POLICY BRIEF NO. 2

CYBERSICHERHEIT UND DAS EUROPÄISCHE DATENSCHUTZRECHT

Die Herausforderung: Mehrere Konflikte zwischen Datenschutz und Sicherheit

Cybersicherheitsvorfälle können ein sehr breites Spektrum abdecken; zum Beispiel Hacking, Erpressung durch Datenverschlüsselung und Daten- oder Identitätsdiebstahl. Es gibt verschiedene Akteure, die aus diversen Gründen Vorfälle verursachen können, welche die Cybersicherheit beeinträchtigen.

Darüber hinaus können solche Ereignisse unterschiedliche, oft unvorhersehbare Auswirkungen haben, welche die Verfügbarkeit, Integrität und Vertraulichkeit digitaler Technologien ernsthaft beeinträchtigen können. Dies kann den Verlust, die Manipulation oder die unbefugte Weitergabe personenbezogener Daten von Personen beinhalten.

Um einen besseren Schutz der Grundrechte des Einzelnen in Bezug auf den Schutz seiner personenbezogenen Daten zu erreichen, hat die Europäische Union die Allgemeine Datenschutzverordnung (DSGVO) vor allem für den Privatsektor sowie die Richtlinie 2016/680 für die Bereiche der Polizei und Justiz verabschiedet.

Das Gesetzgebungsverfahren für eine Verordnung über den Schutz der Privatsphäre und des Datenschutzes, welche speziell für die elektronische Kommunikation gelten soll, ist noch im Gange.

Dies sind die Rechtsinstrumente, die nötig sind, um Konflikte als auch Synergien im Bereich der aktuellen Gesetzgebung und Politik zur Cybersicherheit zu berücksichtigen.

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

Für die Bürger sind die größten Risiken im Zusammenhang mit der Cybersicherheit die Verletzung ihrer Privatsphäre und der Verlust der Kontrolle über ihre Daten.

Es ist bekannt, dass Maßnahmen zur Verbesserung der Cybersicherheit die Grundrechte des Einzelnen beeinträchtigen können, insbesondere sein Recht auf Privatsphäre und den Schutz seiner personenbezogenen Daten. Beispielsweise könnte dies wegen eines privaten Akteurs (z. B. ein Unternehmen) geschehen, welcher das Argument von Geschäftsgeheimnissen umfassend nutzt, um einer betroffenen

Mangelnde Cybersicherheit betrifft alle

Ein Beispiel für einen typischen Cybersicherheitszwischenfall, der ein breites Spektrum der Weltbevölkerung betrifft, ist das sogenannte Mirai-Botnet. Diese Malware wurde 2016 von Studenten in den USA entwickelt und verbreitet. Diese wollten sich Vorteile im Online-Spiel Minecraft verschaffen, indem sie einen groß angelegten Distributed Denial of Service (DDoS)-Angriff auf den Spieleserver starteten. Das Botnet geriet jedoch außer Kontrolle und infizierte weltweit eine große Anzahl von IoT-Geräten, wie z.B. IP-Kameras und Home Router. Dieser Angriff und die Verbreitung der Malware waren möglich, weil Mirai die Tatsache ausnutzte, dass Benutzer die Standardbenutzernamen und -kennwörter des Herstellers auf ihren IoT-Geräten selten ändern. Nach der Infektion wurde ein IoT-Gerät Teil des Botnets und für große Netzwerkangriffe ferngesteuert. Im Oktober 2016 erreichte der Angriff einen Punkt, an dem er das Internet im gesamten Osten der Vereinigten Staaten fast vollständig zum Erliegen brachte. Die Gerätebesitzer selbst bemerkten die Malware-Infektion selten, weil die Geräte weiterhin normal funktionierten, mit Ausnahme einer gewissen Verzögerung bei den Reaktionszeiten und einer erhöhten Nutzung der Internetbandbreite.

Person ihre Rechte zu verweigern – wie zum Beispiel das Recht auf transparente Information, welche personenbezogenen Daten über sie verarbeitet werden.

Ein viel prominenteres Beispiel, das in der öffentlichen Diskussion steht, ist jedoch der Einsatz von überwachungsorientierten Sicherheitstechnologien durch staatliche Stellen; insbesondere durch die nationalen Strafverfolgungs- und Nachrichtendienste. Viele Staaten, auch innerhalb der EU, erlauben in unterschiedlichem Maße und unter unterschiedlichen Voraussetzungen den Einsatz solcher Technologien wie z.B. Deep Packet Inspection, Key Escrow, Verschlüsselungswerkzeuge mit Hintertüren und die Nutzung von Sicherheitsschwachstellen (sogenannte Zero-Day-Exploits).

Dieser Einsatz von Technologien zur Infiltration von Geräten und Kommunikation von Bürgern, um Kriminelle zu finden, ist immer wieder kritisiert worden, da er mit erheblichen Risiken durch Missbrauch, Voreingenommenheit und mangelnder Transparenz einhergeht.

Es besteht ein allgemeiner Glaube von Regierungsbeamten im Bereich der Polizei und der nationalen Sicherheit, dass die Verbrechensbekämpfung solche Mittel – wie die Opferung der grundsätzlichen Sicherheit technischer Geräte durch den Einsatz von überwachungsorientierten Technologien – rechtfertigen.

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

Im Jahr 2011 entdeckte der Deutsche Chaos Computer Club (CCC) eine Trojaner-Malware welche bestimmte Zielgeräte überwachte und dabei eine Fernsteuerung ermöglichte. Der Einsatz dieser Malware wurde kritisiert, da diese die Sicherheit des Zielgerätes beeinträchtigt. Es wurde argumentiert, dass nicht nur die Strafverfolgung, sondern auch Kriminelle und autoritäre Staaten solche Funktionalitäten ausnutzen könnten. Die Offenbarung löste eine große öffentliche Debatte über die Rechtmäßigkeit der Verwendung solcher Technologien in demokratischen Gesellschaften aus.

Viele Sicherheitsforscher warnen jedoch vor unbeabsichtigten Nebenwirkungen und Folgen, wie etwa der Einsatz von solchen Überwachungswerkzeugen durch Unbefugte. Ferner kann eine mangelnde klare Entscheidung von Regierungen zwischen offensiven oder defensiven Strategien zu unauflösbaren Diskrepanzen führen. Darüber hinaus geht es um die schleichende Ausweitung von Einsatzzwecken dieser Technologien, die einen Verstoß gegen demokratische Grundsätze und Werte darstellen kann.

In diesem Zusammenhang ist die konkrete Umsetzung des Verhältnismäßigkeitsprinzips äußerst schwierig. Dazu kommt die allgemeine Frage, ob eine umfassende Überwachung eines großen Teils der Staatsbürger in einer demokratischen Gesellschaft überhaupt erlaubt sein sollte. Ein solcher weitreichender Eingriff durch staatliche Überwachung zu Sicherheitszwecken kann die Gefahr einer Erosion der Privatsphäre sowie anderer Grundrechte und demokratischer Grundsätze mit sich bringen. Beispiele sind die Unschuldsvermutung und das Rechtsstaatsprinzip, welches das Verbot von Strafen ohne Gesetz vorsieht. Dies beispielsweise, indem man Einzelpersonen auf der Grundlage von Annahmen ein höheres Kriminalitätsrisiko zuweist und sie so zu einem Schwerpunkt oder Ziel polizeilicher Aktivitäten macht. Oder weil eine Person wegen wenigen unsicheren sowie willkürlich gewählten persönlichen oder verhaltensbasierten Auswahlfaktoren unter Verdacht gestellt wird. Es ist also auf die Notwendigkeit von Transparenz und wirksamer, auf den Grundsatz der Verhältnismäßigkeit ausgerichteter Kontrolle hinzuweisen. Dies sind auch Schlüsselprinzipien des europäischen Datenschutzrechts.

Im Privatsektor überwiegen Wirtschaftlichkeitserwägungen gegenüber Sicherheit und Datenschutz

Auch wenn private Akteure dies nicht immer erkennen, sind Cybersicherheit und Datenschutz auch für sie relevante Themen. Nicht nur, weil die zuvor genannten Regierungsstellen zunehmend auf private Akteure als Informationsquellen angewiesen sind, sondern auch aus wirtschaftlichen Gründen. Im privatwirtschaftlichen Umfeld gibt es in der Regel Prozesse für das Management der IT-Sicherheit. Diese internen Abteilungen und deren Teammitglieder werden aber oft auch mit Datenschutzfragen betraut, obwohl IT-Sicherheit und Datenschutz sehr unterschiedliche Perspektiven, Ziele und Anforderungen an das Fachwissen haben. Unabhängig von der internen Organisation kann der Schutz personenbezogener Daten eine komplexe und kontextabhängige Angelegenheit sein, die oft die Möglichkeiten der Unternehmen einschränkt, ihre eigenen wirtschaftlichen Interessen zu verfolgen, was insbesondere für datengestützte Geschäftsmodelle gilt.

Überblick über Themen im Zusammenhang mit Cybersicherheit und Datenschutz

- Staatliche Zugänge können Schlupflöcher für böswillige Parteien sein
- Offensive Maßnahmen können die Sicherheit für alle schwächen
- Schwierige Zuordnung von Verantwortung bei Cybersicherheitsvorfällen
- Rechtliche und sachliche Rahmenbedingungen oft unklar
- Zunehmende Abhängigkeit von verwundbarer IT
- Schnelle Weiterentwicklung von Technologien
- „Rüstungswettlauf“ von Offensivstrategien
- Risiko des Missbrauchs
- Unterschiedliche und unhorhersehbare Auswirkungen von Vorfällen
- Cybersicherheit ist ein sehr schwieriges globales Thema
- Komplexes Spielfeld der Akteure, mangelnde Transparenz
- Viele Cybersicherheitsmaßnahmen beruhen auf Überwachung
- Bürger wollen nicht zwischen Privatsphäre und Sicherheit entscheiden müssen
- Datenbasierte Unternehmen wollen nur begrenzt in Sicherheit und Datenschutz investieren
- Verletzung der Grundrechte auf Privatsphäre und Datenschutz
- Fehlgeleitete Vertrauenswürdigkeit von Sicherheitswerkzeugen, die den Datenschutz gefährden können
- Noch immer weit verbreiteter Mangel an minimalen Sicherheitsstandards, der mit der weiteren Verbreitung des „Internet der Dinge“ immer dringlicher wird.
- Fehlende Unterstützung für KMU, z.B. durch Finanzierungs- und Schulungsmaßnahmen für eine bessere IT-Sicherheit.

Technische und organisatorische Maßnahmen sowohl der IT-Sicherheit als auch des Datenschutzes können kostspielig und schwierig zu implementieren sein. Dies gilt insbesondere für kleine und mittlere Betriebe (KMUs), betrifft aber letztlich den gesamten Privatsektor. Das schließt jene Bereiche ein, in denen für die Datenverarbeitung Verantwortliche mit sensiblen personenbezogenen Daten, wie beispielsweise Gesundheitsdaten, umgehen und die sogar als Teil einer kritischen Infrastruktur eingestuft werden können. Beispielsweise fehlt vielen Arztpraxen, Krankenhäusern und medizinischen Forschungseinrichtungen das Problembewusstsein sowie eine ausreichende Finanzierung, um die erforderlichen IT Sicherheitsmaßnahmen umzusetzen. Zudem fehlt ihnen oft auch das Fachwissen dazu.

EU-Bürger wollen alles – Sicherheit, Privatsphäre und Datenschutz

Verschiedene Studien und Forschungsaktivitäten in der EU zeigen, dass die europäischen Bürger einen umfassenderen Ansatz für Sicherheit und Datenschutz wünschen. Im Gesundheitsbereich reagieren die Bürger besonders sensibel auf den Umgang mit ihren Gesundheitsdaten. Die Einwilligung und das Vertrauen in eine ordnungsgemäße Erfassung, Verarbeitung und Speicherung solcher Daten sind stark kontextabhängig. Auch gegenüber Unternehmen sorgen sich die Bürger wegen möglicher Datenschutzverletzungen. Es fehlt zuweilen nicht nur an Vertrauen in diese Privatunternehmen in Bezug auf deren Nutzung personenbezogener Daten, sondern auch die Sicherheit im Bereich von Internet und E-Commerce bereitet Sorge. Im Bereich der Polizei und der nationalen Sicherheit gibt es hingegen eine differenziertere Wahrnehmung der Rolle des Staates und in Bezug auf riskante Technologien. Bürger halten nationale Sicherheitsmaßnahmen allgemein für akzeptabler, wenn sie den Staat nicht als Eindringling, sondern als Beschützer betrachten, was jeweils von ihrer Erfahrung und der Geschichte ihres Landes abhängt.

Die Pflichten des Verantwortlichen einer Datenverarbeitung sind entscheidend

Aus datenschutzrechtlicher Sicht sind die Pflichten des Verantwortlichen einer Datenverarbeitung am relevantesten im Rahmen der Cybersicherheit. Gemäß der DSGVO sind verantwortliche Stellen und ihre Auftragsverarbeiter gesetzlich verpflichtet, geeignete technische und organisatorische Maßnahmen zum Schutz jener personenbezogenen Daten zu ergreifen, die sie erheben und verarbeiten wollen. In bestimmten Fällen muss zunächst eine Datenschutzfolgenabschätzung durchgeführt werden. Welche Maßnahmen letztlich eingesetzt werden müssen, hängt jeweils von Fall, Situation und Stand der Technik ab.

Dies ist der Punkt, wo Synergien mit Cybersicherheitsmaßnahmen möglich werden. Denn obgleich es Cybersicherheitsmaßnahmen gibt, die mit dem Schutz von Betroffenenrechten in Konflikt stehen können, gibt es wiederum auch Maßnahmen, die den Datenschutz verbessern. Beispiele für solche präventiven oder reaktiven Maßnahmen sind Zugangskontrolle, Verschlüsselung, Datentrennung, Anonymisierung, Pseudonymisierung, Verzeichnisse von Verarbeitungsaktivitäten, technische und organisatorische Verfahren für Backup und Wiederherstellung, Protokollierung und vordefinierte Verfahren für die Meldung und Benachrichtigung bei Datenschutzverletzungen. Im Rahmen der technischen und organisatorischen Maßnahmen enthalten sowohl die DSGVO als auch die Richtlinie 2016/680 spezifische Anforderungen zur Gewährleistung der Verarbeitungssicherheit in Bezug auf Vertraulichkeit, Integrität, Verfügbarkeit und Widerstandsfähigkeit von IT-Systemen und -Diensten im Kontext der Verarbeitung personenbezogener Daten.

Solche Maßnahmen können auch aus datenschutzfreundlicher Technikgestaltung und geeigneter Voreinstellungen bestehen. Mit dem neuen Rechtsrahmen der DSGVO erhöht die Nichteinhaltung der rechtlichen Vorgaben das Risiko negativer Konsequenzen für verantwortliche Stellen. Denn zum einen müssen sie die Rechtskonformität nachweisen während die zuständigen Datenschutzbehörden nun über erweiterte Durchsetzungsbefugnisse verfügen. Daher ist

es für die Verantwortlichen ratsam, in ihrem Unternehmen ein wirksames Datenschutzmanagementverfahren einzurichten. Darüber hinaus sind jährliche Sicherheitskontrollen, Audits und die Implementierung von Best Practices aus dem Sicherheitsbereich, wie Penetrationstests und die Dokumentation von Sicherheitsvorfällen, sinnvolle Maßnahmen zur Erreichung und zum Nachweis der Compliance.

Lösungsmöglichkeiten zusammengefasst: Verfolgung und Förderung ganzheitlicher Ansätze

Wie bereits oben ausgeführt, gibt es in den Mitgliedsstaaten der Europäischen Union derzeit eine Vielzahl von Trennungsfaktoren, die es zu überwinden gilt. Durch die Nutzung möglicher Synergien zwischen Sicherheits- und Datenschutzansätzen und -Maßnahmen könnten wesentlich mehr (auch kosteneffiziente) positive Auswirkungen auf die Cybersicherheit erreicht werden. Sicherheitsmaßnahmen, Technologien und Anwendungsszenarien sollten sorgfältig geprüft werden, bevor deren gesellschaftliche Akzeptanz angestrebt wird. Dabei sollte ein ausgewogeneres Verhältnis angestrebt werden, das darauf abzielt, die Ziele von Sicherheit, Privatsphäre, Datenschutz und Grundrechten gemeinsam anzustreben, anstatt der bisherigen Trade-Off Sicht zu folgen.

In diesem Zusammenhang können sich technische und organisatorische Maßnahmen zur Stärkung der Privatsphäre, zum Datenschutz, und für die (Cyber) Sicherheit gegenseitig verstärken. Da diese Fachgebiete viel voneinander lernen können, sollte ganzheitliche und interdisziplinäre Forschung künftig mehr unterstützt werden. Darüber hinaus sind Transparenz, Vertrauen sowie „Checks and Balances“ zentral, um eine wertorientierte Cybersicherheit zu erreichen. Es ist ratsam, diese Werte in einem ersten Schritt im Gesetzgebungsprozess zur Regelung des Datenschutzes in der elektronischen Kommunikation für die Zukunft zu berücksichtigen. Dabei sollte der Schwerpunkt darauf liegen, den Verantwortlichen mehr Verpflichtungen bezüglich Transparenz, Kontrollmöglichkeiten für den Betroffenen und Sicherheitsmaßnahmen aufzuerlegen, als auch verbesserte Rechenschafts- und Durchsetzungsmechanismen zu etablieren.

Mehr Informationen

Dieser Policy Brief basiert auf der Forschungsarbeit des CANVAS-Projekts (Constructing an Alliance for Value-driven Cybersecurity). Detaillierte Berichte über diese Arbeit wurden in vier wichtigen Whitepapers in englischer Sprache veröffentlicht:

1. Cybersecurity and Ethics
2. Cybersecurity and Law
3. Attitudes and Opinions Regarding Cybersecurity
4. Technological Challenges in Cybersecurity

Alle Whitepapers finden Sie auf unserer Website, zusammen mit allen unseren (herunterladbaren und druckbaren) Policy Briefs, kurze Online-Erklärungen zu den wichtigsten Fragen der Cybersicherheit und kommentierte Literaturlisten zur vertieften Lektüre:

canvas-project.eu

Darüber hinaus finden Sie auf unserer Website noch mehr CANVAS Projektmaterial:

CANVAS Reference Curriculum
(Integration der Werteperspektive in die Aus- und Weiterbildung im Bereich Cybersicherheit)

CANVAS MOOC
(Massive Open Online Kurs)

Open Access Buch
“The Ethics of Cybersecurity”

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.

Projektdauer:
September 2016 – Oktober 2019

Ziel von CANVAS:
Die Zusammenführung von Interessengruppen aus Schlüsselbereichen der Europäischen Digitalen Agenda, um der Herausforderung zu begegnen, wie die Cybersicherheit mit den europäischen Werten und Grundrechten in Einklang gebracht werden kann.

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

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

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

Version und Veröffentlichungsdatum:
Version 2.0, Oktober 2019