1. Inhaltsverzeichnis

2. Subjektive Kriterien für Sicherheit

LAIENURTEILE

Bei der Beurteilung von Sicherheit in der Technik spielen die Urteile von Laien eine große Rolle. Sie sind i.d.R. mit Technik nur wenig vertraut, sind aber eine Mehrheit untern den (vorgesehenen) Nutzern einer Technologie. Über die Beurteilung von Technologien an sich, liefert die Befragung von Laien auch noch einen Katalog von Kriterien, nach denen diese derartige Beurteilungen vornehmen. Dies ist naturgemäß der Fall, da Laien, die sich nur eines Teils der Technik überhaupt bewußt sind, auch nur einen (mehr oder weniger großen) Ausschnitt auch als Bewertungsgrundlage verwenden können. Das Fehlen eigener Erfahrungen im Umgang mit bestimmten Technologien sollte dazu führen, daß bei der Technikgestaltung darauf geachtet wird, daß diese durch andere Maßnahmen substituiert werden.
Die Erfahrungen der Laien und ihre Maßstäbe in der Beurteilung von Technik liefern wichtige Anhaltspunkte dafür, wie Technik gestaltet und präsentiert werden soll, damit der Laie als Nutzer sie subjektiv als sicher empfindet. Dafür genügt nämlich die objektiv ausgereifte Technik alleine nicht. Eine Technik kann noch so sicher sein, wenn der Nutzer sie als unsicher empfindet, wird sie abgelehnt. Andererseits können wenig sichere Technologien von Nutzern mit geringen Kenntnissen auf diesem Gebiet als sicher angesehen werden.

WERTE

In [MüS] wurde eine Gruppe von Menschen dahingehend befragt, wie sie gewisse Sicherheitskriterien (in der Kommunikationstechnik) bezüglich ihrer Wichtigkeit einschätzen und wie weit sie tatsächlich offenbar gewährleistet seien.

Die Ergebnisse sind zwar nicht repräsentativ und auf alle Techniken übertragbar, es lassen sich aber gewisse Muster im Sicherheitsempfinden erkennen, die auf andere Gebiete und Fragestellungen übertragen werden können.
Abbildung 1 stellt dar, wie wichtig acht ausgewählte Kriterien für die Testpersonen waren. Die Werte gehen von 1 (unwichtig) bis 5 (sehr wichtig)

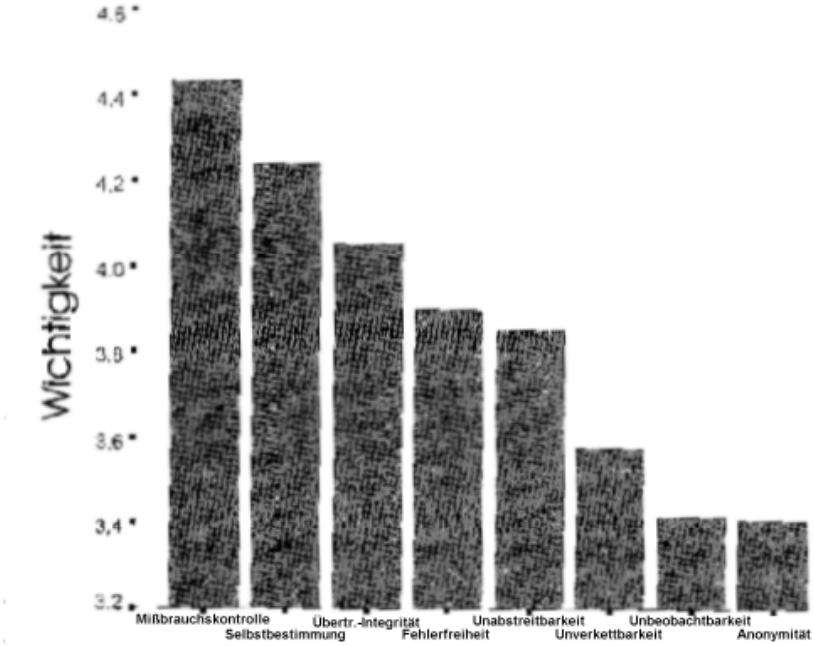

Abbildung 1: Subjektive Wichtigkeit der Sicherheitskriterien, [MüS] S. 106

Eine weitere Fragestellung war, inwieweit die Laien der Eindruck haben, daß diese Kriterien auch erfüllt sind. Das Ergebnis ist in Abbildung 2 zu sehen.

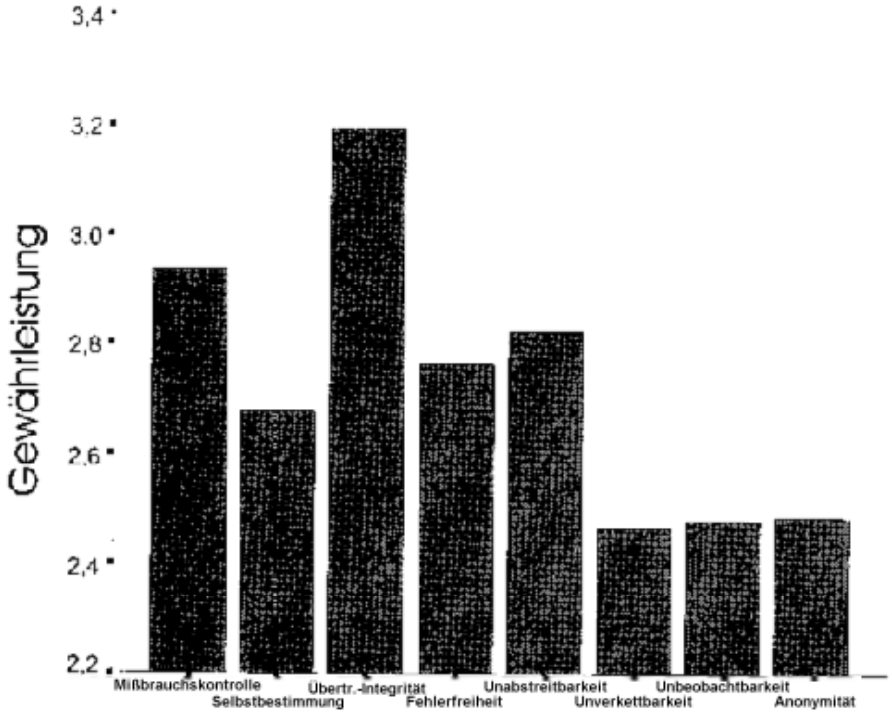

Abbildung 2: Subjektive Gewährleistung der Sicherheitskriterien, [MüS] S. 108

Die beiden Graphiken legen verschiedenes dar. Einmal fällt auf, daß die Gewährleistung keine wirklich hohen Werte erreicht. Außerdem gibt es gewisse Zusammenhänge zwischen Wichtigkeit und Gewährleistung. So werden die wichtigen Sicherheitskriterien nur als mittel gewährleistet angesehen, während die eher unwichtigen Kriterien kritscher gesehen werden. Es sieht so aus, als ob es bei der Entscheidung über die Nutzung moderner Kommunikationstechnologien im besonderen darauf ankommt, daß die als wichtig angesehenen Kriterien erfüllt sind. Offenbar hängt die Bereitschaft zur Nutzung einer Technologie nicht alleine davon ab, wie bedeutsam die Kriterien subjektiv sind, sondern auch davon, inwieweit als wichtig bewertete Aspekte umgesetzt sind.
In der Abbildung 3 wird die Beziehung zwischen den beiden Faktoren Wichtigkeit und Gewährleistung dargelegt.

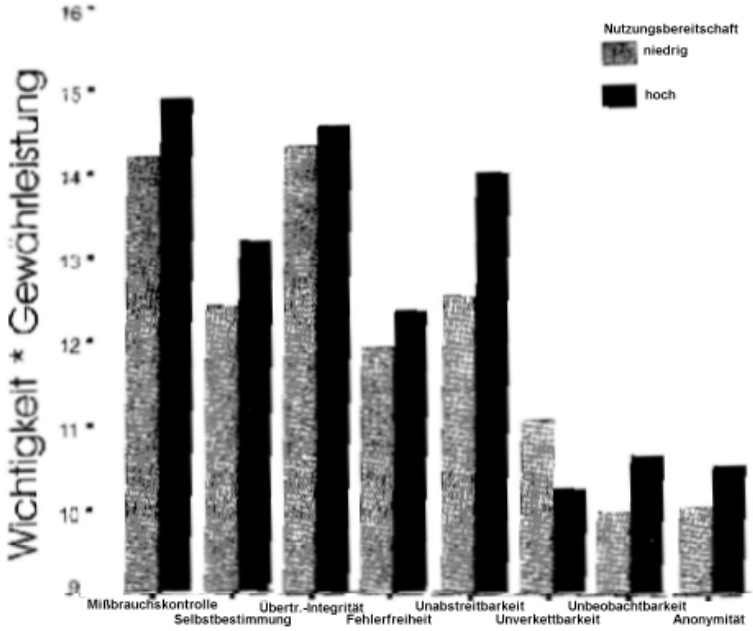

Abbildung 3: Nutzungsbereitschaft und gwichtete Kriterienwichtigkeit für Gruppen mit hoher und niedriger Nutzungsbereitschaft, [MüS] S.110

Es gibt offenbar einen signifikanten Zusammenhang zwischen den wichtigen Kriterien und der Einschätzung der Gewährleistung derselben. Die Gruppen mit hoher Nutzungsbereitschaft bewerten diese Kombination höher, als diejenigen mit niedrige Bereitschaft.

ERGEBNISSE

Folgendes Bild zeichnet sich ab: Diejenigen Gruppen, die bereits heute gewisse Technologien nutzen, werden dies auch in Zukunft tun. Andererseits werden die Menschen, die den aktuellen Technologien ablehnend gegenüberstehen,
Die Bereitschaft zur Nutzung von Technologien hängt auch von individuellen Wertvorstellungen ab.
Menschen, die Wert auf ihre Überzeugungen legen und eher sozial orientiert sind, sind auch modernen Kommunikationstechnologien eher skeptisch und ablehnend eingestellt und haben folglich auch wenig Erfahrungen mit diesen.
Im Gegensatz dazu haben Menschen, für die Effizienz, Autonomie und eigene Handlungsfähigkeit wichtig sind, eine wesentlich größe Bereitschaft zur Nutzung derartige Technologien.

Darüber hinaus spielen ihre inneren Werte für die Bewertung der Sicherheitstechnologien für die erstere Gruppe eine um einiges höhere Rolle als für die letzere.
Sicherheitskriterien sind nur dann von Interesse, wenn diese mit individuellen Werten in Zusammenhang stehen. Ist dies nicht der Fall, wird er pragmatisch vorgegangen und auf Dinge wie eigene Erfahrungen zurückgegriffen.

SCHLUßFOLGERUNGEN

Zunächst möchte ich einmal anmerken, daß ich diese Untersuchungen nur begrenzt für aussagefähig halte. Der Personenkreis ist sehr klein (168 Personen) und kaum repräsentativ (Durchschnittsalter 30 Jahre, 62% Männer, 38% Fraueb mit übermäßig gehobenem Bildungsstand). Dadurch stehen auch die statistischen Methoden auf etwas wackligen Füßen.
Nicht alleine der Stand der Technik oder individuelle Werte sind für die Beurteilung und Nutzung von Technik entscheidet. Darüber hinaus haben die sozialen Rahmenbedingungen, in denen diese Technologie etabliert wird, eine erhebliche, wenn nicht ausschlaggebende Bedeutung.
Eines haben diese Untersuchungen jedoch dargelegt: Wir brauchen nicht nur technische Methoden, um Sicherheit in diesem Bereich zu erreichen. Darüber hinaus müssen bei der Technikgestaltung auch gesellschaftliche Kriterien berücksichtig werden. Dies geht soweit, daß eine Technologie ohne eine derartige Gestaltung abgelehnt wird, obwohl sich technisch mehr als hinreichend sicher ist.
Bei der Information der (potentiellen) Nutzer ist es nicht nur wichtig, auf die technischen und sozialen Sicherheitskriterien hinzuweisen, sondern auch den Menschen die Erfüllung ihrer individuellen Werte zu demonstrieren.

3. Die Rolle des Vertrauens

In diesem Zusammenhang möchte ich Vertrauensbildung in soziologischer Sicht eingehen und diese am Beispiel der Kommunikationtechnik demonstrieren.

EINLEITUNG

Kommunikationstechnik und Anwendungen in offenen Datennetzen haben in den letzen Jahren mehr und mehr an Bedeutung gewonnen. Eine gewisse Euphorie über die Möglichkeiten dieser Technologie ließ Sicherheitsdenken erst langsam entstehen. Erst in letzter Zeit bekam dieses ein Gewicht.
Um eine breite Akzeptanz solcher Technologien zu erreichen, spielt es eine Rolle, daß die Nutzer diese auch als sicher einschätzen. Neben der Gewährleistung, daß Technik durch technische Mittel möglichst sicher gemacht wird, ist es auch unumgehbar, Vertrauen in diese zu schaffen. Dies ist um so mehr der Fall, wie verläßliche Technik keine Garantie für Vertrauen ist.
Leider gibt es kein Patentrezept, um mit sozialtechnischen Mitteln Vertrauen zu schaffen. Offensichtlich gibt es keine Beziehung zwischen der Verläßlichkeit einer Technologie und dem Vertrauen, das in sie gesetzt wird. Ein Zeichen dafür ist, daß in Systeme vertraut, obwohl sie offensichtlich nicht sicher sind. Das Internet per se hat ja bekanntlich kaum Sicherheitsmechanismen eingebaut. Vertrauen in Technik kann in Wirklichkeit auch nur Vertrauen in den sozialen Kontext sein, in den die Anwendung eingebettet ist. Dabei spielt das Vertrauen in die organisatorischen, rechtlichen, kulturellen und instituionellen Strukturen eine große Rolle. Beispielweise war in den 80er Jahren das Mißtrauen gegenüber Diensten wie ISDN oder BTX groß. Dahinter steckte

aber ein großes Mißtrauen gegenüber dem Staat. Andererseits rührt ein Teil des Vertrauens in das Internet daher, daß keine einzelne Institution oder kein einzelner Staat es kontrolliert.
Vertrauen kann nicht zielgerichtet geplant und erzeugt werden. Die Rahmenbedingungen, die Vertrauen entstehen lassen, sind nicht beliebig. Es gibt Maßnahmen, von denen man mit Grund hoffen kann, daß sie mehr Vertrauen entstehen lassen. Eine irgendwie geartete Sicherheit gibt es hier allerdings nicht.
In jüngster Zeit wird viel über Vertrauen oder Mißtrauen in Technik diskutiert. Vertrauen in Technik ist eine notwendige Voraussetzung; sie läßt sich aber nicht mehr alleine rational begründen. Dies fordert die Technikgestaltung als solche heraus.
Jemand, der vertraut, geht gegenüber einer Technologie in Vorleistung. Er weiß, daß das was er erwartet, nicht sicher ist, handelt aber so, als ob dies, worauf er vertraut, auf jeden Fall eintreten wird. Dies bedeutet auch, daß keine Vorbereitung auf den unerwarteten Fall erfolgt.
Vertrauen liegt irgendwo zwischen Wissen und Nichtwissen. Wer alles weiß, braucht nicht zu vertrauen; er ist sich sicher, was geschieht. Der Unwissende kann allerdings auch kein Vertrauen aufbauen.
Hat sich eine Technologie bereits in der Vergangenheit bewährt und hat ein einzelner derartige Erfahrungen gemacht, so wird er sich beinahe sicher sein, daß dies auch in Zukunft so sein wird. Andererseit kann eine neue Technologie nur dann verwendet werden, wenn ein gewissen Vertrauen vorgestreckt wird, auch wenn es noch keine Anhaltspunkte für irgendeine Sicherheit gibt. Aber auch bei vielen Technologien, die wir Tag für Tag erfolgreich nutzen, wissen wir i.d.R. nicht, wie sie genau funktionieren. Selbst meine Komilitonen werden wohl behaupten können, sie kennen jedes Detail in der Steuerung einer Waschmaschine.
Unsere Gesellschaft und Technik versucht immer mehr, Kontrolle der Natur zu entreißen und dem Menschen zu übertragen. Aber gerade dieser Prozeß führt dazu, daß viele Menschen die Technik als solche auch nicht mehr wirklich verstehen und kontrollieren können.
Bei der nun folgenden Betrachtung zum Thema Vertauen steht nicht das Individuum im Blickfeld, sondern die Gesellschaft als Einheit von vielen.

TECHNIK

Der Einfluß der Technik selbst ist naheliegend. Ein Unfall in einem Atomkraftwerk hat beispielsweise einen großen Einfluß auf das Vertrauen in die Technik. Um mit Mitteln der Technik Vertrauen zu schaffen, ist es also notwendig, die Risiken zu minimieren. Nicht nur so drastische Beispiele wie das eben erwähnte, schaden der Vertrauenswürdigkeit einer Technologie. Auch viele kleine häufige Störungen und Pannen erzeugen ein Mißtrauen in die Technik und die Menschen, die sie schaffen. Hierfür seien exemplarisch die EnBw und die Atomaufsicht in Baden-Württemberg genannt, die kürzlich durch eine Serie von Unzulänglichkeiten viel Vertrauen verspielt haben.
Vertrauen und Mißtrauen entsteht nicht durch eine Technologie selbst, sondern auch durch ihre Nutzung. Ein Problem hierbei ist die mögliche Fehlbedienung durch die Nutzer, die gerade Informatikern nicht fremd sein sollte. Techniker beklagen sich – hier am Beispiel der Kommunikationtechnik – darüber, daß PINs gut sichtbar aufgeschrieben werden oder daß leicht zu erratende Paßwörter verwendet werden. Es ist wichtig, nicht auf der Kritik zu verharren, sondern die Technik so zu gestalten, daß Fehlnutzungen so

weit wie möglich vermieden werden. Um am Beispiel der „schwachen“ Paßwörter zu bleiben: Hier muß zweigleisig gefahren werden. Einerseits sollte mit technischen Mitteln verhindert werden, daß derartige Paßwörter verwendet werden (Tests mit Crackprogrammen u.ä.). Andererseits müssen die Benutzer geschult werden und ihnen dargelegt werden, warum der Vorname des Ehepartners kein sicheres Paßwort ist.
Es gibt auch Ansätze, die davon ausgehen, daß jeder einzelne alle Bedrohungen moderner Technologien und die Werkzeuge zur Abschwächung und Beseitigung dieser kennen muß und somit auch nutzen kann. Dieser Ansatz führt meiner Meinung nicht weit genug in die Breite, läßt er nämlich auch institutionelle und kulturelle Aspekt, wie sie weiter unten beschrieben werden, außer acht. Ein umfassendes Wissen in allen für einen Menschen sicherheitsrelevanten Bereich ist eine Illusion – die Zeit der Universalgelehrten ist schon lange vorbei!
Ein weiteres Problem ist, daß gerade stark ausgereifte Technologie dazu führen kann, daß die Menschen leichtsinnig werden. So wurde schon eine riskantere Fahrweise bei Automoblisten mit ABS-Fahrzeugen beobachtet.

INSTITUTIONEN

Der Begriff Institutionen umfaßt verschiedenste Dinge. Dies sind einmal gesellschaftliche Regulationsmuster wie Normen und Werte; darüber hinaus können es auch gesetzliche Regelungen sowie verschiedenste Organisationen sein.
Einen wesentlichen Beitrag zur Vertrauensbildung liefert das institutionalisierte Mißtrauen. Das Mißtrauen und die Kontrolle gewisser Institutionen schafft seinerseits wieder Vertrauen in eine Technologie. Aus diesem Grund ergibt sich die Notwendigkeit für neutrale Instanzen, welche die kommerziellen Anbieter von Kommunikationstechnik kontrollieren. Und in diese Kontrollen wird dann wieder Vertrauen gesetzt, was letztendlich Vertrauen in die Technologie als solche schafft.
Ein weiteres Instrument zur Vertrauensbildung sind Gesetze. Der Eindruck, daß Technik in geregelten Bahnen verläuft und sich so in gewissem Rahmen ab- und einschätzen läßt, bringt die Einschätzung mit sich, daß diese zum Nutzen der Gesellschaft verwendet wird und nicht für Einzelinteressen mißbraucht wird. So entsteht wieder Vertrauen.

KULTUR

Kultur meint hier die Einstellung der Menschen zur Technik im allgemeinen. So ist z.B. interessant, ob in einer Gesellschaft grundsätzlich zunächst die Chancen oder zunächst die Risiken einer Technologie diskutiert werden. Eine andere Frage ist, inwieweit eine Gesellschaft davon überzeugt ist, daß Probleme durch Technik gelöst werden können oder daßTechnik eher Ursache von Problemen ist.
Sicherlich wurden die meisten Technologien eingeführt, bevor alle – vor allem die negativen – Folgen abschätzbar waren. Es ließen sich viele Beispiele dafür aufzeigen: Röntgenstrahlung, Automobile (Unfälle/Umwelt), Pflanzenschutzmittel, Kernkraft (Entsorgungsproblematik), Hochfrequenztechnik (Elektrosmog), Antibiotika (Resistenzen) u.v.a.m. Dennoch gibt es immer wieder Triebfedern, neue Technologien einzuführen: Streben nach Sicherheit, Bequemlichkeit oder finanziellem Gewinn.
Ein möglicher Ansatz ist es, die Traditionen und langfristig gewachsenen Werte einer Gesellschaft zu berücksichtigen. Die Gefahr dabei ist, daß man stattdessen Vorurteile übernimmt und als unabänderliche Wahrheiten ansieht.
In den letzten Jahren hat sich viel in der Einstellung der Menschen zu Kommunikationstechnik geändert. Anfangs der 80er Jahre war das Horrorszenario von

die Welt beherrschenden Computern noch weit verbreitet. Beispiele sind das Orwellsche Jahr „1984“ [Orw] und der Film „Wargames“ [War]. In letzterem wird aufgezeigt, wie durch Schwächen und Hintertüren im System, ein solches sich soweit verselbständigt, daß die Menschheit in ihrer Existenz bedroht wird. Zu jener Zeit war auch das Schlagwort „Computer übernehmen die Macht“ nicht selten anzutreffen.

WAHRNEHMUNG VON UND WISSEN ÜBER TECHNIK

Für Ansehen einer Technologie oder das Vertrauen, das in sie gesetzt wird, ist nicht alleine ihre Verläßlichkeit alleine entscheidet. Viel hängt davon ab, wie sie von der Gesellschaft wahrgenommen wird.
Ein wichtiges Instrument, das Vertrauen in eine Technologie zu erhöhen, ist die Vermittlung von Wissen. Wer nichts weiß, kann auch nicht vertrauen, wer alles weiß, braucht es nicht mehr. Mehr Wissen bedeutet allerdings nicht zwangsläufig mehr Vertrauen. Vertrautheit kann aber auch zu Mißtrauen führen, denn „nicht nur günstige Aussichten, sondern auch Gefahren bedürfen einer gewissen Vertrautheit, ..., um ein vertrauensvolles oder mißtrauisches Hineinleben in die Zukunft zu ermöglichen “ [Luh]
Zu viel Wissen schränkt die Handlungsfähigkeit des Menschen ein, da man je mehr Detailkenntnisse man hat, desto mehr Unsicherheiten und Widersprüche aufwirft. Diese fordern dazu auf, sich noch intensiver mit der Thematik zu beschäftigen, was wieder zu neuen Unsicherheiten führt.
Erfahrungsgemäß ist es so, daß Undurchschaubarkeit von Technologie solange wenig Probleme bereitet, wie die Technik das tut, was von ihr erwartet wird.

ERFAHRBARKEIT

Wieweit ein Mensch in eine bestimmte Technik vertraut, hängt nicht notwendigerweise vom Wissen über die Funktion dieser ab. Vielmehr spielt die Erfahrung der äußeren Wirkungen einer Technik i.d.R. die entscheidende Rolle. Für die Nutzer sind die Möglichkeiten und Folgen einer Technik entscheidend, nicht wie sie zustandekommt oder wie sie funktioniert. Wichtig ist, daß sie meistens so funktioniert, wie der Nutzer es erwartet. Dann vertraut er auf sie, als ob er sicher wäre, das sie funktioniert.
Was steckt hinter diesem Mechanismus? Der Nutzer wägt Risiko und Chancen für sich ab. Er rechnet sich (meist unbewußt) Wahrscheinlichkeiten für bestimmte Folgen aus und bewertet dies. Entscheidend ist also das Verhältnis von möglichem Nutzen zu möglichen Schaden.
Oft kommt es vor, daß Menschen zwar ihr Mißtrauen gegenüber einer bestimmten Technik kundtun, sie jedoch dennoch benutzen. Dies läßt sich mit der Abschätzung erklären, daß eigentlich nicht viel passieren kann und daß das eigene Mißtrauen mit dazu führt, daß Mängel in der Technik beseitigt werden. Andererseits liefert einem das Wissen um eine Gefahr eine gewisse Macht über diese.
Da man nicht immer unbekannte Technologien selbst erfassen, ist oft Wissen aus zweiter Hand notwendig. Eine mögliche Quelle sind die verschiedenen Medien. Über diese kann man an den Erfahrungen anderer teilnehmen. Interessant ist, daß verschiedene Experten darüber klagen, daß gewisse Sicherheitsprobleme erst dann wahrgenommen werden und Gegenmaßnahmen ergriffen werden, wenn die Medien groß darüber berichten.

EXPERTEN

Die Meinungen, die Expertem äußern, haben einen großen Einfluß auf das Ansehen von Technologien. Experten zeichnen sich durch gewisse Qualifikationen aus, die von gewissen Institutionen oder der Gesellschaft selbst bestätigt und getragen werden.
Vertrauen in Technologien kann also auch durch das Vertrauen der Experten, welchen vertraut wird, in diese begründet sein.
Auch können Laien Risiken und notwendige Gegenmaßnahmen nicht erkennen und sind so auf Experten angewiesen. Aber auch Experten müssen zugeben, daß es keine vollständige Sicherheit geben kann und hohe Sicherheit auch nur für einen begrenzten Zeitraum gilt. Was heute sicher ist, kann morgen schon wieder unsicher sein, wenn sich die Technologien weiterentwickelt haben.

INSTITUTIONEN

Welche Rolle spielen die institutionellen Einflüsse für die Vertrauensbildung?
Es ist z.B. möglich, Vertrauen in ähnliche Institutionen auf andere zu übertragen. Gute Erfahrungen mit dem herkömmlichen Versandhandel erhöhen u.U. auch das Vertrauen ins Einkaufen im Internet. Firmen, mit denen bisher auf herkömliche Weise (Telefon, Post, Fax usw.) gehandelt wurde, wird auch in anderen Bereichen ein gewisser Vertrauenvorschuß zugestanden.
Vertraut wird auch gerne Partnern, die ähnliche Interessen als man selbst hat. Es ist einfacher, Vertrauen in ein Unternehmen zu haben, von dem man den Eindruck hat, daß es gerne möchte, daß man ein zufriedener Kunde ist, als in eines, von dem man meint, es wolle nur möglichst viel Profit aus einem herausquetschen.
Leider muß davon ausgegangen werden, daß im Einzelfall Vertrauen durch einzelne mißbraucht wird. Dies stellt aber dann kein unüberwindbares Problem dar, wenn die Institution dies verfolgt und bestraft.
Es gibt verschiedenste Maßnahmen, mit denen durch Regulierung Vertrauen gebildet werden kann:
Einmal gibt es die Möglichkeit die Handlungsmöglichkeiten und den Zugang zu Technologie zu beschränkte. Dies geschieht durch Mechanismen wie Nutzungsbedingungen oder Gesetze.
Ein weiterer Aspekt ist die Konfliktregulierung. Dies bedeutet, daß Gerichte oder Schiedsinstanzen vorhanden sind, die Entscheidungen treffen, wenn verschiedene Seiten verschiedene Vorstellungen haben. Vertrauen entsteht hier, indem man weiß, daß man im Konfliktfall eine Institution – die dann natürlich auch vertrauenswürdig sein muß – hat, die einem zu seinem Recht verhilft.
Versicherungen und Bürgschaften spielen auch eine Rolle bei der Vertrauensbildung. Diese garantieren einem, daß im Schadensfall entweder gar kein oder nur ein kalkulierbar geringer Schaden für den Nutzer entsteht. Typische Beispiele sind Garantien von Herstellern oder Zertifizierungsinstanzen für öffentliche Schlüssel.
Wichtig für den Nutzer sind auch Institutionen, die für den Nutzer eine Stellvertreterfunktion übernehmen, wenn dieser diese nicht wahrnehmen kann. Beispiele hierfür sind Verbraucherverbände oder Computernotfallteams.
Eine andere Möglichkeit sind (neutrale und vertrauenswürdige) Kontroll- bzw. Prüfinstanzen. Diese werden entweder zwangsläufig oder freiwillig von den Anbietern von Produkten und Dienstleistungen in Anspruch genommen, um sich gewisse Standards bescheinigen zu lassen. Beispiele sind Technische Überwachungsvereine u.ä.
Die folgenden Instititutionsklassen spielen eine Rolle bei der Vertrauensbildung:

Technische Evaluierung und Zertifizierung
Institutionen führen technische Tests durch und zertifizieren Firmen, wenn erstere erfolgreich waren. Wichtig ist die Neutralität und Vertrauenswürdigkeit dieser Institutionen, damit die Nutzer deren Zertifikate auch anerkennen, ohne daß sie die Kriterien kennen, die ihnen zugrunde liegen.

Normung
Normen können dem Nutzer den Vergleich und die Bewertung verschiedener Applikationen erleichtern. Allgemein anerkannte (oder vorgeschriebene) Normen sorgen für gewisse Mindeststandards.

Zertifizierungsstellen für öffentliche „Schlüssel" (Trust Center)
Da bei der Authentifizierung über private und öffentliche Schlüssel irgendwie sichergestellt werden muß, daß der öffentliche Schlüssel authentisch ist und der direkte Austausch des Schlüssels zwischen Absender und Empfänger nicht immer praktikabel ist, liegt es nahe, sich die Authentizität des Schlüssels von einer vertrauenswürdigen neutralen Stelle bestätigen zu lassen. Eine Möglichkeit, Mißbrauch zu vermeiden, ist den privaten Schlüssel aufzuteilen und an mehere Institutionen zu verteilen.

Sicherheitsdienstleister und Berater
Derartige Unterstützung ist auch aus finanziellen Gründen wohl nur für Firmen ein Thema. Mit dem Vertrauen in den Berater entsteht auch das Vertrauen darin, daß dieser bei Bedarf die notwendigen Sicherheitsmaßnahmen für einen ergreift.

Computernotfallteams (CERTs)
Diese Teams beraten bei Einbrüchen in Systeme die Administratoren und stellen Informationen zu sicherheitrelevanten Themen zusammen. Es gibt sie z.B. bei Deutschen Forschungsnetzes (zu dem auch die FH Furtwangen über BelWue gehört) oder beim Bundesamt für Sicheheit in der Informationstechnik (BSI). Sie führen auch Schulungen durch und helfen in Notfällen und tragen dadurch letztendlich dazu bei, daß das Vertrauen in die Technologie erhöht wird.

Interessenvertretungen der Nutzer
Verbraucherverbände oder die Stiftung Warentest arbeiten stellvertretend für die Nutzer. Sie sind für den Nutzer gerade deswegen interessant, weil sie nicht neutral sind, sondern die „eigene" Seite zu vertreten versuchen.

Datenschützer
Schon die reine Existenz der Datenschützer bringt das Vertrauen mit sich, daß etwas unternommen wird. Sie haben auch umfangreiche Aufklärungsaufgaben. Sinnvoll wäre in diesem Zusammenhang, auch in Deutschland Datenschutzzertifikate zu etablieren, wie sie in den USA bereits verbreitet sind (TrustE u.ä.).

ZUSAMMENFASSUNG

Schlußendlich läßt sich folgendes sagen:
Der Prozeß der Vertrauensbildung ist hochkomplex und läßt sich nicht sicher vorherbestimmen. Verschiedenste technische, kulturelle und psychologisch-gesellschaftliche Aspekte wirken ein und erschweren eine genaue Einschätzung.
Ein probates Mittel für die Vertrauensgewinnung ist das Vorgehen, bereits Vertrautes, dem auch vertraut wird, mit neuem zu verknüpfen und zu verweben, so daß ein Teil des Vertrauens auf das neue übergeht.
Im wesentlichen muß bei der Gestaltung von Technik darauf geachtet werden, daß alle Aspekte und Seiten berücksichtigt werden und weitsichtig geplant wird.

Die folgenden Faktoren haben nämlich alle zusammen einen Einfluß auf das Vertrauen in Technik:

- Technik
- Kultur
- Institutionen

Abbildungsverzeichnis

Quellenangaben

[MüS] Mehrseitige Sicherheit in der Kommunikationstechnik; Günther Müller, Kurt-Hermann Stapf (Hrsg.); Addison-Wesley

[War] WarGames – Kriegsspiele, Film, 1983, Regie: John Badham; Drehbuch: Lawrence Lasker und Walter F. Parkes

[Luh] Vertrauen. Ein Mechanismus der Reduktion soziale Komplexität; Niklas Luhmann; Enke

[Orw] Nineteen Eighty-Four; George Orwell; Longman Group Limited

Von wesentlicher Bedeutung bei der Erstellung dieser Arbeit waren für mich meine eigenen Erfahrungen mit den verschiedenen Gruppen bezüglich der verschiedenen aktuellen Technologien.