POLICY BRIEF NR. 1

VERTRAUEN IN DIE CYBERSICHERHEIT DER EU SCHAFFEN

Vertrauen und Cybersicherheit

Dieses Slidedoc fasst einige wesentliche Erkenntnisse aus der interdisziplinären Literatur zum Thema Vertrauen und Vertrauenswürdigkeit zusammen.

Es zeigt, dass Cybersicherheit eine wesentliche Voraussetzung für das digitale Vertrauen ist. Darüber hinaus wird ein Fall analysiert, in dem die Cybersicherheit auf Vertrauen angewiesen ist, und ein Fall, in dem sie durch mangelndes Vertrauen untergraben wird.

- Zwischenmenschliches Vertrauen
- Vertrauen und Vertrauens-würdigkeit
- Moralische und nicht-moralische Elemente von Vertrauen und Vertrauenswürdigkeit
- Vertrauen vs. Sanktionen

Erreicht:

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Nichtverkettbarkeit
- Intervenierbarkeit
- Transparenz

Vertrauen in jemanden vs. Vertrauen in etwas

Vertrauen und Vertrauenswürdigkeit bilden positive Feedbackschleifen

Zwischenmenschliches Vertrauen ist eine dynamischere Beziehung als das Vertrauen in Mechanismen und Systeme.
Vertrauen unter Personen/Organisationen ist dynamisches Vertrauen: Vertrauenswürdige Menschen reagieren in besonderer Weise auf Menschen, die ihnen vertrauen (Pettit 1995).

Vertrauenswürdigkeit: moralisch oder nicht?

Vertrauenswürdigkeit kann sowohl moralisch als auch nicht-moralisch motiviert werden.

Vertrauen und Reputation
Vertrauenswürdige Menschen können durch den Wunsch nach einem guten Ruf motiviert werden (Pettit 1995). Diese Motivation ist nicht moralisch (aber nicht unmoralisch). Je mehr die soziale Zusammenarbeit auf Vertrauensbeziehungen angewiesen ist, desto wichtiger wird die Reputation.

Vertrauen und moralische Verpflichtungen
Vertrauenswürdige Menschen können durch moralische Verpflichtungen motiviert werden, denn Vertrauen zu akzeptieren ist ähnlich wie Versprechen. Wenn die Erwartungen an das Vertrauen nicht erfüllt werden, wird das oft als Vertrauensbruch beschrieben (Baier 1986).

Der dynamische Aspekt von zwischenmenschlichem Vertrauen

Transparenz über die Dispositionen und Leistungen von Akteuren (Personen oder Organisationen) beeinflusst den Erfolg von „Meta-Vertrauen“ (Baier 1986), unser Verlass auf zwischenmenschliches Vertrauen, um wichtige soziale Ziele zu erreichen.

Mit vollständigen Informationen überleben nur vertrauenswürdige Akteure.

Ohne Informationen sind egoistische Strategien erfolgreicher als faire und kooperative.

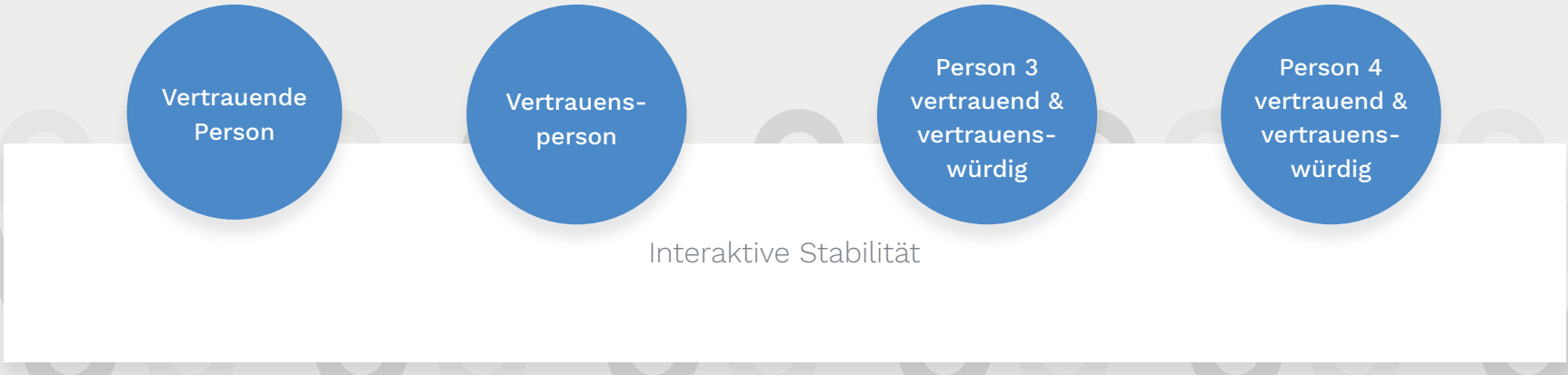
Wenn es nicht möglich ist, zwischen vertrauenswürdigen und nicht vertrauenswürdigen Parteien zu unterscheiden, kann sich keine auf gegenseitigem Vertrauen basierende Zusammenarbeit entwickeln (Olson 2000).

Gegenseitiges Vertrauen beinhaltet gegenseitige Verantwortung

Das Vertrauen in vertrauenswürdige Akteure ermöglicht breite Netzwerke des gegenseitigen Vertrauens.

Informationen

vertrauenswürdig vs. nicht vertrauenswürdig



Vertrauen ist Zuversicht in die Tugenden eines anderen Menschen

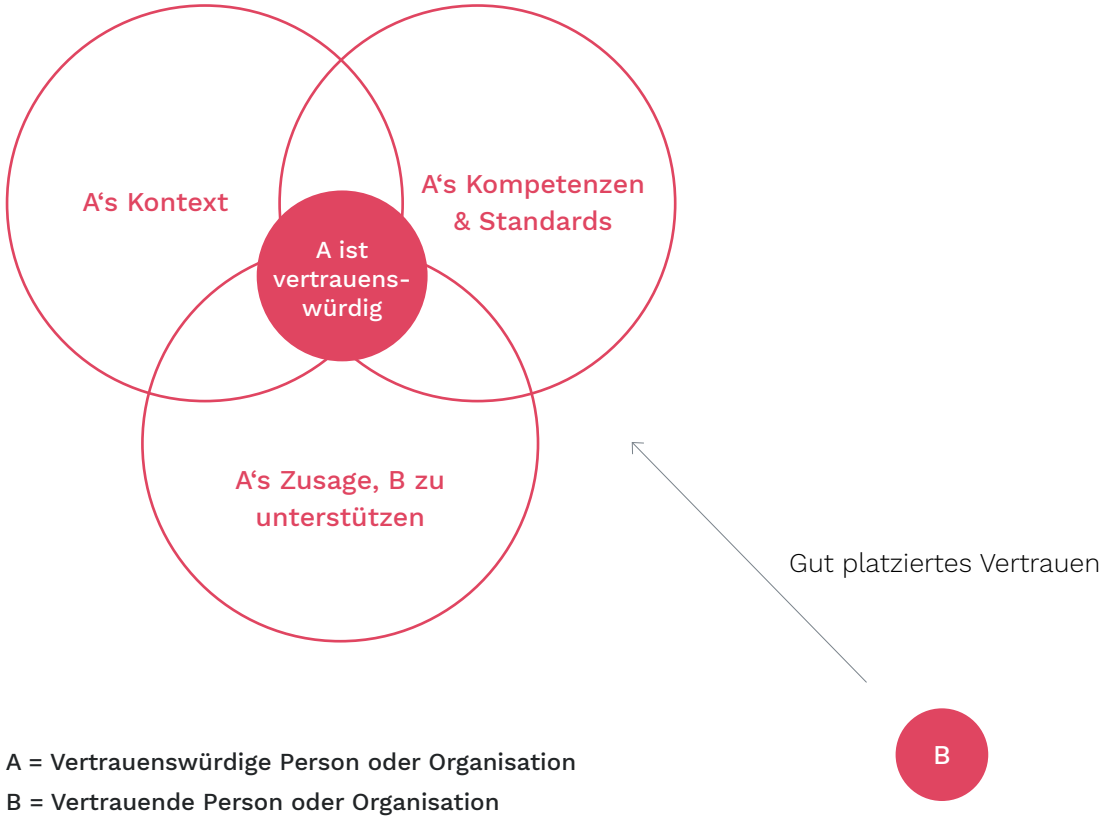
Vertrauen impliziert ein Gefühl der Zuversicht in das Wohlwollen, die Gewissenhaftigkeit, die Reziprotät und das Engagement für Gerechtigkeit (Becker 1996).

Vertrauen hat auch nicht-kognitive Aspekte:

Risiken eingehen
Jemandem zu vertrauen bedeutet, bereit zu sein, auf das kooperative Verhalten eines anderen auch dann zu setzen, wenn keine Vorhersage auf der Grundlage der Ratio einer „Nutzwertmaximierung“ möglich ist (Held 1968).

Optimismus
Es erfordert Optimismus, dass sich der gute Wille und die Kompetenz einer anderen Person auf unsere Interaktion mit ihr erstreckt (Jones 1996), insbesondere wenn zukünftige Interaktionen vorgesehen sind (Olson 2000).

Dieser Optimismus ist nicht streng rational, aber auch nicht töricht. Eine Vielzahl von Experimenten hat gezeigt, dass der Mensch auch in Situationen, in denen die Zusammenarbeit nicht rational im Interesse des Einzelnen zu sein scheint, vertrauensvolle Beziehungen aufbauen kann (Olson 2000).



A = Vertrauenswürdige Person oder Organisation
B = Vertrauende Person oder Organisation

Vertrauen im Vergleich zu rationaler Vertrauens-würdigkeit bei der Vermeidung von Sanktionen

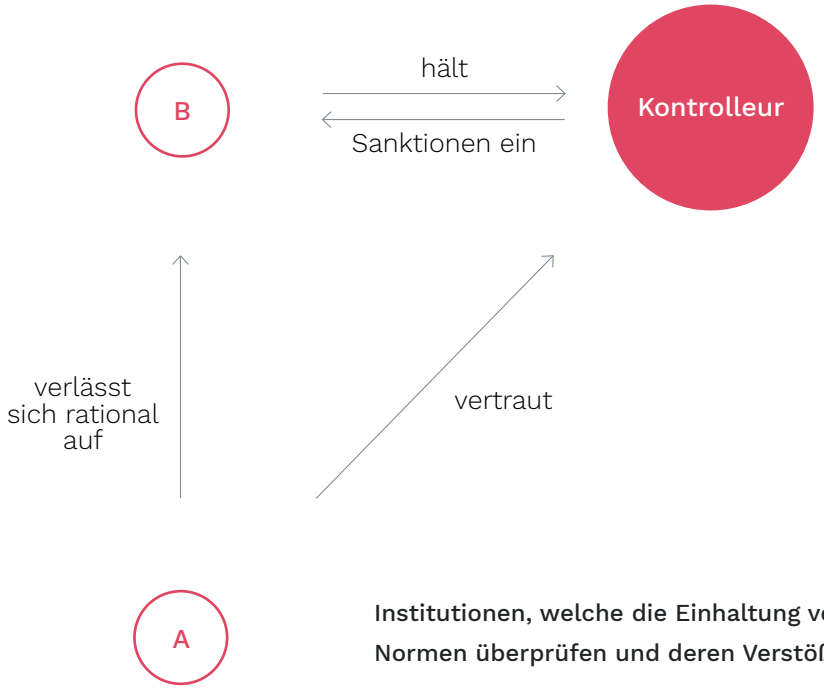
Rechtliche Institutionen und wirtschaftliche Anreize erzeugen eine andere Art von Vertrauenswürdigkeit.

Zuverlässigkeit kann durch Institutionen erreicht werden, die Sanktionen gegen unzuverlässige Parteien verhängen. Dies sind Mechanismen der externen Rechenschaftspflicht.

Rationale Vertrauenswürdigkeit mildert die Unsicherheit und die Notwendigkeit, sich auf gegenseitiges Vertrauen zu verlassen.

Rationale Vertrauenswürdigkeit und Vertrauen funktionieren nicht immer gut in Kombination.

Die empirische Literatur zeigt, dass Sanktionen und wirtschaftliche Anreize jedoch soziale und moralische Motivationen verdrängen können, um vertrauenswürdig zu sein (Frey 1994). Es kann den Menschen schwerer fallen, eine Bedingung für selbstverstärkendes gegenseitiges Vertrauen zu erreichen, wenn Sanktionen gegen Vertrauensbruch aufgehoben werden (Frohlich, Norman und Joe A. Oppenheimer 1996, Ostrom 2000).



Institutionen, welche die Einhaltung von Normen überprüfen und deren Verstöße ahnden

Cybersicherheit als Wegbereiter von Vertrauen

Elemente der Cybersicherheit

Integrität
(Personenbezogene) Daten und Dienste, welche diese Daten verarbeiten, dürfen nicht unbefugt oder unentdeckt verändert werden.

Verfügbarkeit
Der Zugriff auf (personenbezogene) Daten und auf Dienste, welche diese Daten verarbeiten, wird stets nachvollziehbar, verarbeitungsfähig und zeitnah gewährt.

Vertraulichkeit
(Personenbezogene) Daten und Dienste, welche diese Daten verarbeiten, sind für unbefugte Personen nicht zugänglich.

Mechanismen zur Vertrauensbildung

Transparenz
Auf gegenseitigem Vertrauen basierende Beziehungen gedeihen, wenn vertrauenswürdige Akteure (Personen und Organisationen) erkannt werden können.

Reputation
Reputationssysteme bieten nicht-moralische Anreize, um vertrauenswürdig zu sein.

Keine Faktenfälschung
Vertrauen wird durch unzuverlässige Vertrauenswürdigkeitssignale untergraben.

Privatheit (für Einzelpersonen und Gruppen)
Gegenseitiges Vertrauen ermöglicht und fördert den Austausch vertraulicher Informationen. Dies ist nur dann nachhaltig, wenn nicht vertrauenswürdige Parteien von den Informationen ausgeschlossen werden können.

Institutionen beeinflussen das Vertrauen der Bürger in Akteure der Cybersicherheit

Erfolgreiche Gesetze, soziale Praktiken und soziale Normen stützen rationale Erwartungen und emotionale Vertrauenshaltungen.

Akteure, die an der Prävention, Ermittlung und Ahndung von Cyberkriminalität beteiligt sind.

National (Beispiele)	EU (Beispiele)
– Zuständige NIS-Behörden – CERTs266 – Polizeikräfte – Cyberkriminalitäts-einheiten – Verteidigungs- und Sicherheitsbehörden	– ENISA – CERT-EU – EP3R – EC3 (Europol) – CEPOL – Eurojust – EEAS – EDA

Länder mit nationalen Gesetzesmaßnahmen zur Cybersicherheit

– Österreich (2013)
– Kroatien (2015)
– Tschechien (2015)
– Republik Zypern (2012)
– Die Niederlande (2014)
– Estland (2014)
– Finnland (2013)
– Frankreich (2015)
– Italien (2013)
– Deutschland (2011)
– Ungarn (2013)
– Lettland (2013)
– Litauen (2011)
– Luxemburg (2018)
– Malta (2015)
– Polen (2013)
– Slowakische Republik (2015)
– Spanien (2013)
– Großbritannien (2016)

EU-Gesetzgebungsmaßnahmen zur Cybersicherheit

– Vorschlag für eine neue Verordnung über Cybersicherheit (12. September 2018)
– Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 (DSGVO)
– Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009
– Richtlinie 2011/92/EU des Europäischen Parlaments und des Rates vom 13. Dezember 2011
– Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12. August 2013
– Richtlinie (EU) 2015/849
– Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April.
– Richtlinie 2008/114/EG des Rates
– Verordnung Nr. 611/2013 der Kommission vom 24. Juni 2013
– Richtlinie 2016/1148 des Europäischen Parlaments und des Rates

Die Regulierung der Cybersicherheit hat verschiedene Facetten

Die EU-Gesetzgebungsmaßnahmen zur Cybersicherheit befassen sich mit verschiedenen Aspekten der Cybersicherheit.

- Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 (DSGVO)
- Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009
- Richtlinie 2011/92/EU des Europäischen Parlaments und des Rates vom 13. Dezember 2011
- Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12. August 2013
- Richtlinie (EU) 2015/849
- Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April.
- Richtlinie 2008/114/EG des Rates
- Verordnung Nr. 611/2013 der Kommission vom 24. Juni 2013
- Richtlinie 2016/1148 des Europäischen Parlaments und des Rates

Fallstudie 1 Ethisches Hacking und Datenschutz (1/3)

Häufig ist der beste Weg, Schwachstellen zu erkennen, das Vertrauen in einen ethischen Hacker... .

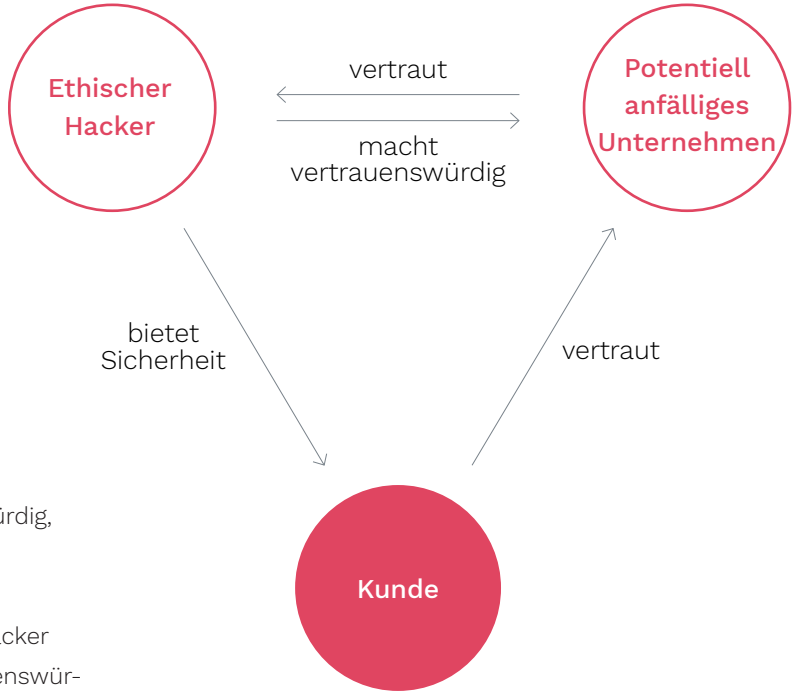
Ethisches Hacking

Ethische Hacker („White Hat"-Hacker) verwenden die gleichen Werkzeuge und Techniken wie bösartige Hacker, um die Cyber-Abwehr eines Unternehmens auf Anfrage und mit dessen Erlaubnis zu testen.

Ein Datenschutzdilemma

Durch Penetrationstests erhält ein ethischer Hacker Zugang zu den personenbezogenen Daten der Kunden. Das Risiko besteht darin, dass der Nutzer vertrauliche Informationen absichtlich missbraucht oder fahrlässig preisgibt.

Die Lösung dieses Dilemmas besteht darin, einen Hacker zu finden, dem man vertrauen kann: Ein vertrauenswürdiger Hacker verhält sich wohlwollend, gewissenhaft und kompetent.



Ein Teufelskreis des Vertrauens?

- Das Unternehmen ist nur dann vertrauenswürdig, wenn seine Cybersicherheitsmaßnahmen ordnungsgemäß getestet werden.
- Penetrations-Tests durch einen ethischen Hacker machen das Unternehmen nur dann vertrauenswürdiger, wenn der Hacker auch vertrauenswürdig ist.
- Wie kann das Unternehmen vertrauenswürdige Hacker identifizieren? Und wie kann der Kunde das wissen?

Fallstudie 1 Ethisches Hacking und Datenschutz (2/3)

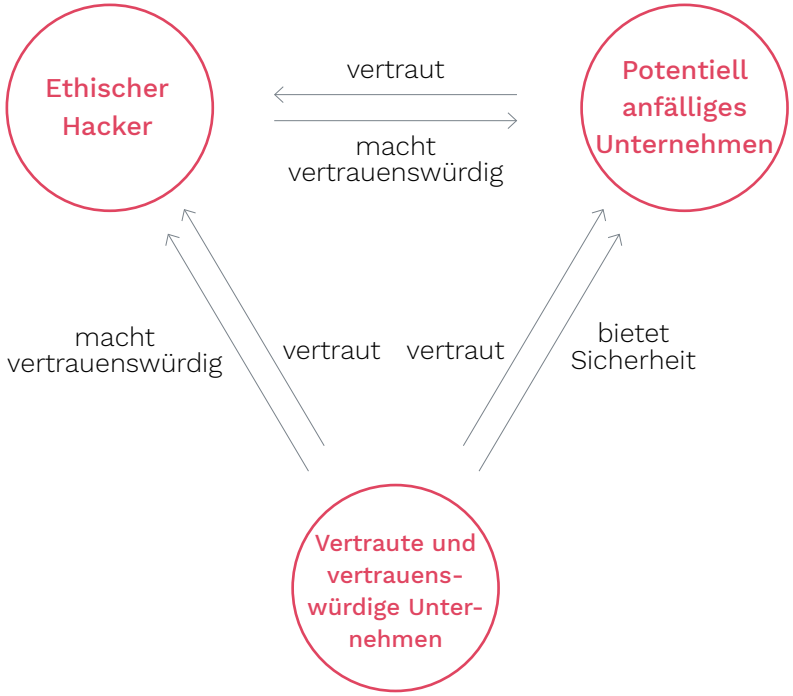
Vertrauenswürdigkeit sickert nach unten durch Vertrauensnetzwerke

Wie stellt man die Vertrauenswürdigkeit eines ethischen Hackers fest?

Es kann schwierig sein zu wissen, ob ein Hacker vertrauenswürdig ist. In der Praxis ist Vertrauen aber rationaler, sofern Informationen über ethische Hacker zwischen Unternehmen mit ähnlichen Cybersicherheits-bedürfnissen und die sich gegenseitig vertrauen geteilt werden. Cluster von vertrauten (und vertrauenswür-digen) Unternehmen können Informationen austauschen, die aufzeigen, dass dem Hacker vertraut werden kann.

Aus Kundensicht:

Unternehmen, die wissen, dass ein Unternehmen zu einem Cluster gehört, welcher ein Vertrauensnetzwerk ist, haben Gründe anzunehmen dass das Unterneh-men geeignete Cybersicherheitspraktiken anwenden wird (z.B. die Einstellung vertrauenswürdiger ethischer Hacker). Dies insbesondere wenn bekannt ist, dass verbundene Unternehmen bewährte Verfahren austau-schen. Weitere Indikatoren für die Vertrauenswürdigkeit können Zertifizierungen sein, einschließlich Selbstzerti-fizierungssysteme.



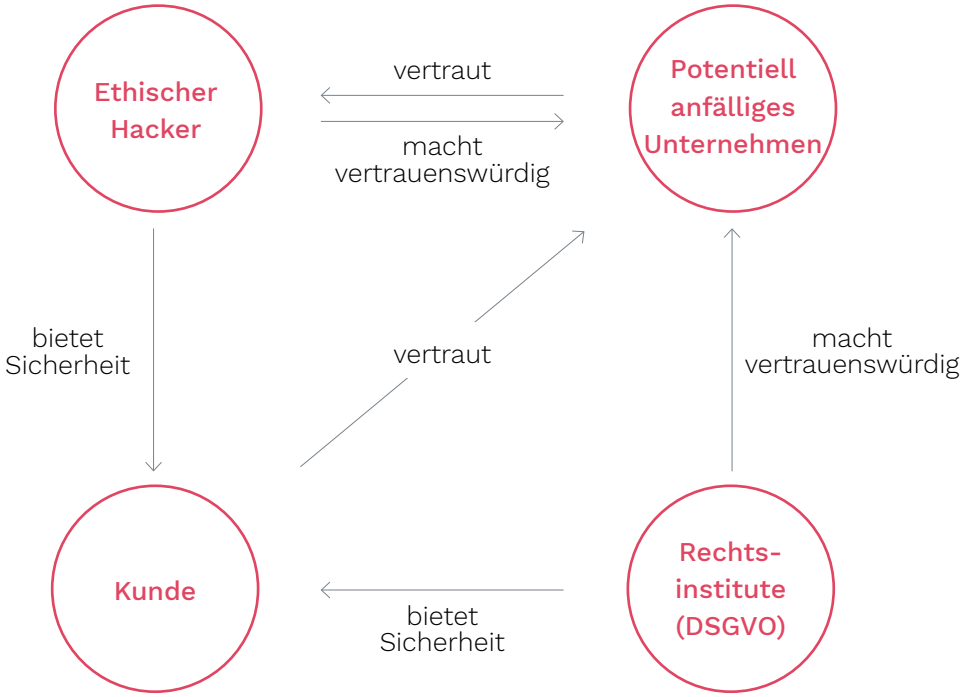
Fallstudie 1 Ethisches Hacking und Datenschutz (3/3)

Welche Rolle spielen Rechtsinstitute?

Gesetzliche Anforderungen tragen dazu bei, die Vertrauenswürdigkeit der Akteure zu sichern.
Die DSGVO verlangt von den Unternehmen, dass sie für eine adäquates Level der Cybersicherheit sorgen. Dies schafft einen Anreiz, eine solche Cybersicherheit tatsächlich zu erreichen, was widerum zur Vertrauenswürdigkeit und langfristig zum Vertrauen beiträgt.

In bestimmten Kontexten (z.B. bei Gesundheitsdaten) können Kunden bestimmte Erwartungen an die Vertraulichkeit ihrer Informationen haben (z.B. dass sie diese nur von ihren behandelnden Ärzten gesehen werden). Der Datenschutz sollte weder als Feind der Cybersicherheit, noch als Ausrede dienen, diese nicht zu gewährleisten.

Die Erwartungen der Kunden an den Datenschutz sollten auch durch effektive Kommunikation adressiert werden. So sollte beispielsweise der Zugriff eines ethischen Hackers auf personenebezogene Daten von Patienten transparent kommuniziert werden (dies ist auch eine rechtliche Anforderung der DSGVO). Dies schließt Information darüber ein, welche Maßnahmen ergriffen werden um den Schutz der Daten bei diesem Vorgang zu gewährleisten.



Fallstudie 2 Regierungen, die Zero-Day-Lücken verwenden (1/2)

Ein Cyber-Rüstungswettlauf, bei dem die Notwendigkeit von Sicherheit das Vertrauen reduziert

Eine neue Art, Feinde anzugreifen und auszuspionieren
Zero-Day-Lücken sind eine Form der Waffe, da sie Computer und deren Netzwerke stören wie auch Zugriff auf relevante Informationen geben könnten. Regierungen erwerben solche Sicherheitslücken käuflich um andere Länder oder politische Gegner anzugreifen oder auszuspionieren.

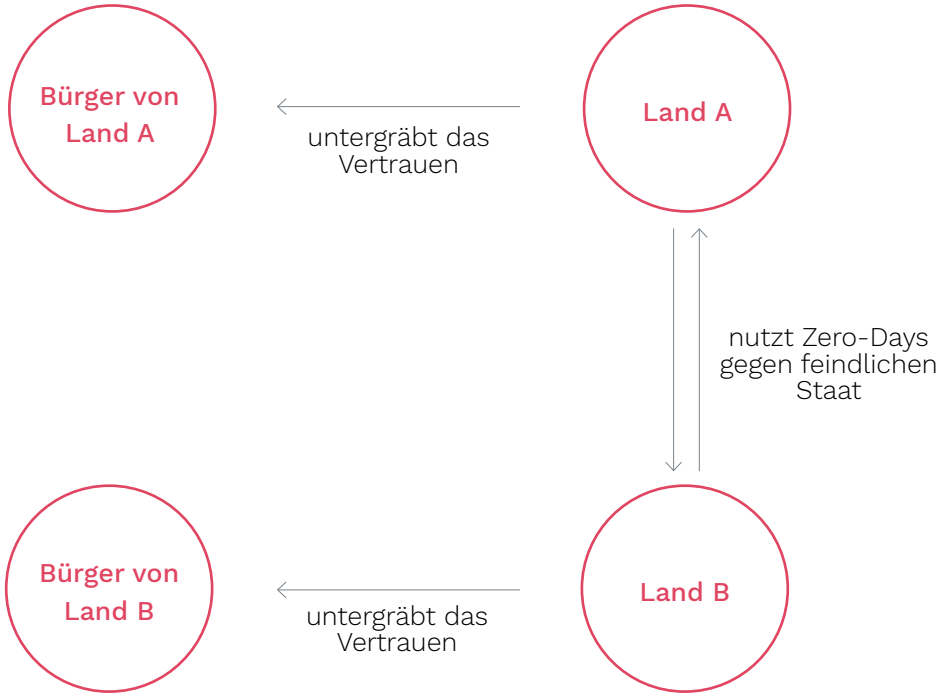
Das Gegenteil von dynamischer Vertrauenswürdigkeit
Wenn jede Regierung nach Schwachstellen anderer Länder sucht um sich selbst zu schützen wird auf lange Sicht jedes Land weniger sicher sein. Die Suche nach „Cyber-Schwachstellen“ der anderen Länder macht Vertrauensbeziehungen zwischen den Ländern unmöglich.

Die Zahlen sind die erwarteten Ergebnisse für die nationale Verteidigung (z.B. Einsparungen bei den traditionellen Verteidigungsausgaben, in Millionen von Dollar).

	Land B	Exploit	Keine Ausnutzung
Land A	Ausnutzung	-100,-100	100,-300
	Keine Ausnutzung	-300,100	30,30

Externe Faktoren der Vertrauenswürdigkeit bei der Nutzung von Zero-Day-Lücken (2/2)

Wenn Regierungen die Zero-Day-Lücken, die sie kennen, geheim halten, können ihre Bürger ihnen dann vertrauen? Kann man sich darauf verlassen, dass die Regierungen sie nicht zur Überwachung ihrer Bürger nutzen?



Vertrauen in die Cybersicherheit gewährleisten: Herausforderungen

Kommerzielle Abwägung (Nutzen vs. Sicherheit)

- Sicherheit und Datenschutz sind Kosten für datenbasierte Unternehmen
- Rüstungswettlauf um offensive Strategien
- Die Verbraucher wollen nicht, dass die mit einer erhöhten Cybersicherheit verbundenen Nutzungskosten anfallen.
- Unternehmen verlassen sich zunehmend auf anfällige IT-Systeme

Abwägung bei der Durchsetzung (Datenschutz vs. Sicherheit)

- Verletzung der Privatsphäre
- Intrusivität von Sicherheitswerkzeugen, die den Datenschutz gefährden
- Schwachstellen, die auf grauen und schwarzen Märkten an Regierungen verkauft werden
- Rechtmäßige Zugriffsversuche können Schlupflöcher für böswillige Parteien sein
- Viele Cybersicherheitsmaßnahmen beruhen auf Überwachung
- Risiko des Missbrauchs
- Offensive Maßnahmen können die Sicherheit für alle schwächen

Regulatorische Abwägung (Komplexität vs. Sicherheit)

- Schwierige Zuordnung bei Cybersicherheitsvorfällen
- Rechtliche und faktische Rahmenbedingungen oft unklar
- Sich schnell entwickelnde Technologien
- Cybersicherheit ist ein sehr komplexes globales Thema.
- Unterschiedliche und unvorhersehbare Auswirkungen von Ereignissen

Herausforderungen, die in Jasmontaite et al 2017 untersucht wurden.

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.