TeleTrusT – Bundesverband IT-Sicherheit e.V.
Der IT-Sicherheitsverband.

Vertrauen und IT-Sicherheit

Vertrauensmodelle für die Informationsgesellschaft

Autoren

Kapitel 1: Christine Ziske
Kapitel 2 und 5: Dr. Christoph F-J Goetz
Kapitel 3: Kerstin Mende-Stief
Kapitel 4: Michael Barth
Kapitel 6: Henning Arendt

Diese Publikation wurde im TeleTrusT - Bundesverband IT-Sicherheit e.V. erarbeitet.

Impressum

Herausgeber:

TeleTrusT – Bundesverband IT-Sicherheit e.V.
Chausseestraße 17
10115 Berlin
Tel.: +49 30 400 54 306
Fax: +49 30 400 54 311
E-Mail: info@ teletrust.de
http://www.TeleTrusT.de

Herstellung:

DATEV eG, Nürnberg

1. Auflage

1 Einleitung

Jeden Tag vertrauen wir anderen Menschen, Organisationen und Systemen. Vertrauen gestaltet das gesellschaftliche Leben kalkulierbar und erleichtert die Zusammenarbeit. Natürlich gibt es in jeder Vertrauensbeziehung die Alternative des Missbrauchs. Das wiederum verlangt nach Maßnahmen zu Durchsetzung und entsprechenden Kontrollmechanismen. Nimmt das Vertrauen ab, wird nach Sicherheit verlangt. Sicherheit senkt das Risiko auf ein erträgliches Maß.

In der realen Welt gibt es bereits sehr lange vertrauensbildende Maßnahmen oder Sicherheitsversprechen, die uns veranlassen, darauf zu vertrauen, dass z.B. die Bremsen in unserem Auto funktionieren, oder dass das Flugzeug, in dem wir reisen, nicht abstürzt. Schwieriger wird es, diese Mechanismen des Vertrauens in die virtuelle Welt zu übertragen. In dieser Welt stehen uns nonverbale Informationen oder physikalische Sicherheitsmechanismen nicht zur Verfügung.

Rasch ergeben sich Fragen:

- Welche Strategien wird es geben, mit diesen Unterschieden umzugehen?
- Wie funktionieren Gütesiegel, wie z.B. "Bio-Äpfel", in der virtuellen Welt?
- Wie stellt man gesellschaftlich sicher, dass Software, die sofort und weltweit verfügbar, vertrauenswürdig ist?
- Welche Rechtssicherheit hat der, dessen Vertrauen missbraucht wird?
- Welche Kontrollmechanismen gibt es oder könnte es geben?
- Wie schafft man Interessenübereinstimmung der einzelnen Beteiligten als Voraussetzung der Bildung von Vertrauenswürdigkeit oder mindestens Konformität?

Außerdem müssen wir nicht nur anderen Menschen anonym im "Netz" vertrauen, sondern auch technischen Instanzen und sogar anderen "Dingen". Unser Zusammenleben mit dem Internet der Dinge wird von vertrauenswürdigen Sicherheitsmechanismen bestimmt. Nicht zu vergessen: in der vernetzten Welt werden auch Maschinen immer mehr Maschinen "vertrauen" müssen.

Zu welchen vernetzten IT-Systemen werden wir Vertrauen entwickeln können?

Können wir, ausgehend von dem guten Funktionieren der einzelnen Komponenten, darauf vertrauen, dass deren Zusammenspiel auch unseren Sicherheitserwartungen entspricht?

Auf einige Fragen wird es nachfolgend Antworten geben, andere Fragen bleiben offen, einiges muss die Zukunft zeigen. Vertrauen bildet sich, wenn man selbst Einfluss und Kontrolle ausüben kann, das setzt wiederum eine digitale Kompetenz voraus, die es zu entwickeln gilt.

2 Psychologie des Vertrauens

Nach Jahren wenig reflektierter Gläubigkeit an Fakten und Fortschritt wird heute deutlich, dass die Serviceangebote der Informationstechnik zu sehr komplexen Infrastrukturen herangewachsen sind. Dort gibt es jetzt genauso Licht wie viel Schatten. Daher muss jeder für sich selbst entscheiden, welche Angebote er nutzt und welchen Diensten er sich und seine Informationen anvertrauen will. Doch was ist Vertrauen?

Vertrauen - Diese Emotion weist hinunter bis in die Grundfeste jedes Menschen. Das Gefühl entwickelt sich so früh in der persönlichen Entwicklung, dass auch von Urvertrauen gesprochen werden kann. Es ist ein Elementargefühl der eigenen Existenz und wird für jeden Menschen zum Ausgangspunkt seiner eigenen Entwicklung in der Welt. Vertrauen entsteht aus der persönlichen Wahrnehmung von Sicherheit: Sicherheit in sich selbst und Sicherheit in seine Umwelt. Es bestimmt die Risikobereitschaft, mit der jeder in das Leben hinausgeht.

Sicherheit hat zwei verschiedene Aspekte: Sie bezeichnet einerseits ein Gefühl und verweist gleichzeitig auch auf eine reale Wirklichkeit. Diese beiden Komponenten sind aber nicht immer kongruent. In der äußeren Welt kann Sicherheit mathematisch beschrieben und sogar gemessen werden, während die Gefühlswelt nicht analysiert oder rechnet, sondern direkt und unmittelbar subjektiv erlebt wird. Aus diesem Grund gibt es eine fundamentale Diskrepanz zwischen objektiver und subjektiver Sicherheit. Ein Mensch kann sich sicher fühlen, ohne sicher zu sein. Er kann sicher sein, ohne sich sicher zu fühlen.

Falsche Wahrnehmung von Sicherheit entsteht meist aus einer falschen Wahrnehmung des zugrunde liegenden Risikos. Menschen sorgen sich vielfach intensiv über kleine Risiken, während sie große Risiken ausblenden. Spektakuläre, seltene Risiken werden über-, während häufige, kleinere Risiken unterbewertet werden. Personifizierte Risiken werden größer eingeschätzt als anonyme Risiken. Menschen unterschätzen Risiken, die sie freiwillig eingehen und überschätzen Risiken von Situationen, denen sie einfach ausgeliefert sind.

Es gibt bekanntlich keine absolute Sicherheit und nur selten unerschütterliches Vertrauen. Daher stellen Sicherheit und Vertrauen immer in gewisser Weise ein Tauschgeschäft dar. Jede Verbesserung von Sicherheit bedeutet auf der anderen Seite der Waagschale einen Zusatzaufwand. Daher macht es wenig Sinn, Sicherheit nur isoliert unter dem Aspekt der Effektivität zu betrachten. Kugelsichere Westen sind einfach zu unbequem für den Alltag. Wichtig ist, ob der eingesetzte Aufwand den Ver-

trauensgewinn rechtfertigt. Solche Abwägungen gehören aber schon seit Menschengedenken zu unserem Leben in der realen Welt. Daher sind wir schon ganz gut in diesen Einschätzungen.

Diese positive Entwicklungsgeschichte kann jedoch nicht einfach auf die elektronische Welt von heute übertragen werden. Die Anpassungen des Stammhirns und kulturgeschichtlichen Erfahrungen liefern einfach nicht die richtigen Bewertungen und Konsequenzen für die abstrakte Medienkultur von heute. Daher ist Vertrauen als Mechanismus zur Reduktion informationstechnischer Komplexität ein schlechter Ratgeber. Blindes Vertrauen ist viel zu oft eine unverantwortliche Vorleistung gegenüber der potenziellen Heimtücke des Internets. Aus diesem Grund erfordert neues Vertrauen eine neue Wachsamkeit und muss neu gelernt werden.

3 Faktoren, die Vertrauen beeinflussen

Doch wie entsteht Vertrauen überhaupt? Ein Schlüssel zur Beantwortung dieser Frage liegt in den Faktoren, welche die Vertrauensbildung beeinflussen. Neben messbaren objektiven Einflüssen sind das oft weiche, subjektive Umstände. Es gibt Faktoren, die sich positiv auf die Vertrauensbildung auswirken und Faktoren, die das Gegenteil tun.

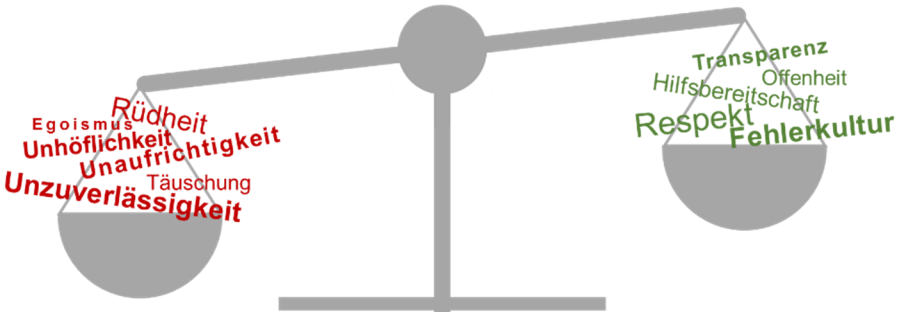

Abbildung 1: Vertrauensbildende und -schmälernde Faktoren

Positiv auf die Vertrauensbildung wirken sich aus: Transparenz, Offenheit, Respekt, Fehlerkultur, Hilfsbereitschaft. Das Vertrauen hingegen negativ beeinflussen: Unaufrichtigkeit, Täuschung, Unzuverlässigkeit, Rüdheit, Unhöflichkeit, Egoismus. An diesem Punkt wird klar, dass man Vertrauen im Laufe der Zeit auch bewusst aufbauen oder wieder verlieren kann.

Den Vertrauensaufbau fördern in jedem Fall alle Arten objektiver Faktoren. Messbare und von Dritten überprüfbare Faktoren sind z. B. Testreihen mit dokumentierten Ergebnissen – ein Verfahren, das auch in der IT als Grundlage für Zertifizierungen und

Gütesiegel dient. Am bekanntesten sind die in Deutschland durch das BSI erteilten Zertifikate nach den "Allgemeinen Kriterien für die Bewertung der Sicherheit von Informationstechnologie" (Common Criteria oder kurz CC) und den Normen der "Internationalen Organisation für Normung" (ISO). Das Prinzip ist einfach: Es gibt ein öffentlich einsehbares Profil, gegen das etwas getestet wird. Anschließend wird bewertet, ob und in welchem Umfang das Produkt oder die Dienstleistung dem Profil entspricht. Das Ergebnis der Tests muss jederzeit von unabhängigen Gutachtern nachvollziehbar und reproduzierbar sein.

Weitere objektive Faktoren zur Vertrauensbildung können der Standort oder bestimmte Kenngrößen des Anbieters eines Produkts oder einer Dienstleistung sein. Das berühmte "Made in Germany" ist schon lange vom Herkunftsnachweis zum Gütesiegel geworden. Einem großen, etablierten Unternehmen vertrauen wir mehr als einem kleinen, vielleicht sogar gerade erst gegründeten Anbieter. Die Einordnung der Schuldnerqualität (Bonitätsauskunft) durch sogenannte Rating-Agenturen entscheidet oft genug darüber, ob eine Geschäftsbeziehung überhaupt in Frage kommt.

Doch reicht das alles schon, um einem Anbieter oder potenziellen Geschäftspartner zu vertrauen? Eine alte Vertriebsweisheit sagt: "Menschen kaufen von Menschen." Damit wird klar, dass weiche Faktoren mindestens so ausschlaggebend sind wie die objektiven sind. Was aber sind diese weichen, subjektiven Faktoren, die unser Vertrauen beeinflussen?

$$\text{Vertrauen} = \sqrt{\left(\frac{\text{Glauben} \times \text{Information}}{\text{Bewertung}}\right) - \frac{\text{Mehrwert}}{\text{Risiko}}}$$

Abbildung 2: Vertrauenskomponenten als Formelkonzept[1]

Vertrauen wird auf allen Sinnesebenen gebildet. Man muss sich "riechen können", "die gleiche Sprache sprechen", "auf einer Wellenlänge" oder "Augenhöhe sein". Bei der Vertrauensbildung auf persönlicher Ebene spielen Instinkte und Erfahrungen eine große Rolle. Vieles spielt sich dadurch allerdings bereits im Unterbewusstsein ab. So entscheidet oft ein Bruchteil einer Sekunde, ob man jemandem oder einer Sache vertraut.

[1] Angelehnt an http://sas-thinkforward.de/

Ist eine Vertrauensbasis einmal da, wird diese häufig auch für Empfehlungen genutzt. Der fast schon sprichwörtliche Golfplatz ist ein bezeichnendes Beispiel für diese Praxis. Wahrscheinlich werden nirgendwo sonst so viele Empfehlungen ausgesprochen wie unter Golfpartnern. Man nutzt die Erfahrung von jemandem, dem man bereits vertraut. Es wird effektiv eine "Vertrauenskette" (Chain of Trust) aufgebaut. Virtuelle Beispiele für Vertrauensketten sind das sogenannte "Web of Trust" und soziale Netze wie LinkedIn oder XING.

Dabei ist interessant, welche Ausmaße eine solche Vertrauenskette annehmen kann. Ermöglicht wird das durch das Jeder-kennt-Jeden-Gesetz. Dieses Kleine-Welt-Phänomen wurde erstmals 1967 von dem amerikanischen Psychologen Stanley Milgram beschrieben. Aktuelle Studien belegen, dass die Kette zwischen zwei beliebigen Personen auf der Welt durchschnittlich 6,6 Personen lang ist[2].

Unternehmen nutzen diese Erkenntnis auch für Referenzen. Die Wahrscheinlichkeit ist hoch, dass unter den Referenzen jemand ist, den man kennt (und dem man somit vertraut).

Eine besondere Form der Chain of Trust ist zugleich auch eine Mischform von objektiven und subjektiven Faktoren. Die Rede ist von einer Vielzahl voneinander unabhängiger Bewertungen. Je mehr ähnliche subjektive Meinungen zu einer Person oder einer Sache vorliegen, desto glaubwürdiger (objektiver) erscheint uns der entsprechende Aspekt. Bekanntestes und ältestes Beispiel dürften die Bewertungen auf der Verkaufsplattform "Amazon" sein. Mittlerweile nutzen viele Anbieter dieses Instrument und lassen sich öffentlich von ihren Anwendern bewerten.

Und dann gibt es noch Faktoren, die zwar objektiv scheinen, im Kern aber einer rein subjektiven Wahrnehmung entsprechen. So führt die Frage nach Sanktionsmöglichkeiten ("Wie hoch ist die Wahrscheinlichkeit, dass ein entstandener Schaden ersetzt wird?") unwillkürlich zu einem Institutionenvertrauen.

Neben den eingangs schon erwähnten Instituten (CC, ISO) genießen bestimmte staatliche sowie öffentliche Einrichtungen per se ein hohes Vertrauen. Eine Kapitalgesellschaft wiederum hat mehr Ansehen als eine Personengesellschaft. Zur Vertrauensbildung sind schließlich sowohl objektive als auch subjektive Faktoren wichtig, wobei die objektiven einen höheren Stellenwert einnehmen als die subjektiven.

[2] Studie http://arxiv.org/abs/0803.0939

Deutlich wird dies in der Studie "Vertrauen beim Online-Einkauf"[3]. Das Ergebnis dieser Studie spiegelt wider, in welchem Maße welche Faktoren das Vertrauen beeinflussen.

Bei den 30- bis 49-Jährigen befragten Käufern legen 81% Wert auf positive Bewertungen, 74% vertrauen deutschen Anbietern, 70% wollen nicht per Vorkasse zahlen, 69% achten auf Gütesiegel und nur 25% sind eigene Erfahrungen wichtig[4].

Der deutsche Soziologe und Gesellschaftstheoretiker Niklas Luhmann definiert Vertrauen als "Mechanismus zur Reduktion sozialer Komplexität". Ihm zufolge lassen sich so all die objektiven und subjektiven Faktoren zur Vertrauensbildung auf das Grundbedürfnis nach Ordnung zurückführen. Ein Faktor, der sich auch in der zunehmenden Automatisierung oder Technologisierung zeigt.

4 Zwei Gesichter der Technologie: Zugleich Vertrauensbasis und Schadensquelle

Technologie bildet heute in vielen Bereichen die Basis des täglichen Lebens. Dies gilt für das Berufs- genauso wie für das Privatleben. Ob Energieversorgung, öffentlicher Personennahverkehr, die bereits allgegenwärtige Vernetzung bis hin zu Alltagsgegenständen und vieles mehr ist ohne Technologie – und Informationstechnologie im engeren Sinne – nicht mehr vorstellbar. In vielen Bereichen ist eine Abhängigkeit erreicht, die (vor allem nach den Enthüllungen von Edward Snowden) weit über die pure Vertraulichkeit hinausgeht. Auch die Verfügbarkeit wird zum Wert an sich, das Vertrauen in die eingesetzten Technologien muss neu gerechtfertigt werden.

Für die meisten Technologieanbieter wird somit das Vertrauen der Kunden zur Basis des eigenen Geschäftsmodells, das im Verlauf der letzten Jahre erschüttert worden ist. Dies gilt sowohl für Sicherheits- als auch für Alltagstechnologien, die viele Menschen nicht mehr missen möchten (z.B. Cloud Services) und die hohe Wertschöpfung für Bürger und Organisationen versprechen.

Dabei wird das Vertrauen in Technologie dort umso wichtiger, wo die Verletzlichkeit des Vertrauensgebers steigt. Dies ist in nahezu allen IT-Bereichen – gerade bei steigender Vernetzung – immer häufiger der Fall. Doch wie kann Technologie Vertrauen

---

[3] Als Sonderstudie im Rahmen des (N)ONLINER Atlas 2012 von der Initiative D21 gemeinsam mit dem Bundesverband des Deutschen Versandhandels mit Unterstützung der Gütesiegel EHI Geprüfter Onlineshop, Trusted Shops und TÜV SÜD bei TNS Infratest beauftragt

[4] http://etailment.de/thema/e-commerce/studie-diese-faktoren-steigern-das-vertrauen-in-webshops-789

erlangen bzw. zurückerlangen? Gerade bei Technologie ist häufig eigenschaftsbasiertes Vertrauen der ausschlaggebende Faktor, denn Technologieentwicklung folgt meist regelhaften Prozessen.

Dazu müssen die tatsächlichen Eigenschaften der genutzten Technologie überprüf- und belegbar sein. Hier ist gleichzeitig der Haken, denn steigende Komplexität von Technologien macht die Überprüfbarkeit schwerer, für Laien und Alltagsnutzer nahezu unmöglich. Hier helfen Zertifizierungen und sonstige Nachweise über die Vertrauenswürdigkeit der eingesetzten Technologien, wie z.B. die Nutzung als vertrauenswürdig anerkannter Standards.

Die Bundesrepublik Deutschland hat – wahrscheinlich unbewusst – seinerzeit mit Ausgründung des BSI und der damit verbundenen Herauslösung aus dem Bundesnachrichtendienst eine richtige Entscheidung getroffen und die Zertifizierungsstelle für IT-Sicherheitsstandards von Geheimdiensten und Polizeikräften getrennt. Der vorhersehbare Interessenskonflikt wurde in anderen Nationen nicht aufgehoben. Als Beispiel seien hier die USA genannt, bei denen eine Zertifizierung von Produkten nach Common Criteria durch das National Institute of Standards and Technology (NIST) und die National Security Agency (NSA) erfolgt.

Weiterhin sind für das eigenschaftsbasierte Vertrauen in Technologien drei Faktoren entscheidend:

1.) Die Kompetenzerwartung: Kann der Anbieter dem Vertrauensnehmer das, was er verspricht überhaupt liefern? Im Fall von Sicherheitstechnologien stellt sich die Frage: Ist Sicherheit der Kern des Anbietergeschäfts oder nur ein als notwendig erachtetes Übel, das irgendwie zur Gesamtlösung gehört?
2.) Die Integritätserwartung: Ist das, was der Anbieter vorgibt zu tun, wirklich sein Beweggrund oder hat er andere Ziele, die zwar legitim sein mögen, aber vielleicht nicht ausreichend für die Generierung von Vertrauen sein müssen?
3.) Die Benevolenzerwartung: Sie ist jene optimistisch-offene Haltung gegenüber anderen Menschen und Beziehungen, die nicht durch besondere Handlungen, sondern durch guten Willen und allgemeine Geneigtheit gekennzeichnet ist, und nicht mit Altruismus verwechselt werden darf.

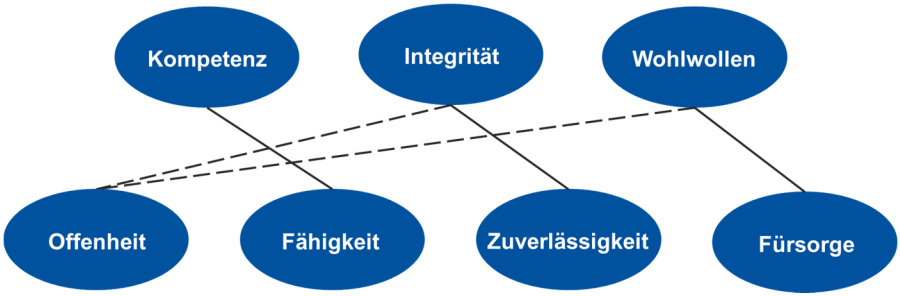

Abbildung 3: Verknüpfung der Vertrauensfaktoren mit anderen Begriffen[5]

So ist z.B. die Generierung von Umsatz per se nicht zu verteufeln. Doch gerade im Bereich von Sicherheitstechnologien sollten die Beweggründe auch einem übergeordneten, gesellschaftlichen Ziel folgen, vor allem dann, wenn ein Technologieversagen gesamtgesellschaftliche Folgen haben kann. Dabei sollte der Vertrauensgeber kritisch prüfen, welchen Unternehmenszielen sich der Anbieter verpflichtet fühlt. Neben formulierten Zielen gibt es hierfür auch Indizien, die sich nicht nur in proklamierter Corporate Social Responsibility, sondern in tatsächlichen Handlungen zeigen. Die Technologien müssen also mit dem Anbieterunternehmen in einen Gesamtzusammenhang gesetzt werden.

Technologie kann als solche nie alleine Garant für Vertrauen sein. Transparenz, Nachvollziehbarkeit und Bewertbarkeit bleiben für IT-Lösungen der wichtigste Faktor zur Vertrauensbildung. Daneben sollte das Anbieterunternehmen im Gesamtkontext betrachtet werden, um Rückschlüsse auf die Vertrauenswürdigkeit zu ermöglichen. Eine rein wirtschaftliche Betrachtung von Lösungen blendet den Vertrauensfaktor jedoch meist aus und reduziert den Beitrag von Technologie auf eine oberflächliche Kosten-Nutzen-Rechnung.

5 Faktor Mensch / Operative Bedrohungslage

Persönlicher Kontakt wird heute immer mehr durch den öffentlichen Datenraum ersetzt. Die Erfahrungswissenschaften sind daher mit der wichtigen Frage konfrontiert: Wie können Menschen mit Laienwissen in den täglichen verwirrenden Abwägungen feststellen, welchen Aussagen von vermeintlichen Experten sie vertrauen können? Obwohl sich jeder für alles ausgeben kann und niemand die Motive hinter seiner Information offenlegen muss, werden heute vermeintliche Expertenmeinungen viel zu häufig ungeprüft übernommen.

[5] angelehnt an http://www.palgrave-journals.com/kmrp/journal/v5/n3/fig_tab/8500143f1.html

Das führt zu einem Dilemma: Kann man wirklich in etwas vertrauen, wenn man den einzelnen Meinungsbildner nicht mehr persönlich kennt? Es ist einerseits viel Information da, aber noch mehr Verunsicherung. "Fünf Personen mit sieben Meinungen" ist nicht nur ein Bonmot. Daher richtet sich jeder nach dem Erkennbaren und Erreichbaren. Werbung und Massentrends ersetzen zunehmend eigenständig informierte Orientierung. Vertrauen goes Crowdsourcing.

Auch in der Informationsgesellschaft wird die Position jedes Menschen in seinem Beziehungsgeflecht durch seine eigene Rolle definiert. Aus dem Spannungsfeld zwischen eigener Meinungsbildung und der ganz realen Kontrolle des gesellschaftlichen Konsenses entsteht daher aber ein unverkennbarer Zwang zur Anpassung. Wer kauft schon heute etwas ohne sich vorher in Verbraucherportalen oder Kundenforen umgesehen zu haben? Individuelle Information wird zur Statistik. Ratings, Klicks und Hit-Listen können immer leichter eigene Meinungsbildung ersetzen.

All das geschieht nicht im luftleeren Raum. Betrachtet man die Bedrohungslage informationstechnischer Infrastrukturen, muss man heute eine wachsende Komplexität der Herausforderungen und eine immer bessere Zielausrichtung der Angriffe feststellen. Die ersten Bedrohungen waren noch recht ungesteuert, wie z.B. Denial-of-Service-Attacken oder Phishing. Die nächste Stufe wurde schon komplexer, hat aber die vorherige nicht abgelöst, sondern nur ergänzt, z.B. durch Massenangriffe zur Spionage oder Sabotage. Die heute neueste Stufe besteht, wie Whistleblower berichten, aus präzisen und verdeckten Angriffen auf meist ahnungslose Einzelziele.

Als Gesamtphänomen betrachtet bietet die Motivlage für Bedrohungen der Informationsgesellschaft oder gezielte Cyberangriffe eigentlich nichts Neues. Praktisch jede Form von bekannter Kriminalität findet sich auch im Cyberspace, sei es Spionage, Sabotage, organisierte Kriminalität oder Betrug.

6 Zusammenfassung

Die sinnvolle Nutzung heutiger und vor allem zukünftiger IT-Anwendungen und Dienstleistungen erfordert Vertrauen in die IT-Sicherheit. Nur punktuell lassen sich wichtige Funktionen, wie Integrität der Systeme, Sicherheit vor Missbrauch, Schutz der personenbezogenen Daten und Schutz vor digitalen Angriffen von einem Benutzer selbst überprüfen. Ähnlich wie man im realen Leben darauf vertraut, dass das, was darauf steht, auch darin ist (die Bremsen des Autos sind vom TÜV geprüft, oder die "Bio-Äpfel" sind bio), ist es auch in der virtuellen Welt.

Dabei spielt die Psychologie des Vertrauens eine wichtige Rolle dafür, wie IT-Sicherheit persönlich wahrgenommen wird. Neben dem "Ur-Vertrauen" sind es einige Faktoren, die das Vertrauen in IT-Sicherheit beeinflussen. Dazu gehören messbare und

von Unabhängigen überprüfbare Faktoren wie evaluierte Sicherheitskomponenten, unabhängige Qualitätssiegel oder Ergebnisse von automatisierten Analyseverfahren. Weitere Faktoren sind "weiche" oder subjektive Faktoren. Das sind z. B. Empfehlungen, wie sie in Foren oder bei Anbietern zu finden sind, aber auch eigene gesammelte Erfahrungen oder die von vertrauenswürdigen Personen sowie Presseveröffentlichungen. Ein wichtiger Faktor ist die wahrgenommene Reputation des Anbieters bzw. der Kombination von Anbietern komplexer IT-Anwendungen. Kann sich der Anbieter überhaupt Lücken in der IT-Sicherheit leisten?

Anbieter informationstechnischer Infrastrukturen sehen eine wachsende Komplexität der Herausforderungen durch immer gezieltere Angriffe, die es abzuwehren gilt. Nur durch enge internationale Kooperation kann der Professionalisierung der vorwiegend kriminellen Angreifer begegnet werden.

Die Wechselwirkungen der Faktoren werden in folgender Abbildung zusammengefasst dargestellt.

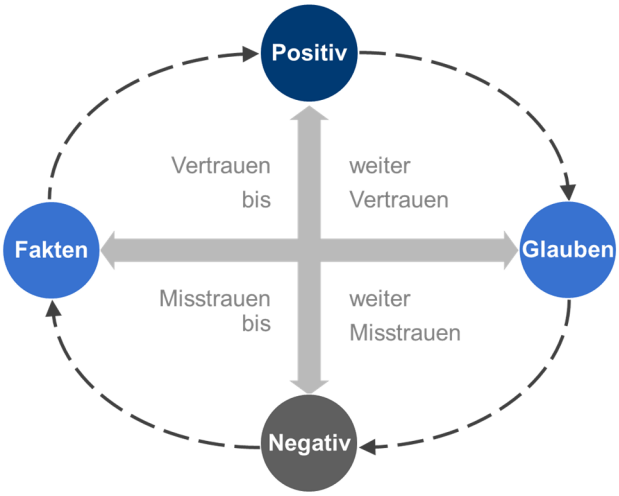

Abbildung 4: Psychologie des Vertrauens[6]

Die Weiterentwicklung von Sicherheitstechnologien und deren Zertifizierung durch unabhängige Experten der eingesetzten Komponenten sind eine Grundvoraussetzung. Dazu kommt die operative Sicherheit, bei der weitgehend sicherzustellen ist, dass die für Betrieb und Wartung zuständigen Personen entsprechend handeln und überprüft werden.

[6] angelehnt an http://www.muezart.com/

Anhang

Diese Broschüre dient der Einführung in das Thema "Vertrauen und IT-Sicherheit" und wird ergänzt durch die Sammlung von Links auf der TeleTrusT-Webseite und den Referenzen im Anhang: evaluierte Sicherheitskomponenten, unabhängige Qualitätssiegel, automatisierte Analyseverfahren für "harte" und "weiche" Faktoren sowie aktuelle Forschungsprojekte.

Unter folgenden Links wird auf aktuelle Forschungsprojekte verwiesen:

DIVSI Entscheider-Studie zu Vertrauen und Sicherheit im Internet (2013)
https://www.teletrust.de/fileadmin/_migrated/content_uploads/DIVSI_Entscheiderstudie.pdf

BSI-Magazin
https://www.bsi.bund.de/DE/Publikationen/BSI-Magazin/BSI-Magazin_node.html

uTRUSTit-Projekt
http://www.utrustit.eu/project_summary/

Weitere Links und Zusatzinformationen sind unter https://www.teletrust.de/publikationen/broschueren/vertrauensmodell zu finden.

TeleTrusT – Bundesverband IT-Sicherheit e.V.

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breit gefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Experten, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Expertenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.) und "TeleTrusT Engineer for System Security" (T.E.S.S.) sowie des Qualitätszeichens "IT Security made in Germany". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

Kontakt:

TeleTrusT – Bundesverband IT-Sicherheit e.V.
Dr. Holger Mühlbauer
Geschäftsführer
Chausseestraße 17
10115 Berlin
Tel.: +49 30 4005 4306
Fax: +49 30 4005 4311
http://www.teletrust.de

TeleTrusT
Pioneers in IT security.


TeleTrusT
Pioneers in IT security.