POLICY BRIEF NO. 1

VERTRAUEN IN DIE CYBERSICHERHEIT DER EU SCHAFFEN

Vertrauen und Vertrauenswürdigkeit

Wie wichtig ist Cybersicherheit für das Vertrauen in der Online-Welt? Und wie kann wiederum Vertrauen in die Cybersicherheit erreicht werden? Wir werden kurz den Kern vieler philosophischer, psychologischer und soziologischer Ansichten über Vertrauen skizzieren. Dann werden wir die Auswirkungen auf die Cybersicherheit erörtern.

Theorien über Vertrauen

Vertrauen wird oft mit einem gewissen Risiko, Unsicherheit und Verletzlichkeit verbunden. Verletzlichkeit ergibt sich aus der Abhängigkeit in einer Situation mit unvollkommenen Informationen, insbesondere über die Motivation und/oder das Verhalten anderer. Wissenschaftler haben Vertrauen so definiert, dass es im Wesentlichen moralische Verpflichtungen beinhaltet (Baier 1986; Nickel 2007), oder eine vorhersehbare Konvergenz der Interessen (Hardin 1992). Andere fordern jedoch gegenseitig verstärkende Motivationen, z.B. sind vertrauenswürdige Menschen von Natur aus motiviert, durch das in sie gesetzte Vertrauen zuverlässig zu sein (Pettit 1995). Vertrauen ist oft kontextabhängig: Ich kann meinem Buchhalter vertrauen um meine Steuererklärungen einzureichen, aber nicht als politischer Berater zu fungieren. Angemessenes Vertrauen ist ein Vertrauen gegenüber Akteuren, die dieses Vertrauen verdienen. Gut platziertes Vertrauen ist sozial vorteilhaft. Umgekehrt ist das Vertrauen in nicht vertrauenswürdige Agenten typischerweise schädlich. Vertrauen ist nicht nur schwer zu gewinnen, sondern noch schwieriger wiederzugewinnen, nachdem es einmal verloren gegangen ist.

Vertrauen kann sowohl rational als auch unvernünftig sein. Der nicht-rationale Aspekt ist eine Art Optimismus bezüglich der Motivation anderer Menschen (Jones 1996). Einige Leute vertrauen anderen, über die sie wenige Informationen haben, sogar völlig Fremden. Dies ermöglicht die Entstehung von sozial vorteilhaften Formen der Zusammenarbeit, die ohne solche Einstellungen nicht aufgebaut werden könnten (Ostrom 2000). Allerdings wird bereits in kleinen Gruppen, in denen man sich trotz fehlender Information über Gruppenmitglieder vertraut, häufiger nicht-kooperatives Verhalten festgestellt (Ostrom 2000). Daher könnte eine ausschließlich auf Vertrauen basierende soziale Zusammenarbeit in komplexen Gesellschaften oder in internationalen Beziehungen gegebenenfalls nicht möglich sein (Hardin 2009).

Online-Vertrauen

In den Anfängen des Internets schien es, dass Online-Vertrauen aufgrund der Anonymität des Internets nicht aufgebaut werden könne (Pettit 2004): Wie das berühmte Zitat sagt, „Im Netz weiß niemand, dass man ein Hund ist". Im heutigen Internet 2.0 ist dies jedoch nicht mehr der Fall. Online-Feedback und digitale soziale Bewertungssysteme basieren alle auf semi-stabilen und semi-überprüfbaren Internet-Identitäten (Etzioni 2017). Diese Lösungen haben es ermöglicht, Online-Märkte (z.B. Ebay und Amazon) und Interaktionen in der sogenannten Sharing Economy (z.B. AirBnB und BlaBlaCar) zu entwickeln.

Zwischenmenschliches und institutionelles Vertrauen

Ein Beteiligter oder eine Organisation, die sich deshalb als zuverlässig erweist, nur weil sie befürchtet, vor Gericht gestellt zu werden, ist nicht vertrauenswürdig. Viele Formen des Vertrauens und der Vertrauenswürdigkeit ergeben sich dann, wenn es keine direkten wirtschaftlichen Anreize oder rechtlichen Sanktionen gibt. Gerade bei wichtiger Zusammenarbeit zwischen völlig Fremden mit hohem Einsatz ist ein starkes, rein zwischenmenschliches Vertrauen schwer zu erreichen, weil es zu riskant ist.

Es ist also keine leichte Aufgabe, ein Umfeld und ein System von Reputation und Anreizen zu schaffen, das Vertrauen ermöglicht und fördert. Effektiv durchgesetzte rechtliche Sanktionen gegen unehrliches Verhalten können vertrauensvolle Beziehungen begünstigen, indem sie die Risiken mindert, die mit dem Vertrauen in Fremde verbunden sind (Hardin 1992). Allerdings setzt das Vertrauen in rechtliche Sanktionen wiederum auch Vertrauen in die Institutionen voraus, die diese Normen durchsetzen.

Cybersicherheit und Vertrauen

Cybersicherheit ist notwendig für Vertrauen

Bevor wir das Vertrauen in die Cybersicherheit betrachten, muss festgehalten werden, dass Cybersicherheit selbst für Vertrauen notwendig ist. Die klassischen Ziele der Cybersicherheit – Vertraulichkeit, Integrität und Verfügbarkeit – sind allesamt Voraussetzungen für das Vertrauen in den digitalen Bereich. Aus datenschutzrechtlicher Sicht ist Integrität definiert als die Eigenschaft, dass Daten und Dienste nicht unbefugt oder unentdeckt verändert werden können. Integrität ist daher ein wesentliches Element, um Vertrauen in Informationen zu schaffen und zu erhalten. DateninteGrität ist beispielsweise unerlässlich, um IKT-Dienste zu bewerten sowie das Vertrauen zu rechtfertigen, dass Unternehmen gute Dienstleistungen erbringen. Die Integrität und Verfügbarkeit von Informationen ist auch notwendig, um die digitale Identität jener Personen zu überprüfen, mit denen man online interagiert. Wenn sich jemand die digitale Identität eines anderen Menschen online aneignen kann, kann dessen Ruf missbraucht werden und keine Online-Identität eines Menschen ist mehr vertrauenswürdig. Des Weiteren ist gegenseitiges Vertrauen durch Vertraulichkeit gekennzeichnet. Vertrauen ermöglicht den Austausch sensibler Informationen. Diejenigen, die vertrauen, machen sich anfällig gegenüber jenen, denen sie vertrauen, da geteilte vertrauliche Informationen gegen sie verwendet werden könnten. Dies kann daher nur mit einem vertrauenswürdigen Gegenüber sinnvoll sein. Daher ist Cybersicherheit für das Online-Vertrauen notwendig: In der Cybersicherheit bedeutet die Vertraulichkeit, dass Daten und Dienste nicht unbefugten Beteiligten zur Verfügung stehen. Cybersicherheit reduziert das Risiko, dass sensible Informationen für nicht vertrauenswürdige Akteure zugänglich werden. In Ermangelung von Cybersicherheit wäre es nicht sinnvoll, sensible Informationen online zu teilen, so dass viele Online-Transaktionen nicht mehr stattfinden könnten.

Vertrauen ist notwendig für Cybersicherheit

Während Vertrauen von Cybersicherheit abhängt, hängt Cybersicherheit umgekehrt auch von Vertrauen ab. Aus diesem Verhältnis können sich sowohl positive als auch negative Auswirkungen ergeben.

Ethisches Hacking

Ethische oder „White-Hat“ Hacker sind Hacker, die legale Ziele verfolgen, wie z. B. die Prüfung der Sicherheit von Informationssystemen gegen böswillige Angriffe. Dabei können sie ähnliche Techniken wie so genannte bösartige oder „Black-Hat“ Hacker einsetzen. Jedoch nutzen White-Hat Hacker IKT-Schwachstellen nicht kriminell zu ihrem eigenen Vorteil aus. Es gibt vertrauenswürdige White-Hat-Hacker, die von vielen Unternehmen eingesetzt werden, um ihre Schwachstellen zu identifizieren. Diese Form der Sicherheitsforschung ist nur möglich, weil einige Unternehmen zunächst bereit waren, einigen White-Hat-Hackern zu vertrauen. Somit kommt die Wahl dieser ersten, mehr risikobereiten Unternehmen auch anderen, weniger risikofreudigen Unternehmen zugute. Auf diese Weise haben Unternehmen, die sich gegenseitig vertrauen, die Möglichkeit, vertrauenswürdige ethische Hacker zu identifizieren. Die Empfehlung eines vertrauenswürdigen Unternehmens bildet die Grundlage für den Glauben an die Vertrauenswürdigkeit des White-Hat-Hackers. Darüber hinaus ermöglicht ein Umfeld, in dem es sich für einen Hacker lohnt, einen guten Ruf zu haben, auch Vertrauen durch solche Anreize.

Die Vertrauenskette wird auf diese Weise ausgebaut. Das Vertrauen zwischen dem Unternehmen und dem ethischen Hacker macht Unternehmen sicherer und damit vertrauenswürdiger für ihre Kunden. Der allgemeine Rechtsrahmen des europäischen Datenschutzes und aller nationalen und internationalen Gesetze zur Förderung der Cybersicherheit tragen zur Cybersicherheit mittels Vertrauen in Institutionen bei. Die Verbraucher könnten sich dann darauf verlassen, dass Unternehmen, welche die Cybersicherheit nicht schützen, bestraft werden können; vorausgesetzt dass diese Unternehmen rational handeln, um Sanktionen zu vermeiden. Vertrauenswürdiger sind demnach jene Unternehmen, welche der Verpflichtung nachkommen, ausreichende organisatorische und technische Maßnahmen zu ergreifen, um ein hohes Maß an Cybersicherheit zu erzielen. Datenschutzgesetze, die eine transparente Kommunikation mit Betroffenen im Falle von Datenschutzverletzungen verlangen, schaffen ebenfalls einen Anreiz für Unternehmen, ein höheres Maß an Cybersicherheit zu erreichen. Unternehmen haben eine größere Motivation, Verletzungen des Schutzes personenbezogener Daten zu vermeiden, wenn sie solche Vorfälle nicht auf legale Weise vor den Betroffenen verbergen können.

Misstrauen schwächt die Cybersicherheit: Die Verwendung von Zero-Day-Exploits

Zero-Day-Exploits sind Schwachstellen in Software, die dem Hersteller der Software noch nicht bekannt sind und deshalb von diesem nicht behoben werden können. Die Ausbeutung von Zero-Days ist eine Art Waffe, da sie Computer und Netzwerke stören und unberechtigten Zugang zu relevanten Informationen gewähren kann.

Regierungen können Zero-Days für Geheimdienstaktivitäten im Ausland nutzen, indem sie diese kaufen und einsetzen, um andere Länder oder einzelne Gegner anzugreifen oder auszuspionieren. In diesem Zusammenhang lässt sich sagen, dass die Motivation, Zero-Day-Exploits für Cyberspionage gegen staatliche Ziele zu kaufen, in der Regel auf ein Versagen des gegenseitigen Vertrauens zwischen Staaten zurückzuführen ist. Dies ist ein sich selbst verstärkender Misstrauensmechanismus, da das Engagement in einem Zero-Day-Markt wiederum die Vertrauenswürdigkeit jener Regierungen auf mehr als eine Weise untergräbt.

Wenn beispielsweise jede Regierung nach Schwachstellen in den Systemen anderer Länder sucht, hat dies den Effekt, dass langfristig jedes Land weniger sicher ist. Dies birgt nicht nur die Gefahr, dass solche Schwachstellen in die Hände von Kriminellen gelangen, sondern kann auch als eine Art Wettrüsten zwischen den Nationalstaaten angesehen werden. In einer solchen Situation kann es sich kein Land leisten, inaktiv zu bleiben, weil es befürchten muss, dass andere Länder einen Vorteil erhalten, der gegen das Land verwendet werden kann. So macht die Suche nach den „Cyber-Verwundbarkeiten“ der anderen Länder Vertrauensverhältnisse zwischen den Ländern unmöglich.

Mit Misstrauen als Ausgangsbasis geht jeder Staat zu Recht davon aus, dass eine solche offensive Strategie im Gegensatz zu rein defensiven Strategien

günstiger ist, um bei ausländischen Spionage- oder Cybersabotageaktivitäten die Oberhand zu gewinnen. Darüber hinaus kann eine nationale Regierung, die nachweislich anfällig für Angriffe ist, auch gegenüber anderen Ländern weniger vertrauenswürdig erscheinen. Wenn vertrauliche Mitteilungen von Diplomaten und Politikern aufgedeckt oder manipuliert werden, kann dies zu schwerwiegenden Störungen in den zwischenstaatlichen Beziehungen führen. Darüber hinaus werden Regierungen, die von diesen Exploits Gebrauch machen, von ihren Bürgern höchstwahrscheinlich eher gefürchtet, als dass diese ihnen vertrauen. Denn wenn Regierungen über diese Waffen verfügen, können auch ihre eigenen Bürger Opfer von Cyber-Spionage und Sabotage werden. Der Erwerb von Zero-Day-Exploits kann strategisch vorteilhaft erscheinen, sogar obligatorisch in einem ungünstigen Umfeld mit geringem internationalen Vertrauen. Das wahrscheinlichste Ergebnis der Entwicklung oder des Erwerbs dieser Werkzeuge ist jedoch ein Wettlauf nach unten in Bezug auf das Vertrauen.

Schlussfolgerungen

Zusammenfassend lässt sich sagen, dass sich Vertrauen und Cybersicherheit gegenseitig stützen. Vertrauen ist vorteilhaft (wenn es gut platziert ist), zerbrechlich und nach einer Beschädigung schwer wieder aufzubauen. Individuelle Strategien (von Personen, Unternehmen und Staaten), die zum Schutz der nationalen Sicherheit rational und wirksam erscheinen können, sollten immer überprüft werden, um ihre Auswirkungen auf das Vertrauen zu beurteilen, da sie sonst Gefahr laufen, den gegenteiligen Effekt zu erzielen. Im kommerziellen Kontext kann Vertrauen mit oder ohne starke Aufsicht und mit rechtlichen Sanktionen, sowie mit einer ausgewogenen Mischung aus rechtlichen Sanktionen und Reputationssystemen erreicht werden.

Mehr Informationen
Referenzen:

- Baier, Annette. 1986. “Trust and Antitrust.” Ethics 96 (2): 231–60.
- Etzioni, Amitai. 2017. “Cyber Trust.” Journal of Business Ethics, July. https://doi.org/10.1007/s10551-017-3627-y.
- Hardin, Russell. 1996. “Trustworthiness.” Ethics 107 (1): 26–42.
- Jones, Karen. 1996. “Trust as an Affective Attitude.” Ethics 107 (1): 4–25.
- Nickel, Philip J. 2007. “Trust and Obligation-Ascription.” Ethical Theory and Moral Practice 10 (3): 309–19. https://doi.org/10.1007/s10677-007-9069-3.
- Ostrom, Elinor. 2000. “Collective Action and the Evolution of Social Norms.” The Journal of Economic Perspectives 14 (3): 137–58.
- Pettit, Philip. 1995. “The Cunning of Trust.” Philosophy & Public Affairs 24 (3): 202–25.
- 2004. “Trust, Reliance and the Internet.” Analyse & Kritik 26 (1): 108–121.

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