POLICY BRIEF NR. 2

CYBERSICHERHEIT UND DAS EUROPÄISCHE DATENSCHUTZRECHT

Die Herausforderung: Mehrere Konflikte zwischen Datenschutz und Sicherheit

Häufig handelt es sich bei Cybersicherheitsvorfällen um den Verlust, die Kompromittierung oder die unbefugte Offenlegung personenbezogener Daten von Personen.

Vorfälle können ein sehr breites Spektrum umfassen
z.B. Hacking, erpresserische Verschlüsselung, Daten- oder Identitätsdiebstahl.

Viele verschiedene Akteure
könnten aus verschiedenen Gründen Cybersicherheitsvorfälle verursachen.

Ereignisse können unterschiedliche, oft unvorhersehbare Auswirkungen haben,
welche die Verfügbarkeit, Integrität und Vertraulichkeit digitaler Technologien ernsthaft beeinträchtigen können.

Viele Herausforderungen und Konflikte für die Cybersicherheit und den Datenschutz

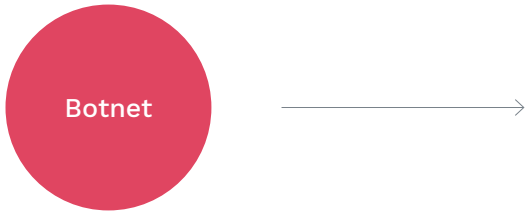
- Datenbasierte Unternehmen wollen nicht in Sicherheit und Datenschutz investieren
- Die Bürger wollen keine Abwägung von Privatsphäre und Sicherheit
- Schutz vor Verletzung der Privatsphäre ist ein verfassungsmäßiges Recht
- Risiko des Missbrauchs
- Vertrauenswürdigkeit von Sicherheitswerkzeugen, die den Datenschutz gefährden
- Sich schnell entwickelnde Technologie
- Zunehmende Abhängigkeit von anfälliger IT
- Viele Cybersicherheitsmaßnahmen beruhen auf Überwachung.
- Offensive Maßnahmen können die Sicherheit für alle schwächen
- „Rüstungswettlauf“ von Offensivstrategien
- Ausnutzung von „rechtmäßigem Zugang“ können Schlupflöcher für böswillige Parteien sein
- Komplexes Spielfeld der Akteure, mangelnde Transparenz
- Rechtliche und faktische Rahmenbedingungen oft unklar

- Schwierige Identifikation von Akteuren bei Cybersicherheitsvorfällen
- Unterschiedliche und unvorhersehbare Auswirkungen von Vorfällen
- Cybersicherheit ist ein sehr komplexes globales Thema
- Noch immer weit verbreiteter Mangel an Grundsicherheit, der mit der steigenden Verbreitung des IoT immer dringlicher wird
- Fehlende Unterstützung für KMU, z.B. durch Finanzierungs- und Schulungsmaßnahmen für eine bessere IT-Sicherheit

Mangelnde Cybersicherheit betrifft alle

Ein Beispiel für einen typischen Cybersicherheitsvorfall, der ein breites Spektrum der Weltbevölkerung betraf, ist das sogenannte Mirai-Botnet.

Ursprünglich wollten junge Schüler nur in einem Online-Spiel betrügen, indem sie das Mirai-Botnet schufen, um den Spielserver zu stören. Aber das Botnet geriet außer Kontrolle. Infizierte Geräte wurden Teil des Botnets und für umfangreiche Netzwerkangriffe ferngesteuert. Im Oktober 2016 brachte der Angriff das Internet im gesamten Osten der USA fast vollständig zum Erliegen.



Botnetze bestehen aus infizierten Geräten, wie Computern und IoT (Internet of Things = Internet der Dinge) Geräten, die von einem böswilligen Akteur kontrolliert werden. IoT ist der Begriff für angeschlossene elektronische Geräte, die Daten austauschen können, z.B. über das Internet. Beispiele sind Internet-Router, Kameras, Fernseher oder digitale Videorekorder.

Das neue europäische Datenschutzrecht ist von Bedeutung

In Europa wird der Schutz der personenbezogenen Daten der Bürger durch die **Allgemeine Datenschutzgrundverordnung (DSGVO)** und die **Richtlinie 2016/680** (für den Polizei- und Justizbereich) geregelt.

Noch im Gange ist der legislative Prozess für eine Verordnung über den Schutz der Privatsphäre und den Datenschutz, welche im Bereich der elektronischen Kommunikation gelten soll (**ePrivacy-Verordnung**).

Die Trade-Off-Sicht zwischen Sicherheit und Datenschutz ist ein Problem

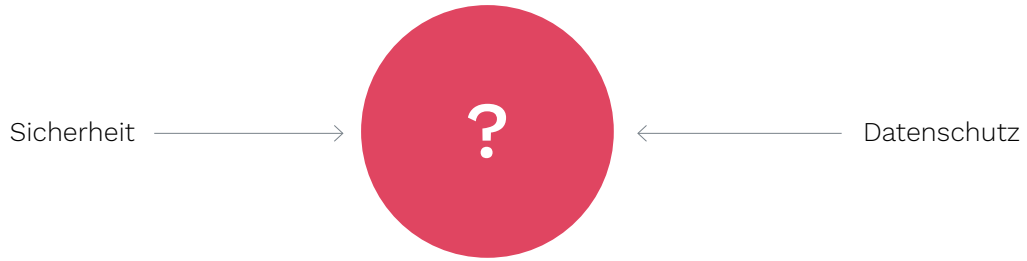
Es ist bekannt, dass einige Maßnahmen zur Verbesserung der Cybersicherheit die Grundrechte des Einzelnen beeinträchtigen können, insbesondere sein Recht auf Privatsphäre und den Schutz seiner personenbezogenen Daten.

Beispiel 1

Ein Privatunternehmen will seine Geschäftsgeheimnisse schützen und setzt daher interne Sicherheitsmaßnahmen wie z.B. eine strenge Zugangskontrolle ein. Aber aus diesem Grund werden auch gültige Rechte der betroffenen Person, wie das Recht auf transparente Informationen und Auskunft verweigert.

Beispiel 2

Strafverfolgungs- und Nachrichtendienste verlassen sich bei ihrer Arbeit oft auf überwachungsorientierte Sicherheitstechnologien und fordern gelegentlich mehr Befugnisse in diesem Bereich. Aber viele dieser Technologien, wie z.B. Deep Packet Inspection, oder das Einkaufen und die Ausnutzung von vorhandenen Sicherheitslücken in Software können die Sicherheit und den Datenschutz für alle schwächen.



Überwachungsorientierte Sicherheits-technologien können gefährlich sein

Rechtfertigt die Verbrechensbekämpfung die Mittel, d. h. die Opferung der Sicherheit technischer Geräten generell und für alle?

Der Einsatz von Technologie zur Infiltration von Geräten und Kommunikationen der Bürger um Kriminelle zu finden wurde wiederholt kritisiert, denn sie geht einher mit **erheblichen Risiken des Missbrauchs, der Voreingenommenheit und der mangelnden Transparenz.**

Sicherheitsforscher haben vor **unbeabsichtigten Nebeneffekten** gewarnt, wie etwa dass Überwachungswerkzeuge in die Hände von Kriminellen fallen können, oder dass neben Strafverfolgungsbehörden auch bösartige Akteure dieselben Softwareschwachstellen nutzen.

Ist die Schwächung der Sicherheit der richtige Weg, um Sicherheit zu erreichen?

Im Jahr 2011 entdeckte der Deutsche Chaos Computer Club (CCC) eine Trojanische Pferd Malware („Bundestrojaner“ oder „Staatstrojaner“ genannt), die bestimmte Geräte überwachte und dabei **Fernkontrolle durch Hintertüren** ermöglicht.

Die Enthüllung des Einsatzes dieser Malware löste Kritik aus, da dieser die Sicherheit des Zielgeräts beeinträchtigt. Es wurde argumentiert: **nicht nur die Strafverfolgung, sondern auch Kriminelle und autoritäre Staaten könnten solche Funktionalitäten nutzen.** Die Aufdeckung löste eine große öffentliche Debatte über die Rechtmäßigkeit der Verwendung solcher Technologien in demokratischen Gesellschaften aus.

Die Bürger wollen nicht ständig überwacht werden

Sollte Technologie dazu beitragen, Menschen zu einem Schwerpunkt oder Ziel polizeilicher Aktivitäten zu machen, indem für eine Person eine **Zuordnung eines höheren Kriminalitätsrisikos auf der Grundlage von Mutmaßungen** erfolgt?

Was ist mit Transparenz, Grenzen und effektiven Kontrollen, wenn eine Person **aufgrund weniger, unsicherer oder sogar selektiv ausgewählter Faktoren der Lebensumstände, Persönlichkeit oder des Verhaltens konstant unter Beobachtung** steht, wie z.B. arm sein, im falschen Stadtteil leben oder eine andere Hautfarbe haben?

Fairness, Rechtsstaatlichkeit und ein ordnungsgemäßes Verfahren

Eine weitreichende Eingriff durch staatliche Überwachung kann die Erosion von Privatsphäre und anderer Grundrechte sowie demokratischer Grundsätze begünstigen.

Es geht um demokratische Prinzipien wie die Unschuldsvermutung und das Verbot von Strafen ohne Gesetz.

Verhältnismäßigkeit ist ein äußerst schwieriges Thema, abgesehen von der allgemeinen Frage, ob eine umfassende Überwachung eines großen Teils der Bevölkerung in einer demokratischen Gesellschaft zulässig sein sollte.

Im Privatsektor überwiegen Wirtschaftlichkeitserwägungen gegenüber Sicherheit und Datenschutz

Sicherheit und Datenschutz können ein Hemmnis für die wirtschaftlichen Interessen eines Unternehmens darstellen, insbesondere wenn es sich um ein datenbasiertes Business handelt.

Da der Aufbau und die Aufrechterhaltung effektiver IT-Sicherheits- und Datenschutzmanagementprozesse **mit Kosten verbunden** ist, tun im Unternehmensbereich viele Firmen nicht genug in Bezug auf Cybersicherheit und Datenschutz.

Um Geld zu sparen, werden interne IT-Sicherheitsexperten sehr oft auch mit Datenschutzfragen betraut. Dies ist jedoch kontraproduktiv, da IT-Sicherheit und Datenschutz in der Regel **sehr unterschiedliche Standpunkte, Ziele und fachliche Anforderungen** haben.

Fehlende Investitionen betreffen auch kritische Infrastrukturen

Die Kosten für den Einsatz von technischen und organisatorischen Maßnahmen werden oft als zu hoch eingestuft. Dies betrifft auch Bereiche, in denen die verantwortlichen Stellen mit sensiblen personenbezogenen Daten, wie beispielsweise Gesundheitsdaten, umgehen.

Einrichtungen des Gesundheitswesens werden als Teil der kritischen Infrastruktur eines Landes angesehen.

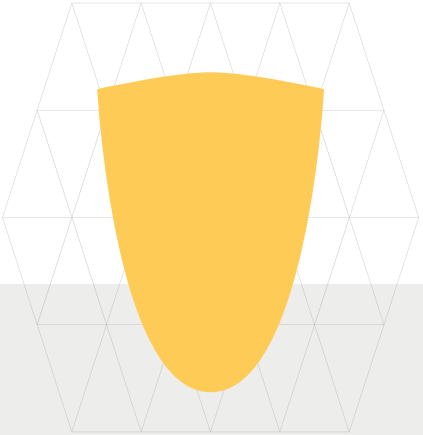
Vielen Arztpraxen, Krankenhäusern und medizinischen Forschungseinrichtungen fehlt noch immer die **Finanzierung und das Know-how, um umfassend die notwendigen Maßnahmen zu ergreifen**, so dass verhindert wird, dass z.B. medizinische Geräte mit Viren infiziert werden, oder dass Gesundheitsdaten verloren gehen oder gefährdet werden.

EU-Bürger wollen alles – Sicherheit, Privatsphäre und Datenschutz!

Verschiedene Studien und Forschungsarbeiten in der gesamten EU haben ergeben, dass sich die europäischen Bürger einen ganzheitlicheren Ansatz für Sicherheit und Datenschutz wünschen.

Im **Gesundheitsbereich** scheinen die Bürger besonders sensibel auf den Umgang mit ihren Patientendaten zu reagieren. Zustimmung und Vertrauen hängen stark davon ab, mit wem und in welchem Kontext sie die Daten teilen.

In der **Privatwirtschaft** sorgen sich die Bürger auch um Datenschutzverletzungen und IT-Sicherheit, insbesondere bei der Nutzung von Internetdiensten wie Oline-Shops. Sie haben kein großes Vertrauen darin, dass Privatunternehmen mit ihren personenbezogenen Daten verantwortungsvoll umgehen.



Im **Bereich der Polizei und der nationalen Sicherheit** halten die Bürger die staatlichen Sicherheitsmaßnahmen für akzeptabler, wenn sie den Staat eher als schützende Institution und nicht als Angreifer betrachten, was oft von der Erfahrung und der Geschichte des Landes abhängt.

Die Pflichten des Verantwortlichen einer Datenverarbeitung sind entscheidend

Nach der DSGVO sind die Verantwortlichen und Auftragsverarbeiter personenbezogener Daten gesetzlich verpflichtet, geeignete technische und organisatorische Maßnahmen zum Schutz dieser Daten zu ergreifen. In einigen Fällen muss zunächst eine Datenschutzfolgenabschätzung durchgeführt werden.

Welche Maßnahmen eingesetzt werden müssen, hängt von Fall, Situation und Stand der Technik in bestimmten Bereichen ab. Bei den jeweiligen Lösungen für Cybersicherheit und Datenschutz gibt es Synergien, die genutzt werden sollten.

Beispiele für technische und organisatorische Maßnahmen

- Zugriffskontrolle
- Verschlüsselung
- Datentrennung
- Anonymisierung
- Peudonymisierung
- Verfahrensverzeichnis
- Verfahren zur Sicherung und Wiederherstellung
- Protokollierung
- Vordefinierte Benachrichtigungsverfahren für Datenschutzverletzungen.

Sowohl die DSGVO als auch die Richtlinie 2016/680 regeln spezifische Sicherheitsanforderungen an IT-Systeme und -Dienste in Bezug auf ihre

- Vertraulichkeit,
- Integrität,
- Verfügbarkeit,
- und Belastbarkeit
- im Rahmen der Verarbeitung personenbezogener Daten.

Effektive Managementverfahren und Privacy by Design können helfen.

Die für die Datenverarbeitung Verantwortlichen und Auftragsverarbeiter müssen angemessene Maßnahmen ergreifen, um die Einhaltung der DSGVO nachzuweisen.

Es ist ratsam, dass die für die Datenverarbeitung Verantwortlichen ein **effektives Datenschutzmanagement innerhalb der eigenen Organisation aufbauen**, welches zwar von der IT-Sicherheitsabteilung getrennt ist, aber eng mit ihr zusammenarbeitet.

Darüber hinaus können **jährliche Sicherheitskontrollen, Audits und die Implementierung von Best Practices**, z.B. aus dem Sicherheitsbereich, sowohl die Cybersicherheit als auch den Datenschutz verbessern. Beispiele sind Penetrationstests und die Dokumentation von Sicherheitsvorfällen.

Zusammengefasst: Anwendung wertorientierter und interdisziplinärer Ansätze

- Anerkennung von **Transparenz, Vertrauen und Kontrolle** als Schlüsselfaktoren zur Erzielung werteorientierter Cybersicherheit.
- Berücksichtigung dieser **Werte im Gesetzgebungsprozess der ePrivacy-Verordnung** für die elektronische Kommunikation.
- Sicherheitsmaßnahmen, Technologien sowie Anwendungsszenarien sollten Bestandteil einer **Datenschutzfolgenabschätzung** sein.
- **Aufgabe der Trade-off-Sich** bei Sicherheit und Datenschutz.
- Vielmehr, **Beachtung eines sorgfältigeren Gleichgewichts** mit fairen und rechtskonformen Kompromissen zwischen Sicherheit, Privatsphäre, Datenschutz und Grundrechten.
- **Nutzung von Synergien** zwischen Cybersicherheit und Datenschutzansätzen sowie -maßnahmen.
- **Verstärkte Rechenschaftspflicht** verantwortlichert Stellen und ihrer Auftragsverarbeiter.
- **Unterstützung** interdisziplinärer Forschung.

Weitere Informationen finden Sie hier

Die Folien basieren auf der Forschungsarbeit des CANVAS-Projekts (Constructing an Alliance for Value-driven Cybersecurity).

Ziel von CANVAS ist es, Stakeholder aus Schlüsselbereichen der Europäischen Digitalen Agenda zusammenzubringen, um der Herausforderung zu begegnen, wie Cybersicherheit mit europäischen Werten und Grundrechten in Einklang gebracht werden kann.

Insbesondere stellen wir die folgenden CANVAS-Ressourcen zur Verfügung:

- Briefing packages
- CANVAS Reference Curriculum
- CANVAS MOOC
- Open Access Book
  ‘The Ethics of Cybersecurity’

Die Folgefolie verweist direkt auf jene unserer White Paper, die sich ausführlich mit den Herausforderungen der Cybersicherheit befassen.

Bibliographie: Herausforderungen der Cybersicherheit (CANVAS White Papers)

Ethische Herausforderungen

Yaghmaei, Emad, Ibo van de Poel, Markus Christen, Bert Gordijn, Nadine Kleine, Michele Loi, Gwenyth Morgan, and Karsten Weber. 2017. “Canvas White Paper 1 – Cybersecurity and Ethics.” SSRN Scholarly Paper ID 3091909. Rochester, NY: Social Science Research Network.

https://papers.ssrn.com/abstract=3091909.

Rechtliche Herausforderungen

Jasmontaite, Lina, Gloria González Fuster, Serge Gutwirth, Florent Wenger, David-Olivier Jaquet-Chiffelle, and Eva Schlehahn. 2017. “Canvas White Paper 2 – Cybersecurity and Law.” SSRN Scholarly Paper ID 3091939. Rochester, NY: Social Science Research Network.

https://papers.ssrn.com/abstract=3091939.

Technische Herausforderungen

Domingo-Ferrer, Josep, Alberto Blanco, Javier Parra Arnau, Dominik Herrmann, Alexey Kirichenko, Sean Sullivan, Andrew Patel, Endre Bangerter, and Reto Inversini. 2017. “Canvas White Paper 4 – Technological Challenges in Cybersecurity.” SSRN Scholarly Paper ID 3091942. Rochester, NY: Social Science Research Network.

https://papers.ssrn.com/abstract=3091942.

Bibliographie

Vertrauen – generell – philosophisch

- Held, Virginia. 1968. “On the Meaning of Trust.” Ethics 78 (2): 156–59.
- Baier, Annette. 1986. “Trust and Antitrust.” Ethics 96 (2): 231–60.
- Pettit, Philip. 1995. “The Cunning of Trust.” Philosophy & Public Affairs 24 (3): 202–25.
- Becker, Lawrence C. 1996. “Trust as Noncognitive Security about Motives.” Ethics 107 (1): 43–61.

Vertrauen – generell – Sozialwissenschaften

- Frey, Bruno S. 1994. “How Intrinsic Motivation Is Crowded out and In.” Rationality and Society 6 (3): 334–52.
- Ostrom, Elinor. 2000. “Collective Action and the Evolution of Social Norms.” The Journal of Economic Perspectives 14 (3): 137–58.
- Frohlich, Norman, and Joe A. Oppenheimer. 1996. “Experiencing Impartiality to Invoke Fairness in the N-PD: Some Experimental Results.” Public Choice 86 (1): 117–35. https://doi.org/10.1007/BF00114878.

Vertrauen – online – digital

- Erlich, Yaniv, et al. 2014. “Redefining Genomic Privacy: Trust and Empowerment.” PLOS Biology 12 (11): e1001983.
- Etzioni, Amitai. 2017. “Cyber Trust.” Journal of Business Ethics, July. https://doi.org/10.1007/s10551-017-3627-y.
- Chakravorti, B., Bhalla, A., Chaturvedi, R.S., 2018. The 4 Dimensions of Digital Trust, Charted Across 42 Countries. Harvard Business Review.

Fakten zum Projekt

Projektkoordination und Kontakt:
PD Dr. sc. sc. ETH Markus Christen
Universität Zürich (UZH), Digital Society Initiative
Rämistrasse 66, 8001 Zürich

Slidedocs-Version:
Version 2.0 Oktober 2019

Projektdauer:
Sept. 2016 - Okt. 2019

Partner:
Das CANVAS-Konsortium besteht aus 11 Partnern (9 akademische Institutionen und 2 Partner außerhalb der akademischen Welt) in 7 europäischen Ländern.

Finanzierung:
1,57 Mio. €, wovon 1 Mio. € von der Europäischen Kommission finanziert wird und der restliche Teil aus dem Schweizer Staatssekretariat für Bildung, Forschung und Innovation stammt.

Förderhinweis für CANVAS

Kofinanziert durch das Programm
„Horizont 2020“ der Europäischen Union

Das Projekt CANVAS (Constructing an Alliance for Value-driven Cybersecurity) wurde im Rahmen der Fördervereinbarung Nr. 700540 aus dem Forschungs- und Innovationsprogramm Horizon 2020 der Europäischen Union finanziert. Diese Arbeit wurde (teilweise) vom Staatssekretariat für Bildung, Forschung und Innovation (SERI) unter der Vertragsnummer 16.0052-1 unterstützt. Die darin geäußerten Meinungen und Argumente spiegeln nicht unbedingt die offizielle Meinung der Schweizer Regierung wider.