Ulla Coester, Norbert Pohlmann

Vertrauen – ein elementarer Aspekt der digitalen Zukunft

Die digitale Evolution schreitet unaufhaltsam voran. Das führt auch zu der Konsequenz, dass die innovativen Technologien und somit die gesamte Internet-/IT-Infrastruktur nicht nur zunehmend vielschichtig, sondern auch intransparent wird. Daraus resultiert ein gravierendes Dilemma: gegenläufig zu dem steigenden Einsatz sinkt das Wissen über deren Hintergründe und Zusammenhänge. Dies könnte im Weiteren zu folgender Handlungsalternative führen – entweder unverhältnismäßige Ablehnung der Technologie und entsprechender Dienste oder blindes Vertrauen. Beides verhindert eine sinnvolle Nutzung neuer Anwendungen oder innovativer Dienste – auch wenn Vertrauen, im Sinne des Soziologen Niklas Luhmann, grundsätzlich positiv konnotiert ist. Denn gemäß seiner Definition ist Vertrauen ein Mechanismus der Komplexitätsreduktion [1] – also etwas, wodurch sich das Leben leichter gestalten lässt. Doch sollte hier die Interpretation im Sinne des Philosophen und Soziologen Georg Simmel weiter präzisiert werden. Dieser sieht „Vertrauen als einen Zustand zwischen Wissen und Nicht-Wissen, als eine Hypothese künftigen Verhaltens", auf die Menschen ihr konkretes Handeln gründen [2]. Das zeigt die Relevanz von Vertrauen beim Einsatz innovativer Technologien und unterstreicht gleichzeitig die Notwendigkeit, dass Unternehmen vertrauenswürdig agieren müssen, damit dieses auch gerechtfertigt ist.

Ulla Coester

als Gründerin/CEO des Unternehmens xethix-empowerment, berät sie bei Prozessen zur digitalen Ethik sowie Digitalisierungsprojekte. Zudem ist sie Lehrbeauftragte für digitale Ethik (Hochschule Fresenius, Köln) und Mitglied der Standardization Evaluation Group 10/IEC: Ethics in Autonomous and Artificial Intelligence Application.
E-Mail: uc@ucoester.de

Norbert Pohlmann

ist Professor für Informationssicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT und im Vorstand des Internetverbandes – eco.
E-Mail: pohlmann@internet-sicherheit.de

1 Einführung

Bevor innovative Technologien, im Sinne von Anwendungen und Diensten, eine breite Akzeptanz in der Gesellschaft allgemein sowie beim Nutzer im speziellen erfahren, müssen bestimmte Rahmenbedingungen erfüllt sein. Ein Kriterium und ebenso ein entscheidender Erfolgsfaktor, über den ein hoher Grad an Zustimmung zu erreichen ist, wird hierbei zukünftig die Vertrauenswürdigkeit der Hersteller und Anbieter sein. Diese Hypothese lässt sich inter alia erst einmal allgemein daraus ableiten, dass die Art und Weise wie die großen Technologie-Konzerne agieren zunehmend in weiten Kreisen auf Kritik stößt. Dass diese skeptische Einschätzung vonnöten ist und letztendlich auch gerechtfertigt zu sein scheint, belegen unter anderem die Gegenreden in der vor kurzem erfolgten Anhörung von Apple, Google, Amazon und Facebook. Hier wurde etwa der Gründer von Amazon befragt, „ob Amazon Daten von Händlern nutze, die Waren auf der Plattform des Konzerns verkaufen, um ihnen mit ihren eigenen Produkten Konkurrenz zu machen" [3]. Die Antwort von Jeff Bezos lautete sinngemäß, dass es dagegen zwar Regeln gäbe, er aber nicht garantieren könne, ob diese auch eingehalten würden. Dass Machtmissbrauch nicht länger akzeptiert wird zeigt sich am Beispiel von Facebook, die konkret Auswirkungen auf mehrere Fehlverhalten, unter anderem im Kontext von Cambridge Ana-

lytica, in 2019 zu spüren bekamen: im vergangenen Jahr rangierte das Unternehmen nicht mehr unter den Top 10 der globalen Brands sondern rutschte von Platz 9 in 2017 auf den Platz 14 – der Marktwert war in diesem Zeitraum um knapp 9 Milliarden gesunken [4].

In der Konsequenz daraus muss jetzt ein Diskurs eingeleitet werden, um die Fragestellung zu beantworten, wer was zu tun hat beziehungsweise was notwendigerweise zu tun ist, um Vertrauen und damit Akzeptanz bei den Nutzern aufzubauen. Entsprechende Maßnahmen zu ergreifen ist im Weiteren definitiv unumgänglich. Dies gilt jedoch nicht nur für die großen Technologie-Konzerne, sondern prinzipiell für jedes Unternehmen, das innovative Lösungen für die vernetzte Informations- und Wissensgesellschaft offeriert.

2 Vertrauensbereitschaft in Technologie?

Allgemein könnte Vertrauen als der Glaube daran, dass es möglich ist sich auf jemanden (Hersteller/Anbieter) oder auf etwas (Technologie) zu verlassen, definiert werden. Weiterhin ist Vertrauen das Zutrauen in eine relativ bestimmte beziehungsweise erahnte Zuverlässigkeit, Fähigkeit und/oder Tugendhaftigkeit. Vertrauen gilt als hoffnungsvoller Vorschuss hinsichtlich bestimmter Erwartungen [5]. Daraus lässt sich in Bezug auf innovative Technologien ableiten, dass diese allgemein vertrauenswürdig sind, wenn sie sich immer in der erwarteten Weise für den beabsichtigten Zweck verhalten.

Prinzipiell anerkannt ist, dass Vertrauen die Grundvoraussetzung für die Weltwirtschaft ist – allein aufgrund der Tatsache, dass viele Geschäftsmodelle ohne Vertrauen unmöglich wären. Eine plausible Erklärung für die absolute Bedeutung der Vertrauenswürdigkeit auch im Kontext von innovativer Technologie lieferte der Soziologe Kai-Uwe Hellmann bereits 2004: „Je unvorhersehbarer die Zukunft, desto essenzieller wird Vertrauen in zeitlicher, sozialer und sachlicher Hinsicht“ [6]. Damit lässt sich die allgemeine Prämisse der Vertrauenswürdigkeit auf den Einsatz innovativer Anwendungen und Dienste unmittelbar anwenden.

Warum? Zum einen, weil die Zukunft – auch aufgrund der, in immer kürzeren Intervallen entwickelten, innovativen Technologien – zunehmend unvorhersehbar wird. So herrscht beispielsweise selbst unter Wissenschaftlern keine Einigkeit darüber, ob beziehungsweise wann die Singularität erreicht oder ob es tatsächlich leistungsstarke Quantencomputer geben wird. Dass dies Auswirkungen hat zeigt sich an den Ergebnissen des aktuellen Online-Vertrauens-Kompass (ovk) des ‚Bundesverband Digitaler Wirtschaft' (BVDW) in der 46 Prozent der Befragten angeben: „Die schnelle Veränderung unserer Lebensbedingungen durch zunehmende Technisierung und Vernetzung macht mir Angst“ [7]. Zum anderen müsste es im Prinzip, allein unter der Annahme, dass der Vertrauensbegriff nur unscharf von anderen Terminologien wie Glaubwürdigkeit oder Verlässlichkeit zu trennen ist, schwer fallen neuen Technologien, respektive den Anwendungen und Diensten zu vertrauen – denn deren Funktionsweise lässt sich im besten Fall noch von Experten nachvollziehen. Den Gedanken fortsetzend könnte sich daraus dann folgendes ableiten lassen: mit der Nutzung jeglicher Technologie begehen Menschen potentiell eine Risikohandlung. Denn eine solche zu vollziehen bedeutet primär, die Entscheidung für eine Handlung zu treffen, ohne vollständiges Wissen über deren Ergebnis zu besitzen. Was zwar – notabene – auf nahezu alle Handlungen zutrifft, aber im Regelfall nicht bewusst ist, denn kaum einer würde seine Alltagshandlungen als riskant bezeichnen. Selbst dann nicht, wenn keine Sicherheit darüber besteht, dass sie im Sinne des Handlungsziels gelingen. Erst in dem Moment, wenn im Falle des Misslingens einer Aktion zugleich die Gefahr eines Verlusts besteht, also der Einzelne tatsächlich spürbar ‚etwas aufs Spiel setzt', wird das Risiko als solches auch empfunden.

3 Aktuell: Vertrauenswürdigkeit gewollt?

Ausgehend von dem Grundgedanken, dass die Nutzung einer Technologie, eines Dienstes oder einer Anwendung theoretisch eine Risikohandlung darstellt, wirft dies konsequenterweise die Frage auf, was sichergestellt sein muss, damit deren Einsatz trotzdem erfolgt. Hierfür gilt schlüssig die Prämisse von Vertrauen. Anhand bestimmter Kriterien lässt sich die Vertrauenswürdigkeit sowohl näher definieren als auch beleuchten, was Vertrauen in der sowie für die vernetzte(n) Wissens- und Informationsgesellschaft bedeutet.

3.1 Vertrauen heißt in erster Linie Zutrauen

Ein relevantes Kriterium für die Vertrauenswürdigkeit ist Zutrauen. Generell kann Zutrauen in die Funktionalität dadurch erzeugt werden, dass Hersteller und Diensteanbieter sowohl die beste Absicht als auch die Fähigkeit haben, eine verlässliche sowie sichere Technologie, respektive Dienste und Anwendungen, zur Verfügung zu stellen.

Obwohl diese Anforderung von hoher Bedeutung ist, wurde sie bis dato keinesfalls immer optimal erfüllt, da die zur Verfügung gestellten Technologien bislang aus verschiedenen Gründen nicht konstant ordnungsgemäß funktionierten. Dies hat teilweise zur Folge, dass innovative Technologien per se infrage gestellt werden.

3.2 Vertrauen bedeutet Zuverlässigkeit

Mit Zuverlässigkeit ist gemeint, dass Technologien und Lösungen nur die Dinge tun, die gewünscht sind und das möglichst hundertprozentig zuverlässig.

Momentan gibt es jedoch weder eine reglementierte Produkthaftung noch ein wahrnehmbares Verantwortungsbewusstsein seitens der Hersteller, wie es beispielsweise in der Automobil-Branche gang und gäbe ist. Das heißt, es ist möglich Anwendungen und Dienste zu offerieren, die nicht zwangsläufig einen normierten Grad an Zuverlässigkeit bieten.

3.3 Vertrauen benötigt auch Gewissheit

Für die Gewissheit bedarf es der Grundannahme, dass seitens der Hersteller und Diensteanbieter alle Faktoren berücksichtigt werden, die jeweils die relevanten Aspekte der Vertrauenswürdigkeit beinhalten, und hier insbesondere auch die der IT-Sicherheit sowie der ethischen Dimensionen.

Aktuell ist dies noch nicht der Fall – so binden beispielsweise Hersteller und Diensteanbieter nicht die heute zur Verfügung stehenden IT-Sicherheitsmaßnahmen angemessen in ihre Anwen-

dungen und Dienste ein. Das zeigt, dass Hersteller und Diensteanbieter momentan nicht ausreichend daran interessiert sind, ihre Reputation mit Hilfe bestimmter Maßnahmen zu verbessern – also letztendlich nicht im notwendigen Maße bereit sind Verantwortung für das Allgemeinwohl der Gesellschaft zu übernehmen, um Gewissheit als Kriterium für ihre Vertrauenswürdigkeit aufzubauen.

3.4 Vertrauen baut insbesondere auf Sicherheit

Mit Sicherheit ist gemeint, dass Technologien, respektive Dienste und Anwendungen, im Internet risikoarm zu nutzen sind.

Dieser Anspruch ist jedoch (noch) eine Fiktion da Ransomware, DDoS oder Phishing heute an der Tagesordnung sind. Alltäglich genutzte Dienste, wie etwa E-Mail-Programme oder Online-Banking, haben bei weitem nicht den Level an Vertrauenswürdigkeit der notwendig ist, um kritische Geschäftsprozesse damit sicher abwickeln zu können. Insbesondere private Nutzer sind mit den Sicherheitsproblemen überfordert. Sie haben oft kaum Chancen und Möglichkeiten sich adäquat zu verhalten, weil sie nicht genau wissen, wie sie sich angemessen schützen können.

Die Abfrage der Vertrauenswürdigkeitskriterien belegt, dass ein Vertrauen in Technologie, Anwendungen und Dienste noch nicht uneingeschränkt gerechtfertigt ist. Hier die notwendigen Voraussetzungen zu schaffen, mittels derer sich ihr Grad an Vertrauenswürdigkeit steigern lässt, bedeutet für Hersteller und Diensteanbieter, dass sie ihre Strategie künftig deutlich modifizieren müssen.

4 Zukünftig: Vertrauen bald entscheidbar?

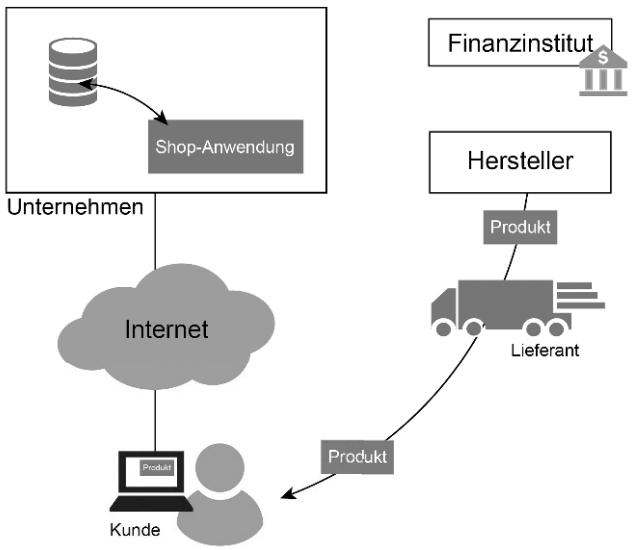
Es zeigt sich also, dass eine wechselseitige Dependenz zwischen Herstellern, Diensteanbietern und Nutzern besteht bei der sich jedoch die Interessen teilweise diametral gegenüberstehen. Zum Beispiel dann, wenn für den Kunden bei einer Anwendung die größtmögliche Zuverlässigkeit eine hohe Relevanz hat, während der Hersteller vorrangig darauf fokussiert ist, den Dienst möglichst schnell in den Markt zu bringen und dementsprechend notwendige Testläufe unterlässt. Hieraus lassen sich jedoch noch keine Rückschlüsse auf die Vertrauensbereitschaft ableiten. Denn diese ist spezifisch und steht einerseits in Abhängigkeit von dem Risiko das der Nutzer mit einer Handlung eingeht, aber ebenso von der Intention, die damit erfüllt werden soll. In jedem Fall ist davon auszugehen, dass der Nutzer die für ihn relevanten Informationen generiert, die ihm als Kriterien zum Aufbau von Vertrauen dienen können. Hierfür gibt es grundsätzlich zwei Modelle.

4.1 Eigene emotionale Referenz:

Der Nutzer sammelt spezifische Erfahrungen in Bezug darauf, dass eine Anwendung oder ein Dienst für seinen beabsichtigten Zweck in der erwarteten Weise funktioniert.

Bei einem aus Nutzersicht transparenten Vorgang – zum Beispiel der Bestellung von Waren im Internet – lässt sich anhand selbst definierter impliziter oder expliziter Kriterien leicht nachvollziehen, dass die Anwendung in erwarteter Weise vonstattengegangen ist. Nämlich dann, wenn die Ware in der angenommenen Qualität eintrifft und beim Zahlungsvorgang keine Unregelmäßigkeiten aufgetreten sind. (Siehe Abb. 1) Selbst unter der Bedingung, dass kein vollständiges Wissen über alle Abläufe vorliegt und die Vorannahmen zur Beurteilung nicht vollständig sind, da für den Nutzer nicht nachvollziehbar ist, welche Prozesse parallel dazu beim Diensteanbieter stattfinden – etwa in Bezug auf die Nutzung seiner Daten – ist es ihm möglich dieser Anwendung zu vertrauen und entsprechend die Handlung durchzuführen. Nämlich dann, wenn er der Bedürfnisbefriedigung einen hohen Stellenwert einräumt und die Gefahr des Verlusts für ihn in einem akzeptablen Rahmen ist – er also ‚nicht wirklich etwas aufs Spiel setzt'.

Abb. 1 | Selbsterlebte Bestätigung des erwarteten Verhaltens



4.2 Neutrale Referenz:

Der Nutzer vertraut einer Instanz, die Referenzen dahingehend bereitstellt, dass eine Anwendung oder ein Dienst in erwarteter Weise den beabsichtigten Zweck erfüllt.

Nicht immer können die Kriterien bezüglich der Vertrauensbereitschaft auf eigenen emotionalen Referenzen basieren, unter anderem dann, wenn es sich um eine neue Anwendung handelt. Für den Fall, dass dem Nutzer dabei das Risiko zu hoch erscheint, kann er seine Entscheidung nur treffen, wenn ihm hierfür Belege von neutraler Seite zur Verfügung gestellt werden. Zu diesem Zwecke können verschiedene Mechanismen zum Einsatz kommen.

a) Reputationssysteme

Die Möglichkeit Rezensionen bezüglich Nutzererfahrungen abzugeben werden bereits seitens vieler Diensteanbieter offeriert und sind somit bestens etabliert. Von daher kann diese Methodik als Grundidee für ein unabhängiges Reputationssystem dienen. Allerdings unter Berücksichtigung von zwei Aspekten: Zum einen bedarf es hier der Unabhängigkeit. Zum anderen muss ein Reputationssystem – in Abgrenzung zu Rezensionen, die rein subjektiv ausfallen können, weil sie nicht auf absoluten Kriterien sondern individuellen Präferenzen einzelner Nutzer basieren – bei weitem mehr Anforderungen gerecht werden. Denn aufgrund der gestiegenen Komplexität der Technologie wird einem Reputa-

tionssystem eine wesentliche Rolle bei der Einschätzung künftiger Anwendungen und Dienste zukommen, vor allem in Bezug auf solche, die nur unvollständig beziehungsweise noch gar nicht erfasst werden (können).

Eine essentielle Bedingung, die autarke Reputationssysteme erfüllen müssen ist, Nutzer dabei zu unterstützen eine Vertrauensbereitschaft auf objektivierten Kriterien aufzubauen, um deren Risikoabschätzung versachlichen und damit konkretisieren zu können. Hierfür ist es notwendig, dass die Organisation dieser Systeme unabhängigen Institutionen obliegt, die auch entsprechende Kriterienkataloge definieren, mittels derer es möglich ist, die Erfahrung der Kunden bezüglich der Vertrauenswürdigkeit einwandfrei und sachlich zu erfassen sowie zu analysieren. Unter anderem bezüglich der Funktionalität der Anwendung respektive des Dienstes aber auch im Hinblick auf weiche Faktoren zum Beispiel, ob der Anbieter / Hersteller ethische Werte berücksichtigt. Da Vertrauen dediziert ein wesentlicher Rohstoff der digitalen Zukunft ist, sollten sowohl Nutzer als auch Hersteller daran interessiert sein, am Aufbau und Betrieb solcher autonomen Reputationssysteme mitzuwirken.

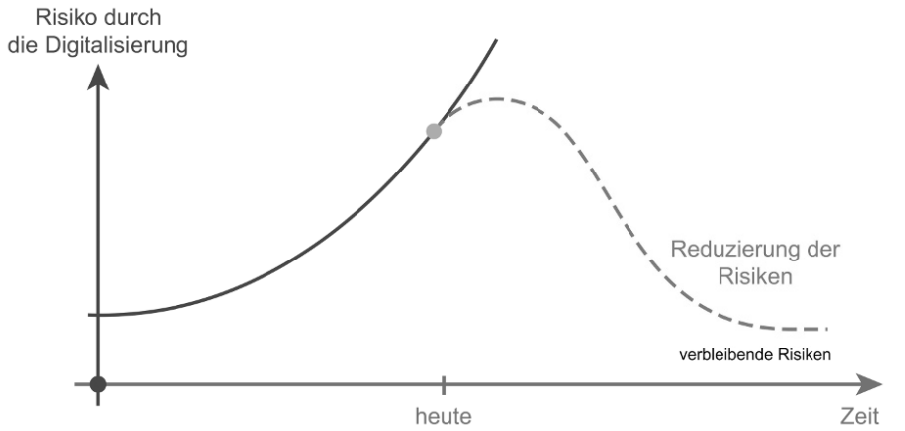
b) Evaluierung / Zertifizierung

Vor und bei dem Einsatz komplexer Technologien, Anwendungen und Diensten wird künftig unabhängigen Kontrollinstanzen eine höhere Bedeutung zukommen. Für die Durchführung der hier notwendigen Maßnahmen müssen bereits existierende unabhängige Organisationen, wie etwa der TÜV, erweitert oder möglicherweise vergleichbare Institutionen neu aufgebaut werden, die umfänglich die Evaluierung der Qualität sowie Vertrauenswürdigkeit sowohl von Anwendungen und Diensten als auch von Herstellern und Anbietern vornehmen. Hierbei wird es jedoch in zunehmendem Maße elementar sein, dass nicht die Hersteller den Umfang der Evaluierung definieren. Zukünftig gilt es sicherzustellen, dass diese Bewertung – analog zu der Überprüfung von Fahrzeugen – gemäß standardisierter Kriterien, anhand deren die Qualität ebenso wie die Vertrauenswürdigkeit von Anwendungen und Diensten sowohl zu auditieren als am Ende auch zu gewährleisten ist, erfolgt.

Nach einem entsprechenden Zertifizierungsvorgang der rechtmäßigen Evaluierung wird mit dem Zertifikat der Nachweis bezüglich der Einhaltung aller vorgegebenen Kriterien erbracht und somit der Grad der Vertrauenswürdigkeit der examinierten Anwendungen und Diensten dokumentiert. In diesem Kontext fällt dem BSI in Deutschland eine große Bedeutung zu. Für den Wirkungsraum Europa hat im Rahmen des neuen Cybersecurity-Act die ENISA die Aufgabe ein Framework für die Evaluierung und Zertifizierung von Produkten und Dienstleistungen für die EU zu erstellen – in Analogie zu der Datenschutz-Grundverordnung (DSGVO).

Insgesamt unterstützen dergleichen Zertifizierungen und Evaluierungen den Nutzer dabei seine Vertrauensbereitschaft zu erhöhen und eine entsprechende Handlungsentscheidung zu treffen.

Abb. 2 | Handlungsoptionen: Umgang mit Risiken



5 Reduzieren der Sicherheitsrisiken

Die Unternehmen, die Anwendungen entwickeln oder Dienste anbieten, sind dafür verantwortlich, den Stand der Technik von Sicherheitslösungen zu berücksichtigen, sodass generelle Sicherheitsbedürfnisse der Nutzer – wie Gewährleistung der Vertrauenswürdigkeit, Gewährleistung der Authentifikation, Gewährleistung der Integrität oder Gewährleistung der Verfügbarkeit – erfüllt werden. Hierfür sollten Unternehmen Konzepte entwerfen, wie sich Sicherheitsrisiken optimalerweise reduzieren lassen (Abb. 2, grüne Kurve).

Dazu können diverse Sicherheitsmechanismen wie Verschlüsselung, Authentifikationsverfahren, sichere Betriebssysteme, digitale Signaturen, Anti-Malware-Lösungen aber auch etablierte Prozesse etwa zur Sicherstellung einer hohen Softwarequalität oder des Patch-Managements zum Einsatz kommen. Aufgrund ihres hohen Wirkungsgrad gegen bekannte Angriffe ist es so möglich sowohl den Nutzer als auch seine digitalen Werte, gemäß seines individuellen Sicherheitsbedarfs, angemessen zu schützen. Unterlassen Unternehmen es hier zu agieren, potenziert sich das Risiko eines Schadens (Abb. 2, rot Kurve).

Akut müssen deshalb – um mehr Sicherheit und Vertrauenswürdigkeit in der Digitalisierung zu erzielen – die Entwicklungsparadigmen Security-by-Design, Privacy-by-Design sowie nachvollziehbare Qualitätssicherung nicht nur für IT-Produkte bedingungslos definiert und umgesetzt werden, sondern ebenso für alle Anwendungen und Dienste. In diesem Kontext manifestiert sich der Vorteil von Open Source-Software. Dieser liegt in der Möglichkeit, einen höheren Grad an Vertrauenswürdigkeit erreichen zu können, da im Rahmen der Entwicklung grundsätzlich sehr viele Personen involviert sind und damit mehr Kompetenz zur Verfügung steht, um die Qualität der Software zu verbessern sowie Schwachstellen zu finden und zu schließen. Transparenz ist insgesamt eine wichtige Voraussetzung für Vertrauen, denn offene Systeme ebenso wie IT-Architekturen und IT-Produkte erlauben es, Sicherheit und Vertrauenswürdigkeit zu überprüfen. Von daher gilt es das Verbesserungspotenzial für sichere und vertrauenswürdigere Open Source-Software zu fördern und in Europa auf die Verifizierung der Open Source-Technologien zu fokussieren, um hohe Sicherheits- und Wertestandards gewährleisten zu können.

Doch eine hundertprozentige Sicherheit kann nicht erzielt werden. Aus diesem Grund müssen weitere Sicherheitsstrategien für

die restlichen Unwägbarkeiten Anwendung finden. Dies können beispielsweise Versicherungen sein, über die das verbleibende Risiko und somit der Schadensfall abgedeckt wird, damit hierdurch – zum Beispiel beim Online-Banking – dem Nutzer kein Nachteil entsteht. Alternativ ließe sich auch mit einem Alert-System für Online-Banking die Sicherheit der Transaktion verbessern, da mit diesem transparent jeweils die Bedrohungslage und somit das aktuelle Risiko eines Angriffs aufgezeigt würde. Bekäme der Bankkunde dieses Ergebnis zur Verfügung gestellt, mit dem Hinweis, dass es aufgrund der aktuellen Situation besser wäre, die Transaktion zu einem späteren Zeitpunkt durchzuführen, könnte ein hoher Anteil an Schadensfällen vermieden werden [8][9].

6 Ohne Ethik keine Vertrauenswürdigkeit

Fragwürdig ist, warum Konzerne und Diensteanbieter vielfach heute noch in Bezug auf ihre Vertrauenswürdigkeit so konträr zu den Bedürfnissen der Nutzer handeln, obwohl diese zunehmend offen kundtun, was für sie in diesem Kontext relevant ist. Beispielsweise Privatsphäre – so zeigen Studien, unter anderem der aktuelle ovk [7], dass 70 Prozent der befragten Personen sagen: „Ich achte darauf, welche Cookies ich auf Websites zulasse, lösche Cookies regelmäßig oder benutzte Browser, die ein Tracking einschränken“ oder das 89 Prozent sehr vorsichtig im Internet agieren „weil man nie weiß, wen man im Internet vor sich hat“ [7]. Denn in der Realität zeigen Analysen, wie jene in diesem Jahr von Mozilla bezüglich ‚Minimum Security Standards' durchgeführte: „Holiday gifts are getting 'smarter' each year: from watches that collect more and more health data, to drones with GPS, to home security cameras connected to the cloud," said Ashley Boyd, Mozilla's Vice President of Advocacy. "Unfortunately, these gifts are often getting creepier, too. Poor security standards and privacy practices can mean that your connected gift isn't bringing joy, but rather prying eyes and security vulnerabilities [10]."

Daran offenbart sich die insgesamt diffizile Situation: Die Handlung einer Person ist nicht zwangsläufig kongruent mit deren Einstellung und oftmals fehlt hier die entsprechende kognitive Verknüpfung bezüglich möglicher Konsequenzen. Dabei trägt jeder Einzelne als (sozial) Handelnder – bisweilen teilweise unbewusst – mit seinen Entscheidungen dazu bei, die Gesellschaft zu prägen und manifestiert dies auch im Bezug die Nutzung von Technologie. Aufgrund diesem Fakt bedarf es hier grundsätzlich erst einmal einer Klärung auf der Metaebene dahingehend, ob der individuelle Grad der Risikobereitschaft pauschal eine persönliche Angelegenheit sein kann. Denn jedes Verhalten ist dazu geeignet, Unternehmen potentiell dazu zu verleiten, bestimmte Anwendungen oder Dienste zu offerieren, selbst wenn sie nur von

einer kleinen Minderheit – den Meinungsführern – für gut befunden werden. Oder ob zuerst ein Diskurs darüber geführt werden müsste, was die Gesellschaft überhaupt bereit ist ‚aufs Spiel zu setzen' – wobei in diesem Kontext noch zu berücksichtigen ist, dass mit der zunehmenden Komplexität der Technologie die Konsequenzen, die aus der Entwicklung resultieren für den Großteil der Bevölkerung immer weniger verständlich sind.

Daraus ergeben sich für Unternehmen zwei Handlungsoptionen: Im Rahmen ihrer Strategie die eigenen Interessen – etwa mit jeglichen Mitteln eine Gewinnmaximierung zu erzielen – priorisieren. Oder alternativ – auch aufgrund der Tatsache, dass das Verhalten der Nutzer volatil ist und diese mittlerweile zunehmend sensibel auf Vertrauensbrüche seitens der Unternehmen reagieren – alle erforderlichen Maßnahmen ergreifen, um die eigene Vertrauenswürdigkeit zu steigern. Einschränkend ist hierbei jedoch die realistische Annahme zu berücksichtigen, dass jedes Individuum bestimmte Präferenzen hat die inkohärent ausgeprägt sein können und somit bei einzelnen Sachverhalten zu unterschiedlichen Risikobewertungen kommt. Von daher müssen hier die bereits vorhandenen Maßnahmen übergeordneter Instanzen wie beispielsweise Ethik-Kommissionen aufgegriffen werden. Denn deren definierte Aufgaben bestehen darin, die grundlegenden Werte wie Solidarität oder Freiheit sowie die Moral einer Gesellschaft zu ermitteln und zu beschreiben, anhand derer sich Kriterien für den Umgang mit der Technologie festlegen lassen. Die Unternehmen können sich dann im Weiteren an diesem Konsens orientieren, um daraus einen eigenen kontinuierlichen Prozess zu initiieren mit dem sichergestellt wird, dass ihre Technologien und Dienste ethische Prinzipien berücksichtigen.

Einige Unternehmen erkennen bereits die daraus resultierende Möglichkeit zum Aufbau der Vertrauenswürdigkeit und gehen mit gutem Beispiel voran: Die reale Gefahr des Machtmissbrauchs während der Rassenunruhen in den USA sehend gab der CEO von IBM, Arvind Krishna in einem Brief an den US-Kongress die Entscheidung gegen Gesichtserkennung bekannt. Krishna zufolge „besteht hier das Potenzial für Verstöße gegen die Prinzipien von Vertrauen und Transparenz. IBM stelle sich gegen den Missbrauch von Technologie zur Unterdrückung der Freiheit". Seiner Ansicht nach ist die Politik bei der Digitalisierung naiv. Von daher plädiert er für einen nationalen Dialog, besonders durch die Gesetzesvertreter, denn „die immer wieder auftretenden Fälle von rassistisch motivierter Polizeibrutalität haben gezeigt, dass Autoritäten mehr Verantwortung für Verfehlungen tragen müssen. Künstliche Intelligenz sei für die Polizei ein mächtiges Werkzeug. Jedoch müssen sowohl die User als auch die Hersteller damit achtsam umgehen und Befangenheit vermeiden" [11].

7 Ausblick: Vertrauenswürdige Zukunft

Die Welt wird – nicht zuletzt bedingt durch die Digitalisierung mit permanent kürzeren Innovationszyklen – zunehmend komplex. Damit die Nutzer diese Veränderungen kontinuierlich akzeptieren und die Technologien, Anwendungen und Dienste auch einsetzen, müssen Unternehmen den Aufbau von Vertrauen unterstützen. Dies gelingt in erster Linie, indem sie die Vertrauenswürdigkeitskriterien optimal erfüllen. Da jedoch technologische Entwicklungen teilweise im Kontext der Anwendung beurteilt werden müssen, ist es unmöglich alle Fragen bezüglich der Vertrauenswürdigkeit a priori zu beantworten. Ungeachtet dessen sind potentielle Risiken bereits im Vorfeld evident. Von daher ist es sinnvoll einen Lösungsansatz anzustreben, der einbezieht, dass Unternehmen grundsätzlich das Ziel einer digitalen Ethik verfolgen, sodass alle Nutzer in der Interaktion mit Technologien, respektive Anwendungen und Diensten, nach ihren moralischen Überzeugungen gut handeln können und auch selber nicht in Rechten, Autonomie und Freiheit beschnitten werden.

Denn nur ein transparentes, verantwortliches und vertrauenswürdiges Handeln von Unternehmen schafft langfristig Akzeptanz und Vertrauen beim Kunden, worauf letztendlich die Voraussetzung für die Nutzung von innovativen Technologien, Anwendungen und Diensten basiert.

Literatur

[1] Niklas Luhmann, Vertrauen: Ein Mechanismus der Reduktion sozialer Komplexität, 1968

[2] Georg Simmel, Soziologie(1908). Gesamtausgabe, hg. von O. Rammstedt, Bd. 11, 1992

[3] https://www.focus.de/digital/digital-news/anhoerung-vor-dem-us-ko...cebook-haben-die-vier-tech-riesen-zu-viel-macht_id_12263014.html

[4] Jährliches Ranking der US-Consulting-Firma Interbrand – http://interbrand.com

[5] https://www.wertesysteme.de/vertrauen/

[6] Solidarität, Sozialkapital und Systemvertrauen Formen sozialer Integration, Kai-Uwe Hellmann

[7] Online-Vertrauens-Kompass 2020 https://www.bvdw.org/themen/publikationen/detail/artikel/online-vertrauens-kompass/

[8] U. Coester, N. Pohlmann: „Wie können wir der KI vertrauen" https://norbert-pohlmann.com/wp-content/uploads/2020/11/420-Wie-koennen-wir-der-KI-vertrauen-Mechanismus-fuer-gute-Ergebnisse-Prof.-Norbert-Pohlmann.pdf

[9] N. Pohlmann: „Cyber-Sicherheit – Das Lehrbuch für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung", Springer-Vieweg Verlag, Wiesbaden 2019

[10] Holiday gifts getting smarter, but creepier when it comes to privacy and security https://www.helpnetsecurity.com/2020/11/12/holiday-gifts-privacy-security/

[11] Racial Profiling: IBM stoppt Gesichtserkennung https://www.pressetext.com/news/20200609014