Kriterien für das Vertrauen von Anwenderunternehmen in Hersteller und deren IT-Sicherheitslösungen

OHNE VERTRAUEN GEHT ES NICHT

Die Beschaffung von IT-Sicherheitslösungen ist für Unternehmen oft eine Herausforderung. So führt die Komplexität der Systeme dazu, dass die für eine Kaufentscheidung erforderlichen Kompetenzen und Informationen nicht immer vorhanden sind. Grundvoraussetzung für eine erfolgreiche Geschäftsbeziehung ist deswegen ein valides Vertrauensverhältnis zwischen Anwender- und Herstellerunternehmen. Das setzt jedoch voraus, dass die Herstellerunternehmen vertrauenswürdig auftreten und im Interesse ihrer Kunden handeln. Eine Studie der Westfälischen Hochschule Gelsenkirchen hat untersucht, welche Vertrauenskriterien Kunden bei Herstellern und deren Produkten wichtig sind. So ist zum Beispiel ein Hersteller bei den Kunden unten durch, wenn er zu viele Buzzwords nutzt.

Während es in der Vergangenheit Anwendern genügte, dass Herstellerunternehmen eine gewisse Größe hatten und gut etabliert waren, erfordert die zunehmende Digitalisierung und die daraus resultierende Komplexität, dass künftig der Vertrauenswürdigkeit ein weitaus höherer Stellenwert eingeräumt werden muss. Doch worauf gründet sich das Vertrauen der Kunden und wie ist es für Herstellerunternehmen möglich, ihre Vertrauenswürdigkeit zu demonstrieren[1]?

Vertrauen *gilt als hoffnungsvoller Vorschuss hinsichtlich bestimmter Erwartungen, den allgemein jemand bereit ist, zu geben.*

Somit kann Vertrauen auch als Bereitschaft des Anwenders/Kunden (als Vertrauensgeber) definiert werden, sich durch die Interaktion mit einem Herstellerunternehmen und seiner IT-Lösung (als Vertrauensnehmer) einem bestimmten Risiko auszusetzen, da er nicht weiß, ob seine Annahme zutreffend und gerechtfertigt ist.

Vertrauenswürdigkeit *kann sich grundsätzlich sowohl auf Herstellerunternehmen als auch auf IT-Sicherheitslösungen beziehen. Vertrauenswürdigkeit basiert auf der Annahme, dass es möglich ist, sich auf etwas Bestimmtes verlassen zu können.*

Eine verbreitete These ist, dass sich Vertrauenswürdigkeit nicht nachweisen lässt. Um das zu widerlegen und die relevanten Kriterien für ein valides Vertrauensverhältnis identifizieren zu können, haben Mitarbeiter des if(is) in einer selektiven Befragung Anwenderunternehmen um ihre Einschätzung hierzu gebeten.

Insgesamt nahmen 35 IT-Verantwortliche teil, darunter befanden sich sowohl Start-ups mit weniger als zehn Mitarbeitern als auch Technologiekonzerne mit mehreren Milliarden Euro Umsatz pro Jahr. Ein Auswahlkriterium bestand darin, ein breites Spektrum an Anwenderunternehmen abzudecken – unter anderem aus den Branchen Telekommunikation, Energie, Gesundheit und Bildung – um einen möglichst umfassenden Eindruck zu erhalten. Methodisch wurden zunächst offene Fragen zur Vertrauenswürdigkeit gestellt, um einen unvoreingenommenen Einblick zu erhalten. Anschließend bewerteten die Befragten anhand geschlossener Fragen ihre substanziellen Kriterien zu verschiedenen Kategorien.

Basis für die Befragung bildet ein wissenschaftliches Modell (vgl. Abbildung 1), in dem die relevanten Aspekte und Schnittstellen zwischen Anwendern und Herstellern mit dem Ziel modelliert wurden, ein Höchstmaß an Vertrauen zu schaffen [2]. Die definierten Aspekte wurden den Anwenderunternehmen vorgelegt, um deren Signifikanz in Bezug auf Vertrauenswürdigkeit zu ermitteln.

Trotz des nicht repräsentativen Stichprobenumfangs konnten interessante Erkenntnisse herauskristallisiert werden:

Insgesamt gewährt die Befragung einen tieferen Einblick in die Relevanz einzelner Vertrauenswürdigkeits-Aspekte für die Anwenderunternehmen sowie eine gute Innenansicht bezüglich deren spezifischer Ausgestaltung. Grundsätzlich hat sich eines gezeigt: Anwenderunternehmen haben ein großes Interesse daran, dass ihnen sowohl für die Herstellerunternehmen als auch für deren Produkte definierte Kriterien – die sie im Sinne der Vertrauenswürdigkeit als wichtig erachten – mittels eines objektivierbaren Schemas präsentiert werden.

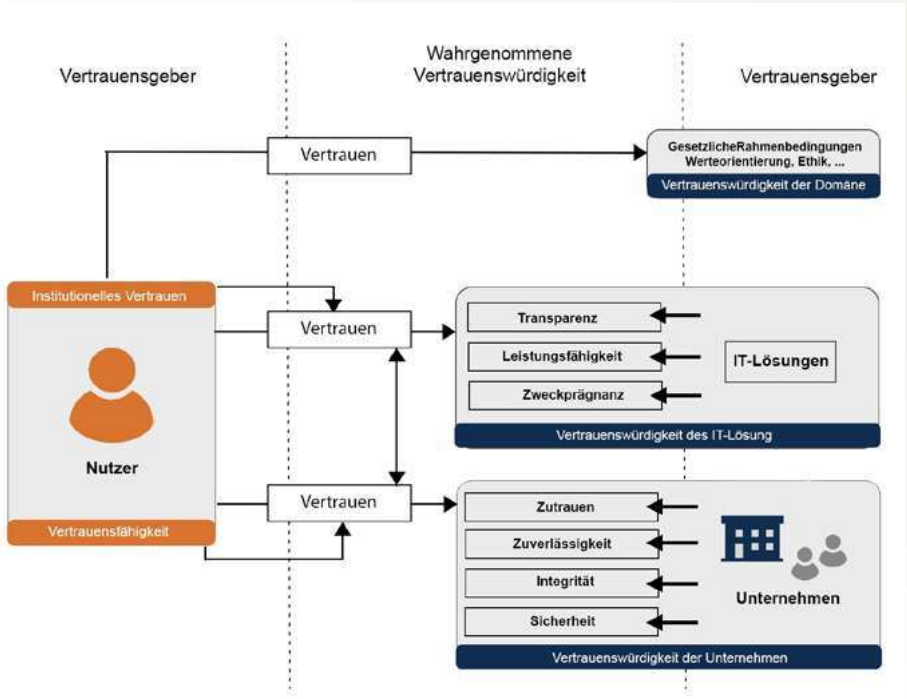

Abbildung 1: Vertrauenswürdigkeits-Modell

Einer IT-Sicherheitslösung kann man bezüglich verbriefter Attribute und/oder Funktionalität vertrauen, wenn Herstellerunternehmen einen Nachweis für die Erfüllung der zugesicherten Eigenschaften vorlegen. Die Vertrauenswürdigkeit eines Herstellerunternehmens entsteht dadurch, dass diesem zugetraut wird, geeignete Maßnahmen durchzuführen sowie (Management-) Strukturen zu etablieren, um die Erwartungen ihrer Kunden/Anwender zu erfüllen.

DAS BEDÜRFNIS AN CYBER-SICHERHEIT IST HOCH

Besonders augenfällig ist das ausgeprägte Cyber-Sicherheitsbedürfnis der Anwenderunternehmen. Zertifizierungen der Herstellerunternehmen und IT-Sicherheitslösungen, ganzheitliche IT-Sicherheitskonzepte und unabhängige Prüfberichte zählen zu den fünf am häufigsten genannten Kriterien. So ist eine schnelle Versorgung mit Informationen rund um die elementaren IT-Sicherheitsthemen für die meisten Anwenderunternehmen zwingend erforderlich. Dabei wünschen sich die Anwender vor allem eine Aufklärung über neue Bedrohungen und Restrisiken. Durch den offenen Umgang mit diesen Informationen handeln die Hersteller verantwortungsvoll und beweisen Mut, da diese Offenheit auch eine potenzielle Angriffsfläche bieten könnte.

Im Folgenden werden die wichtigsten Ergebnisse der Anwenderbefragung dargestellt.

DIE VERTRAUENSWÜRDIGKEITS-ASPEKTE DES UNTERNEHMENS

Die Vertrauenswürdigkeits-Aspekte, die bei einem Unternehmen für das Aufbauen von Vertrauenswürdigkeit eine substanzielle Rolle spielen, sind: Zutrauen, Zuverlässigkeit, Integrität und Sicherheit. Abbildung 2 zeigt die wichtigsten Vertrauenswürdigkeits-Aspekte für die Hersteller insgesamt und die Bewertungen der Anwenderunternehmen.

Zutrauen

Generell kann Zutrauen zu einem Hersteller im Hinblick auf die Funktionalität der IT-Sicherheitslösung dadurch erzeugt werden, dass er sowohl über die Fähigkeit als auch die entsprechenden Mittel verfügt, um qualitativ hochwertige und verlässliche IT-Sicherheitslösungen bereitzustellen. Dazu zählen qualifizierte Mitarbeiter, Qualitätsstandards in der Entwicklung, die verfügbaren Betriebsmittel und Ausgaben für die IT-Sicherheit.

Qualifizierte Mitarbeiter sind aus Sicht der Befragten das wichtigste Kriterium im Hinblick auf den Vertrauenswürdigkeits-Aspekt Zutrauen. Sie stehen für die Kompetenzen, die bei der Entwicklung, aber auch für den Betrieb der IT-Sicherheitslösung zur Verfügung stehen. Zur notwendigen Qualifizierungsoffensive gehören unter anderem regelmäßige Trainings und Schulungen, um möglichst schnell auf Veränderungen reagieren zu können. Zwischen der Beschäftigungsdauer der Befragten und ihrer Einschätzung der Relevanz von qualifizierten Mitarbeitern ist eine deutliche Korrelation zu erkennen – je länger die IT-Verantwortlichen schon in der entsprechenden Position sind, desto mehr Bedeutung maßen sie diesem Kriterium bei. Auch die Höhe der Qualitätsstandards in der Entwicklung ist ein substanzieller Indikator

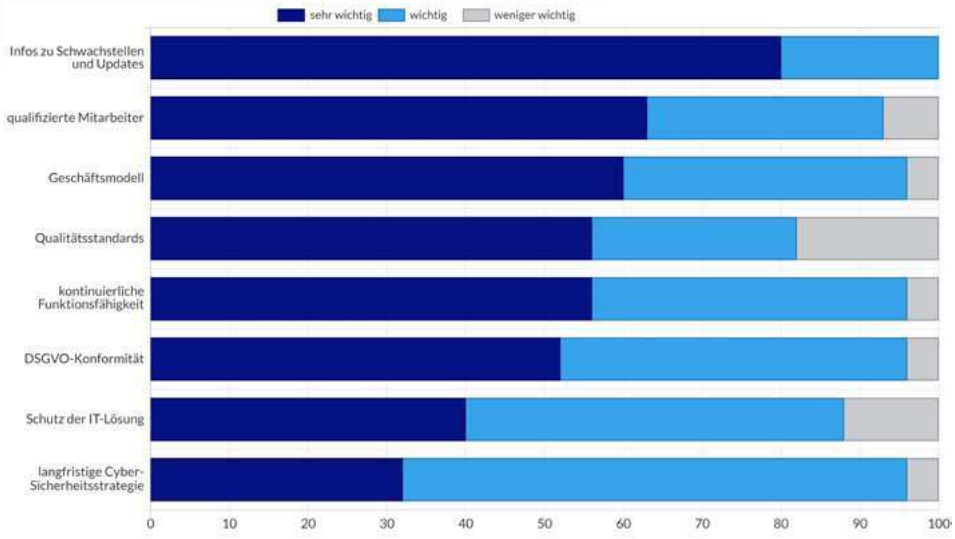

Abbildung 2: Wichtige Vertrauenswürdigkeits-Aspekte der Hersteller

für eine verlässliche IT-Sicherheitslösung. Kundenreferenzen und Case-Studies stellen Praxisbezug her und erhöhen so zusätzlich das Zutrauen. Die Markt-Etablierung und Bekanntheit des Herstellers spielen eine eher untergeordnete Rolle und werden meist nur dann betrachtet, wenn keine anderen verlässlichen Kriterien zur Verfügung stehen.

Unseriöse Angebote und aggressive Marktstrategien wirken sich negativ auf das Zutrauen aus ebenso wie die häufige Verwendung von Buzzwords. Anwender bevorzugen Hersteller, die sich transparent und seriös präsentieren.

Zuverlässigkeit

Die Zuverlässigkeit eines Herstellers zeichnet sich dadurch aus, dass deren IT-Sicherheitslösungen nur Prozesse ausführen, die seitens des Anwenders gewünscht sind. Das impliziert, dass Hersteller grundsätzlich wohlwollend sind und im besten Sinne ihrer Anwender handeln, anstatt ihre eigenen Bedürfnisse in den Mittelpunkt zu

WELCHE BEDEUTUNG HABEN ZERTIFIZIERUNGEN?

Während Zertifizierungen bei den offenen Fragen mit am häufigsten genannt werden, wird ihnen im direkten Vergleich zu anderen Kriterien eine deutlich geringere Relevanz beigemessen. Der Ursprung dieses vermeintlichen Widerspruchs könnte daran liegen, dass Anwenderunternehmen meist keine anderen aussagekräftigen Bewertungsgrundlagen zur Verfügung stehen. So werden transparente Informationen über eine langfristige IT-Sicherheitsstrategie [3] oder die verwendeten Cyber-Sicherheitsmechanismen als deutlich relevanter für die Bewertung der Vertrauenswürdigkeit angegeben. Sicherlich sind Zertifikate in besonders kritischen Anwendungsfällen absolut notwendig, doch letztendlich nicht maßgeblich an der Vertrauensbildung zwischen Anwender- und Herstellerunternehmen beteiligt.

stellen. Dabei sind vor allem zwei Faktoren von Relevanz: Erstens kooperatives Handeln, um die wahren Bedürfnisse der Anwender besser identifizieren zu können und bei Problemstellungen den Anwender individuell zu unterstützen. Zweitens verantwortliches Handeln, um durch den richtigen Einsatz von Funktionen – die zum Vorteil der Anwender sind – für diese einen Mehrwert zu schaffen.

Das zeitnahe Kommunizieren von Informationen über gravierende Schwachstellen und die schnellstmögliche Bereitstellung von Sicherheitspatches sind, laut der Befragten, die wichtigsten Kriterien für die Vertrauenswürdigkeit des Herstellers. Über 80 Prozent der Anwender bewerteten dies als sehr wichtig. Mit dieser offenen Form der Kommunikation beweisen die Hersteller Verantwortungsbewusstsein im Sinne ihrer Anwender. Ebenfalls ist es aus Sicht der Anwender elementar, dass Hersteller sie über neu aufgetretene Angriffsmöglichkeiten in Kenntnis setzen. Insgesamt hat für Anwender das Informationsmanagement eine hohe Bedeutung – sie erwarten eine unmittelbare Aufklärung über neuartige Angriffsvektoren und einen strategischen Überblick über den Produktlebenszyklus.

Zudem ist ein ausgewogenes Verhältnis zwischen den Interessen der Anwender auf der einen und des Herstellers auf der anderen Seite entscheidend. Durch eine partnerschaftliche Kooperation auf Augenhöhe ergibt sich eine Win-Win-Situation, also beide Parteien partizipieren gleichermaßen.

Ein zu hoher Fokus auf Shareholder Value beziehungsweise Eigeninteressen sowie aggressive Marktstrategien sprechen aus Sicht der Anwender gegen die Zuverlässigkeit eines Herstellers und sorgen für einen Vertrauensverlust.

Integrität

Unter dem Aspekt Integrität werden insbesondere ethische Dimensionen betrachtet. Dabei ist es wichtig, dass ein Hersteller prinzipiell in der Lage ist, alle Versprechen, die er gegeben hat, auch einhalten zu können. Das betrifft sowohl den Umgang mit Kundendaten als auch die Berücksichtigung von Normen und Werten der Gesellschaft.

Die Integrität eines Herstellers ist aus Sicht der Anwender eng mit seiner Transparenz verknüpft – hier wird in erster Linie die Offenlegung des Geschäftsmodells als sehr wichtig erachtet. Hiervon betroffen sind primär datengetriebene Geschäftsmodelle, die die Auswertung von Nutzerinformationen miteinschließen. Des Weiteren spielt sowohl die Einhaltung der ethischen Grundsätze als auch der Datenschutzrichtlinien eine bedeutende Rolle für die Anwender. Eine gemeinsame rechtliche Basis ist für die Anwender eine Grundvoraussetzung, besonders die Einhaltung der Datenschutzgrundverordnung.

Informationen über die Einschränkung der IT-Sicherheitsfunktionen – etwa schwache Zu-

fallszahlengeneratoren, Verschlüsselungen oder weitere Kryptografie-Verfahren sowie eingebaute Backdoors – sind extrem relevant und sollten den Anwendern definitiv vorliegen, damit sie eine informierte Entscheidung bezüglich der Nutzung fällen können. Aufgrund der Nichtbeachtung von Datenschutz und das Geheimhalten von IT-Sicherheitsvorfällen klassifizieren Anwender einen Hersteller als nicht vertrauenswürdig ein.

IT-Sicherheit

Der Vertrauenswürdigkeits-Aspekt IT-Sicherheit beinhaltet alle Maßnahmen, die ein Hersteller ergreifen muss, um sowohl das Unternehmen als auch die IT-Sicherheitslösung vor potenziellen Angreifern zu schützen. Dies umfasst unter anderem eine adäquate IT-Sicherheitsrichtlinie, um den bestmöglichen Schutz gewährleisten zu können – dabei sollten auch regelmäßige Überprüfungen der IT-Sicherheitslösung und des Herstellerunternehmens zur Reduzierung möglicher Angriffsvektoren berücksichtigt werden. Die generelle Erwartungshaltung der Anwender ist, dass IT-Sicherheit nicht nur auf die IT-Sicherheitslösung angewandt, sondern als fester Bestandteil der Unternehmenskultur des Herstellers etabliert wird. Zudem sollten sich die Hersteller bei der Umsetzung an europäischen Sicherheitsstandards orientieren.

Speziell im Kontext der Unternehmenssicherheit erachten die Anwender eine langfristige IT-Sicherheitsstrategie als substanziell. Sie ist zwingend notwendig, um die kontinuierliche Leistungsfähigkeit und den Schutz der IT-Sicherheitslösung gewährleisten zu können – hier insbesondere durch das Schwachstellen- und Incident-Management. Das insgesamt große Cyber-Sicherheitsbedürfnis spiegelt sich darin wider, dass sie von einem Herstellerunternehmen ganzheitliche IT-Sicherheitskonzepte erwarten sowie Zertifizierungen und unabhängige Prüfberichte. Aber auch das aktive und regelmäßige Überprüfen auf Schwachstellen mithilfe von Penetrationstests, Red-Teams und Bug-Bounty-Programmen – auch innerhalb der IT-Sicherheitslösung – betrachten sie als wichtig.

VERTRAUENSWÜRDIGKEITS-ASPEKTE DER IT-SICHERHEITSLÖSUNG

Die Vertrauenswürdigkeits-Aspekte der IT-Sicherheitslösung sind Transparenz, Leistungsfähigkeit und Zweckprägnanz. In Abbildung 3 werden die wichtigsten Vertrauenswürdigkeits-Aspekte für die IT-Sicherheitslösungen und die Bewertungen der Anwenderunternehmen dargestellt.

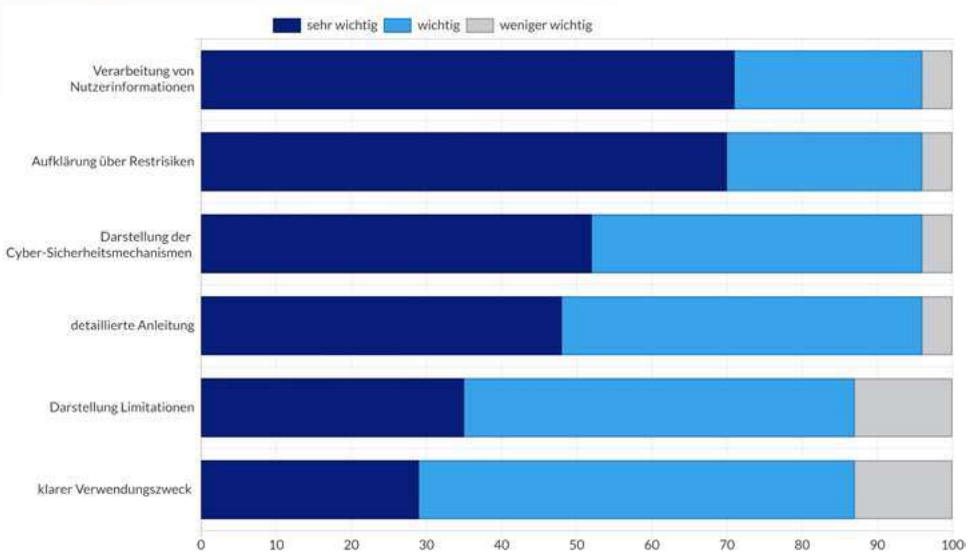

Abbildung 3: Wichtige Vertrauenswürdigkeits-Aspekte von IT-Sicherheitslösungen

Transparenz

Transparenz bedeutet in diesem Kontext, dass alle relevanten Informationen zur Gewährleistung der Cybersicherheit durch die IT-Sicherheitslösung beschrieben werden. Dies beinhaltet auch die Aufklärung über potenzielle und vorhandene Restrisiken.

Ein wesentlicher Bestandteil für die Transparenz der IT-Lösung ist die Darstellung von angewandten Cyber-Sicherheitsmechanismen, die zum Schutz der Lösung beitragen. Die Aufklärung über die verbleibenden Restrisiken erachten die Anwender als das wichtigste Kriterium für die IT-Sicherheitslösung im Allgemeinen. Das ermöglicht, potenzielle Gefährdungen im geplanten Einsatzszenario frühzeitig zu erkennen und geeignete Maßnahmen zu planen. Die Anwenderunternehmen legen ebenfalls großen Wert darauf, dass sie sowohl über Systemberechtigungen als auch den Einsatz von Online-Updates informiert werden. Auch eine transparente Darstellung von Zertifikaten der IT-Sicherheitslösungen ist wünschenswert.

Ein hohes Maß an Intransparenz verhindert den Aufbau von Vertrauen zum Hersteller. Um das zu verhindern, sollten diese möglichst genaue Auskunft über IT-Sicherheitsmechanismen, verwendete Code-Bausteine und Systemberechtigungen geben. Dadurch werden eventuelle Inkompatibilitäten für den Anwender schnell erkennbar.

Leistungsfähigkeit

Leistungsfähigkeit beschreibt, was die Anwenderunternehmen unmittelbar erfassen und auch kontrollieren können. Daraus ergeben sich die messbaren Kriterien für eine Beurteilung, ob die IT-Sicherheitslösung für den beabsichtigten Einsatzzweck tatsächlich geeignet ist. Dazu zählen im Weiteren auch die Bedienbarkeit und die Interoperabilität.

Bei der Leistungsfähigkeit erwarten die Anwenderunternehmen an erster Stelle eine detaillierte Leistungsbeschreibung und eine darauf angepasste Anleitung. Dabei sollten diese auch die entsprechenden Informationen zu Limitationen der IT-Sicherheitslösung enthalten. Analog zu den möglichen Restrisiken ist die Offenlegung von Einschränkungen essenziell für die Planung des Einsatzes und gibt Auskunft über potenziel-

DIE GRENZEN DER FUNKTIONALITÄT KLAR VERDEUTLICHEN

Nicht nur die Darstellung von dem, was die IT-Sicherheitslösung tatsächlich leistet, sondern besonders Informationen darüber, was sie nicht erfüllt, welche Restrisiken noch bestehen und wie Anwenderunternehmen damit umgehen können, tragen einen beachtlichen Anteil zur Bewertung der Vertrauenswürdigkeit bei. Ebenso wird die Bereitstellung von Informationen zu potenziellen Angriffsvektoren und Darstellung von Limitationen und Kompatibilitäten von Anwendern für sehr relevant befunden. Die exakte Definition und Abgrenzung der Rahmenbedingungen und Offenheit über den Umfang der Funktionalität demonstriert, dass die Hersteller sich verantwortlich fühlen und im besten Sinne der Anwender handeln möchten.

le Inkompatibilitäten von Hard- und Software. Geeignete Benchmarks unterstützen die Anwender bei der Wahl einer adäquaten IT-Sicherheitslösung. Werkzeuge, die diese Funktionalität bereitstellen, sind ebenfalls sehr gefragt. Unzuverlässige oder fehlerhafte Software schaden nicht nur dem Anwenderunternehmen, sondern wirken sich auch negativ auf die Reputation des Herstellers aus.

Zweckprägnanz

Die Zweckprägnanz manifestiert sich im Verwendungszweck der IT-Sicherheitslösung. Das bedeutet, dass bei der Entwicklung von Funktionen die Intention der IT-Sicherheitslösung genau definiert ist. Inkludiert eine IT-Sicherheitslösung neben der eigentlichen Anwendung weitere Features, die nur im Sinne des Herstellerunternehmens oder dritter Parteien sind, müssen diese klar dargestellt und beschrieben werden.

Die Offenlegung aller Funktionen, besonders wenn diese die Verarbeitung von Nutzerinformationen einschließen, ist ein zentraler Bestandteil der Zweckprägnanz. Der Einsatzzweck der IT-Sicherheitslösungen muss aus Sicht der Anwenderunternehmen exakt dargestellt werden. Generell sollten dabei nur Funktionen zum Einsatz kommen, die im Rahmen der Erfüllung der Leistungsbeschreibung notwendig sind. Insbesondere bei der Verarbeitung von Nutzerinformationen – zu denen zählen in diesem Fall neben persönlichen Daten auch sensible Firmeninterna – ist es aus Sicht der Anwender als vertrauensbildende Maßnahme wichtig, über entsprechende Vorgänge informiert zu werden. Zudem ist es für Anwender elementar, dass Herstellerunternehmen sie frühzeitig darüber in Kenntnis setzen, wenn sie neue Features einführen. Sie erwarten ebenfalls eine transparente Auskunft über verwendete Algorithmen mit künstlicher Intelligenz, einschließlich der dafür verwendeten Daten.

Den Abfluss von sensiblen Nutzerdaten erachten Anwenderunternehmen als kritisch für die Vertrauenswürdigkeit. Daher sollte die Verarbeitung von Nutzerinformationen klar dokumentiert und kommuniziert werden.

FAZIT

Die Fähigkeit zu Vertrauen ist tief in uns verwurzelt und lässt sich auch auf den digitalen Raum übertragen. Dazu ist es allerdings notwendig, eine Vielzahl von Informationen bereitzustellen, die Anwenderunternehmen dabei unterstützen, Vertrauen zum Hersteller aufbauen zu können. Aus den Ergebnissen der selektiven Befragung geht hervor, dass die zur Verfügung gestellten Informationen den objektiven Nutzen für den Anwender klar darstellen, aber auch Risiken detailliert aufgeführt werden müssen. Zudem sehen die meisten Anwenderunternehmen eine Vertrauenswürdigkeits-Plattform[4], auf der sich Herstellerunternehmen mit ihren IT-Sicherheitslösungen transparent gemäß den Vertrauenswürdigkeits-Aspekten präsentieren, als sehr hilfreich an, um die Vertrauenswürdigkeit eines Herstellers detailliert einschätzen zu können. ■

Literatur

[1] *N. Pohlmann: Grundlagen zur Vertrauenswürdigkeit und Vertrauenswürdigkeitsmodell, https://norbert-pohlmann.com/glossar-cyber-sicherheit/vertrauenswuerdigkeit/*

[2] *U. Coester, N. Pohlmann: „Vertrauenswürdigkeit schafft Vertrauen – Vertrauen ist der Schlüssel zum Erfolg von IT- und IT-Sicherheitsunternehmen", DuD Datenschutz und Datensicherheit – Recht und Sicherheit in Informationsverarbeitung und Kommunikation, Vieweg Verlag, 2/2022*

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

[4] *Website des if(is) zum Thema Vertrauenswürdigkeit und Vertrauenswürdigkeits-Plattform: https://vertrauenswürdigkeit.com/*

MARCEL BRAUER
studiert im Master Internet-Sicherheit an der Westfälischen Hochschule Gelsenkirchen und beschäftigt sich im Rahmen des Studiums mit Vertrauen und Vertrauenswürdigkeit.

ULLA COESTER
ist Doktorandin und Leiterin des Forschungsprojektes „Vertrauenswürdigkeits-Plattform für KI-Anwendungen und Datenräume im Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen.

NORBERT POHLMANN
ist Professor für Cybersicherheit 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.