METHODEN DER CYBERSECURITY IN ANWENDUNG UND RECHT. EINE METHODOLOGISCHE REFLEXION

Nikolaus Schatt

Technische Universität München, Lehrstuhl für Philosophie und Wissenschaftstheorie
Arcisstraße 21, 80333 München, DE
Nikolaus.schatt@tum.de

Schlagworte: ***Cybersecurity, Datensicherheit, Datenschutz, Verhalten, Normen, Forderungen***

Abstract: *Warum ist Akzeptanz von Cybersecurity und ihrer Umsetzung in der Gesellschaft schwierig, betreffen doch Störungen oder Missbrauch nicht nur einen einzelnen Menschen? Die Anforderung an Datensicherheit und die Cybersecurity sind offenbar zwischen einzelnen Nationen und Altersgruppen unterschiedlich. Menschen fühlen sich durch prinzipiell sicherheitsfördernde Maßnahmen im Umfeld der Cybersecurity offenbar behindert, wie nahezu jeder durch Restriktionen kennt. Dieses Akzeptanzproblem führt zu Umgehungsmaßnahmen, die das eigentliche Schutz-Ziel ausbremsen. Daher ist die Betrachtung notwendig, wie aktuell angewandte Methoden zu bewerten sind und inwieweit diese dazu beitragen können, vorhandene oder verbesserbare übergeordnete Schutz-Ziele zu stützen. Die Ausrichtung von Technik und Normen auf die künftigen Anforderungen haben Attacken mit zunehmend gravierenden Auswirkungen einzubeziehen. Prinzipiell ist methodisch der gesamte Zeithorizont von Prävention, über die Reaktion bei einem Angriff bis hin zu notwendigen Nachforschungen und der Akzeptanz von deren Umsetzung in der Gesellschaft zu lösen. Dazu erfolgt eine Beurteilung mit Sichtweisen der Wissenschaftstheorie, Rechtstheorie und Rechtsphilosophie. Darauf baut eine Beleuchtung der technischen Sichtweise von Cybersecurity (Informatik) sowie der Leistungsfähigkeit (normativen Seite) und Anwendbarkeit von Kalkülen aus dem Logiversum (beispielsweise Modal-Logik-Ansätze mit temporalen Eigenschaften und Anwendung der Strategisch Juristischen Entscheidungslogik SJDL) auf.*

1. Einführung

Sicherheit ist gekennzeichnet durch den Spagat zwischen Schutzzielsetzungen, schutzwürdigen Bereichen, getroffenen oder geplanten Schutzmaßnahmen und dem Gegenpart von Angriffen, ein Wettlauf zwischen Angreifern und Verteidigern. Ein Realitätscheck zur aktuellen Situation unter Nutzung wissenschaftstheoretischer Analysen zur Bewertung von Methoden der Cybersecurity trifft auf die Gesellschaft, die Praxis in Behörden, Unternehmen, bei Service-Providern und Produktherstellern. Der Trend zur digitalen Gesellschaft und dem ständigen Einsatz von Informations- und Kommunikations-Technologie (IKT) verstärkt die Abhängigkeit von Cybersecurity. Normen (Gesetze) und Standards (Industrienormen) stützen Vorsorge, Aktionen im Problemfall und die Analyse von Sicherheitsvorfällen (Forensik). Die Bewertung bezieht den Nutzenbeitrag zur Stützung übergeordneter Schutz-Ziele ein. Technik, Betrieb, Nutzung, Standards und Normen sowie erweiterte IKT-Anforderungen stehen im Fokus zunehmender Attacken und der Akzeptanz in der Gesellschaft. Die Ergebnisse werden aus einer Metasicht der Wissenschaftstheorie[1] betrachtet.

[1] Wissenschaftsphilosophie (philosophy of science) steht in engem Bezug zu Karl Popper (wissenschaftliche Weltanschauung) und wird nach Wolfgang Stegmüller auch als Wissenschaftstheorie bezeichnet. Sie wird oft dem logischen Empirismus zugeordnet und arbeitet mit logischen Instrumenten und methodologischen Begriffen (nach Carnap, Hempel, Reichenbach und Nagel).

2. Methodenuntersuchung und Bewertung zur Cybersecurity

2.1. Auslöser, Angreifer und neue Risiken

Vor Beginn einer Analyse von Cybersecurity-Methoden steht die Betrachtung möglicher Ursachen von Sicherheitsverstößen. Im Ursachen-Umfeld finden sich nicht beeinflussbare oder vorhersagbare Auslöser wie Naturkatastrophen (Hochwasser, Erdbeben, Tsunami, Unwetter, etc.) oder politische Ereignisse (Streiks, Krieg, Aufstände). Vorsorge-Methoden konzentrieren sich auf physische Sicherheitsmaßnahmen, Standortwahl und -alternativen sowie Sicherheit für Daten und Menschen. Das Kernfeld zur Cybersecurity umfasst das permanent hohe Angriffsniveau z.B. mit neuer Malware[2] aus Terrorismus, Spionage, Geheimdiensten, politischen Organisationen (NGO), organisierter Kriminalität bis hin zur Hackerszene. Angreifer finden sich als Einzeltäter bis zu wohl organisierten Einheiten mit teils nicht vorstellbarer finanzieller und technischer Ausstattung. Weitere Risiken ergeben sich aus Eigenverschulden beim Verlust von IKT-Systemen (Smartphones, Tablets, USB-Sticks) und reichen bis zur kriminellen Energie (Diebstahl, heimlicher Zugriff, Ausspähung von Daten an Arbeitsplätzen, in öffentlichen Einrichtungen Anzapfen von Übertragungswegen oder ungeschützte WLANs). Künftige Zielgebiete werden autonome Systeme und intelligente Netze (Robotik, Steuerungen, Assistenzsysteme in Automobilen, Ausbau der E-Mobilität) sowie neue Anwendungen (digitales Gesundheitswesens, eGovernment, eBanking) mit neuen Angriffszielen und Sicherheitslücken liefern. Das Kuratorium Sicheres Österreich (KSÖ) beschreibt heutige potentielle Risiken und stellt in einer Matrix gewichtete Ursachen aus Sicht von Betroffenen dar [KSÖ b, 2012]; dies ähnelt vergleichbaren Untersuchungen / Strategien[3] in Deutschland.

Aktuell rückt der Terror[4] gegenüber Menschen und Einrichtungen in den Vordergrund. Typische Handlungsweisen mit Terror und Aktionen des Extremismus zeigen als deren unverzichtbare Basis die Nutzung modernster Kommunikationswege über verschleierte IKT-Komponenten zur schnellen Koordination bei Terror-Anschlägen. Cyberangriffe betreffen auch die allgemeine Sicherheit (ein Angriff erhöht das Risiko einer Störung der öffentlich genutzten IKT Infrastruktur). Die Vorsorge erfordert präventiv wirkende Maßnahmen und über klassische Abwehrtechniken hinaus bereits im Vorfeld Auswertungen im Netz.

Auf Expertenebene ist klar, es kann keine 100%ige Sicherheit geben. In der Bevölkerung wächst die Sorge um öffentliches freies Leben, nimmt Angst zu und es wird mit Risiken und Einschränkungen[5] der Freiheit des Menschen gerechnet bis zum Missbrauch gespeicherter Daten und Freiheitsverlust (z.B. Telekommunikationsgeheimnis). Dies ist unabhängig von der Zuordnung[6] zu Begriffen wie Cyber-War, Cyber-Terrorismus, Cyber-Kriminalität oder Cyber-Spionage. Weltweite Attacken auf die Cybersecurity finden immer wieder auf unterschiedliche Ziele statt, verbunden mit sich rasch ändernden Randbedingungen. Mit Cybersecurity-Strategien, Methoden[7] bis hin zu nationalen Cyber-Abwehrzentren, gemeinsamen Melde- und Lagezentren und Cybercrime-Kompetenz-Zentren[8] wird versucht, Angriffen koordiniert zu begegnen und zum Scheitern zu bringen. Ein großes Manko resultiert in Deutschland in Folge der föderalen Struktur und unterschiedlichsten

[2] Dies umfasst täglich etwa 200.000 neue Versionen von Malware.

[3] «Ziel der Strategie ist es, Cybersicherheit auf einem der Bedeutung und der Schutzwürdigkeit der vernetzen Informationsinfrastrukturen angemessenen Niveau zu gewährleisten, ohne die Chancen und den Nutzen des Cyber-Raums zu beeinträchtigen» [Bundesministerium des Inneren (BMI), cyber.pdf, 2011].

[4] Ursachen finden sich möglicherweise in ideeller und moralischer Entwurzelung und fehlendem Vertrauen in demokratische Institutionen [vgl. Navid Kermani, Wer ist Wir, C.H.Beck, 2015, 96].

[5] Die Aufdeckung von Hintergründen nach Anschlägen erfordert die nachträgliche Auswertung von Informationen aus der Vorratsdatenspeicherung.

[6] Dies wurde nicht weiter untersucht (liefert beispielsweise potentielle Quellen bis hin zu Täterprofilen).

[7] Diese werden unterstützt von Institutionen wie dem Bundesamt für Sicherheit in der Informationstechnologie (BSI, beim BMI) und Forschungseinrichtungen / Universitäten / Arbeitskreisen.

[8] In Deutschland ist das nationale Cyberabwehrzentrum NCAZ seit 2010 etabliert [vgl. BMI, cyber.pdf, 2011, 8].

zu beteiligenden Organisationen auf Bundes-, Landes und Kommunal-Ebene. Das Bundesamt für Sicherheit in der Informationstechnik in Deutschland (BSI) propagiert (ebenso wie das KSÖ) Bedarf zur Verbesserung einer «staatliche[n] und unternehmerische[n] Sicherheitsvorsorge» gestützt durch gegenseitige Information zur «Risikoanalyse und -bewertung, zu konkreten Sicherheitsstrategien[9] und zu vorhandenen sicherheitsrelevanten Fähigkeiten» [KSÖ b, 2012, 2].

2.2. Betroffene Bereiche, Wirtschaft und Gesellschaft

Zur Analyse sind die betroffenen Bereiche segmentiert zu betrachten, so die breite Bevölkerung, mittelständische Unternehmen, kleine Einrichtungen und andererseits große Behörden, Forschungseinrichtungen und Unternehmen. Eine andere Segmentierung gliedert die IKT-Systeme von klassischen Arbeitsplatzsystemen, Servern, Großrechnern bis hin zu neuen Technologien wie Robotik, autonome Systeme, neue allgemeine bzw. künftige Anwendungen (Gesundheitskarte, allgemeine Überwachungssysteme, Haus- und Senioren-Unterstützung) bis hin zu Drohnen mit ihren verschiedenartigen Einsatzgebieten, überall wird wesentlicher Einfluss vom Staat gefordert. Zu diesen Segmenten wurde durch viele Beteiligten in Österreich in der KSÖ-Studie Risikofelder und deren Bedeutung erarbeitet. Dabei fehlen noch eine Reihe der oben aufgezeigten Segmente (deren Bedeutung hat erst in den letzten Jahren zugenommen). KSÖ nennt als Topthemen «manipulierte IKT-Systeme der Energieerzeugung und -versorgung», gefolgt von «Cybercrime, Social Engineering, fahrlässiges Verhalten in strategischen Infrastrukturbetrieben und mangelndes Sicherheitsbewusstsein» [KSÖ b, 2012, 8]. Als großen Risikofaktor bezeichnet KSÖ unter den fünf Topthemen den Mensch und verweist dazu, die «Experten lassen damit keinen Zweifel daran, dass alle Bemühungen im Bereich der Cybersicherheit mit der Expertise der Mitarbeitenden – und in weiterer Folge aller IKT-Nutzer – stehen und fallen» [KSÖ b, 2012, 8]. Dies gilt bereits lange für das Thema Sicherheit in Unternehmen, ein Mensch gilt mit potentiellem Fehlverhalten immer als nicht analysierbar oder vorhersagbar und stellt damit ein unkalkulierbares Risiko dar.

Inzwischen sind nahezu alle Menschen durch Störungen oder Missbrauch der Cyber-Infrastruktur direkt oder mittelbar betroffen. Anforderungen, Handlungsmöglichkeiten und Bereitschaft der Menschen unterscheiden sich zwischen einzelnen Nationen, Nutzergruppen und Altersgruppen. Jüngere Menschen betrachten die Digitalisierung der Welt als etwas Selbstverständliches und akzeptieren ein niedriges Schutzniveau. Hingegen nutzen etwa 20% der Bevölkerung in Deutschland keine Online-Services und werden durch digitale Services nicht erreicht, sind aber wie alle anderen mittelbar den Gefahren von Störungen bei Cybersecurity-Angriffen ausgesetzt (z.B. Ausfall von Infrastrukturen bei Stromversorgung, Kommunikation oder öffentlichen Transportsystemen). Dies bestimmt Ängste. Untersuchungen mit Methoden der Soziologie und zugehörige Theorien wie Science and Technology Studies (STS), sozio-technische Systeme oder Actor Network Theorie (ANT) machen Zusammenhänge und Hintergründe objektivierbar und analysierbar [vgl. Andreas Lösch in: Maasen et al., 2012, 97, 256].

Mit einem interdisziplinären Ansatz kann eine Bündelung entsprechender Methoden in Studien aufzeigen, «wie vorhandene Defizite in der Erkennung, der Abwehr und der Bewältigung von Cyberrisiken in Österreich überwunden und vorhandene Stärken ausgebaut werden können.» [KSÖ b, 2012, 7]. Passend verweist das KSÖ in seinem geschichtlichen Rückblick[10] auf die gesellschaftliche Bedeutung [KSÖ a, 2015].

[9] Dazu formuliert die österreichische Innenministerin: «Sicherheit im Cyberspace und die Sicherheit der Menschen im Cyberspace sind ein Rechtsgut, das mit allen rechtsstaatlichen Mitteln geschützt werden muss. Cyberattacken finden zwar virtuell statt, haben aber höchst reale Auswirkungen auf unsere Sicherheit sowie das Funktionieren von Staat, Wirtschaft und Gesellschaft.» [KSÖ b, 2012, 3].

[10] «Schon damals [1975] … hatte man erkannt, dass Sicherheit kein ausschließliches «Produkt» der Exekutive sein kann, sondern dass die gesamte Gesellschaft ihren Beitrag dazu leisten kann. Das KSÖ hat sich daher zum Ziel gesetzt, durch seine Veranstaltungen und Aktivitäten das Verhältnis zwischen Bürgern, Exekutive, Politik, Medien und Wirtschaft permanent zu verbessern und friktionsfrei zu gestalten» [KSÖ a, 2015].

Ein weiterer Methodenkomplex umfasst Austausch (Expertenebene, Foren, Kongressen) mittels Netzwerkbildung sowie Informationsverteilung in Medien. Die Methodenanalyse (beispielsweise BSI, KSÖ) identifiziert aus Sicht der Metaebene der Wissenschaftstheorie technische, organisatorische und kommunikative Ebenen und Betrachtungsweisen, sichtbare und verborgene Bereiche, Strukturen, Organisationsformen sowie Handlungsbereiche zu Bereichen von Sicherheit und Cybersecurity. Dabei stößt man in Bereiche vor, in denen Methoden bereits teilweise durch Algorithmen und Programme gestützt abgearbeitet oder komprimiert visualisiert werden, um unter hohem Zeitdruck zu helfen, notwendige Entscheidungen zu treffen und Sicherheitsrisiken zu verringern.

Zur Frage nach der Tragweite der durch das BSI oder das KSÖ gestützten Methoden zu Sicherheitsstandards könnten empirische bzw. wissenschaftssoziologische Untersuchungen dies öffentlich nachweisen und konkrete Wirkungen auf die Nutzer von IKT zeigen. Es ist belegt[11], dass Wissensaustausch und Kommunikation auf Expertenebene durch Austausch von Ergebnissen, Entwicklungen, Erfolgen und Thesen zu Integration und neuen Ideen führen. Informelle Gespräche zwischen Teilnehmern liefern wesentliche Impulse zu künftigen Entwicklungen, Korrekturen und Weichenstellungen für die Zukunft. Insofern ist dieser Methodeneinsatz für die Expertenebene positiv zu bewerten.

Information zur Sicherheit von IKT in der Gesellschaft erreicht die Betroffenen nicht in ausreichender Wirkung. Menschen fühlen sich durch Maßnahmen im Umfeld der Cybersecurity eher behindert als unterstützt. Menschen verkennen die Wichtigkeit ihres von sich selbst zu leistenden Beitrags zum Aufbau eines höheren Sicherheitsniveaus. Deutlich wird dies z.B. bei der Passwortvergabe[12] beim Umgang mit Zugangsberechtigungen. Dies alles passiert, obwohl bekannt ist, dass die meisten der erfolgreichen Angriffe[13] durch Malware auf Ausspähung von Zugriffsberechtigungen und zugehöriger Passwörter basieren. Offenbar sind die eingesetzten Kommunikations- und Schulungs-Methoden nicht ausreichend, um zur Erhöhung der Akzeptanz und zur Eigenleistung zur Sicherheit in der Gesellschaft zu motivieren. Dieses Angriffsniveau zeigt die Bedeutung der Forderung nach persönlicher Bereitschaft, selbst aktiv zu werden und nicht nur durch Restriktionen erzwungen zu handeln. Virenschutzanbieter wiegen Menschen in großer Sicherheit, obwohl dies nur teilweise[14] zutrifft. Die Behebung originärer Schwachstellen in Betriebssystemen und Anwendungen passiert nur in zu großen Zeitabständen, Sicherheitskopien und Sicherheitsgenerationen eigener Daten fehlen oft, aktueller Schutz und Verschlüsselung von Netzwerkkomponenten, WLAN und Rechnern ist oft nicht vorhanden. Nach einer Sicherheitsstörung (wie beim Hardware-Defekt) werden zuvor nicht beachtete Risiken und fehlende Wiederherstellungsbasis für die Betroffenen ersichtlich. Die Unkenntnis vieler Verbraucher ist erschreckend[15]. Schadensbeseitigung und Ermittlung[16] eines Fremdverursachers sind dem Nutzer meist nicht möglich.

---

11 Vgl. Netzwerke der Wissenschaft [Thomas Heinze in: Maasen et al., 2012, 191 ff.].

12 Vorschläge zur Passwortvergabe und die Forderung nach regelmäßiger Aktualisierung werden gerne ignoriert, Zugangsberechtigungen samt Passwort hängen deutlich sichtbar für alle neben dem System, Passwörter sind der Name oder Vorname und werden nicht regelmäßig geändert.

13 Untersuchungen an der Technischen Universität München (TUM) und im Leibniz-Rechenzentrum (LRZ) in München zeigen diese Schwachstelle auch im universitären Umfeld. Ein hoher Anteil erfolgreicher Sicherheitsangriffe ist auf entsprechende Schwächen im Umfeld der einzelnen Nutzer zurückzuführen.

14 Angriffe zur Infektion eines Systems werden nicht immer durch einen installierten und aktualisierten Virenschutz entdeckt. Es dauert oft mehrere Tage und darüber hinaus, bis überhaupt die notwendigen Erkennungsmuster (pattern) erstellt, an die Nutzer von Schutzsystemen verteilt und dann meist mit Verzug installiert werden. Untersuchungen verschiedener Virenschutzsysteme zeigen, dass diese Systeme bereits bekannte Malware nur zu einem hohen Prozentsatz und nicht zu 100% erkennen oder beseitigen können; Malware kann auf einem Rechner monatelang aktiv sein, ohne dass dies jemand bemerkt.

15 Beispielsweise über die Wege und Methoden eine Verschleierung eines Angriffs oder eine Veränderung von Daten oder über Höhe und Umfang von Schutzmaßnahmen und Schutzbedürfnis vor Störungen, Attacken bis hin zu Terror und Spionage wird zu wenig gesprochen.

16 Hilfe durch Dritte ist sehr teuer oder wird nicht geleistet. Die wenigen Spezialisten sind mit großen Fällen überlastet oder können mangels fehlender Verbindungsdaten (auch in Drittländern) die Analyse nicht weiter durchführen, denn Verursacher von Sicherheits-

2.3. Standards zu Datenschutz und Cybersecurity

Ein ganzes Bündel von Standards (im üblichen Sprachgebrauch als Industrie-Normen bezeichnet) stützen Datenschutz und Cybersecurity. Dazu zählen ISO/EN-Normen und ihre Ausführungsbestimmungen/-Hinweise sowie Sicherheits-Portfolios[17]. Die Erstellung erfordert eine Abstimmung in Normierungsgremien für europäische Standards. Leider sind Forderungen mit Ausrichtung auf Technologien schon bei der Veröffentlichung teils veraltet oder in der Praxis überholt. Mit der Veröffentlichung einer Norm ist diese noch nicht etabliert, zuerst sind Experten zur Umsetzung und Überprüfung (Auditoren) zu qualifizieren, dann Umsetzungsprojekte und Lernkurven zu starten.

In vielen Fällen erfolgt in Unternehmen beim Einsatz solcher Standards eine Umsetzung unter Ausrichtung auf aktuell vorhandene IKT-Ausprägungen und deren Betriebsorganisation. Damit ist systemimmanent eine Diskrepanz durch Zeitverzug zwischen technischer Entwicklung, Produkt, dessen betrieblicher Nutzung und Festlegung in Industrie-Standards und deren Umsetzung verbunden. In der Bewertung der Leistungsfähigkeit ist festzustellen, dass diese zur Verbesserung der Sicherheitssituation beitragen, insbesondere dann, wenn die Menschen und das Management der Unternehmen und Behörden hinter den in den Formulierungen dokumentierten Ideen stehen und diese auch auf neue Technologien und Betriebsformen übertragen. Diese Chancen sind verbunden mit einer individuellen Auslegung und Erweiterung des Regelumfangs. Betrachtet man die mit den Standards verbundenen Zertifizierungen, so liefern diese nur einen geringen Beitrag zur Sicherheit, wenn sich ein Unternehmen nur auf den Erwerb oder den Erhalt eines Zertifikats konzentriert. Die Ideen einer Industrienorm sind vom Management bis zum einzelnen Mitarbeiter zu verinnerlichen (Forderung in einzelnen Normen).

2.4. Normen zu Datenschutz und Cybersecurity

Rechtstheorie und Rechtsphilosophie liefern Methoden und Kriterien zur Beurteilung von Normen, allerdings lassen sie sich nicht einfach aus einer Dogmatik aufbereiten, sie erfordern nach Arthur Kaufmann[18] auch heute noch kritisches Mitdenken und Nachdenken. Nach Kaufmann geht es in Deutschland bei der vielfältig auslegbaren Rechtsphilosophie um die Bandbreite zwischen den diametralen Standpunkten zu «Naturrecht und Rechtspositivismus» und der Weiterentwicklung zum «gerechten Gesetz» bis zur Zuordnung der «Rechtsphilosophie [… als] Teil der Philosophie» [Kaufmann, 1971, 6/7] und um das Spektrum[19] zwischen Naturrecht und Rechtspositivismus. Zur Methodenanalyse liefert Niklas Luhmann mit seiner Systemtheorie, seinem Verständnis zu Recht als System und der Einbeziehung von Soziologie eine Definition von Legitimation [vgl. Luhmann, 1972, 259] und in den Untersuchungen an der Grenze zwischen empirischen und normativen For-

verstößen nutzen überwiegend ein internationales Umfeld.

17 In Österreich propagiert das KSÖ ein Portfolio unter dem Arbeitstitel Cyber-Security «Risikopotenziale und Handlungserfordernisse am Beispiel ausgewählter Infrastruktursektoren» [KSÖ b, 2012, 1].

18 In den 70er Jahren standen Fragen der Gerechtigkeit und die Beziehung zwischen Gesetz und Richterspruch im Vordergrund [vgl. Kaufmann, 1971, 3]. «Anders als in einer rechtstheoretischen oder methodologischen Betrachtung, welche […] das Problem der Richtigkeitskriterien in der Ableitung des Richterspruchs aus dem Gesetz sieht, und insofern die Existenz eines Gesetzes immer voraussetzt, sind Kriterien der Gerechtigkeit in rechtsphilosophischer Betrachtungsweise von Existenz und Inhalt eines Gesetzes grundsätzlich unabhängig. […] das Gesetz [ist] nicht nur technische Entscheidungsregel, sondern möglicher Träger von Kriterien der Gerechtigkeit. Eine Rechtsphilosophie macht […] Aussagen über den Richtigkeitscharakter […] selbst» [Kaufmann, 1971, 5].

19 Kaufmann stellt mit einem historischen Überblick eine Entwicklung vielfältiger Rechtsformen dar, so etwa den Positivismus (in Sophistik, Nominalismus, Subjektivismus), die «reine Rechtslehre» (Hans Kelsen), den «Rechtspositivismus» und auf der anderen Seite das «rationalistische Naturrechtsdenken», die Suche nach Wurzeln des Naturrechts (zwischen Antike und Thomas von Aquin) oder die institutionelle Rechtslehre, die phaenomenologische Rechtslehre bzw. die existentialistische Rechtslehre; diese Entwicklungen sind stark mit Arbeiten von Hans Kelsen und Gustav Radbruch verknüpft, aber auch durch spezifische Ausprägungen im Dritten Reich belastet und durch den Einfluss der Philosophie wie der Existenzphilosophie (Martin Heideger), der Phaenomenologie (Edmund Husserl) und dem Neokantianismus [vgl. Kaufmann, 1971].

schungsbereichen [vgl. Luhmann, 1972, 343] einen Fundus für rechtsphilosophische, soziologische und methodologische Maßstäbe[20] zur Bewertung. Einen weitergehenden Ansatz liefert Michel Foucault mit seiner Diskursanalyse [vgl. Dirk Verdicchio in: Maasen et al., 2012, 101] unter Einbeziehung von Praktiken, Artefakten, Bildern und Technologien neben sprachlichen Äußerungen. Nicht alle Ansätze sind in der Realität von Wissen und Macht angekommen. Daher wird nachfolgend die Frage nach Wirkung und Nutzen mit einem methodischen Nachdenken über Umgang und Handlungsfähigkeit auf den verschiedenen Arbeitsgebieten der Cybersecurity angewandt.

Auf Grund schneller technologischer Entwicklung in der IKT fehlen immer wieder aktuell passende Gesetze oder existierende Regeln sind technisch veraltet oder man trifft auf die bereits bei Industriestandards erörterten Probleme des Zeitverzugs zwischen technischer Entwicklung und Gesetzes-Formulierung. Erschwert bieten Gesetze durch nationale Ausprägung nur partielle Unterstützung für eine effektive Cybersecurity im internationalen Umfeld. Das deutsche «Gesetz[21] zur Erhöhung der Sicherheit informationstechnischer Systeme (IT Sicherheitsgesetz)» macht bisher freiwillig vereinbarte Formen der Zusammenarbeit durch Änderung verschiedener Gesetze zu einer normativen Verpflichtung. Schwierigkeiten bei der Erarbeitung sind typisch für ein neu zu regelndes Umfeld mit hoher Dynamik und vielen Beteiligten und Betroffenen. Das neue IT-Sicherheitsrecht findet sich traditionell im klassischen «technischen Sicherheitsrecht» wieder, in dessen Rahmen sich ein «dichtes Kontrollnetz rechtlicher und nichtrechtlicher Instrumente [entwickelte, sowie sich …] Zivilrecht und öffentliches Recht mit Problemen der Risikovorsorge und Gefahrenabwehr ebenso wie mit Fragen von Schadenersatz und Haftung befasst» [Alfons Bora in: Maasen et al., 2012, 342]. So wird auch das IT-Sicherheitsgesetz zu detaillierten Ausführungs-Bestimmungen oder -Empfehlungen führen, charakterisiert durch vielfältige Anreize und Kontrollmechanismen bis hin zu freiwilligen Maßnahmen (wie z.B. Audits oder vertragsförmlichen Vereinbarungen) führen. Die Wissenschaftssoziologie verweist dabei auf folgende Trends, in die sich auch das neue Gesetz einzupassen hat: «von der Intervention zur Kooperation, 2. von der reinen Gefahrenabwehr zur Risikovorsorge und 3. von der Belastung der Allgemeinheit hin zur Belastung der Verursacher» [Alfons Bora in: Maasen et al., 2012, 343]. Dies wird ergänzt durch sich verstärkende Forderungen nach Partizipation der verschiedenen Gruppen der Gesellschaft. Das IT-Sicherheitsgesetz ist auch im Zusammenhang mit einer möglichen Steuerungskrise[22] zu sehen, in der «die Instrumente staatlichen Handelns […] reflexiv, prozedural und temporal [werden]. Sie setzen in stärkerem Maß auf Verfahren, beanspruchen […] nur begrenzte Gültigkeit und versuchen, die Folgen regulierender Intervention […] einzubauen»; die Debatte dieser Änderungen spricht dann vom Übergang von politischer und «interventionalistischer Steuerungstheorie» in die Richtung von partizipativer Governance einer «polyzentrischen Gesellschaft» und einer Einbindung einer Vielzahl von Gremien, im «Vordergrund steht nun eine Betrachtungsweise, die eine Vielzahl von Akteuren, Ebenen der Entscheidung und möglicher Einflüsse voraussetzt, also eher netzwerkförmig, reflexiv und rekursiv gebaut ist» [Alfons Bora in: Maasen et al., 2012, 344 u. 345]. Passend dazu wird das deutsche Gesetzespaket aus 2015 bereits bei seiner Verabschiedung mit Kritik begleitet, die u.a. seine Verfassungsmäßigkeit, aber auch z.B. die Frage nach dem Nutzen (was kann mit Meldungen erreicht werden) oder einer Konkretisierung der Betroffenen (was gehört zu den kritischen Unternehmen) aufwirft.

Nun liefern das Sammeln von Daten und deren statistische Auswertung sowie eine Verfolgung potentieller Auslöser im Sinne einer nachlaufenden Analyse Erkenntnisse, die sich auch präventiv einsetzen lassen. Für eine effektive Prävention reichen ein um Tage versetzte Berichte nicht aus, vielmehr sind Anwendungen erforderlich, die diese Daten bei Beginn eines Angriffs oder sogar davor sammeln, quasi in Echtzeit mit anderen

[20] Die gewählten Messlatten orientieren sich an den Beiträgen und dem erzielbaren Nutzen zur Strukturanalyse, zur Analyse von Systemen, Regelkreisen, Kommunikationsnetzen und zum betroffenen Menschen als Akteur.

[21] Veröffentlicht im Bundesgesetzblatt Teil 1 Nr. 31 vom 24. Juli 2015.

[22] Beispielsweise im Zusammenhang mit Jürge Habermas und seiner «Theorie zum kommunikativen Handeln» (1981) und zugehörigen sozialen Bewegungen [Alfons Bora in: Maasen et al., 2012, 344].

Angriffsdaten korrelieren und möglichst automatisiert Gegenmaßnahmen einleiten. Dies erfolgt inzwischen in verschiedenen CERT Organisationen (in Behörden/Privatwirtschaft) mit rund um die Uhr mit Personal besetzten Einheiten und ist sicher noch ausbaufähig. Dabei werden sich weitere Anforderungen an normativer Unterstützung ergeben, auch was Zugriffe auf sensible und geschützte Daten in der Telekommunikation betrifft.

Eine Harmonisierung auf europäischer Ebene durch Urteile des EU-Gerichtshofes und neue EU-Gesetze zu Datenschutz[23] und Datensicherheit verbessert die europäische Position (auf national weiter reichende Schutzregeln wird verzichtet). Die international schwache Rechtssituation bietet keine Lösungen, z.B. wenn benutzte Rechner oder Datenspeicher außerhalb der EU stehen oder deren Standorte nicht bekannt oder geregelt sind. Gerichte müssen Lücken in der Rechtssprechung durch Urteile schließen und sich auf Grundsätze in Gesetzestexten abstützen, soweit dies die einzelnen Rechtsräume zulassen, einschließlich Einbeziehung unterschiedlicher Art der Rechtssysteme (angelsächsisches und deutsches Recht) und Unternehmen, die in unterschiedlichen Rechtsräumen agieren. Datenschutz ist in vielen Staaten als schutzwürdig verankert, aber mit unterschiedlichen Ausprägungen[24], vergleiche dazu z.B. das deutsche BDSG und entsprechende Gesetze in USA. Durch restriktive Sichtweise auf personenbezogene Daten wird deren Sonderbehandlung konform im Sinne dieser Gesetze auf ein Minimum reduziert.

Ein neuer Aspekt betrifft Daten, die Rückschlüsse auf eine Person geben können, z.B. über das Einkaufsverhalten (Rabattkarten, Paybacksysteme, Internetkäufe), Surfverhalten (Abfragen in Suchmaschinen), Kommunikationsverhalten (Mailverkehr, soziale Dienste) oder sogar Kommunikationsinhalte (Emails, Bilder, Videos). Diese Informationen stehen den Anbietern auf Grund der Nutzer-Zustimmung (in Geschäftsbedingungen) berechtigt zu und werden kontinuierlich ausgewertet.

Die neue Disziplin Big Data zeigt, wie aus der kaum überschaubaren Datenmenge mittels neuer Algorithmen sowohl Profile mit Nutzerbezug als auch gesellschaftliche Trends oder Epidemien[25] quasi vorhersagbar werden. Prinzipiell kann sich ein Mensch dagegen entscheiden, diese Geschäftsbedingungen nicht akzeptieren und die positive Seite dieser Dienste nicht in Anspruch nehmen, aber wer will diesen Nachteil in Kauf nehmen? Gleiches gilt für die Frage nach Löschung von Daten. Hier helfen nur gesetzliche Regelungen oder höchstrichterliche Urteile. Bahnbrechend gilt dazu das mit dem «Recht auf Vergessen» titulierte Urteil des EU-Gerichtshofs.

Über den Datenschutz hinausgehende Felder der Cybersecurity sind normativ noch schwerer mit internationaler Wirkung zu regeln bzw. bisher international geordnet. Eine Verfolgung von Sicherheitsverstößen im internationalen Umfeld erfordert schnelle funktionierende wirksame Einrichtungen zusammen mit nationalen Ermittlungen, die sich auf einen durchgängigen Rechtsraum abstützen können. Dieser Rahmen muss noch durch die Nationen geschaffen bzw. ausgebaut werden. Die aktuelle Terrorgefahr ist Anlass, Cybersecurity ins politische Rampenlicht zu bringen und eine internationale Zusammenarbeit von Ermittlungsbehörden politisch zu wollen.

[23] Auf eine Besonderheit ist in der Methodendiskussion an dieser Stelle einzugehen, auf den wichtigen Unterschied zwischen Datenschutz (im Sinne des BDSG) und Datensicherheit bzw. Cyber-Sicherheit. Datenschutz bezieht sich in der deutschen Sichtweise auf den Schutz personenbezogener Daten (Daten wie Geburtsdatum, Adresse, Herkunft, Religion, Familienstand) und regelt damit den Schutz aller anderen Daten nicht.

[24] Differenzen werden durch gesellschaftliche Unterschiede und politische Systeme gestützt.

[25] Aussagen durch Google über Grippe-Epidemien durch Auswertung von Suchanfragen liegen früher vor als Meldungen über Ärzte und Gesundheitsämter.

2.5. Unternehmerische Verantwortung (Betreiber und Produzenten)

Die unternehmerische Verantwortung aller Betreiber aber auch jeder einzelne Nutzer fordert durch geeignete Cybersecurity Maßnahmen den Missbrauch und den Effekt durch Störungen im IKT-Umfeld weitgehend zu verhindern und abzuwenden. Grundsätzlich beschreibt[26] Ferri Abolhassan, Schwächen in der Orientierung und Erwartungserfüllung und deren Messung bzw. Quantifizierung, Forderungen an IKT-Service-Provider, ihr Qualitätsniveau hoch zu halten und Erwartungen zu übertreffen, um erfolgreich zu sein. Dieser Maßstab hilft, Dienstleistungen durch geeignete Produkte und Services mit langfristiger Qualität sicherzustellen, Prozesse optimieren einschließlich der Beziehung zu Kunden. Mit neuer Technik werden Unternehmensprozesse und Innovation in neuer Form möglich, beispielsweise durch Cloud Services (auf höhere Rechnerkapazitäten zugreifen), Big-Data-Technologien (Marktanalysen und -prognosen), neue Angebote und Produkte am Markt bis hin zu verbesserter Kundenzufriedenheit unter Betrachtung der Wertschöpfungskette [vgl. Abolhassan, 2013]. Ein prinzipiell formulierter Qualitätsanspruch ist praktisch nicht immer zu realisieren oder nachzuweisen. Umsetzungsanalysen reichen nicht immer aus, Modelle wie Service Level Agreements (SLAs) sind nicht immer leicht zu definieren und zu vereinbaren[27] Grundlagen für nachhaltige Qualität und hochverfügbare Technik liefern Management und automatisierte Prozesse in der IKT [vgl. Abolhassan, 2014, 3].

Im Komplex Sicherheit bewegt sich die Umsetzung in einer Bandbreite zwischen unmöglich erreichbar (weil utopisch), akzeptabel, kritisch bzw. nicht akzeptabel. Über einen dafür notwendigen Grundstock an Sicherheitsspezialisten verfügen meist nur größere Unternehmen, die sich vorwiegend um Präventivmaßnahmen, Schadensanalyse und Beseitigung kümmern. Es verfügt über ein mehr oder weniger tiefes Wissen auf einzelnen Gebieten der Cybersecurity, kann keine Spezialanforderungen abdecken oder selber wesentlich zur Prävention beitragen. Unternehmen und Nutzer sind durch die Entwicklung der technischen IKT-Infrastruktur von singulären Systemen zu vernetzten Systemen einer wachsenden Komplexität ausgesetzt. Waren früher wesentliche IKT-Komponenten noch im lokalen eigenen Betrieb abzuschotten, wird dies nun an externe Betreiberfirmen unter Nutzung internationaler Netzwerke und damit fremder Rechtsräume übertragen.

Risiken sind in modernen Gesellschaften im Zusammenhang mit Handlungsoffenheit (und mit der Offenheit von Gesellschaften) zu sehen, die sich durch unterschiedliche Wahlmöglichkeiten ergeben, über deren Konsequenzen aber vorab nicht genug Wissen oder überhaupt Nichtwissen (welches prinzipiell eine Antizipation von Entscheidungsfolgen verhindert) vorliegt [vgl. Stefan Böschen in: Maasen et al., 2012, 317 u. 320]. Es stellt sich nun die Frage, ob es sich beim Wissen um Cybersecurity um «illusorische Sicherheitserwartungen» handelt, obwohl man sich «immer auf dem neuesten Stand unwiderlegten möglichen Irrtums» [BVerfGe 49, 89, Absatz 126][28] bewegt [vgl. Stefan Böschen in: Maasen et al., 2012, 319]. Risiken, deren Objektivierung und Analysen zeigen einen unterschiedlichen Umgang mit Risiken und deren Bewertung bei Sicherheitsverletzungen auf. Oft spielen dabei übersehene oder blinde Flecken eine wichtige Rolle. Manipulationen von IKT-Systemen und deren Verhinderung oder Beseitigung sind nur eine Seite. Es finden sich immer wieder organisatorische Mängel, die von fehlender Zertifizierung und umgesetzter Sicherheit bis hin zu unzureichender Notfallvorsorge (Business Continuity Management) reichen [vgl. KSÖ b, 2012, 9].

Eine andere Risiko-Quelle liefern Produzenten von Hard- und Software. Die Freiheit der Wahl ist hier technisch

[26] Aktuell ist, dass beim «optimalen Einsatz von Informationstechnologie für den Geschäftserfolg […] häufig noch Verbesserungsbedarf» besteht. Dies bezieht sich auf «zunehmendem globalen Wettbewerb und Innovationsdruck. […] es] muss der Kunde umfassend […] subjektiv nachweisbar, zufriedengestellt werden» [Abolhassan, 2014, 1].

[27] Darauf verweisen verschiedene Service Provider unter Bezug auf ein Customer Perception Management (einer Managementmethode zur Optimierung von Qualität/Kundenzufriedenheit mit systematischer und möglichst exakter Erfassung von objektiver und subjektiver Qualität und einer Beschreibung aktueller Kundenzufriedenheit) [vgl. Abolhassan, 2014, 3].

[28] Urteil des Bundesverfassungsgerichts Az. 2 BvL 8/77 vom 8. August 1978 (Schneller Brüter, Kalkar I), Fundstelle: openJur 2011, 92758, Absatz 126.

eingeschränkt, es gibt kaum Alternativen im IKT-Einsatz. Produktfehler und Schwachstellen entsprechen nicht den Qualitätsanforderungen. Schlimm sind die für viele Cyber-Attacken offenen oder versteckten Hintertüren, deren Beseitigung sich oft monatelang hinzieht und Nutzer unnötigen Risiken aussetzt, ohne dass Produzenten für deren Folgen einzustehen haben.

Anforderungen an Cybersecurity bei Endnutzern, Privatwirtschaft und staatlichen Behörden zeigen vielfältige und unterschiedliche Bewertungen, damit verbundener Risiken und abzuleitende Maßnahmen. Durch die Umsetzung des neuen deutschen IT-Sicherheitsgesetzes aus 2015 wird zumindest ein Aspekt für wichtige Industrien und Einrichtungen angegangen, über den niemand gerne spricht, über Sicherheitsverletzungen. Nunmehr kann es leichter zur vertieften Diskussion über Auslöser, Wirkung und gemeinsame Lösungen kommen.

3. Meta-Sichtweisen, Logiversum und Ausblick

Anhand der wissenschaftstheoretischen Metabetrachtung und ihrer normativen, rationalen und idealen Orientierung und Ausrichtung auf kognitive Inhalte[29] ist erkennbar, dass viele der betrachteten Methoden sich auf Beschreibungen, Ausführungen und Lösungsansätze technischer und physischer Fragestellungen konzentrieren. Die normative Seite der IKT-Sicherheit wird durch Ungewissheit und Nichtwissen in der öffentlichen Meinung begleitet und sucht Antworten zur Verhinderung gravierender Störungen. Gleichzeitig blockieren sich nationale und europäische bzw. internationale Regelungen durch die Vielzahl zu beteiligender Interessen und Organisationen in komplexen Abstimmprozessen und sind der zunehmenden Beschleunigung von IKT Entwicklung und Digitalisierung der Gesellschaft mit verstärktem Zeitdruck ausgesetzt.

Das Risikofeld Mensch hat Einfluss auf Attacken und ist ein großer Risikofaktor bei Sicherheitsvorfällen (wie auch in der Studie des KSÖ). Es hat mit dem Feld Organisation höhere Bedeutung als das technische Feld der IKT. Die effektiv wirksamen Methoden zur Beeinflussung der Menschen reichen nicht aus, um Sicherheitsverständnis und Akzeptanz zum eigenen Handeln zu etablieren. Die Wirkung in der Gesellschaft ist eher dürftig. Offenbar unterstellt die Vermittlung ein rezeptives und aufklärungsbedürftiges Publikum im Sinne von PUS und die Gesellschaft ist noch nicht im Stadium der Modelle von PEST[30] angekommen.

Obwohl viele Einzelsysteme immer wieder und sogar gehäuft Information über Sicherheitsverstöße durch Malware liefern, bleiben diese Informationen verstreut in unterschiedlichen Umgebungen; die Gesetzesänderung (wie in Deutschland Mitte 2015) zeigen noch keine Wirkung. Kommentatoren fragen, was man denn mit einer Information über die vielen Spams, Virenattacken usw. auf den einzelnen Systemen anfangen will und was man daraus lernen sollte. Seit Jahren pflegen lediglich Spezialunternehmen auf dem Gebiet der Cybersecurity solche Zusammenführungen im Rahmen ihres Produkt- und Beratungsgeschäfts und nutzen diese für ihre Geschäftstätigkeit. Eine integrierte gesamthafte Darstellung fehlt, steht für Entscheidungen nicht zur Verfügung oder trägt nicht zur akut notwendigen Prävention bei. Für Entscheidungen in Politik und Wirtschaft fehlen verlässliche integrierte oder visualisierte Informationen in Echtzeit. Prävention moderner Attacken bis hin zu massiven Angriffen wird wenigen im Krisenfall überforderten Einrichtungen überlassen. Das führt oft länger zur Blockade der Nutzbarkeit eigener oder nationaler IKT.

Positiv sind die Schaffung neuer normativer Regelungen wie beispielsweise in Deutschland (2015) und die internationale Zusammenarbeit zur Stützung der Cybersecurity, decken noch nicht alle Problemfelder der Cybersecurity ab, aber unterstützen die Entwicklung zu einer besser gesicherten Gesellschaft. Ausarbeitungen [wie KSÖ b] mit Einschätzungen zu Risikofeldern aus Wirtschaft und Behörden lösen bei ihrer Durchführung Handlungen bei den Beteiligten aus und führen so zur Verbesserung des Sicherheitstandes. Dokumentierte

[29] Vgl. Aussagen zur Wissenschaftsphilosophie [Marcel Weber in: Maasen et al., 2012, 229 ff.].

[30] Public Engagement with Science and Technology (PEST) und Public unterstanding of Science (PUS), britische Modelle zur Wissenschaftskommunikation [vgl. Martina Franzen in: Maasen et al., 2012, 356].

Profile zu Anfälligkeit und Angriffsrisiken bedürfen einer Fortschreibung unter Einbeziehung zwischenzeitlich geänderter Bedrohungsszenarien und eine Ergänzung durch eine Erhebung potentieller Risiken bei Zukunftstechnologien. Zu Technologien, die sich derzeit noch im Forschungsstadium befinden, empfiehlt sich die frühzeitige Einbeziehung in die Problemstellung Cybersecurity, um bereits entstehende Prototypen mit Sicherheitsfunktionen auszustatten und dies in künftigen Produkten und Anwendungen zu etablieren. Dies gilt auch für Produkte im Rahmen von Industrie 4.0, Big Data oder mit autonomen Systemen.

Eine Balance zwischen Freiheit und Restriktionen betrifft alle. Es ist unwichtig, welche Angreifer konkret welches Ziel auswählen oder ob die Auswahl zufällig passiert. Entscheidungsproblem und richtiges Handeln bleibt bei betroffenen Verantwortlichen. Ansätze[31] zur Unterstützung der Entscheider im Problemfall und der Richter bei nachträglichen Überprüfungen sind auszubauen. Weiter sind die technische Sichtweise von Cybersecurity in der Informatik sowie die Leistungsfähigkeit von Methoden aus dem Logiversum wie beispielsweise Modal-Logik-Ansätze (mit temporalen Eigenschaften, die Strategisch Juristischen Entscheidungslogik SJDL) zusammenzubringen.

4. Literatur

Abolhassan, Ferri, Der Weg zur modernen IT-Fabrik. Wiesbaden: Springer, 2013.

Abolhassan, Ferri,. Kundenzufriedenheit im IT-Outsourcing. Wiesbaden: Springer, 2014.

BMI, Cyber-Sicherheitsstrategie für Deutschland, http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile, 2011, abgerufen 5. Februar 2016.

Kaufmann, Arthur, Hassemer, Winfried, Grundprobleme der zeitgenössischen Rechtsphilosophie und Rechtstheorie, Athenäum, 1971.

KSÖ a, Geschichte – KSÖ – Kuratorium Sicheres Österreich KSÖ, https://kuratorium-sicheres-oesterreich.at/verein/historie/, 2015, abgerufen 19. Dezember 2015.

KSÖ b, Cyber-Sicherheit in Österreich, https://kuratorium-sicheres-oesterreich.at/wp-content/uploads/2015/02/Cyberrisikoanalyse.pdf, 2012, abgerufen 19. Dezember 2015.

Luhmann, Niklas, Rechtssoziologie, RoRoRo, 1972.

Luhmann, Niklas, Zweckbegriff und Systemrationalität, Suhrkamp, 1973.

Maasen Sabine, Kaiser Mario, Reinhart Martin, Sutter Barbara (Hrsg.), Handbuch der Wissenschaftssoziologie, Springer, 2012.

[31] Der begrenzte Umfang dieser Ausarbeitung erlaubt keine Vertiefung der Betrachtung der technischen Sichtweise von Cyber-Security in der Informatik und eine Vertiefung der Ansätze mit Methoden aus dem Logiversum wie z.B. in der Modal-Logik mit temporalen Eigenschaften und der Strategisch Juristischen Entscheidungslogik (SJDL); vergleiche integrative Forschungsarbeiten an der TUM.