Matthias Fuhrland (HTW Dresden), 2023

Vertrauen in der digitalen Welt?

Fake-News, Fake-Shops, Fake-Produkte, Fake-Profile, Trojaner, Viren, Phishing Mails, unerlaubte Speicherung und Weitergabe personenbezogener Daten, Datendiebstahl, Hackerangriffe und Spionage - Angesichts des riesigen Betrugspotentials und der -schäden, die durch Anonymität und Pseudonymität im Internet begünstigt werden, stellt sich die Frage: Kann man in digitale Informationen oder bei digitalen Interaktionen überhaupt Vertrauen haben? Wie weit kann ich einer netten, aber wildfremden Person in einem Chatraum vertrauen? Kann ich einer völlig unbekannten chinesischen Firma, die plötzlich mit mir Geschäfte machen möchte, einfach so vertrauen? Stammt diese Email wirklich von meiner Bank? Arbeiten die künstlichen Intelligenzen von Facebook, Google, Apple, Samsung oder BlackRock mit den Daten, die ich ihnen über mein Smartphone / Tablet jeden Tag schenke, für mich oder gegen mich? Bin ich der Kunde oder bin ich das Produkt?

Das Designziel für das World Wide Web war einfacher Informationsaustausch. Die generelle Überprüfbarkeit von Informationen war nicht Bestandteil der Konzeption. Im Nachhinein entstand zwar ein regelrechter Wildwuchs an Verfahren, um Akteure identifizierbar und Informationen überprüfbar zu machen, aber die daraus entstandene Vielzahl an Insellösungen kann das grundlegende Vertrauensproblem im digitalen Raum nicht lösen. Es ist Zeit, die DNA des World Wide Web zu verändern, um dem Bedarf der Nutzer nach Vertrauen und gefühlter Rechtssicherheit bei digitalen Interaktionen endlich Rechnung zu tragen. Um ein Trustnet konzipieren zu können, muss man zunächst die Natur von Vertrauen ergründen. Was ist eigentlich Vertrauen und wie entsteht es?

Vertrauen ist im soziologischen Sinne der Wille, sich verletzlich zu zeigen. Das heißt, Vertrauen entsteht in Situationen, in denen der Vertrauensgeber mehr verlieren als gewinnen kann – er riskiert einen Schaden bzw. eine Verletzung, wenn er beschließt, seinem Gegenüber zu vertrauen. Der Vertrauensgeber erwartet von seinem Gegenüber drei Eigenschaften: Kompetenz, Integrität und Wohlwollen. In der realen Welt können wir Vertrauen zu uns unbekannten Personen, Unternehmen oder Institutionen herstellen auf Basis von:

a) Nachweis von **Eigenschaften**, die Vertrauen rechtfertigen,
b) **Situationen**, in denen der Vertrauensgeber einen Vorteil erfährt,
c) **Identifikation** mit den Werten, Zielen und Bedürfnissen des Anderen

Die Herstellung von Vertrauen beinhaltet das Kennenlernen, d.h. a) bis c) gehen einher mit der Übermittlung überprüfbarer Identitätsmerkmale. Empfehlungen von Dritten, die bereits unser Vertrauen besitzen, erleichtern die Vertrauensbildung. Zur Natur des Vertrauens gehört aber ebenso, dass es auch leicht entzogen werden kann, wenn die vertrauensbildende Basis wegfällt oder die Erwartung des Vertrauensgebers enttäuscht wird. Die zugehörige Eigenschaft ist Vertrauenswürdigkeit. Welche Muster gibt es nun bei der Herstellung von Vertrauen?

Vertrauensanker und Vertrauensketten

In der realen Welt vertrauen wir Autoritäten, wie zum Beispiel staatlichen Institutionen. Diese staatlichen Institutionen und ihre Prozesse wirken für die gesamte Gesellschaft als **organisatorische Vertrauensanker**. Einem Auszug aus einem staatlich geführten Register z.B. kann man prinzipiell vertrauen. Die Autorität besteht in der gesellschaftlichen Position (kraft Gesetzes oder öffentlicher Beleihung/Bestellung), in der unterstellten Kompetenz zu sicheren Prozessen und in fehlendem Eigeninteresse der Institution, gegen das Interesse der Vertrauensgeber zu handeln. Wie bei einem Schiffsanker, der sicherstellt, dass ein Schiff nicht abdriftet, können zwischen einem Vertrauensanker und der zu beantwortenden Vertrauensfrage mehrere Kettenglieder liegen. Eine solche **Vertrauenskette** entsteht zum Beispiel, wenn die Meldestelle/Bürgeramt mir einen Personalausweis

ausstellt, den ich der Bank bei der Eröffnung eines Kontos vorweise (Know-Your-Customer-Prozess). Meine Bank erteilt einem Autohändler eine Bonitätsauskunft, woraufhin der Autohändler meinem 18-jährigen Sohn, für den ich bürge, ein Fahrzeug mit Ratenzahlung verkauft. Letztlich vertraut der Autohändler weder meinem Sohn, noch mir, sondern meiner Bank, die wiederum der Staatsmacht vertraut, die hinter dem Bürgeramt steht und dafür sorgen kann, dass ich im Falle eines Betrugs dingfest und haftbar gemacht werde. Im vorliegenden Beispiel wären der gesetzlich geregelte, sichere Prozess und die Autorität der Meldestelle zur Erstellung von Ausweisdokumenten der organisatorische Vertrauensanker. Und – um im sprachlichen Bild zu bleiben – die Staatsmacht wäre der Meeresboden, an dem der Anker hängt.

Digitale Beispiele für organisatorische Vertrauensanker und Vertrauensketten gibt es bereits. Die eID und der digitale Führerschein sind Beispiele staatlich ausgestellter Identifizierungsmittel, die in digitalen Verwaltungsprozessen und auch bei digitalen Prozessen der Privatwirtschaft Vertrauen erzeugen sollen. Organisatorische Vertrauensanker sind dabei die sicheren digitalen Prozesse der ausstellenden Behörden, die für eine Verifizierbarkeit der digitalen Dokumente sorgen. Ein Beispiel für digitale Vertrauensketten sind Zertifikatsketten in einer Public Key Infrastructure (PKI).

Spätestens im Zuge der Entwicklung der Blockchain-Technologie kam der Gedanke auf, dass anstelle von Autorität im digitalen Umfeld auch die Mathematik als **technischer Vertrauensanker** dienen könnte, weil man der Mathematik im Gegensatz zu Staaten immer vertrauen könne. Ein Großteil des Vertrauens in digitale Technologien und in die Richtigkeit von Informationen gründet sich heute bereits (auch unabhängig von Blockchains) auf die Sicherheit von Kryptografie, die Verkettung von Informationen und die Redundanz verteilter Systeme. Bei der Frage, ob man der Person vertrauen kann, die diese Informationen mit diesen Technologien übermittelt, hilft die Mathematik allein aber nicht wirklich weiter. Prinzipiell soll daher in den folgenden Ausführungen zwischen technischen und organisatorischen Vertrauensankern unterschieden werden, denn im Trustnet wird beides benötigt.

Vertrauensmechanismen

Neben Vertrauensankern und den daran hängenden Vertrauensketten gibt es in der Realwelt Mechanismen, mit denen Vertrauen zwischen einander unbekannten Akteuren hergestellt werden kann. In Fortführung der o.g. Systematik zielen diese Mechanismen entweder

auf den *Nachweis von Kompetenz/Integrität/Wohlwollen* des künftigen Vertrauensträgers,

- ⇨ Transparenz und Nachvollziehbarkeit (=> Kennenlernen, Verstehen, Kompetenznachweis)
  Bsp.: ein Anbieter erklärt dem Kunden, wie eine neue Technologie funktioniert
- ⇨ Demonstration (=> Kompetenznachweis)
  Bsp.: ein Anbieter führt dem Kunden die neue Technologie vor und zeigt das Ergebnis
- ⇨ Vertrauensbildende Prozesse (=> Kompetenz- und Integritätsnachweis)
  Bsp.: Nachweis der Zertifizierung nach DIN ISO 9001, TÜV-Plakette
- ⇨ Verifizierung von Informationen durch vertrauenswürdige Dritte (=> Integritätsnachweis)
  Bsp.: TÜV, Gutachter, Notare etc.
- ⇨ Empfehlungen (=> Kompetenznachweis durch Vertrauensnetzwerk)
  …

erzeugen eine *vorteilhafte Situation*

- ⇨ Anreizmechanismus (=> Vorteil für den Vertrauensgeber, Wohlwollen des Vertrauensträgers)
  Bsp.: Preisvorteil, Aussicht auf Kosteneinsparung
- ⇨ Sicherheitsmechanismus (=> Risikoreduktion für den Vertrauensgeber, Wohlwollen des Vertrauensträgers)
  Bsp.: Übernahme von Risiken des Vertrauensgebers durch den Vertrauensträger / staatliche Regulierung verpflichtet den Vertrauensträger

- ⇨ Vertrauensbildende Infrastruktur zum Aus-/Eingrenzen von Risikofaktoren (=> Risikoreduktion für den Vertrauensgeber)
  Bsp.: abhörsicherer Raum, Hochsicherheitsgefängnis, Reallabor
- ⇨ Gegenseitige Ab-/Besicherung (=> Sanktionierungsoption des Vertrauensgebers)
  Bsp.: Aufteilung des Wissens bei gemeinsamer Verwertung, Pönale in einer Geheimhaltungsvereinbarung
- ⇨ Überwachung/Monitoring (=> Beobachtbarkeit der Nichtkooperation des Vertrauensträgers)
  Bsp.: Überwachungskameras, Stechuhr am Arbeitsplatz
  …

oder führen zu einer *Identifikation des Vertrauensgebers mit dem anderen Akteur* durch

- ⇨ Abgleich von Werten (=> Kennenlernen)
  Bsp.: Tragen eines Eherings wirkt i.d.R. vertrauenserweckend bei Geschäftsverhandlungen
- ⇨ Abgleich von Zielen (=> Kennenlernen, Verstehen)
  Bsp.: Klarmachen der Notwendigkeit des gemeinsamen Abwendens einer Gefahrensituation
- ⇨ Abgleich von Bedürfnissen (=> Kennenlernen, Verstehen)
  Bsp.: Kunde vertraut dem Referenzkunden eines Verkäufers, weil der identischen Problemlösungsbedarf hat(te)

Die zu beantwortende Frage im Hinblick auf das Trustnet ist: Welche dieser Mechanismen für Vertrauensbildung, die in der realen Welt funktionieren, lassen sich wie auf die digitale Welt übertragen?

Vertrauensfragen

In der digitalen Welt stellt sich zum Aufbau von Vertrauen zunächst einmal die Frage der **Identifizierung** des Gegenübers anhand verifizierbarer Identitätsmerkmale. Teilfragen in dieser Kategorie sind z.B.:

- Wie kann eine mir unbekannte Person digital glaubhaft machen, dass sie die Person ist, für die sie sich ausgibt?
- Und wie gelingt mir das im Gegenzug bei ihr?
- Welche verifizierbaren Identitätsmerkmale sind bei welcher Art von Interaktion erforderlich?

Die nächste Kategorie von Vertrauensfragen betrifft den **Wahrheitsgehalt von Informationen** bzw. die Echtheit von übermittelten Dokumenten.

- Wie kann man prüfen, ob das gesendete Diplomzeugnis eines Stellenbewerbers echt ist?
- Wie kann man prüfen, ob ein Nachweis noch aktuell bzw. eine Berechtigung noch gültig ist?
- Hatte der Herausgeber des Nachweises das Recht, diesen Nachweis auszustellen?

Die dritte Kategorie von Vertrauensfragen betrifft das digitale Endgerät, das meinen Willen in digitale Informationspakete übersetzt, und die Übertragungstechnologie. Was schafft **Vertrauen in Technologie**/Produkte?

- Kann ich meinem Smartphone, der App darauf und den Servern entlang des Übertragungsweges vertrauen, dass die Informationen korrekt und ausschließlich an den von mir gewünschten Adressaten übermittelt werden?
- Kann ich mit Hilfe der Technologie automatisiert Bedingungen für die Herausgabe von Informationen stellen und deren Einhaltung prüfen?
- Und da die Geräte selbst immer intelligenter werden, muss letztlich auch gefragt werden: Was schafft gegenseitiges Vertrauen zwischen intelligenten Produkten?

All diese Fragen müssen und können im Zusammenhang mit dem **Trustnet** beantwortet werden.