu gezielten und hochspezialisierten Cyberangriffen (advanced persistent threats) stellen nur einige der Herausforderungen dar. Ständige Veränderungen, einerseits was cyber-kriminelle Formen betrifft, aber auch was neue Produkte und Technologien betrifft, lassen rechtliche Aspekte der Informationssicherheit oft hinterherhinken. Eine Herausforderung ist es, nicht bloß auf Cyber-Kriminalität zu reagieren, sondern bereits in der Entwicklungsphase so gut wie möglich Schwachstellen zu erkennen und zu vermeiden (vgl. Abbildung 17). Die Herausforderungen an die Informationssicherheit einschließlich der rechtlichen und gesellschaftlichen Aspekte sind im Detail in den Kapiteln 2 und 3 beschrieben.

Ziele sind die Erreichung einer bestmöglichen Cybersicherheit für die NutzerInnen neuer Technologien unter Berücksichtigung unterschiedlicher Maßnahmen in den Bereichen Recht, Technik, Forschung, Entwicklung und Bildung sowie die Prävention bzw. das rechtzeitige Erkennen von Gefahren. Die Etablierung Österreichs als attraktiver, wettbewerbsfähiger Standort innerhalb Europas ist ein weiteres Ziel für Institute und Unternehmen im Bereich Sicherheitsforschung- und Entwicklung.

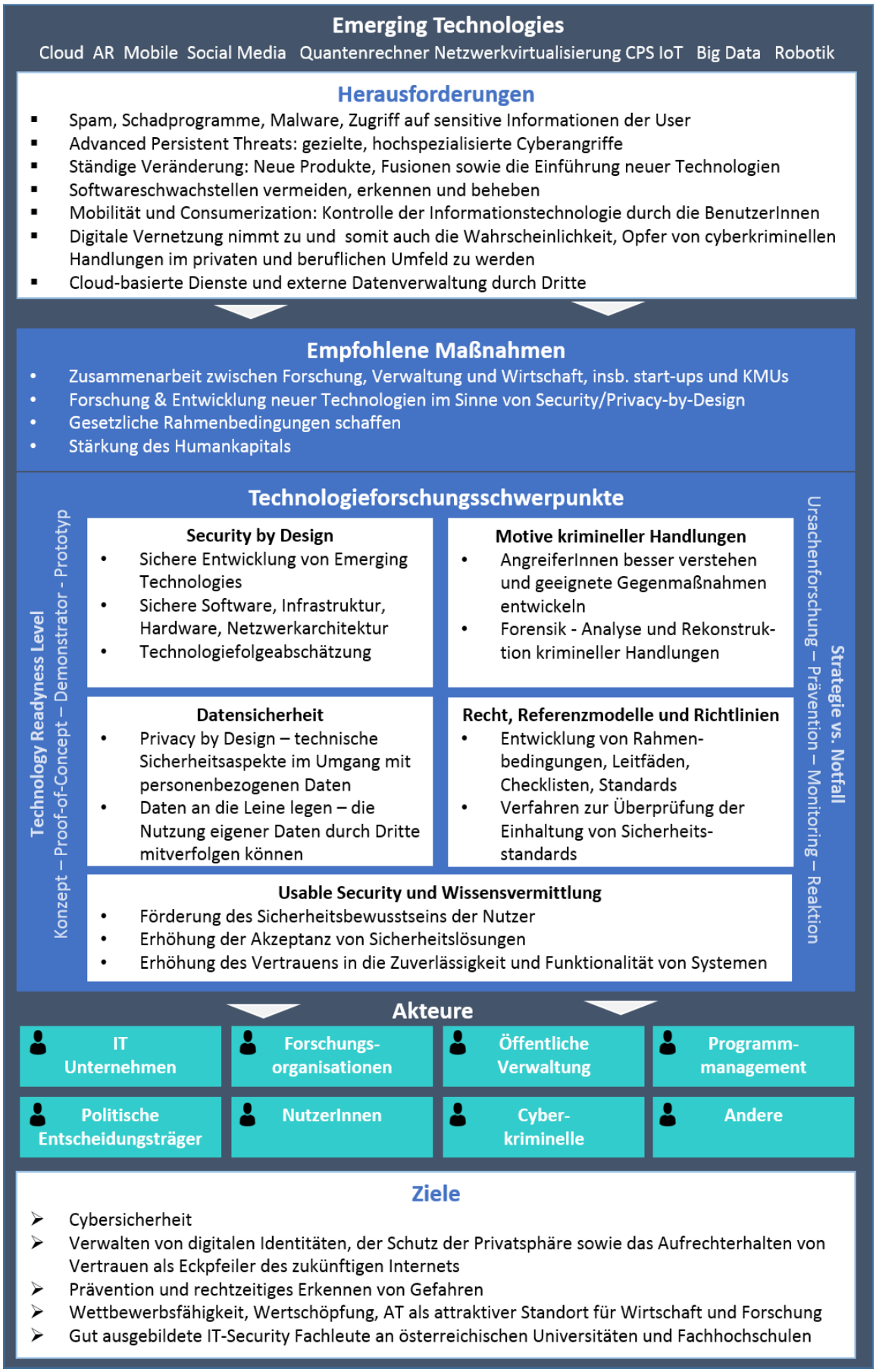


Abbildung 17: Empfohlene Schwerpunkte in der österreichischen Sicherheitsforschung

Akteure

IKT-Sicherheit ist ein interdisziplinäres Themenfeld, bei dem eine Vielzahl an Akteuren – häufig auch mit unterschiedlichen Intentionen und Interessen – involviert ist. Die wesentlichen Akteure in Österreich werden im Folgenden gruppiert und beschrieben.

IT-Unternehmen

Diese Gruppe umfasst in Österreich ansässige Technologieunternehmen bzw. IT-Abteilungen in Unternehmen vom Start-up bis hin zu etablierten KMUs oder große Unternehmen, die eigene Produkte und Dienstleistungen entwickeln und/oder beratend tätig sind. Unabhängig davon, ob es sich um Services und Applikationen im Bereich Gesundheitswesen, Verkehr, Energie, Kommunikation, Finanzen, etc. handelt, die Sicherheit von IKT-Systemen und Widerstandsfähigkeit gegen Angriffe oder Missbrauch spielt in allen Domänen eine wesentliche Rolle und es gilt Sicherheitsaspekte in allen Phasen der Produktentwicklung und auf allen organisatorischen Ebenen zu berücksichtigen.

Forschungsorganisationen

Universitäten, Fachhochschulen sowie außeruniversitäre Forschungseinrichtungen verschiedener Disziplinen befassen sich intensiv mit IKT-Sicherheit aus wirtschaftlicher, sozialwissenschaftlicher, kriminologischer, rechtlicher sowie technischer Sicht und können wesentliche Beiträge im Bereich der Grundlagenforschung sowie Forschung und Entwicklung in Zusammenarbeit mit der Wirtschaft und/oder der öffentlichen Verwaltung leisten.

Öffentliche Behörden und politische Entscheidungsträger

Eine Vielzahl von Behörden auf Bundes-, Landes- und Gemeindeebene ist mit Sicherheit in der IKT befasst. Auf Bundesebene sind hervorzuheben das Bundeskanzleramt (Datenschutz und E-Government), die Ministerien, insbesondere BM.I, BMLVS (Heeres-Nachrichtenamt, Abwehramt), BMVIT (insbesondere Fernmeldebehörde), die Rundfunk- und Telekom Regulierungs-GmbH (RTR) und die Datenschutzbehörde.

Mit dem Thema Cyberkriminalität sind in Österreich speziell ausgebildete Beamte befasst. Das im Bundeskriminalamt angesiedelte Cybercrime-Competence-Center „C4“ ist die nationale und internationale Zentralstelle zur Bekämpfung von Cyber-Kriminalität in Österreich und arbeitet mit dem Landeskriminalämtern und lokalen IT-ErmittlerInnen sowie mit GovCERT[320] zusammen[321]. Eine Zuständigkeit des Bundesamtes für Verfassungsschutz und Terrorismusbekämpfung (BVT) besteht, wenn kritische Infrastruktur betroffen ist.

Forschungsprogrammmanagement

[320] Government Computer Emergency Response Team für den Bereich der öffentlichen Verwaltung, GovCert Austria Webseite.

[321] Bundeskriminalamt Österreich, 2014.

Öffentliche Fördergeber und das Programmmanagement beeinflussen Forschungs- und Entwicklungsmöglichkeiten in Österreich durch das Festlegen neuer Ausschreibungsschwerpunkte speziell im Bereich Technologie (IKT der Zukunft), Sicherheit (KIRAS Sicherheitsprogramm) bzw. andere Programme mit Technologiebezug (z.B. Stadt der Zukunft, benefit im Bereich Active & Assisted Living, Produktion der Zukunft, uvm.).

NutzerInnen von IKT-Systemen und Applikationen

Diese Gruppe umfasst die breite Öffentlichkeit bzw. alle, die Informations- und Kommunikationstechnologien sowie Emerging Technologies privat oder beruflich nutzen. Alle Altersgruppen sind eingeschlossen, von den digital natives bis hin zu betagteren Personen. Gerade Datenschutz ist ein Thema, das so gut wie alle InternetnutzerInnen betrifft.

Cyberkriminelle

Nicht zuletzt sind es Hacker, Cyberactivisten, Hacktivisten, etc. (Begriff im negativen Sinne gemeint), die Schwachstellen in IKT-Systemen ausnutzen und zu TäterInnen werden. Zunehmende Professionalisierung, Organisation und Wirtschaftlichkeit der Cybercrime-Szene sind in den letzten Jahren zu beobachten.

Empfehlungen für F&E Projekte und Ausschreibungsschwerpunkte

Ausgehend von der Bedrohungslandschaft sowie von neuen technologischen Innovationen können Forschungsaspekte und rechtliche Rahmenbedingungen für verschiedene Bereiche (d.h. übergreifende Aspekte, Hardware/physische Assets, Betriebssysteme, Netzwerke, Anwendungen, Informationen) identifiziert werden. In den Kapiteln 2-6 dieser Studie werden insgesamt an die 50 konkreten Empfehlungen, welche F&E Schwerpunkte und Projekte im Rahmen von zukünftigen Ausschreibungen im Programm IKT der Zukunft bzw. auch der Sicherheitsforschung gefördert werden sollen, ausgesprochen (hellblaue Boxen im Text). Hinzu kommen an die rund 70 ausformulierten Forschungsfragen für die beschriebenen Forschungsfelder in Kapitel 5, die es kurz- mittel, aber auch langfristig zu beantworten gilt. Ebenso leiten sich Forschungsschwerpunkte aus den Kapiteln 7.1 und 7.2 (Tabelle 5) ab. All diese Empfehlungen, Forschungsfragen und Schwerpunkte werden hier im Wesentlichen zusammengefasst (vgl. Abbildung 17). Dabei ist zu beachten, die Grenzen der unten beschriebenen Forschungsschwerpunkte sind verschwommen und mit Überschneidungen ist zu rechnen, was darauf zurückzuführen ist, dass IKT-Sicherheit ein interdisziplinäres Forschungsfeld ist, das die Zusammenarbeit unterschiedlicher Akteure (siehe oben) aus verschiedenen Disziplinen wie Technik, Sicherheit, Recht, Soziologie, Kriminologie und Wirtschaft erfordert.

Fokus auf die Entwicklung sicherer technischer Lösungen wie Applikationen, Software, Hardware und Netzwerke unter Berücksichtigung von Security by Design, Secure Engineering und die Durchführung von Technologiefolgeabschätzung.

Es wird empfohlen in Österreich Projekte zu fördern, welche die sichere Verwendung von Emerging Technologies ermöglichen. Ein Forschungsschwerpunkt ist die Entwicklung technischer Lösungen im Sinne von Security by Design mit unterschiedlichem technology readyness level, d.h. von der Grundlagenforschung über die Konzeption, Demonstration, bis hin zu prototypischen Lösungen und Implementierung am Markt in enger Zusammenarbeit mit KMUs oder start-up Unternehmen. Forschungsprojekte im Technologiebereich sollten verpflichtend eine Komponente zur Technikfolgenabschätzung enthalten, die schon – wie auch die Komponenten Privacy und Security by Design – im Förderantrag zu beschreiben ist. Angesprochen sind vor allem Forschungsfelder rund um sichere Software Security Engineering, Secure Coding, Software Security Testing und Assurance, die Entwicklung sicherer Hardware und die Bekämpfung von Schadsoftware über alle Technologien hinweg.

Unmittelbarer Handlungsbedarf besteht bei den kurzfristigen Technologieinnovationen in den nächsten ein bis zwei Jahren rund um Big Data, Cloud Computing, vernetzte Gesellschaft, und Mobile Devices. Bei den letzten drei Technologien sind zusätzliche Forschungsschwerpunkte mit hoher Priorität die Bekämpfung von Botnetzen und Self-healing bzw. Self-Protection. Speziell im Bereich Cloud sind zusätzliche relevante Forschungsfelder Intelligence Driven Network Security, sichere Netzwerkprotokolle und Software Defined Network Security. Bei den mobilen Geräten sind zusätzliche Forschungsfelder gehärtete Betriebssysteme, Sicherheit von Firmware und eingebetteter Systeme und sichere Netzwerkprotokolle.

Mittelfristige Technologieinnovationen für die kommenden zwei bis sechs Jahre sind Netzwerkvirtualisierung, Internet der Dinge, Augmented Reality und cyber-physikalische Systeme, wobei v.a. letztere viel F&E Potential in einer Vielzahl an Anwendungsbereichen wie AAL, vernetzte Sicherheits- und Fahrassistenzsysteme für Automobile, industrielle Prozesssteuerungs- und Automationssysteme, Energieversorgungsmanagementsysteme, etc. bieten. Cyber-physikalische Systeme sind zusätzlich zu den oben hervorgehobenen Forschungsfeldern (Software Security Engineering, sichere Hardware, die Bekämpfung von Schadsoftware und Privacy by Design) eng mit den Forschungsfeldern gehärtete Betriebssysteme, Bekämpfung von Botnetzen, Sicherheit von Systemen in fremden Umgebungen, sichere Netzwerkprotokolle, Software Defined Networks Security und Self-healing bzw. Self-protection verknüpft.

Langfristige Technologieinnovationen sind zwar noch sehr weit von der tatsächlichen Umsetzung entfernt, dennoch gibt es hier zum Teil schon bedeutende

Forschungsbewegungen rund um Quantenrechner, Robotics und Cybernetics. (Vgl. Abbildung 14 und Tabelle 5)

Gefördert werden sollen sowohl Technologieprojekte aus der Ursachenforschung, der Prävention, der laufenden Beobachtung (Monitoring), als auch Projekte zur raschen und effizienten Reaktion auf Bedrohungen.

Fokus auf Technologieentwicklungen zur Prävention von Gefahren und auf laufendes Monitoring mittels moderner Analyse- und Visualisierungstechniken sowie Verfahren zur Risikobewertung und -management.

Das rechtzeitige Erkennen von Risiken, Risikobewertung und -Management zur Durchführung präventiver Maßnahmen sind zu fördern. Dazu sollen Projekte durchgeführt werden, die Beschreibungs-, Analyse- und Visualisierungstechniken sowie Bewertungsmodelle für Risiken entwickeln. Kennzahlen, Kriterien, bzw. Indikatoren sollen entwickelt werden, die Aufschluss über die Sicherheit bestimmter Technologien, z.B. beim Einsatz in Unternehmen, geben. Gefördert werden sollten zudem Projekte zu neuen Verschlüsselungskonzepten der Kryptographie, zur Ursachenanalyse von Zwischenfällen (digitale Forensik), zur Früherkennung von Schadprogrammen, zur Sicherheitsanalyse und Risikoeinschätzung von komplexem Systemen unter Einbezug verschiedener Geräte (z.B. mobile Endgeräte), zur Unterstützung von Sicherheitsframeworks und sicheren Entwicklungswerkzeugen, zur sicheren Entwicklung von Software und zum Aufdecken von Schwachstellen, der Netzwerkanalyse und damit verbundene Frühwarnsysteme. Präventive Maßnahmen und Monitoring sind als Teil langfristiger Strategieentwicklung zu verstehen und haben kurz-, mittel- und langfristig eine sehr hohe Priorität (vgl. Tabelle 5).

Fokus auf Notfallmanagement und rasche Reaktion in Ausnahmesituationen wie Cyberangriffen oder Systemausfällen, durch sichere und vertrauliche Kommunikation und effiziente Notfallpläne.

Es wird empfohlen Projekte zu fördern, die den schnellen und effizienten Umgang mit Gefahren und Bedrohungen (Notfallsituationen), durch Verarbeitung von Informationen in Echtzeit erkennen. Relevant ist das zum Beispiel im Fall von Cyberangriffen wie Phishing, Betrug, Cyberstalking etc. und die damit verbundene Verletzung der Privatsphäre. Darüber hinaus wird eine tiefere Auseinandersetzung mit der Bekämpfung von Schadprogrammen, der raschen Aufdeckung von Schwachstellen, der Analyse von Angriffen und deren Folgen/Auswirkungen auf die Infrastruktur (Netzwerk, Betriebssystem und Applikationen) vorgeschlagen. Es sollten in Österreich Projekte gefördert werden, die sich mit Infrastruktur und Technologien für sichere und vertrauliche Kommunikation im Notfallszenario, mit der

Erstellung und Erprobung von Notfallplänen für Notfallszenarien und dem Austausch sicherheitsrelevanter Informationen im Bedrohungsfall beschäftigen. Im Idealfall sind präventive Maßnahmen so ausgereift, dass Notfällen vorgebeugt wird. In der Realität sind wir jedoch mit Notfällen in der IKT-Sicherheit konfrontiert, weshalb das Forschungsfeld Risiko- und Notfallmanagement vor allem kurzfristig hohe Priorität hat. Betroffen sind speziell die Technologiebereiche Cloud, mobile Lösungen, Netzwerkvirtualisierung und cyber-physikalische Systeme (vgl. Tabelle 5).

Fokus auf Datensicherheit, Schutz der Privatsphäre und der digitalen Identität durch die Anwendung des "Privacy by Design"-Ansatzes und unter Berücksichtigung von Sicherheit, Zuverlässigkeit, Rechtmäßigkeit und NutzerInnenfreundlichkeit.

Wesentliche Aspekte sind die Datensicherheit, der Schutz der digitalen Identität und der Privatsphäre aus technischer Perspektive sowie Privacy by Design mit der Zielsetzung einer angemessenen Balance aus Sicherheit, Zuverlässigkeit, Rechtmäßigkeit und NutzerInnenfreundlichkeit. Unter Privacy by Design werden Sicherheitsaspekte im Umgang mit personenbezogenen Daten verstanden, die in der Softwareentwicklung von Beginn an einfließen und bereits Teil der Anforderungsanalyse sein müssen. Dennoch sollen Forschung und Entwicklung dringend erschließen, welche genauen Möglichkeiten und Grenzen Privacy by Design im Hinblick auf die Risiken, allen voran in den Technologiebereichen Big Data, soziale Netzwerke, Cloud, Mobile Devices, Augmented Reality und zum Teil auch cyber-physikalische Systeme und IoT bietet. „Daten an die Leine legen“, also die Nutzung eigener Daten durch Dritte mitverfolgen und nachvollziehen können, ist ein wesentliches Ziel im Bereich Datensicherheit und bedarf langfristig orientierter Grundlagenforschung. Dabei sind Forschungsfelder im Bereich von Verschlüsselungstechnologien, das Rechnen und Suchen in verschlüsselten Daten, Pseudonymisierung/Anonymisierung, Data Leakage/Loss Protection, Identitätsmanagement und Privacy Impact Assessment sowie generelle grundrechtliche und ethische Auseinandersetzungen beim Umgang mit Daten gefragt. Das Thema Datensicherheit ist eng verknüpft mit technischen und rechtlichen Aspekten, wird stark von ökonomischen Modellen beeinflusst und wird uns auf jeden Fall kurz- und mittelfristig beschäftigen. (vgl. Tabelle 5)

Fokus auf die grundlegende Erforschung der Motive Cyberkrimineller unter besonderer Berücksichtigung ökonomischer Modelle krimineller Handlungen.

Ergänzend zu einer soweit eher technischen Herangehensweise wird empfohlen, in einem sozioökonomischen Schwerpunkt die Motive von Cyberkriminellen zu erforschen. Hier sind v.a. ökonomische Modelle des zum Teil lukrativen Geschäftsfeldes "Cyberkriminalität" näher

zu beleuchten, um AngreiferInnen besser zu verstehen und geeignete Gegenmaßnahmen bzw. präventive Maßnahmen über alle Technologieschwerpunkte hinweg setzen zu können. Generell sollten interdisziplinäre Projekte gefördert werden, welche Fachwissen der Technik, Sicherheit, Wirtschaft, Soziologie und Kriminologie verbinden, z.B. im Forschungsbereich der Sicherheitsökonomie & -kennzahlen (vgl. Tabelle 5). Da sich die Formen, Motive und Muster Cyberkrimineller genauso schnell ändern wie Technologien selbst, bedarf es einer kurz-, mittel- und langfristigen Betrachtung.

Fokus auf rechtliche Rahmenbedingungen und die Erarbeitung von Richtlinien, Referenzmodellen und Standards in der IKT-Sicherheit und von Verfahren zur Überprüfung deren Einhaltung.

Generell sollte ein wesentlicher Forschungsschwerpunkt auf den rechtlichen Rahmenbedingungen liegen. Zu nennen sind zum Beispiel die Entwicklung von Datenschutz-Zertifizierungen für Organisationen und die Entwicklung von neuen, der österreichischen Rechtslage entsprechenden (Informations)sicherheitsstandards und von Verfahren zur Überprüfung deren Einhaltung. Interdisziplinäre Forschungsansätze aus Recht und Technik. z.B. Pseudonymisierung/Anonymisierung, Data Leakage/Loss Protection, Identitätsmanagement und Privacy Impact Assessment sowie generelle grundrechtliche und ethische Auseinandersetzungen, sollen dabei gefördert werden.

Projekte, welche speziell dem Schutz von Daten und der Privatsphäre aus rechtlicher Sicht dienen, erscheinen förderwürdig. Im Bereich des Datenschutzes sind das Projekte, die sich spezifisch mit den Gründen der unzureichenden Rechtsdurchsetzung im Datenschutzrecht beschäftigen. Im Bereich des Schutzes der Privatsphäre sind zum Beispiel Projekte notwendig, welche die Verhältnismäßigkeit betrieblicher Kontrollmaßnahmen zum Schutz der betrieblichen IT-Sicherheit gegenüber dem Recht der ArbeitnehmerInnen auf Schutz personenbezogener Daten (ArbeitnehmerInnendatenschutz) untersuchen und wahren. Durch die Ergebnisse der Projekte sollen Möglichkeiten geschaffen werden, kurz-, mittel-, bzw. langfristig aufkommende Technologien unter Berücksichtigung der Privatsphäre nutzbar zu machen. Beispiele sind Big Data Analysen, oder der sichere Umgang mit sozialen Medien, der Cloud, Augmented Reality Anwendungen, cyber-physikalischen Systemen und IoT Applikationen unter Einhaltung der Privatsphäre (vgl. Tabelle 5). Auch die Integration privater Endgeräte in eine betriebliche IT-Infrastruktur verlangt eine Auseinandersetzung. Interessant sind dabei Projekte, welche Fragen adressieren, die sich unternehmens- und branchenübergreifend im Zusammenhang mit "bring your own device" stellen.

Im Bereich der Sicherheitsstandards wird empfohlen, eine Studie anzufertigen, welche die vorhandenen Standards von Systemen am internationalen und österreichischen Markt

aufzeigt. Die Studie muss auch Informationen über Schwachstellen liefern und Hinweise darauf, wo weitere Akzente gesetzt werden können. Es wird nahegelegt, Projekte umzusetzen, deren Ziel die Erarbeitung praxisorientierter Leitfäden, Checklisten, Mustervertragsklauseln und Referenzmodelle ist. Diese können insbesondere im Bereich intelligente Produktionssysteme („Industrie 4.0“), in der Technologiefolgenabschätzung oder der Risikobewertung Anwendung finden und könnten vor allem für KMUs ohne eigene Rechtsabteilung eine große Hilfestellung beim Vollzug der für Österreich zukunftssichernden vierten industriellen Revolution von Vorteil sein.

Es wird angeregt, bereits bei der Ausschreibung neuer Forschungsvorhaben auf Standard-Unterstützung zu achten. Dies kann entweder aktiv durch die Einforderung einer Beschreibung bei der Einreichung, oder passiv durch bessere Gewichtung von Projekten, welche auf offene, standardisierte Systeme setzen, geschehen.

Fokus auf die Wissensvermittlung, Stärkung des Sicherheitsbewusstseins und Erhöhung der Akzeptanz von Sicherheitslösungen innerhalb des ExpertInnenkreises und in der breiten Bevölkerung durch innovative Lernkonzepte.

Ein abschließender abzudeckender Forschungsschwerpunkt ist Usable Security (vgl. Tabelle 5), also die Schaffung benutzerInnenfreundlicher Sicherheitsmechanismen, da ohne Wissen über mögliche Gefahren, ohne Sicherheitsbewusstsein und ohne Akzeptanz von Sicherheitslösungen kein ausreichender Schutz erreicht werden kann. Zielsetzung muss die Stärkung des Risikobewusstseins sowie der digitalen Medienkompetenz auf Seiten der NutzerInnen von unterschiedlichsten IKT-Systemen sein.

Dies schließt die Evaluierung und gegebenenfalls die Optimierung der Usability bestehender Sicherheitslösungen (Authentifizierungsmechanismen, NutzerInnenvereinbarungen, Privacy Agreements, etc.) ein. Die Entwicklung alternativer Authentifizierungsmechanismen mit hoher Benutzerfreundlichkeit und Akzeptanz soll nicht nur Unternehmen, sondern auch die österreichische Bevölkerung generell besser schützen. Projekte, welche sich damit beschäftigen, wie Anreize für BenutzerInnen und Unternehmen geschaffen werden können, um in Sicherheit zu investieren, sollten durchgeführt werden. Ein Know-how-Aufbau wird v.a. rund um die kurzfristigen Technologieinnovationen empfohlen, d.h. im Bereich verteilte Systeme (Cloud), soziale Netzwerke, mobile Lösungen und Big Data sowie im Bereich der cyber-physikalischen Systeme betreffend die Anwendungsfelder AAL, vernetzte Sicherheits- und Fahrassistenzsysteme für Automobile, industrielle Prozesssteuerungs- und Automationssysteme und Energieversorgungsmanagementsysteme, da hier bereits ein breiter NutzerInnenkreis erreicht wurde. Forschungsfragen betreffen auch den Informationsaustausch, z.B. um ein umfassendes Lagebild komplexer, hochdynamischer

Systeme zu erhalten, bzw. zum effizienten Austausch von Informationen im Notfall. Das bestehende und neu zu erwerbende ExpertInnenwissen soll anhand innovativer Lernkonzepte in Kursen und Disseminierungsworkshops für interessierte TeilnehmerInnen bereitgestellt werden.

8 Literaturverzeichnis

ABC News, 2014. Shellshock: Bash software bug leaves up to 500 million computers at risk of hacking, abc.net vom 26.09.2014, http://www.abc.net.au/news/2014-09-26/shellshock-bug-leaves-up-to-500-million-computers-at-risk/5770952 (abgerufen am 15.12.2015).

ACATECH – Deutsche Akademie der Technikwissenschaften, 2013. Umsetzungsempfehlungen Industrie 4.0., http://www.bmbf.de/pubRD/Umsetzungsempfehlungen_Industrie4_0.pdf (abgerufen am 15.12.2015).

Aigner, F., 2013. Industrie 4.0, Presseaussendung 59/2013 der TU Wien vom 03.07.2013, https://www.tuwien.ac.at/aktuelles/news_detail/article/8293/ abgerufen am 15.12.2015).

AFOR, 2008. Studie zu digitaler Forensik: Erfordernisse der Beweissicherung und Möglichkeiten der Verknüpfung von Daten, http://www.kiras.at/gefoerderte-projekte/detail/?tx_ttnews[tt_news]=258&cHash=6402d16f1f01a43d8726265ff0a510f0 (abgerufen am 15.12.2015).

Ahokangas, M., et al., 2014. Strategic Research Agenda for Cyber Trust, www.digitale.fi (abgerufen am 15.12.2015).

Antilope Projekt Webseite, http://www.antilope-project.eu/ (abgerufen am 11.3.2015).

Asimo Webseite, http://asimo.honda.com/ (abgerufen am 15.12.2015).

A-SIT, 2013. Übersicht über das Angebot an österreichischen Fachhochschulen und Universitäten, https://www.onlinesicherheit.gv.at/generation_60plus/rat_und_hilfe/bildung/ausbildung_an_universitaeten_und_fachhochschulen/74509.html (abgerufen am 16.10.2015).

Aspern Smart City Research Webseite, http://www.ascr.at (abgerufen am 14.10.2015).

Bencsáth, B., Pék, G., Buttyán, L., Félegyházi, M., 2012. The Cousins of Stuxnet: Duqu, Flame, and Gauss.

BITKOM, 2011. Enterprise Architecture Management – neue Disziplin für die ganzheitliche Unternehmensentwicklung, http://www.bitkom.org/files/documents/EAM_Enterprise_Architecture_Management_-_BITKOM_Leitfaden.pdf (abgerufen am 14.10.2015).

Bos, H., Etalle, S., Poll, E., 2014. National Cyber Security Research Agenda - Trust and Security for our Digital Life v 1.2.

Bos, H., Etalle, S., Fransen, F., Poll, E., 2013. National Cyber Security Research Agenda II.

Bridge, C., 2009. Enhancing Research into Usable Privacy and Security, Proceedings of the 27th ACM International Conference on Design of Communication, SIGDOC, S. 221-226.

Brown, T., 2015. Design Thinking - Thoughts by Tim Brown, http://designthinking.ideo.com (abgerufen am 14.10.2015).

Bundesamt für Sicherheit in der Informationssicherheit, 2013. Fokus IT-Sicherheit, Bonn.

Bundesamt für Sicherheit in der Informationssicherheit, 2014. Die Lage der IT-Sicherheit in Deutschland, Bonn.

Bundesamt für Sicherheit in der Informationssicherheit, o.J., BSI für Bürger, Drive-by-Exploits, Bonn.

Bundesamt für Sicherheit in der Informationstechnologie, 2006. Mobile Endgeräte und mobile Applikationen: Sicherheitsgefährdungen und Schutzmaßnahmen, Bonn.

Bundesamt für Sicherheit in der Informationstechnik, 2014. Industrial Control System Security - Top 10 Bedrohungen und Gegenmaßnahmen 2014, Bonn.

Bundeskriminalamt Österreich, 2014. Cybercrime 2014: Zahlen, Initiativen, Projekte 2014, Trends 2015.

Byres, E., 2013. Privacy and security the air gap: SCADA's Enduring Security Myth.

Cameron, K., 2005. The Laws of Identity, http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf (abgerufen am 14.10.2015).

Center for Automotive Embedded System Security Webseite, http://www.autosec.org/publications.html (abgerufen am 13.10.2015).

CERT.at, 2014. Schweres Sicherheitsproblem mit OpenSSL ("Heartbleed"-Lücke), cert.at vom 08.04.2014. https://www.cert.at/warnings/all/20140408.html (abgerufen am 14.11.2015).

CERT, 2014. Jahresbericht 2014, https://www.cert.at/static/downloads/reports/cert.at-jahresbericht-2014.pdf (abgerufen am 14.11.2015).

Chief Information Office - Stabsstelle IKT-Strategie des Bundes (Hrsg.), 2013. Österreichisches Informationssicherheitshandbuch, Version 4, https://www.sicherheitshandbuch.gv.at/ (abgerufen am 08.12.2015).

Cisco, 2014. Visual Networking Index: Forecast and Methodology 2013–2018, http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.html (abgerufen am 14.10.2015).

Cloud Security Alliance, 2012. Top Ten Big Data Security And Privacy Challenges, Cloud Security Alliance (CSA).

Conforti, R., Fortino, G., Rosa, M. L., and Hofstede, A. H. T., 2011. History-Aware, Real-Time Risk Detection in Business Processes, in: On the Move to Meaningful Internet Systems: OTM 2011, Crete, Greece.

Council of Europe, 2013. Convention on Cybercrime. CETS No. 185, http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 (abgerufen am 23.11.2015).

Cox, L., 2010. Software aims to prevent crime. MIT Technology Review, http://www.technologyreview.com/news/422008/software-aims-to-prevent-crime/ (abgerufen am 14.10.2015).

Curry, S., Kirda. E., Schwartz, E., Stewart, W. H. und Yoran, A., 2013. Big Data Fuels Intelligence Driven Security, RSA / EMC.

Cyberspace Policy Review, o.J. Assuring a Trusted and Resilient Information and Communications Infrastructure, S. vi u. 37, Action Item 3, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (abgerufen am 14.10.2015).

Damien, G., 2013. Facebook is the worst social network for bullying with 19-year-old BOYS the most common victims, Mail Online vom 15.03.2013, http://www.dailymail.co.uk/sciencetech/article-2294023/Facebook-worst-social-network-bullying-New-survey-shows-youngsters-targeted-online-else.html (abgerufen am 14.10.2015).

Degelsegger, A., Torgersen, H., 2011. Participatory paternalism: citizens' conferences in Austrian technology governance. In: Sci. and Pub. Pol 38 (5), S. 391–402.

Deutsche Bundesregierung, 2012. Zukunftsprojekte der Hightech-Strategie (HTS Aktionsplan), http://www.bmbf.de/pub/HTS-Aktionsplan.pdf (abgerufen am 25.8.2014).

Deutsches Bundesministerium für Bildung und Forschung, 2013. Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0: Abschlussbericht des Arbeitskreises Industrie 4.0, https://www.bmbf.de/files/Umsetzungsempfehlungen_Industrie4_0.pdf (abgerufen am 25.8.2014).

Dohr, W., Pollirer, H. J., Weiss, E., Knyrim, R., 2013. DSG online - Kommentar zum Datenschutzrecht, Manz, Wien.

Dornmayr, H., 2012. Kurzfassung des ibw-Forschungsberichts Nr. 170, IT-Qualifikationen 2025 – Analysen zu Angebot und Nachfrage, Wien, http://www.ibw.at/de/ibw-studien/1-studien/fb170/P580-it-qualifikationen-2025-2012 (abgerufen am 16.10.2015).

dosomething.org Webseite, 11 Facts about Cyber Bullying, https://www.dosomething.org/facts/11-facts-about-cyber-bullying (abgerufen am 25.8.2014).

Drucker, W., 2015a. Industrie 4.0: der lange Weg zur Pilotfabrik, Wirtschaftsblatt vom 25.08.2015, http://wirtschaftsblatt.at/home/nachrichten/oesterreich/4805728/Industrie-40_Der-lange-Weg-zur-Pilotfabrik (abgerufen am 23.09.2014).

Drucker, W., 2015b. Industrie 4.0 bleibt für österreichische Betriebe ein Fremdwort, Wirtschaftsblatt vom 10.04.2015, http://wirtschaftsblatt.at/home/nachrichten/oesterreich/4704603/Industrie-40-bleibt-fur-osterreichische-Betriebe-ein-Fremdwort (abgerufen am 23.09.2014).

Eckert, C., 2013. IT-Sicherheit: Konzepte-Verfahren-Protokolle, 8., aktualisierte und korrigierte Auflage, München: Oldenbourg Verlag.

Egelman, S., Cranor, L.F. und Hong, J., 2008. You've been warned: an empirical study of the effectiveness of web browser, phishing warnings, in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.

Energiesysteme der Zukunft Webseite, http://www.energiesystemederzukunft.at (abgerufen am 14.10.2015).

ENISA, 2014. Privacy and Data Protection by Design – from policy to engineering, https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design/at_download/fullReport (abgerufen am 06.08.2015).

Europe vs. Facebook, http://www.europe-v-facebook.org/ (abgerufen am 23.01.2016).

European Commission, Robotics Webseite, http://ec.europa.eu/programmes/horizon2020/en/h2020-section/robotics (abgerufen am 23.01.2016).

Europäische Kommission, 2013. Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0048:FIN:EN:PDF (abgerufen am 19.11.2015).

Europäische Kommission, 2010. Special Eurobarometer 340: Science and Technology Report.

Europäische Kommission, 2005. Special Eurobarometer 224: Europeans, Science and Technology.

Europäisches Parlament, 2012. COM (2012) 11: Vorschlag für VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), http://eur-lex.europa.eu/procedure/DE/201286 (abgerufen am 13.01.2016).

European Union Agency for Fundamental Rights (FRA), 2014. Access to data protection remedies in EU Member States, http://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states (abgerufen am 11.3.2015).

EUROPOL, 2014. The Internet Organised Crime Threat Assessment (iOCTA).

EuroPriSe Webseite. The European Privacy Seal for IT Products and IT-Based Services, https://www.european-privacy-seal.eu/ws/EPS-en/Home (abgerufen am 23.01.2016).

Factory, 2014. Industrie 4.0 - Österreich unter Zugzwang vom 12.05.2014, http://www.factorynet.at/home/artikel/Industrie_4.0/Oesterreich_unter_Zugzwang/aid/23585?analytics_from=archiv (abgerufen am 25.8.2014).

Felser, R., 2015. Carbanak: Der größte Online-Bankraub aller Zeiten, Computerwelt vom 16.02.2015, http://www.computerwelt.at/news/technologie-strategie/security/detail/artikel/109844-carbanak-der-groesste-online-bankraub-aller-zeiten/ (abgerufen am 23.01.2016).

Felser, R. 2014. 250 Mio. Euro für Industrie 4.0 in Österreich, Computerwelt vom 23.8.2014, http://www.computerwelt.at/news/wirtschaft-politik/unternehmen/detail/artikel/105637-250-mio-euro-fuer-industrie-40-in-oesterreich/ (abgerufen am 25.8.2014).

Felt, U., Fochler, M., 2010. Machineries for Making Publics: Inscribing and Describing Publics in Public Engagement, Minerva 48/3, 219-238.

Felt, U., Fochler, M., 2008. The Bottom-up Meanings of the Concept of Public Participation in Science and Technology. In: Science and Public Policy 35 (7), S. 489–499.

Felt, U., Fochler, M., Müller, A., 2006. Sozial robuste Wissenspolitik? Analyse partizipativ orientierter Interaktionen zwischen Wissenschaft, Politik und Öffentlichkeit im österreichischen Kontext. In: U. Felt und E. Buchinger (Hrsg.): Technik und Wissenschaftssoziologie in Österreich. Stand und Perspektiven. Wien: Verlag für Sozialwissenschaften.

Fercher, N., 2009. Innerbetriebliche Kontrollmaßnahmen und Datenschutz im Arbeitsrecht, S. 9.

Fochler, M., Müller, A., 2006. Vom Defizit zum Dialog? Zum Verhältnis von Wissenschaft und Öffentlichkeit in der europäischen und österreichischen Forschungspolitik (ITA Manuskripte, 06/04).

Fraunhofer Austria Webseite, http://www.fraunhofer.at/de/pl/leistungsspektrum/industrie_4_0.html (abgerufen am 25.8.2014).

Fraunhofer, Cyber-Physical Systems Webseite, https://www.sit.fraunhofer.de/de/cyberphysicalsystems/ (abgerufen am 23.01.2016).

F-Secure Webseite, 2014. Police-themed' ransomware - what is ransomware, http://www2.f-secure.com/en/web/labs_global/removing-police-themed-ransomware (abgerufen am 23.01.2016).

FutureID Shaping the Future of Electronic Identity Webseite, http://www.futureid.eu/ (abgerufen am 27.01.2016).

FutureZone, 2012. Spam-Botnetz auf Android-Basis entdeckt, 05.07.2012, http://futurezone.at/digital-life/spam-botnetz-auf-android-basis-entdeckt/24.581.833 (abgerufen am 27.01.2016).

Gantz, J. F., et al., 2014. The Link between Pirated Software and Cybersecurity Breaches How Malware in Pirated Software Is Costing the World Billions, IDC#247411.

Geisberger, E., Broy, M., o.J. Integrierte Forschungsagenda Cyber-Physical Systems.

Gerichtshof der Europäischen Union, 2014. Pressemitteilung Nr. 70/14, http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070de.pdf (abgerufen am 14.8.2014).

Goodwin, G., 2013. Takeaways from the MIT/Accenture Big Data in Manufacturing Conference, LNS Research, 27 November 2013, http://blog.lnsresearch.com/blog/bid/190482/Takeaways-from-the-MIT-Accenture-Big-Data-in-Manufacturing-Conference (abgerufen am 03.11.2014).

GovCert Austria Webseite, http://www.govcert.gv.at/index.html (abgerufen am 29.10.2015).

Gragido, W., 2012. Lions at the Watering Hole – The “VOHO” Affair, RSA Security, https://blogs.rsa.com/lions-at-the-watering-hole-the-voho-affair/ (abgerufen am 27.01.2016).

Griessler, E., 2012. One size fits all? On the institutionalization of participatory technology assessment and its interconnection with national ways of policy-making: the cases of Switzerland and Austria. In: Poiesis Prax 9 (1-2), S. 61–80.

Heinze, R., 2014. Cyber-Physical Systems als Basis für Industrie 4.0, ftp://ftp.ni.com/pub/branches/germany/2014/artikel/03-march/17_cyber_physical_systems_als_basis_fuer_industrie_4.0_ronald_heinze_etz_1-2014.pdf (abgerufen am 02.02.2016).

Henkel, C. H., 2014. Suche nach der Steuerung von Icann: Die USA lockern Kontrolle über das Internet. Neue Zürcher Zeitung vom 17.03.2014. http://www.nzz.ch/wirtschaft/wirtschafts-und-finanzportal/die-usa-lockern-ihre-kontrolle-ueber-das-world-wide-web-1.18264234 (abgerufen am 11.08.2014).

Honeywell, 2012. Users Group Asia Pacific - Industrial Control System Cyber Security.

Hope, C., 2013. Facebook is a 'major location for online child sexual grooming', head of child protection agency says, The Telegraph vom 15.10.2013, http://www.telegraph.co.uk/technology/facebook/10380631/Facebook-is-a-major-location-for-online-child-sexual-grooming-head-of-child-protection-agency-says.html (abgerufen am 02.02.2016).

Huckle, T., 2015. Collection of Software Bugs, http://www5.in.tum.de/~huckle/bugse.html (abgerufen am 02.02.2016).

Hutchins E. M., et al., o.J. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf (abgerufen am 02.02.2016).

IDC, 2015a. Austria IT Services Market 2015–2019 Forecast and 2014 Analysis.

IDC, 2015b. Western Europe Security Software 2014–2018 Forecast.

IDC, 2015c. IDC's Worldwide IT Cloud Services Taxonomy.

IDC, 2015d. Austria Cloud Services Market 2015–2019 Forecast and 2014 Analysis.

IDC, 2014a. Western Europe 2013 Security Services Market and 2014-2018 Forecast.

IDC, 2014b. Press Release: Smartphone Momentum Still Evident with Shipments Expected to Reach 1.2 Billion in 2014 and Growing 23.1% Over 2013, 28 Mai 2014, http://www.idc.com/getdoc.jsp?containerId=prUS24857114 (abgerufen am 02.02.2016).

IDC, 2014c. Worldwide Software-Defined Networking Market Expected to Reach $8 Billion by 2018, press release on 20.08.2014, https://www.idc.com/getdoc.jsp?containerId=prUS25052314 (abgerufen am 02.02.2016).

IDC Event, 2015, http://www.cvent.com/events/idc-directions-industrie-4-0-2015-germany/event-summary-16282e14ec1447d18f35f1a22781026b.aspx (abgerufen am 02.02.2016).

International Cyber Security Protection Alliance, 2013. EUROPOL EC3, Project 2020 Scenarios for the Future of Cybercrime - White Paper for Decision Makers, https://www.europol.europa.eu/content/project-2020-scenarios-future-cybercrime (abgerufen am 02.02.2016).

Internet Live Stats, 2014. Google Search Statistics vom 22.11.2014, http://www.internetlivestats.com/google-search-statistics/ (abgerufen am 22.11.2014).

Irwin, A.,1995. Citizen science - A study of people, expertise and sustainable development. London: Routledge.

Jasanoff, S., 2003. Technologies of humility: Citizen participation in governing science. In: Minerva 41, S. 223–244.

Jasanoff, S., 2006. The idiom of co-production. In: Sheila Jasanoff (Hrsg.): States of Knowledge: The Co-Production of Science and the Social Order: Routledge, S. 1–12.

Kammer der Wirtschaftstreuhänder, 2014. Fachgutachten der Kammer der Wirtschaftstreuhänder über Abschlussprüfung bei Einsatz von Informationstechnik vom 20. Oktober 2004,

http://www.kwt.or.at/de/PortalData/2/Resources/downloads/downloadcenter/53-KFS-DV2.pdf (abgerufen am 10.02.2015).

Kammer der Wirtschaftstreuhänder, 2011. Fachgutachten der Kammer der Wirtschaftstreuhänder über die Ordnungsmäßigkeit von IT-Buchführungen vom 20. März 2011, http://www.kwt.or.at/de/PortalData/2/Resources/downloads/downloadcenter/52-KFS-DV1.pdf (abgerufen am 10.02.2015).

Kannenberg, A., 2014. Internet of Things: Mein Kühlschrank als Spammer, Heise online am 17.01.2014, http://www.heise.de/newsticker/meldung/Internet-of-Things-Mein-Kuehlschrank-als-Spammer-2088336.html (abgerufen am 02.02.2016).

Kaspersky, 2014. Global IT Risks Report, http://media.kaspersky.com/en/business-security/Global-IT-Risks-Report-2014-Threat-Security-Data-Breaches.pdf (abgerufen am 02.02.2016).

Kearney, A.T., 2013. Big Data and the Creative Destruction of Today's Business Models, http://www.atkearney.com/strategic-it/ideas-insights/article/-/asset_publisher/LCcgOeS4t85g/content/big-data-and-the-creative-destruction-of-today-s-business-models/10192#stha (abgerufen am 02.02.2016).

Keßler, M., 2013. Internet der Dinge hat Startschwierigkeiten, Futurezone vom 17.05.2013, http://futurezone.at/digital-life/internet-der-dinge-hat-startschwierigkeiten/24.596.097 (abgerufen am 17.05.2013).

King, S. T., et al., 2008. Designing and implementing malicious hardware, USENIX LEET, https://www.usenix.org/legacy/event/leet08/tech/full_papers/king/king.pdf (abgerufen am 02.02.2016).

Klasnja, P., Consolvo, S., Jung, J., Greenstein, B.M., LeGrand, L., Powledge, P. and Wetherall, D., 2009. When I am on Wi-Fi, I am fearless: privacy concerns & practices in everyday Wi-Fi use, in 27th International conference on Human factors in computing systems.

Kotschy, W., Reimer, S., 2004. Die Überwachung der Internet-Kommunikation am Arbeitsplatz, ZAS 2004/29.

Köhler, M., Meir-Huber, M., 2014. #Big Data in #Austria: Österreichische Potenziale und Best Practice für Big Data.

KrebsonSecurity, 2012. The Scrap Value of a Hacked PC, Revisited am 12.10.2012, http://krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/ (abgerufen am 02.02.2016).

Lehofer, P., 2014. EuGH: Google muss doch vergessen - das Supergrundrecht auf Datenschutz und die Bowdlerisierung des Internets, Blog zum österreichischen und europäischen Recht der elektronischen Kommunikationsnetze und –dienste, Blog vom 13.05.2014 http://blog.lehofer.at/2014/05/eugh-google-muss-doch-vergessen-das.html (abgerufen am 14.8.2014).

LeTrent, S., 2014. Twist and shout: NASA prints 3-D wrench in space, CNN am 19.12.2014, http://edition.cnn.com/2014/12/19/tech/feat-3d-wrench-nasa/ (abgerufen am 02.02.2016).

Lévy-Leblond, J. M., 1992. About misunderstandings about misunderstandings. In: Public Understanding of Science 1 (1), S. 17–21.

Loske, A., Widjaja, T., Buxmann, P., 2013. Cloud Computing Providers' Unrealistic Optimism regarding IT Security Risks: A Threat to Users? International Conference on Information Systems (ICIS).

Loskyll, M., 2013. Industrie 4.0 - Kernparadigmen der vierten industriellen Revolution, MC-report - Informationen aus dem Mechatronik-Cluster, Ausgabe 3/2013, http://www.mechatronik-cluster.at/files/MC_Report_03_2013.pdf (zuletzt abgerufen am 25.8.2014).

MacGillivray, C., et al., 2015. IDC's Worldwide Internet of Things Taxonomy.

Marinos, L., 2014. ENISA Threat Landscape 2014 - Overview of current and emerging cyber-threats.

Markatos, E.; Balzarotti, D., Athanasopoulos, E., et al., 2013. The Red Book - A Roadmap for Systems Security Research.

Massachusetts Institute of Technology Projektwebseite, bigdata@csail - MIT Big Data Initative, http://bigdata.csail.mit.edu/ (abgerufen am 01.12.2015).

Menn, J., 2015. Russian researchers expose breakthrough U.S. spying program, Reuters am 16.02.2015. http://www.reuters.com/article/2015/02/16/us-usa-cyberspying-idUSKBN0LK1QV20150216 (abgerufen am 14.12.2015).

Messmer, E., 2013. Gartner: Cloud-based security as a service set to take off, Networkworld am 31.10.2013. http://www.networkworld.com/article/2171424/data-breach/gartner--cloud-based-security-as-a-service-set-to-take-off.html (abgerufen am 14.12.2015).

Miller, B.; Rowe, D., 2012. A Survey of SCADA and Critical Infrastructure Incidents.

Mitra et al., o.J. Stopping Hardware Trojans in Their Tracks, http://spectrum.ieee.org/semiconductors/design/stopping-hardware-trojans-in-their-tracks (abgerufen am 14.12.2015).

MITRE, Structured Threat Information Expression Webseite, http://stix.mitre.org/ (abgerufen am 21.01.2016).

Mulliner, C. R., 2006. Security of Smart Phones.

Nadkarni, A., Vesset, D., 2015. IDC's Worldwide Big Data Taxonomy.

National Science Board, 2014. Science and Engineering Indicators 2014. National Science Foundation. Arlington, VA, http://www.nsf.gov/statistics/seind14/ (abgerufen am 20.07.2014)

Neeraj, T., 2013. Botnets Remain a Leading Threat, https://blogs.mcafee.com/business/security-connected/tackling-the-botnet-threat (abgerufen am 14.12.2015).

NIST National Strategy for Trusted Identities in Cyberspace Webseite, http://www.nist.gov/nstic/ (abgerufen am 14.12.2015).

NIST, 2013. Guidelines for managing the security of mobile devices in the enterprise, SP800-124r1.

NIST, 2011. Guide to industrial control systems (ICS) security, 800-82, http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf (abgerufen am 21.01.2016).

Nunes, B.A.A., Mendonca, M., Nguyen, X.-N., Obraczka, K. und Turletti, T., 2014. A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks, IEEE Communications Surveys & Tutorials, pp. 1617-1634.

Open IOC Indicators of Compromise Webseite, http://www.openioc.org/ (abgerufen am 21.01.2016).

Open Networking Foundation, o.J. Software-Defined Networking (SDN) Definition, https://www.opennetworking.org/ja/sdn-resources-ja/sdn-definition (abgerufen am 20.01.2016).

Open Networking Lab (ON.LAB) Webseite, What is SDN, http://onlab.us/what-is-onlab.html#vision (abgerufen am 15.12.2014).

Österreichischen Akademie der Wissenschaften Webseite, http://www.oeaw.ac.at/ita/projekte/europrise/ueberblick (abgerufen am 21.01.2016).

Panda Labs, 2014. Quaterly Report Q3/2014, http://www.pandasecurity.com/mediacenter/src/uploads/2014/11/Quarterly-Report-PandaLabs_Q3.pdf (abgerufen am 21.01.2016).

Payr, S., Werner, F., Werner, K., 2015. Potential of Robotics for Ambient Assisted Living.

Pilar Torres, M., 2014. Comprehensive Approach to Cyber Roadmap Coordination and Development: Main Research Gaps in Cyber Security. Power Point Presentation on 18.09.2014, http://www.dfrc.ch/wp-content/uploads/2014/09/06_Mapi_CAMINO_Main-Research-Gaps-in-Cyber-Security-Research-Bern-18-09-14.pdf (abgerufen am 21.12.2015).

Predpol Webseite, http://www.predpol.com/ (abgerufen am 21.01.2016).

Rack, F., 2013. Cybersicherheit: Richtlinienvorschlag der EU-Kommission vom 20.02.2013 auf Telemedicus Recht der Informationsgesellschaft, http://www.telemedicus.info/article/2521-Cybersicherheit-Richtlinienvorschlag-der-EU-Kommission.html (abgerufen am 21.01.2016).

Reisinger, P., 2015. Informationssicherheit in Deutschland, Österreich und der Schweiz 2015, Diplomarbeit, FH St. Pölten, https://www.fhstp.ac.at/de/mediathek/pdfs/news/diplomarbeit_philippreisinger.pdf/@@download/file/Diplomarbeit_PhilippReisinger.pdf (abgerufen am 13.12.2015).

Rosenbush, S., 2013. Visa Says Big Data Identifies Billions of Dollars in Fraud, The Wall Street Journal vom 11.03.2013, http://blogs.wsj.com/cio/2013/03/11/visa-says-big-data-identifies-billions-of-dollars-in-fraud/ (aufgerufen am 05.11.2014).

Rothmann, R., Sterbik-Lamina, J., Peissl, W., Čas, J., 2012. Aktuelle Fragen der Geodaten-Nutzung auf mobilen Geräten – Endbericht. Bericht-Nr. ITA-PB A63; Institut für Technikfolgen-Abschätzung (ITA): Wien; im Auftrag von: Österreichische Bundesarbeitskammer, http://www.oeaw.ac.at/ita/projekte/geodaten-nutzung-bei-mobilen-geraeten/publikationen/ (abgerufen am 21.12.2015).

Russell, A. W., Vanclay, F. M., Aslin, H. J., 2010. Technology Assessment in Social Context: The case for a new framework for assessing and shaping technological developments. In: Impact Assessment and Project Appraisal 28 (2), S. 109–116.

Rutkowski, A., et al., 2010. CYBEX – The Cybersecurity Information Exchange Framework (X.1500), ACM SIGCOMM Computer Communication Review, Volume 40, http://www.sigcomm.org/sites/default/files/ccr/papers/2010/October/1880153-1880163.pdf (abgerufen am 21.12.2015).

SANS, 2011. CWE/SANS TOP 25 Most Dangerous Software Errors, 27.06.2011, http://www.sans.org/top25-software-errors/ (abgerufen am 21.12.2015).

SAS Institute Inc., 2012. Big Data Meets Big Data Analytics, USA.

Schweighofer, E., Hötzendorfer, W., 2012. Die Identitätskrise des Internet. In: Schweighofer, Kummer, Hötzendorfer (Hrsg.), Transformation juristischer Sprachen: Tagungsband des 15. Internationalen Rechtsinformatik Symposions IRIS 2012, Wien: Österreichische Computer Gesellschaft (OCG), S. 429-438.

Schneier, B., 2000. Secrets and Lies.

Sherwood, J., Clark, A., Lynas, D., 2005. Enterprise Security Architecture.

sicherheit.info, 2009. 52 Prozent der Datenschädlinge existieren nur 24 Stunden, Fachartikel vom 08/17/2009, http://www.sicherheit.info/artikel/1106166 (abgerufen am 23.01.2016).

Smart Grids Austria Webseite, http://www.smartgrids.at (abgerufen am 14.10.2015).

Social Media Crime Projektwebseite, http://www.kiras.at/gefoerderte-projekte/detail/?tx_ttnews[tt_news]=313&cHash=7966883d2fd6655db7dc010f4c2c1cf5 (abgerufen am 21.12.2015).

Social Media Radar Austria, http://socialmediaradar.at/ (abgerufen am 23.01.2016).

Sophos, 2014. Security Threat Report 2014: Smarter, Shadier, Stealthier Malware. https://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf (abgerufen am 23.01.2016).

Spath, D., Ganschar, O., Gerlach, S., Hämmerle, M., Krause, T., Schlund, S., o.J. Produktionsarbeit der Zukunft – Industrie 4.0, Studie des FRAUNHOFER-INSTITUT für Arbeitswirtschaft und Organisation IAO,
http://www.produktionsarbeit.de/content/dam/produktionsarbeit/de/documents/Fraunhofer-IAO-Studie_Produktionsarbeit_der_Zukunft_-_Industrie_4.0.pdf (abgerufen am 25.8.2014).

Spiegel, 2015. Botnetze: 40 Prozent der PC in Deutschland infiziert, 02.03.2015, http://www.spiegel.de/netzwelt/netzpolitik/botnetze-40-prozent-der-rechner-vireninfiziert-a-1021412.html (abgerufen am 23.01.2016).

Springer Gabler Verlag (Hrsg.), Gabler Wirtschaftslexikon, http://wirtschaftslexikon.gabler.de (abgerufen am 23.01.2016).

Staheli, D., Yu, T., Jordan Crouser, R., Damodaran, S., Nam, K., O'Gwynn, D., Harrison, L., and McKenna, S., 2014. VizSec: Visualization Evaluation for Cyber Security: Trends and Future Directions, https://vimeo.com/112868269 (abgerufen am 23.01.2016).

Statistik Austria, Bevölkerung nach demografischen Merkmalen, 2014, http://www.statistik.at/web_de/statistiken/bevoelkerung/volkszaehlungen_registerzaehlu

ngen_abgestimmte_erwerbsstatistik/bevoelkerung_nach_demographischen_merkmalen/index.html (abgerufen am 27.11.2014).

Strassmann, P., 2013. IT Security: Using Big Data for Enterprise Security, IDC, USA.

Stouffer, K., Falco, J., Scarfone, K., 2011. NIST SP800-82: Guide to Industrial Control Systems (ICS) Security.

Sulzbacher, M. 2015. Österreich bekommt 2016 Teststrecken für selbstfahrende Autos - derStandard vom 27.08.2015, http://derstandard.at/2000021354958/Oesterreich-bekommt-2016-Teststrecken-fuer-selbstfahrende-Autos (abgerufen am 23.01.2016).

Suriadi, S., et al., 2014. Current research in risk-aware business process management: overview, comparison, and gap analysis. Communications of the Association for Information Systems, 34(1), pp. 933-984.

Surprise Projektwebseite, http://surprise-project.eu/ (abgerufen am 23.01.2016).

Svajcer, V., 2014. Sophos Mobile Security Threat Report 2014.

Tehranipoor, M. und Koushanfar, F., 2010. A Survey of Hardware Trojan Taxonomy and Detection. www.trust-hub.org/resources/36/download/trojansurvey.pdf (abgerufen am 24.01.2016).

Tene, O., Polonetsky, J., 2012. Privacy In The Age Of Big Data: A Time For Big Decisions, 64 STAN. L. REV. ONLINE 63. http://www.stanfordlawreview.org/sites/default/files/online/topics/64-SLRO-63_1.pdf (abgerufen am 11.3.2015).

The Heartbleed Bug Webseite, http://heartbleed.com/ (abgerufen am 23.01.2016).

The Royal Society, 1985. The public understanding of science. London, https://royalsociety.org/~/media/Royal_Society_Content/policy/publications/1985/10700.pdf (abgerufen am 19.07.2014).

Thurm, S., Yukari Iwatani, K., 2010. Your Apps Are Watching You, The Wall Street Journal vom 17.12.2010, http://online.wsj.com/news/articles/SB10001424052748704694004576020083703574602 (abgerufen am 23.01.2016).

Torres, R., et al. 2014. CAPITAL (Cyber security research Agenda for Privacy and Technology Challenges), D 3.1 Initial set of research activities listed to meet Gaps.

US CERT/NIST, 2014. Vulnerability Summary for CVE-2014-6271 (ShellShock), https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271 (abgerufen am 23.01.2016).

US National Science Foundation Webseite, Science and Engineering Indicators, http://www.nsf.gov/statistics/seind/ (abgerufen am 23.01.2016).

Valasek, C., Miller, C., o.J. Adventures in Automotive Networks and Control Units.

VALCRI Projektwebseite, http://kti.tugraz.at/css/projects/valcri/ (abgerufen am 22.01.2016).

Van der Aalst, W.M.P., 2010. Challenges in Business Process Mining, http://bpmcenter.org/wp-content/uploads/reports/2010/BPM-10-01.pdf (abgerufen am 22.01.2016).

Van Kessel, P., Allan, K., 2014. Get ahead of cybercrime, EY's Global Information Security Survey 2014.

VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik, 2013. Thesen und Handlungsfelder Cyber-Physical Systems: Chancen und Nutzen aus Sicht der Automation.

VIS-Sense Webseite, http://www.vis-sense.eu (abgerufen am 23.01.2016).

Vutukuru, M., Balakrishnan, H. and Paxson, V., 2008. Efficient and robust TCP stream normalization, in IEEE Symposium on Security and Privacy, S&P, IEEE.

Wangen, G., Snekkenes, E., 2013. A Taxonomy of Challenges in Information Security Risk Management, Norwegian Information Security Conference.

Weber, R.H., 2010. Internet of Things: New security and privacy challenges, Computer Law & Security Review 26, S. 23-30.

Wehling, P., 2012. From invited to uninvited participation (and back?): rethinking civil society engagement in technology assessment and development. In: Poiesis Prax 9 (1-2).

Weisel, D.L., 2005. Analyzing repeat victimization. US Department of Justice, Office of Community Oriented Policing Services.

Weiss, H., 2014. Cloud Computing: Anbieter reagieren auf Sicherheitsbedenken der Unternehmen. VDI Nachrichten, Ausgabe 19 vom 09.05.2014, http://www.vdi-nachrichten.com/Technik-Wirtschaft/Cloud-Computing-Anbieter-reagieren-Sicherheitsbedenken-Unternehmen (abgerufen am 23.01.2016).

West-AAL Webseite, http://www.west-aal.at/ (abgerufen am 24.01.2016).

Whitten, A., Tygar, J., 2005. Why Johnny Can't Encrypt, in In Security and Usability: Designing Secure Systems that People Can Use, pp. 679-702.

Wirtschaftskammer Österreich, 2011. IT-Sicherheitshandbuch für KMU, https://www.onlinesicherheit.gv.at/services/publikationen/sicherheitshandbuecher/75509.html?4 (abgerufen am 23.01.2016).

Wolschmann, A., 2014. Big-Data-Implementierung in Österreich. Computerwelt am 08.05.2014, Printausgabe 10/2014, http://www.computerwelt.at/news/technologie-strategie/big-data/detail/artikel/103517-big-data-implementierung-in-oesterreich/ (abgerufen am 23.01.2016).

Wrigh, D., De Hert, P., 2012. Introduction to Privacy Impact Assessment, in Wright und De Hert (Hrsg.), Privacy Impact Assessment, S. 3–32.

Zirm, J., 2014. Die große Angst vor smarten Zählern. Die Presse am 14.01.2014, http://diepresse.com/home/wirtschaft/economist/1546024/Die-grosse-Angst-vor-smarten-Zaehlern (abgerufen am 11.9.2014).

Liste der zitierten Rechtsakte

Arbeitsverfassungsgesetz (ArbVG) – Bundesgesetz vom 14. Dezember 1973 betreffend die Arbeitsverfassung (Arbeitsverfassungsgesetz - ArbVG) BGBl 1974/22 i.d.F. BGBl I 2013/71.

Verordnung der Bundesregierung über die private Nutzung der Informations- und Kommunikationstechnik-Infrastruktur des Bundes durch Bedienstete des Bundes (IKT-Nutzungsverordnung – IKT-NV)

Datenschutzgesetz (DSG) – Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 – DSG 2000) BGBl I 1999/165 i.d.F. BGBl I 2015/132.

Datenschutzkonvention – Übereinkommen 108 des Europarats (Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten), auch Europäische Datenschutzkonvention.

Elektrizitätswirtschafts- und –organisationsgesetz 2010 (ElWOG 2010) – Bundesgesetz, mit dem die Organisation auf dem Gebiet der Elektrizitätswirtschaft neu geregelt wird (Elektrizitätswirtschafts- und –organisationsgesetz 2010 – ElWOG 2010) BGBl I 2010/110 i.d.F. BGBl I 2013/174.

OECD-Richtlinien – Richtlinien über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD), C(80)58/FINAL, in der Fassung von 11. Juli 2013 (C(2013)79).

Sicherheitspolizeigesetz – Bundesgesetz über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei (Sicherheitspolizeigesetz - SPG) BGBl 1991/566 i.d.F. BGBl I 2014/97

Strafprozessordnung 1975 (StPO) BGBl 1975/631 i.d.F. BGBl I 2015/112.

9 Anhang

9.1 Workshop Einladung und Programm

Persönliche Einladung zum Workshop

Bedrohungs- und Sicherheitslandschaft Österreich

im Rahmen der Technologie-Roadmap-Studie „**Vertrauen rechtfertigen: Sichere Systeme**“
Eine Studie im Auftrag der **Österreichische Forschungsförderungsgesellschaft (FFG)** und des **Bundesministeriums für Verkehr, Innovation und Technologie (bmvit)**

Zukunftsweisende IKT-Schlüsseltechnologien und ihre Sicherheitsrisiken

Ein Workshop zur Bedarfserhebung von Technologielösungen um Vertrauen zu gewährleisten.

Die Frage von Vertrauen und Akzeptanz durch NutzerInnen ist zentral, wenn es um die Einführung und Verwendung neuer Technologien geht – auch und gerade im Bereich der IKT. Vielfach ist bei den (potenziellen) NutzerInnen Skepsis und Unsicherheit vorhanden, nicht zuletzt durch Medienberichte und öffentliche Debatten. Tatsächlich haben viele neue Technologien (potenziell) bedeutsame Auswirkungen auf Wirtschaft und Gesellschaft. Aber mit welchen Technologieentwicklungen im Hinblick auf Vertrauen und Sicherheit ist kurz-, mittel- und langfristig zu rechnen? Wie sind sie im Hinblick auf Vertrauen und Sicherheit zu bewerten?

Am **28. Oktober** kommen ausgesuchte Expertinnen und Experten zu einem Workshop zusammen, um aktuelle Erkenntnisse rund um Technologietrends und ihre Auswirkungen aus **technischer, rechtlicher/gesellschaftlicher** und **wirtschaftlicher Sicht** zu diskutieren.
Wir dürfen Sie recht herzlich dazu einladen!

Referenten

Mario Meir-Huber, Lead Analyst für Big Data in der IDC Central Europe GmbH
Mag. Dr. Christof Tschohl, wissenschaftlicher Leiter des Research Institute – Zentrum für digitale Menschenrechte
FH-Prof. Mag. Dr. Simon Tjoa, Wissenschaftlicher Mitarbeiter Institut für IT Sicherheitsforschung, FH St. Pölten

Ablauf

09:30 Uhr: Registrierung
10:00 Uhr: Begrüßung, Impulsreferate
10:30 Uhr: Expertendiskussionen in mehreren Gruppen
15:00 Uhr: Ende der Veranstaltung, Get-Together

Ort

Österreichische Computer Gesellschaft (OCG), Wollzeile 1, 1010 Wien

Anmeldung

Die Teilnahme an der Veranstaltung ist kostenlos. Die Anzahl der Plätze jedoch beschränkt.
Bitte um Anmeldung per Mail an: mmeir-Huber@idc.com

Wir freuen uns sehr, Sie am 28. Oktober 2014 begrüßen zu dürfen und einen spannenden und aufschlussreichen Workshop mit Ihnen zu verbringen.

Die Organisatoren des Workshops

9.2 Leitfragen des Workshops

Session 1: Erarbeitung von Bedrohungen und Trends:

- Wie schätzen Sie die Gefahr von Cyberbedrohungen in der Zukunft ein
- Welche Quellen (Hacker, MitarbeiterInnen, organisierte Kriminalität, etc.) sehen Sie für derzeitige Bedrohungen / zukünftige Bedrohungen?
- Wie schätzen Sie die Lage österreichischer Unternehmen ein?
- Welche Gefährdungstrends können Sie feststellen?
- Wie schätzen Sie die Entwicklung des Sicherheitsbudgets ein?
- Welche strategischen Sicherheitsprojekte haben Sie geplant?

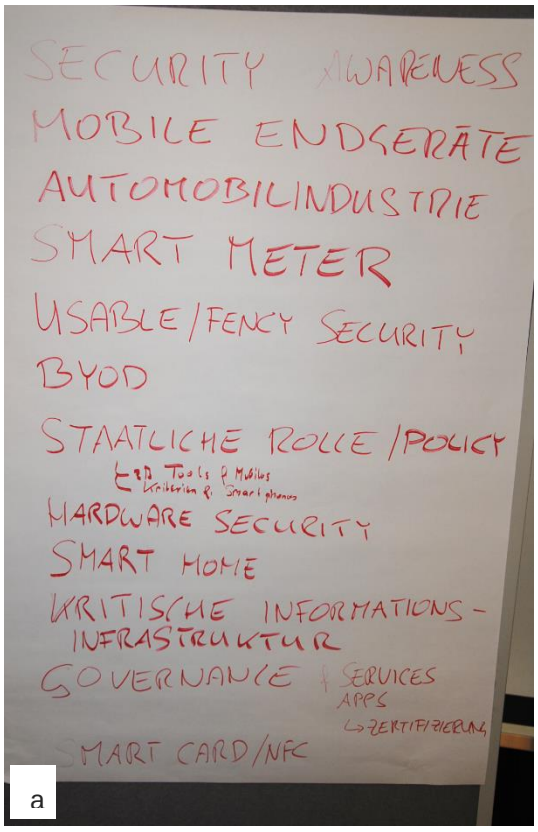
Session 2: Erarbeitung von möglichen Forschungsfeldern:

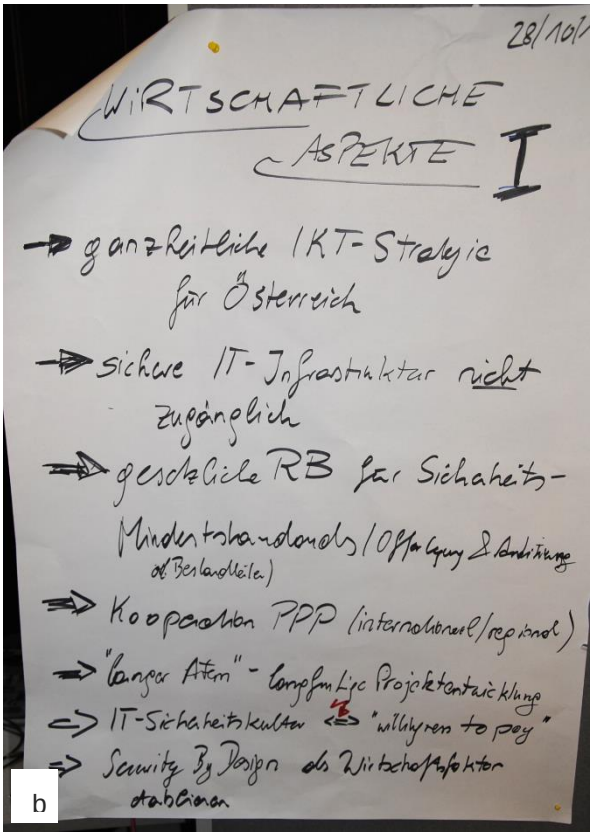
- Welche Forschungsgebiete sollten aus Ihrer Sicht priorisiert werden?
- Welche neuen technologischen Entwicklungen sehen Sie in Ihrem Bereich?
- Wenn möglich, Entwicklung von Szenarien.

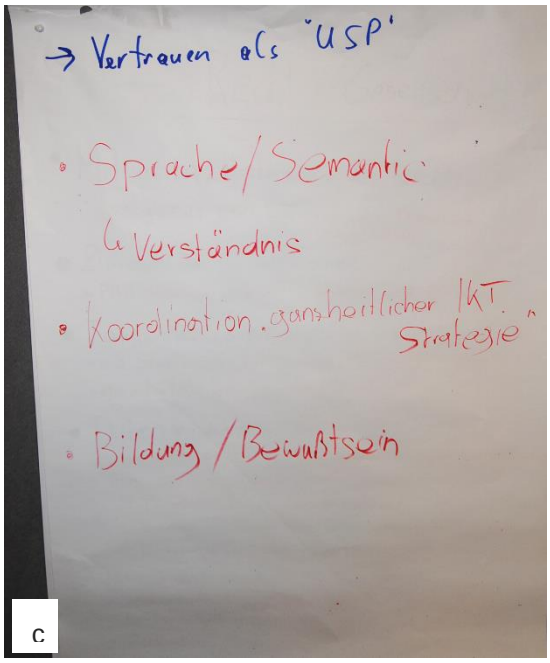
9.3 Whiteboards

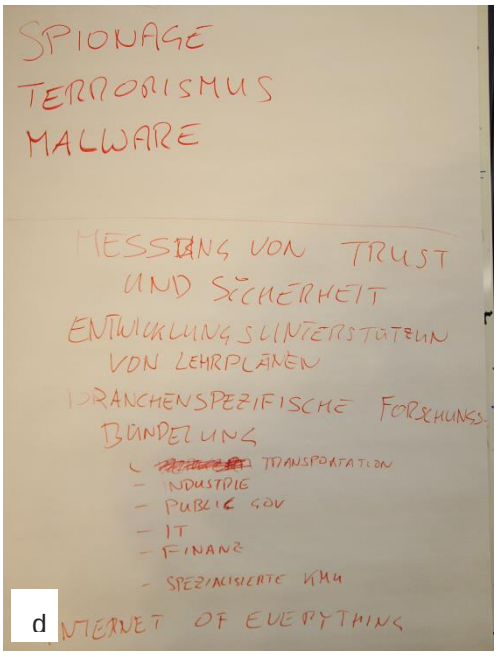
In einer ersten Diskussion zu technischen Aspekten wurden Bedrohungen und Trends im Bereich sichere Systeme und Emerging Technologies identifiziert und diskutiert (a); dabei wurde auch auf ökonomische Aspekte eingegangen (b). Ergänzend wurden weitere Einflussfaktoren auf IKT-Sicherheit wie Politik, Bewusstseinsschaffung und Bildung besprochen (c und d). Diese Ergebnisse sind in Kapitel 2 und 3 dieses Reports eingeflossen.

Eine zweite Diskussion beschäftigte sich damit, relevante Forschungsgebiete zu sammeln, zu priorisieren und den Forschungsgebieten die Emerging Technologies zuzuordnen. Die Ergebnisse der zweiten Diskussionsrunde lieferten einen wesentlichen Input für die Kapitel 4, 5 und 6 dieses Berichtes sowie natürlich Kapitel 7 – Roadmap. TeilnehmerInnen des Workshops waren ExpertInnen aus IT-Geschäftsführung, IT-Projekt- und Servicemanagement, Technik und Beratung aus KMUs und größeren IT-Unternehmen. Ebenso vertreten waren InformationssicherheitsberaterInnen der öffentlichen Verwaltung und VertreterInnen der angewandten Forschung. Geographisch kamen die TeilnehmerInnen aus Österreich und der Slowakei.


SECURITY AWARENESS
MOBILE ENDGERÄTE
AUTOMOBILINDUSTRIE
SMART METER
USABLE/FENCY SECURITY
BYOD
STAATLICHE ROLLE/POLICY
HARDWARE SECURITY
SMART HOME
KRITISCHE INFORMATIONS-INFRASTRUKTUR
GOVERNANCE
SMART CARD/NFC
a


WIRTSCHAFTLICHE ASPEKTE I
ganzheitliche IKT-Strategie für Österreich
sichere IT-Infrastruktur nicht zugänglich
gesetzliche RB für Sicherheits-
Kooperation PPP
"langer Atem" - langfristige Projektentwicklung
IT-Sicherheitskultur
Security By Design als Wirtschaftsfaktor
b


→ Vertrauen als "USP"
Sprache/Semantic
↳ Verständnis
Koordination „ganzheitlicher IKT-Strategie"
Bildung/Bewußtsein
c


SPIONAGE
TERRORISMUS
MALWARE
MESSUNG VON TRUST UND SICHERHEIT
ENTWICKLUNG SLINIENSTÄTTEN VON LEHRPLÄNEN
BRANCHENSPEZIFISCHE FORSCHUNGS-BÜNDELUNG
TRANSPORTATION
INDUSTRIE
PUBLIC GOV
IT
FINANZ
SPEZIALISIERTE KMU
INTERNET OF EVERYTHING
d

9.4 Interview-Fragebogen

1 - Daten Interviewpartner	
1.1 Organisation	
1.2 Name der Organisation	
1.3 Name des Interviewpartners	
1.4 Beschreibung des Forschungs- bzw. Unternehmensumfeldes	
1.5 Anzahl der Mitarbeiter/Forscher im Unternehmen	
1.6 Für Unternehmen: Zielmärkte und Regionen	

2 - Aktuelle Situation	
2.1 Welche aktuellen Sicherheitsbedrohungen sehen Sie?	
2.2 Wo besteht besonderer Handlungsbedarf?	
2.3 Anderes	

3 - Zukünftige Bedrohungen	
3.1 Welche zukünftigen Sicherheitsbedrohungen sehen Sie?	
3.2 Wie wird sich Ihrer Meinung die Bedrohungslage (erwartetes Szenario, Worst Case Szenario) in ihrem (Forschungs)gebiet in den nächsten 2, 5, 10 Jahren ändern?	
3.3 Welche Research-Gaps entstehen aus Ihrer Sicht?	
3.4 Welche aufkommenden Technologien (z.B.: Big Data, Cybernetics, Quantencomputer, etc.), Einsatzgebiete und Entwicklungen nehmen Ihrer Meinung nach in den nächsten 2, 5, 10 Jahren eine bedeutende Rolle ein?	
3.5 Welche Themen werden in Zukunft besonders wichtig sein um Innovationen zu unterstützen?	
3.6 Welche Themen/Forschungsprojekte (z.B.: Erkennung von gezielter Schadsoftware) der Sicherheitsforschung (im Bereich Grundlagenforschung, industrieller Forschung, experimentelle Entwicklungen) sollten aus Ihrer Sicht besonders gefördert werden?	
3.6.1 Welche Probleme könnten dadurch gelöst werden?	

3.6.2 Welche innovativen Lösungen könnten dadurch ermöglicht werden bzw. welche innovativen Sicherheitslösungen könnten dadurch geschaffen werden?	
3.6.3 Welche Einsatzgebiete (privat, geschäftlich, öffentlich) würde die Forschung adressieren?	
3.7 Anderes	

4 - Der Standort Österreich aus wirtschaftlicher und wissenschaftlicher Sicht: Stärken, Schwächen und Möglichkeiten	
4.1 Wo sehen Sie die Stärken der österreichischen Sicherheitsforschung?	
4.2 Welche Schwächen bestehen?	
4.3 Wo entstehen eventuell Nischen, welche in Österreich zu Wachstum führen könnten?	
4.4 Anderes	

ExpertInnen-Interviews wurden mit folgenden Institutionen durchgeführt. Die Ergebnisse werden aufgrund von Vertraulichkeitserwägungen nicht pro Person publiziert. Die Ergebnisse sind in das Gesamtwerk eingeflossen.

- Cryptas IT-Security
- IBM
- TU Graz
- Fabasoft
- Fachhochschule Salzburg
- A-SIT
- JKU Linz
- Bundeskanzleramt
- FH Hagenberg
- WU Wien
- SEC Consult
- BBFA, UK
- AIT
- Universität Klagenfurt
- TU Wien