Ulla Coester, Norbert Pohlmann

Vertrauenswürdigkeit schafft Vertrauen

Vertrauen ist der Schlüssel zum Erfolg von IT- und IT-Sicherheitsunternehmen

Aufgrund der zunehmenden IT-Technisierung und damit einhergehend stetigen Veränderung der Lebensbedingungen ist es notwendig, dass Menschen den IT-Lösungen und Unternehmen weiterhin und kontinuierlich vertrauen können. Denn durch den höheren Grad der IT-Technisierung steigt die Komplexität, wodurch es für den Nutzer zunehmend schwieriger wird, einzelne IT-Lösungen und deren Hintergründe zu verstehen sowie zu bewerten. Diese Veränderung hat Auswirkungen: Zum einen macht sie grundsätzlich den Nutzern – den Menschen – Angst [1], da gewohnte Vorgänge beständig ihre Gültigkeit verlieren. Zum anderen entsteht dadurch sowie durch die Komplexität latent das Gefühl, eine falsche Entscheidung zu treffen, weil nicht alles bedacht werden kann. So fällt dem Aspekt der Interdependenz von Vertrauen und Vertrauenswürdigkeit für deutsche und europäische Unternehmen eine hohe Bedeutung zu, insbesondere auch da sich internationale Tech-Unternehmen zunehmend weniger vertrauenswürdig im komplexen Cyber-Raum verhalten. Dies eröffnet die Möglichkeit, sich über den Aufbau von Vertrauen weltweit gegen internationale Unternehmen nachhaltig zu profilieren und positionieren. Um dieses Ziel zu realisieren, bedarf es einer strategischen Vorgehensweise – zum Beispiel auf Basis des Vertrauenswürdigkeitsmodells.

Ulla Coester

als Gründerin/CEO des Unternehmens xethix Empowerment, berät sie in Prozessen zur Corporate Digital Responsibility, Fokus Vertrauenswürdigkeit/Digitale Ethik. 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 Informatikprofessor für Cyber-Sicherheit 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

Im Prinzip möchten Menschen Vertrauen schenken und müssen dies auch, um grundsätzlich handlungsfähig zu sein. Denn die damit verbundene Gewissheit – also die Annahme, dass es möglich ist, sich auf etwas Bestimmtes zu verlassen – reduziert Komplexität, weil dadurch die subjektive Überzeugung der Richtigkeit von Handlungen entsteht. Übertragen auf die digitale Transformation lässt sich daraus ableiten, dass Unternehmen ihre IT-Lösungen so gestalten müssen, dass Nutzer Vertrauen aufbauen können. Denn nur so gewährleisten sie, dass es möglich ist, die damit verbundenen, potenziell risikobehafteten Handlung zu akzeptieren und schaffen darüber für Nutzer die Möglichkeit zur Teilhabe an der digitalen Zukunft.

Doch für diese Komplexitätsreduzierung ist die Qualität der Vertrauensgrundlage zwischen Unternehmen und Nutzer von Bedeutung, da diese entscheidend dafür ist, dass ein erforderliches Maß an Vertrauen aufgebaut werden kann. Unternehmen müssen daher über eine wahrgenommene Vertrauenswürdigkeit Nutzer in die Lage versetzen, ihre grundsätzliche Vertrauensfähigkeit auf IT-Lösungen und Hersteller zu übertragen [2].

1 Framework: Vertrauenswürdigkeitsmodell

Das Vertrauenswürdigkeitsmodell zeigt auf, was Unternehmen tun können, um ein Vertrauen, das normalerweise zwischen zwei Menschen entsteht, auf Unternehmen zu übertragen.

Relevant im Vertrauenswürdigkeitsmodell sind der Vertrauensgeber – also der Nutzer – auf der einen Seite sowie der Vertrauensnehmer auf der anderen Seite [3].

Bei dem Nutzer – der generisch sowohl für Privatanwender als auch für Mitarbeiter von Anwendungsunternehmen, die IT-Lösungen nutzen, steht – sind zwei Eigenschaften von Bedeutung beziehungsweise notwendig: einerseits die Kompetenz zum Aufbau eines institutionellen Vertrauens, andererseits die eigene Vertrauensfähigkeit.

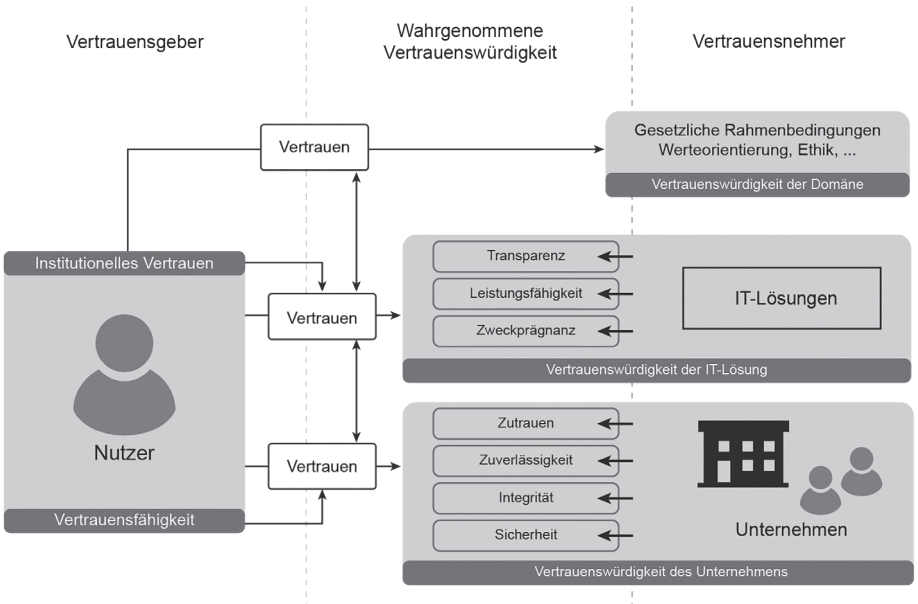
Bei dem Vertrauensnehmer sind verschiedene Dimensionen zu unterscheiden, die jeweils mit entsprechenden Aspekten ihre Vertrauenswürdigkeit dokumentieren:

1) Unternehmen als Hersteller oder Anbieter von IT- und IT-Sicherheitslösungen.

2) IT-Lösungen – im Kontext der IT-Sicherheit – sind allgemein Technologien, Anwendungen, Produkte oder Dienstleistungen mit entsprechenden IT-Sicherheitsmechanismen oder separate IT-Sicherheitssysteme.

3) Domänen im Sinne eines kollaborativen Zusammenwirkens von Herstellern und Stakeholdern aus einer Branche sowie Nutzern.

Abbildung 1 | Vertrauenswürdigkeitsmodell



Warum es für zwei Personen möglich ist, einander zu vertrauen, lässt sich unter anderem darüber erklären, dass Menschen die Fähigkeit zur Empathie besitzen. Das bedeutet, ein Mensch kann anhand seiner eigenen subjektiven Kriterien – wie Sprache oder Gestik – festlegen, ob er sein Gegenüber für vertrauenswürdig hält. Einen Lösungsansatz dahingehend, was Unternehmen tun können, um als Institution ein entsprechendes Vertrauensverhältnis zu den Nutzern aufzubauen, bietet das Vertrauenswürdigkeitsmodell.

Zum einen lässt sich darüber der Zusammenhang zwischen Vertrauen und Vertrauenswürdigkeit aufzeigen. Zum anderen macht es transparent, was getan werden muss, damit auf Basis der Vertrauensfähigkeit eines Nutzers ein institutionelles Vertrauen mithilfe der wahrgenommenen Vertrauenswürdigkeit der IT-Lösung, des Unternehmens und der Domäne aufgebaut werden kann. Dieses Vertrauensverhältnis wird als institutionelles Vertrauen bezeichnet. Es entsteht dadurch, dass ein Nutzer dazu bereit und in der Lage ist, seine generelle Vertrauensfähigkeit auf ein Unternehmen beziehungsweise eine IT-Lösung zu übertragen. Diese Transferleistung ist dadurch möglich, dass individuelle Kriterien zur Vertrauensbildung auf Basis von kognitiven Faktoren erfüllt werden.

Die konkrete Aufgabe, die mithilfe des Vertrauenswürdigkeitsmodells bearbeitet werden kann (und soll), ist somit, die richtigen Maßnahmen zu ergreifen, um das Vertrauen eines Nutzers zu gewinnen. Hierbei spielt die wahrgenommene Vertrauenswürdigkeit eine entscheidende Rolle. Denn Vertrauen basiert allgemein auf der Annahme, dass es möglich ist, sich auf etwas bestimmtes zu verlassen. Dies können Unternehmen ihren Nutzern aufzeigen, indem sie relevante Aspekte der Vertrauenswürdigkeit sowohl für die IT-Lösung als auch für das Unternehmen explizit darstellen.

So ist es möglich, eine Vertrauensgrundlage zu schaffen – wobei sich deren Güte in der Übereinstimmung der wahrgenommenen Vertrauenswürdigkeit mit der echten Vertrauenswürdigkeit widerspiegelt. Mit anderen Worten, Unternehmen sind schlecht beraten, wenn sie den Nutzern etwas vormachen würden.

2 Konkrete Umsetzung

Unternehmen müssen sich darstellen, um über eine hohe wahrgenommene Vertrauenswürdigkeit dem Nutzer die Möglichkeit zu geben, ihnen vertrauen zu können. Dazu ist es notwendig die Vertrauenswürdigkeitsaspekte der IT-Lösungen und des Unternehmens zu formulieren – exakt so, dass der Nutzer sie versteht – und zu veröffentlichen. Flankierend dazu ist es wichtig zusätzlich zu beachten, dass insbesondere bei innovativen IT-Lösungen – zur Schaffung und Steigerung einer grundsätzlichen Vertrauenswürdigkeit –– die Domäne einen hohen Einfluss hat.

Nachfolgend werden die Aspekte der wahrgenommenen Vertrauenswürdigkeit aller vorab definierten Dimensionen der Vertrauensnehmer detaillierter ausgeführt.

2.1 Vertrauenswürdigkeit der IT-Lösung

Aspekte, die bei IT-Lösungen für das Aufbauen von Vertrauen eine Rolle spielen, sind: Transparenz, Leistungsfähigkeit und Zweckprägnanz.

Durch die Darstellung aller Aspekte der wahrgenommenen Vertrauenswürdigkeit wird der Nutzer prinzipiell in die Lage versetzt, einen Einblick in die für ihn notwendigen Details der ange-

botenen IT-Lösung nehmen zu können und so Vertrauen in diese aufzubauen, beziehungsweise zu verstetigen.

2.1.1 Aspekt: Transparenz

Für den Nutzer ist es aufgrund der zunehmend intelligenteren Angriffe und komplexeren IT-Sicherheitsmechanismen immer wichtiger, dass insbesondere seine IT-Sicherheitsbedürfnisse auch angemessen durch die IT-Lösung befriedigt werden. Transparenz bedeutet alle relevanten Informationen zur Verfügung zu stellen, die für den Nutzer erforderlich sind, um im gegebenen Kontext eine valide Entscheidung über die Vertrauenswürdigkeit und IT-Sicherheit der IT-Lösung treffen zu können. Beispiele für die Transparenz der IT-Sicherheit einer IT-Lösung sind:

Beipackzettel IT-Sicherheit: Der bedarfsorientierte Beipackzettel macht für den Nutzer transparent, wie mithilfe von IT-Sicherheitsmechanismen in der IT-Lösung dafür gesorgt wird, die Wahrscheinlichkeit der verschiedenen Angriffe zu reduzieren. Ebenso wichtig ist zudem aufzuzeigen, welche Restrisiken bestehen, wie der Nutzer damit umgehen soll und wie das Unternehmen dabei unterstützen kann.

Darstellung von Zertifikaten: Durch die Zurverfügungstellung von Zertifikaten kann der Nutzer überprüfen, welche Aspekte von IT-Sicherheitsexperten einer Zertifizierungsstelle analysiert und bewertet worden sind.

2.1.2 Aspekt: Leistungsfähigkeit

Die Leistungsfähigkeit einer IT-Lösung ist das, was der Nutzer unmittelbar erfassen und auch kontrollieren kann. Daher ergeben sich daraus die messbaren Kriterien für dessen Beurteilung, inwieweit er sich bei der Erreichung des beabsichtigten Einsatzzweckes unterstützt fühlt und wie gut die IT-Lösung tatsächlich dafür geeignet ist. Dieser Aspekt wird in der Regel von den Unternehmen schon grundsätzlich gut ausgeführt, da er für die Vermarktung sehr relevant ist.

Beispiele für die Leistungsfähigkeit einer IT-Lösung mit besonderem Fokus auf IT-Sicherheit sind:

Bedienbarkeit: Sind IT-Sicherheitsmechanismen und -Management für den Nutzer einfach und intuitiv zu bedienen, um die angestrebten IT-Sicherheitsziele umzusetzen? Also zum Beispiel, ob das Versprechen eingehalten wird, dass sich die IT-Lösung in fünf Minuten problemlos und sicher einrichten lässt.

Leistungsfähigkeit der IT-Sicherheitsmechanismen: Hier sind alle Ergebnisse und Nebeneffekte der IT-Sicherheitsmechanismen darzustellen. Zum Beispiel ist bei einem Angriffserkennungssystem der genaue Zeitrahmen zu definieren – etwa von dem Entdecken bis zur Reaktion sowie der weiteren Handlungen, etwa dem Versenden des Alarms oder der automatischen Reaktion darauf. Hier könnte beschrieben werden, in welchem Zeitraum agiert wird, um Schäden zu verhindern oder zu minimieren und welche Voraussetzungen für eine optimale Nutzung zu schaffen sind. Insgesamt ist es empfehlenswert die Leistung der IT-Lösung zu beschreiben, beispielsweise ob sich durch Verschlüsselung der Daten die Leistungsfähigkeit verringert und was das für den Nutzer bedeutet. Wenn also bei der Verschlüsselung einer Festplatte circa 3 Prozent der CPU-Leistung dafür verwendet werden, sollte – auch wenn der Nutzer dies nicht bemerkt – ein entsprechender Hinweis dahingehend gemacht werden und dass diese Minderung irrelevant ist, weil sie keinen Einfluss auf die Leistungsfähigkeit hat.

2.1.3 Aspekt: Zweckprägnanz

Die Zweckprägnanz manifestiert sich im Verwendungszweck der IT-Lösung. Dies bedeutet, dass bei der Entwicklung von Funktionen die Intention der IT-Lösung zielgenau definiert ist. Bietet eine IT-Lösung neben der eigentlichen Anwendung weitere Funktionen an, die nur im Sinn des Unternehmens oder dritter Parteien sind, müssen diese klar dargestellt und beschrieben werden. Beispiele für die Zweckprägnanz einer IT-Lösung sind:

Offenlegen des Geschäftsmodells: Wird eine IT-Lösung kostenfrei angeboten, muss das dahinterliegende Geschäftsmodell offen kommuniziert werden, zum Beispiel, dass mithilfe des Geschäftsmodells „Bezahlen mit persönlichen Daten" sensitive Daten der Nutzer gesammelt und für individualisierte Werbung genutzt oder/und gewinnbringend an Dritte verkauft werden. Auf dieser Basis kann der Nutzer dann eine informierte Entscheidung für oder gegen die Verwendung der IT-Lösung treffen.

Einblick geben in neue Features: Zum Beispiel in das neue Erkennungssystem von Apple. Mit dem Client Side Scanning (CSS) ist es möglich, anlasslos die Daten auf einem iPhone im Hinblick auf Kinderpornografie zu durchsuchen. Obwohl gesellschaftlich betrachtet von hohem Wert, stellt dies jedoch für den Nutzer ein Risiko im Sinne seiner Privatsphäre dar – allein aus dem Grund, da der Abgleich auf dem Endgerät stattfindet. Aufgrund der Tatsache, dass es darüber zudem auch prinzipiell möglich ist, beliebig nach anderen Inhalten zu suchen, kann damit sogar für bestimmte Gruppen (in einigen Ländern) eine echte Gefährdung einhergehen. Da neue Features immer der grundlegenden Zweckprägnanz entsprechen sollten und CSS nichts mehr mit dem eigentlichen Zweck eines Smartphones zu tun hat, muss diese gravierende Abweichung vom eigentlichen Zweck für den Nutzer – im Sinne einer informierten Entscheidung – unmittelbar und klar transparent gemacht werden.

2.2 Vertrauenswürdigkeit der Unternehmen

Aspekte, die bei einem Unternehmen für das Aufbauen von Vertrauen eine Rolle spielen, sind: Zutrauen, Zuverlässigkeit, Integrität und Sicherheit. Daher ist die Darstellung der Aspekte, der wahrgenommenen Vertrauenswürdigkeit wichtig, um aufgrund kognitiver Faktoren ein institutionelles Vertrauen der Nutzer zum Unternehmen grundsätzlich möglich zu machen.

2.2.1 Aspekt: Zutrauen

Zutrauen ist ein relevantes Kriterium für die Vertrauenswürdigkeit. Generell kann dieses im Hinblick auf die Funktionalität dadurch erzeugt werden, dass Unternehmen sowohl über die Fähigkeit als auch über die entsprechenden Mittel verfügen, um verlässliche IT-Lösungen bereitzustellen.

Wichtig für Unternehmen ist hierbei eine Strategie zu entwerfen, um dieses Kriterium sowohl zu erfüllen als auch in einer *Zutrauens-Leitlinie* zu dokumentieren. Hierzu muss unter anderem ein Konzept erstellt werden bezüglich der Parameter, die zwingend erfüllt sein müssen. Beispiele für das Zutrauen in ein Unternehmen sind:

Mitarbeiter: Aufzeigen der Qualifikationen der Mitarbeiter: Haben die Mitarbeiter einen Studiengang mit Ausrichtung IT-Sicherheit absolviert oder eine entsprechende fachliche Weiterbildung, welche Erfahrung können sie in diesem Bereich vorweisen oder über welche Zusatzqualifikation wie T.I.S.P. oder CISSP verfügen sie [4].

Qualitätsstandards: Darstellung der umgesetzten Qualitätsstandards von Entwicklung und Produktion, um eine verlässliche IT-Lösung bereitstellen zu können.

Betriebsmittel: Beschreibung zur Qualität und Quantität von IT-Systemen und deren Software zu Entwicklung/Betrieb der IT-Lösung.

Ausgaben für IT-Sicherheit: Offenlegung des Anteils der Investition in IT-Sicherheit in Relation zum Gesamtbudget für Informationstechnologien. Der Prozentsatz für IT-Sicherheit vom IT-Budget ist ein guter Indikator zur Einschätzung der IT-Sicherheit eines Unternehmens. Die aktuellen Zahlen von Statista ergeben hierfür einen Wert von 6 Prozent – der BSI-Präsident fordert für die Zukunft sogar einen Anteil von 15 Prozent. Anhand des Verhältnisses zeigt sich, ob ein Unternehmen besonders engagiert ist, seine IT-Infrastruktur und folglich auch seine IT-Lösungen zu schützen.

2.2.2 Aspekt: Zuverlässigkeit

IT-Lösungen führen nur Prozesse aus, die seitens der Nutzer gewünscht sind, beziehungsweise die er erwartet und dies sehr verlässlich. Das impliziert, dass Unternehmen grundsätzlich wohlwollend sind. Das bedeutet, dass sie im besten Sinne ihrer Nutzer handeln, sich also an deren Bedürfnissen orientieren, statt ihre eigenen Interessen besonders in den Mittelpunkt zu stellen. Wie müssen Unternehmen hier zukünftig agieren – was sollte in deren *Zuverlässigkeitsmanagement* einfließen und beschrieben werden? Nachfolgend einige Faktoren, die dabei von Relevanz sind:

Kooperativ handeln, um die wahren Bedürfnisse der Nutzer besser identifizieren zu können und bei Problemstellungen den Nutzer individuell zu unterstützen. Die Übernahme einer Gesamtverantwortung im Schadensfall oder Rückrufaktionen bei identifizierten Problemen sind Beispiele für ein kooperatives Handeln. Das bedeutet, Hersteller müssen – wenn möglich auf direktem Weg – ihre Nutzer bei Erkennen von gravierenden Schwachstellen umgehend informieren. Wird diese Information zuerst von anderen Quellen zum Beispiel über Soziale Medien oder die Fachpresse veröffentlicht, mindert dies die Vertrauenswürdigkeit der Hersteller.

Verantwortlich handeln, um durch den richtigen Einsatz von Funktionen – die zum Vorteil der Nutzer sind – für diese ebenso einen Mehrwert zu schaffen wie durch die Abgabe einer Garantie für die Funktionen beziehungsweise die Haftung bei Fehlverhalten. Aber auch die Überprüfung und kontinuierliche Kontrolle der Lieferketten unter den verschiedensten Aspekten sowie das Ergreifen aller IT-Sicherheitsmaßnahmen, um Betrugsprävention durchzuführen, gehören dazu. Das bedeutet zum Beispiel, Hersteller müssen alles tun, um Supply-Chain-Angriffe zu verhindern, etwa durch Überprüfung der Lieferanten und/oder auch der Kontrolle der Inhalte sowie der Software des jeweiligen Lieferanten. Speziell hier, aber ebenso in vergleichbaren Konstellationen kann Vertrauenswürdigkeit nur durch Übernahme einer Gesamtverantwortung aufgebaut werden.

2.2.3 Aspekt: Integrität

Es werden alle Faktoren der Vertrauenswürdigkeit und hier insbesondere die ethischen Dimensionen beachtet. Wichtig ist, dass ein Hersteller als Vertrauensnehmer prinzipiell in der Lage ist, alle Versprechen, die er abgegeben hat, überhaupt einhalten zu können und auch tatsächlich einhält sowie generell dazu bereit ist, sowohl Normen als auch Werte der Gesellschaft zu berücksichtigen. Von daher gilt es für Unternehmen – als einer der wichtigsten Schritte – hier eine *Integritäts-Maxime* zu entwerfen, mit klaren Bekenntnissen zu ihrem Geschäftsmodell und im Weiteren den unternehmensspezifischen Aspekten. Dazu gehört definitiv, die ethischen Anforderungen klar zu adressieren. Einige ethische Anforderungen werden nachfolgend exemplarisch vorgestellt:

Rechenschaftspflicht: Darstellung der ethischen Grundsätze, wie etwa Fairness, Gerechtigkeit, Gleichheit, Solidarität, zu deren Einhaltung sich ein Unternehmen im Sinne ihrer Kunden, Mitarbeiter, Zulieferer sowie der Gesellschaft verpflichten will. In diesem Kontext sollte für Unternehmen die Überprüfung eingesetzter Technologien inklusive entsprechender Offenlegung von eventuell negativen Auswirkungen auf die Gesellschaft obligatorisch sein.

Schutz der Privatsphäre: Diese Forderung beinhaltet zum einen den sicheren und vertrauenswürdigen Umgang mit Kundendaten – etwa das sofortige Löschen, wenn diese nicht mehr benötigt werden. Aber auch das Versprechen, diese persönlichen Daten der Nutzer durch Verschlüsselung zu schützen sowie die privaten Daten der Nutzer nicht für weitere wirtschaftliche Zwecke zu verwerten.

Keine eingeschränkte IT-Sicherheit: Die Hersteller und Anbieter müssen sich öffentlich dazu verpflichten, dass die genutzten IT-Sicherheitsmechanismen keine geschwächten Verschlüsselungen, Zufallszahlengeneratoren oder weitere Kryptografie-Verfahren verwenden sowie sichere Schlüssel nutzen. Ebenso ist sicherzustellen, dass keine Backdoors in den IT-Sicherheitslösungen eingebaut sind. In der Darstellung zum Nutzer hin können Hersteller dies zum Beispiel mithilfe des Vertrauenszeichens „IT Security made in Germany" deklarieren [6]. Diese Anforderung kann ebenso über eine Zertifizierung umgesetzt werden.

2.2.4 Aspekt: Sicherheit des Unternehmens

Das Anerkennen der Bedeutung von IT-Sicherheit sowie deren Umsetzung gewährleistet, dass IT-Lösungen im Cyber-Raum risikoarm zu nutzen sind. Dieser Anspruch ist jedoch (noch) eine Fiktion, da unter anderem Ransomware, DDoS- oder Phishing-Angriffe heute an der Tagesordnung sind. Alltäglich genutzte Dienste, wie etwa E-Mail-Programme, Online-Banking oder Online-Shops, bieten bei Weitem nicht den Level an IT-Sicherheit und Vertrauenswürdigkeit, der notwendig ist, um damit kritische Geschäftsprozesse sicher abwickeln zu können.

Von daher benötigen Unternehmen eine adäquate und ausformulierte *IT-Sicherheits-Richtlinie*, um im Sinne der Kunden den bestmöglichen Schutz gewährleisten zu können. Die kontinuierliche Umsetzung gemäß aktueller IT-Sicherheitsanforderungen ist notwendig, da Nutzer im Allgemeinen nicht dazu in der Lage sind, sich allein angemessen zu schützen. Unter anderem haben die folgenden Faktoren im Kontext der Sicherheit eine hohe Relevanz:

Darstellung der verwendeten IT-Sicherheitsmaßnahmen: Hier sollten die Hersteller aufzeigen, was sie tun, um sowohl die jeweilige IT-Lösung als auch ihr eigenes Unternehmen vor IT-Sicherheitsrisiken zu schützen. Anders als beim „Beipackzettel IT-Sicherheit" können Beschreibungen und Hintergrundinformationen hier detaillierter ausfallen.

Zertifizierung der IT-Lösung und des Unternehmens: Die Zertifizierung von Qualität und Vertrauenswürdigkeit der IT-Lösungen und Unternehmen müssen durch qualifizierte unabhängige Organisationen erfolgen, die nach definierten Kriterien überprüfen und testieren. Die Zertifizierungen unter verschiedenen Perspektiven sind eine wichtige Maßnahme zur Vertrauensbildung.

Regelmäßige Überprüfung der IT-Lösungen und des Unternehmens: Das Ziel hierbei ist, Schwachstellen aktiv und kontinuierlich mithilfe von Penetrationstests, Red-Teams und Bug-Bounty-Programme zu identifizieren, damit Sicherheitslücken so schnell als möglich durch Updates eliminiert – und somit nicht für Angriffe verwendet – werden können. Dies gilt sowohl für die angebotenen IT-Lösungen als auch für die Unternehmen und deren Zulieferer. Dadurch lässt sich ein – für den Nutzer jederzeit nachweisbares – hohes IT-Sicherheitsniveau im laufenden Entwicklungsprozess und der Nutzung der IT-Lösung erreichen.

IT-Sicherheitsstrategie: Eine IT-Sicherheitsstrategie ist ein längerfristig ausgerichtetes, planvolles Vorgehen mit dem Ziel, die vorhandenen Risiken eines Angriffes auf digitale Werte des Unternehmens so gering wie möglich zu halten. Da deren Darstellung die Vertrauenswürdigkeit eines Unternehmens erhöht, sollte die prinzipielle Strategie auch nach außen kommuniziert werden. In diesem Rahmen ist es möglich darzulegen, wie durch Vermeiden und Entgegenwirken von IT-Angriffen die vorhandenen Risiken reduziert sowie mit Erkennen von und Reaktion auf IT-Angriffe die verbleibenden Risiken behandelt werden.

2.3 Kosten-/Nutzen-Diskussion

Die digitale Transformation ist gewünscht und notwendig, um international im Wettbewerb zu bestehen. Aber das Vertrauen der Nutzer ist – aus verschiedenen (und teilweise nachvollziehbaren) Gründen – noch nicht in dem dafür notwendigen Maße stabil vorhanden. Daraus lässt sich schlussfolgern, dass sowohl Unternehmen als auch Institutionen und nicht zuletzt staatliche Organisationen dazu aufgefordert sind, hier etwas zu tun. Denn allein aufgrund der steigenden Komplexität haben sie eine Bringschuld, wenn es um die Vertrauensbildung geht. Mit anderen Worten: es besteht die Notwendigkeit alles zu tun, um Misstrauen, das möglicherweise beim Nutzer entstanden ist – oder bereits vorhanden war – zu beseitigen. Oder aus der Perspektive des Nutzers gedacht: es gilt die Basis dafür zu schaffen, dass dieser den Unternehmen, Institutionen sowie staatlichen Organisationen respektive entsprechender IT-Lösung vertrauen und somit auch anwenden kann.

Aber hier ist noch ein weiterer Punkt relevant: Nicht zuletzt können sich deutsche/europäische Unternehmen damit weltweit gegen internationale Unternehmen nachhaltig profilieren und positionieren.

3 Vertrauenswürdigkeit der Domänen

Kollaborativ mit anderen Herstellern und Stakeholdern (wie Staat, Politik, Nutzer, Wissenschaft oder Anwendungsunternehmen) gesellschaftliche Werte kreieren oder Wertevorstellungen umsetzen, um die gesamte Branche respektive Domäne gemeinsam vertrauenswürdig zu entwickeln. Durch die Schaffung einer Vertrauenswürdigkeit in einer Domäne kann eine erfolgreiche Einführung von neuen Geschäftsmodellen oder IT-Lösungen begünstigt werden. Nachfolgend einige Beispiele in Bezug auf die wahrgenommene Vertrauenswürdigkeit von Domänen:

Schaffung von Rahmenbedienungen: Der Staat schafft die Randbedingungen, indem Domänen-spezifisch vorgegeben wird, wie Unternehmen den Einsatz von IT-Lösungen zu gestalten haben. Beispielsweise mit dem IT-Sicherheitsgesetz, in dem die Rahmenbedingungen für die IT-Sicherheit von Kritischen Infrastrukturen definiert sind beziehungsweise mit Verordnungen wie der Datenschutz-Grundverordnung (DSGVO) oder der eIDAS-Verordnung. Insgesamt schaffen die entsprechenden Bestimmungen Vertrauenswürdigkeit, weil sie die gesetzlichen Möglichkeiten und Grenzen klar aufzeigen.

Motivierung von Ökosystemen: Ein Beispiel in diesem Bereich stellt Self-Sovereign Identity (SSI) dar. Mit SSI soll die Basis eines europäischen Ökosystems zur Ausgabe und Verifizierung digitaler Identitäten sowie Nachweise aufgebaut werden. Darüber lassen sich relevante Ziele verwirklichen: unter anderem der Schutz der Privatsphäre, da auf diese Weise Nutzer zukünftig selbstbestimmt entscheiden könnten, welcher Anwendung sie wann ihre digitalen Identitätsdaten zur Verfügung stellen. Letztendlich führt der souveräne Umgang mit den eigenen digitalen Identitätsdaten auch dazu, dass die Abhängigkeit von einzelnen monopolierten Anbietern minimiert wird, womit das Ziel einer unabhängigen schnelleren Digitalisierung gefördert wird.

Ein weiteres Beispiel stellt das Industriekonsortium GAIA-X dar. Denn nicht nur für neue IT-Technologien kann es relevant sein, eine Vertrauenswürdigkeit zu etablieren – auch bei bereits eingeführten ist es teilweise notwendig Werte-orientierte Standards neu zu definieren und damit zu erhöhen. Aufgrund der Intention von GAIA-X soll den Nutzern garantiert werden, dass die eingesetzten IT-Lösungen europäisches Recht einhalten und Datenportabilität, höchste Kriterien der IT-Sicherheit sowie eine klare Transparenz rund um die Datenverwendung gewährleisten. Darüber ist es dann möglich, eine verstärkte Speicherung von Daten in Europa zu forcieren.

Etablierung gemeinsamer Vertrauenssiegel: Vertrauenssiegel helfen den Unternehmen, ihre Vertrauenswürdigkeit darzustellen. Beispiel für ein Vertrauenssiegel ist „IT Security – Made in Germany". Dadurch, dass der Bundesverband IT-Sicherheit – TeleTrusT dieses Vertrauenssiegel definiert hat, sind die IT-Sicherheitsunternehmen in der Lage, dieses auch zu deklarieren und darüber Vertrauenswürdigkeit für ihre Nutzer aufzubauen.

Schutzmechanismen des Staates: Ein Negativ-Beispiel ist die Anwendung des Bundestrojaners. Dessen Einsatz schwächt die IT-Sicherheit von Bürgern und Unternehmen, weil das Wissen über bestimmte Sicherheitslücken nicht an die Hersteller weitergegeben, sondern für den Bundestrojaner genutzt wird [6].

4 Zusammenfassung und Ausblick

Vertrauenswürdigkeit wird zunehmend zum Erfolgsfaktor für Unternehmen, denn nur so lässt sich zukünftig eine ausreichende Akzeptanz bei den Nutzern für die jeweils angebotene IT-Lösung erreichen.

Um dort hinzukommen, werden Möglichkeiten benötigt, die den Unternehmen helfen, eine Vertrauensgrundlage zu ihren Kunden zu schaffen. Die grundsätzlichen Aspekte der verschiedenen Dimensionen sind klar. Bei der Realisierung der Darstellung müssen jetzt entsprechend Umsetzungen ausprobiert werden, um dadurch eine gute Vertrauensgrundlage aufbauen zu können.

Dazu ist es notwendig, dass Unternehmen sich eingehend damit auseinanderzusetzen, wie sie ihre Vertrauenswürdigkeit durch Umsetzung der relevanten Aspekte erhöhen und ebenso wie sie diese explizit nachweisen können. Dies lässt sich auf Basis des Vertrauenswürdigkeitsmodells realisieren, da darüber die Möglichkeit entsteht, alle Aspekte der Vertrauenswürdigkeit einer IT-Lösung, eines Unternehmens sowie der Domäne darzustellen.

Eine stringente Umsetzung des Vertrauenswürdigkeitsmodells ist der Aufbau einer unabhängigen Vertrauenswürdigkeitsplattform basierend auf der Darstellung der wahrgenommenen Vertrauenswürdigkeit der IT-Lösungen, Unternehmen und Domänen. Perspektivisch: Durch diese unabhängige Vertrauenswürdigkeitsplattform, erweitert mit einem hochwertigen Reputationssystem sowie ergänzt mit einem anerkannten Vertrauenswürdigkeitsindex, wird sowohl ein hoher Nutzen für die Verbraucher generiert als auch – letztendlich – für die Unternehmen.

Literatur

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

[2] N. Pohlmann: „Cyber-Sicherheit – Das Lehrbuch für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung“ 2. Auflage, Springer Vieweg Verlag, Wiesbaden 2022

[3] Nils Backhaus: „Nutzervertrauen und -erleben im Kontext technischer Systeme: Empirische Untersuchungen am Beispiel von Webseiten und Cloudspeicherdiensten“, Dissertation, Technischen Universität Berlin, 2016

[4] N. Pohlmann: „Ex schola pro vita – Studien- und Fortbildungsangebote zur Cybersicherheit“, KES – Die Zeitschrift für Informations-Sicherheit, DATAKONTEXT-Fachverlag, 3/2021

[5] TeleTrusT: „IT Security made in Germany”, https://www.teletrust.de/it-security-made-in-germany/

[6] Tagesspiegel-Background: „Über Zielkonflikte in der Cybersicherheitspolitik wieder mehr diskutieren“, https://background.tagesspiegel.de/digitalisierung/cybersicherheitspolitik-lauter-zielkonflikte