TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

"TeleTrusT-Konferenz 2021"

Berlin, 25.11.2021

Vertrauen und Vertrauenswürdigkeit

Prof. Dr. (TU NN)
Norbert Pohlmann
TeleTrusT-Vorstandsvorsitzender
Professor für Informationssicherheit und
Leiter des Instituts für Internet-Sicherheit - if(is)

if(is) internet-sicherheit.

→ **These:**

Vertrauenswürdigkeit *ist der Schlüssel zum Erfolg von* ***IT- und IT-Sicherheitsunternehmen***

Daher ist es für DE- und EU-Unternehmen essenziell, sich über das ***Schaffen von Vertrauen*** *international* ***sehr gut zu positionieren****.*

Vertrauen / Vertrauenswürdigkeit
→ Grundsätzlich

- **Vertrauen** bezeichnet die ***subjektive* Überzeugung** der **Richtigkeit von Handlungen**.
- Dabei **reduziert Vertrauen die Komplexität** einer Handlung, dadurch ist der Nutzer auch in einer *ungewissen* oder *unsicheren* Situation handlungsfähig.
- Diese Komplexitätsreduzierung ist besonders hilfreich, wenn der **Ausgang einer Handlung risikobehaftet** sein kann.
- Zu **vertrauen bedeutet** daher die **Bereitschaft**, seine *Handlung nicht infrage zu stellen* und sich folglich einem bestimmten **Risiko auszusetzen**.
- Die **Qualität** der **Vertrauensgrundlage** ist entscheidend dafür, dass ein hohes Maß an **Vertrauen aufgebaut** werden kann.
- Aus diesem Grund *schafft* die **Darstellung von Aspekten der Vertrauenswürdigkeit** der *IT-Lösungen im Einzelnen* sowie des *Unternehmens insgesamt* **Vertrauen beim Nutzer**.

Interpersonales → institutionelles Vertrauen
→ Eine Herausforderung

- **Interpersonales Vertrauen** ist das **Vertrauensverhältnis**, das aufgrund bestimmter eigener Kriterien **zwischen Menschen** entsteht, wie Stimme, Mimik und Gestik.
- **Vertrauen** zwischen zwei **Menschen** kann insbesondere aufgrund der Fähigkeit zur **Empathie** aufgebaut werden.
- **Unternehmen** müssen in der IT und im Cyber-Raum andere **Vertrauenswürdigkeitskriterien** nutzen, um **Nutzer** in die Lage zu versetzen, ihre **grundsätzliche Vertrauensfähigkeit** auf IT-Lösungen und dem Hersteller zu übertragen.
- Das **institutionelle Vertrauen** ist das **Ergebnis der erfolgreichen Transferleistung**, basierend auf der Bereitschaft des **Nutzers**, seine Vertrauensfähigkeit auf *ein Unternehmen* beziehungsweise *deren IT-Lösungen* zu übertragen.
- Dieses **Vertrauen** kann in erster Linie **durch das Unternehmen** selbst, **über die IT-Lösung** sowie auch über die **Domäne** *(positiv)* beeinflusst werden.
  (siehe Vertrauenswürdigkeitsmodell)

Vertrauen und Vertrauenswürdigkeit
→ Zunehmende Notwendigkeit

- Die **Digitalisierung** bringt **für den Nutzer** einen immer **höheren Grad an Komplexität** mit sich, wodurch es für den Nutzer zunehmend schwieriger wird, einzelne IT-Lösungen und deren Hintergründe **verstehen** und **bewerten** zu **können**.

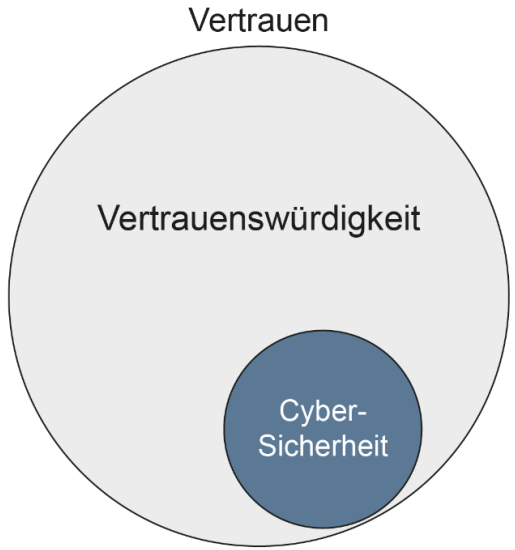
- Aber auch die **Vertrauenswürdigkeit der Unternehmen** spielt eine besondere Rolle, weil **Nutzer** zunehmend **IT-Lösungen** nur noch **nutzen**, wenn sie diesen beziehungsweise den Unternehmen **vertrauen** können.

- Aus diesem Grund müssen Unternehmen alles tun, damit es einem Nutzer möglich ist, einer **IT-Lösung** und dem **Unternehmen,** das diese herstellt, zu **vertrauen**.

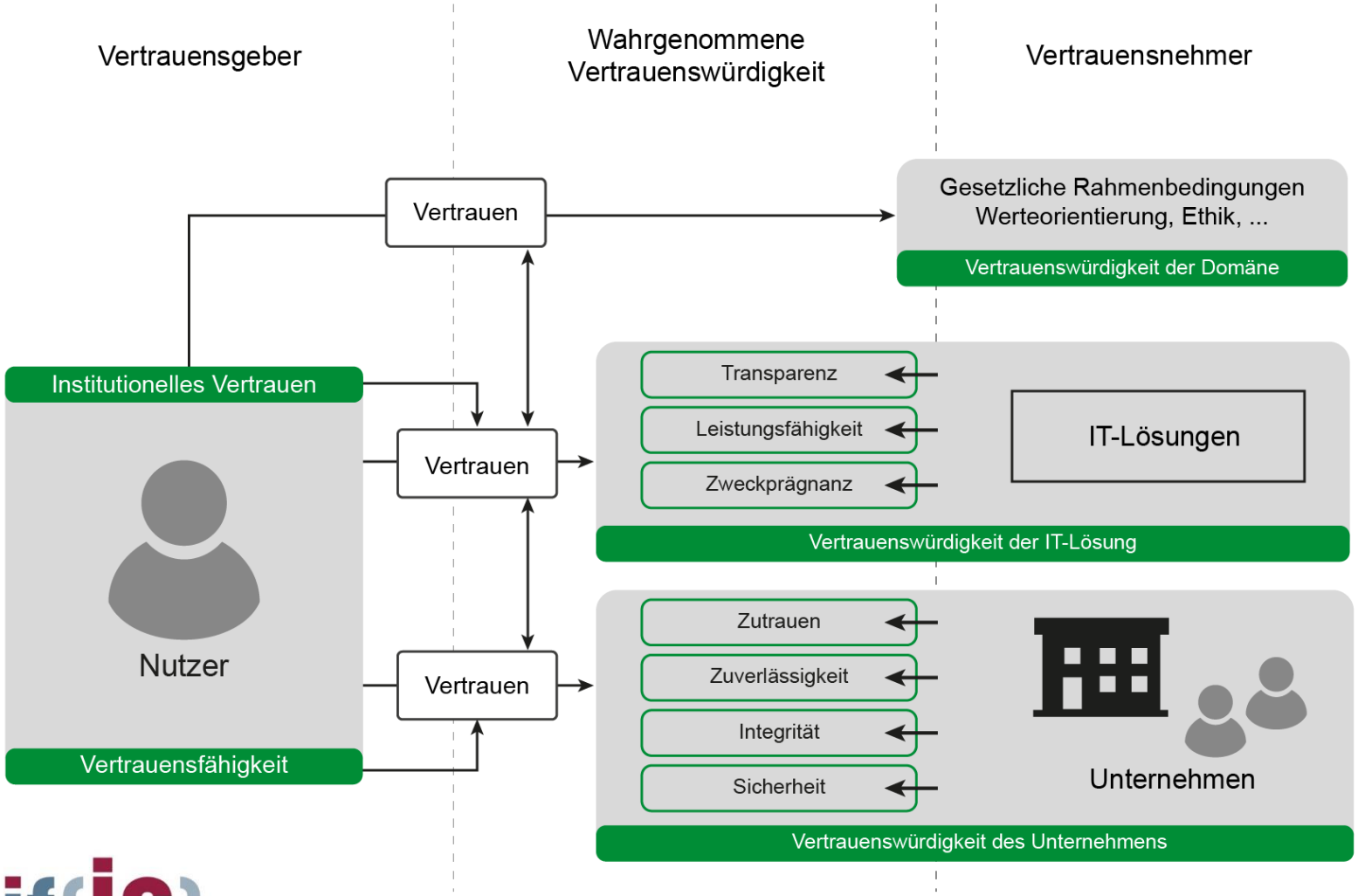
- **Vertrauen schafft Akzeptanz** und damit **loyale Kunden**.

Vertrauen, Vertrauenswürdigkeit
→ und Cyber-Sicherheit

- **Vertrauen bedeutet** das Unternehmen den Nutzern eine **Vertrauensgrundlage** über eine **wahrgenommene Vertrauenswürdigkeit** bieten, das diese eine IT-Lösung trotz bestehender Risiken nutzen wollen.
- Die Umsetzung und Darstellung von **Cyber-Sicherheit** ist *ein* **wichtiger Bestandteil bei der Darstellung** der **Vertrauenswürdigkeit**, aber nicht der einzige.
- Viele weitere **Aspekte der Vertrauenswürdigkeit** spielen bei **Aufbau von Vertrauen** eine wichtige Rolle.

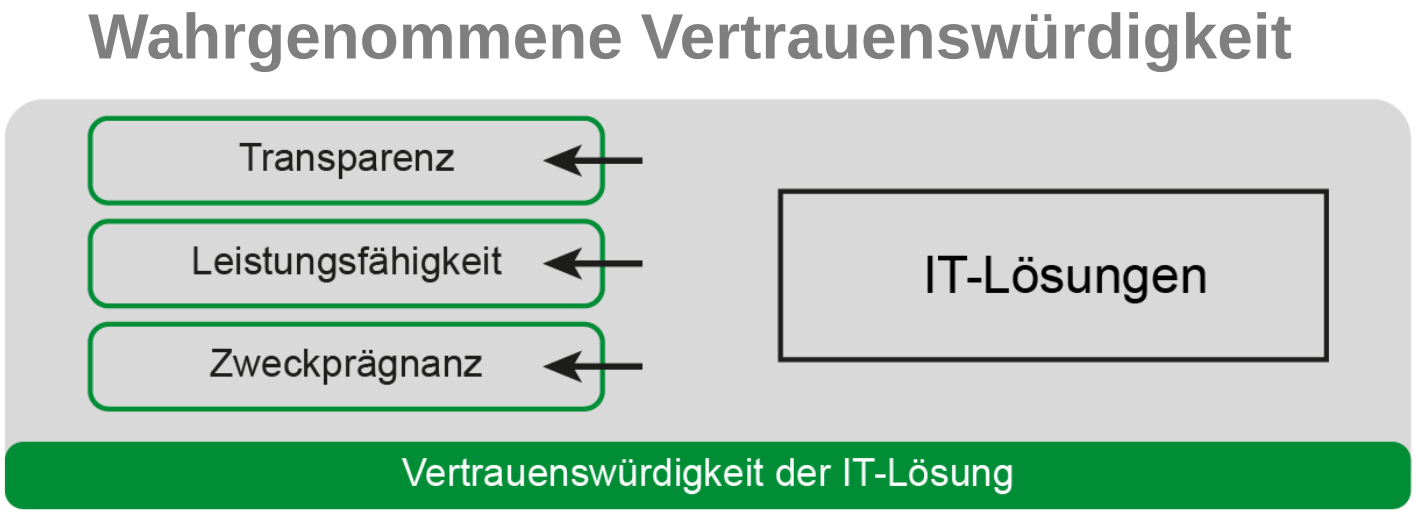


Vertrauenswürdigkeitsmodell
→ Übersicht



- **Unternehmen** müssen sich **darstellen**, um über eine hohe **wahrgenommene Vertrauenswürdigkeit** den Nutzer die Möglichkeit zu geben, ihnen zu vertrauen.
- Dazu müssen die **Vertrauenswürdigkeitsaspekte** der IT-Lösungen und des Unternehmens **formuliert** und **veröffentlich** werden.
- Auch die **Vertrauenswürdigkeit** der **Domäne** hat einen **hohen Einfluss** auf das Vertrauen der Nutzer.

Vertrauenswürdigkeit der IT-Lösung
→ Übersicht



- **Aspekte, die bei IT-Lösungen für das Aufbauen von Vertrauen eine Rolle spielen:** Transparenz, Leistungsfähigkeit und Zweckprägnanz
- Durch die **Darstellung** dieser Aspekte der **wahrgenommenen Vertrauenswürdigkeit** wird der Nutzer prinzipiell in die Lage versetzt, **Vertrauen** zu angebotenen IT-Lösungen **aufzubauen**.

Vertrauenswürdigkeit der IT-Lösung
→ Aspekt: Transparenz einer IT-Lösung

- Für den Nutzer ist es aufgrund der zunehmend intelligenten Angriffe und komplexeren Cyber-Sicherheitsmechanismen immer wichtiger, dass seine **Cyber-Sicherheitsbedürfnisse** auch **angemessen** durch die IT-Lösung / IT-Sicherheitslösung **befriedigt** werden.

- **Transparenz** bedeutet alle **relevanten Informationen** zur Verfügung stellen, die für den Nutzer erforderlich sind, um im gegebenen Kontext **eine valide Entscheidung** über die **Vertrauenswürdigkeit der IT-Lösung** treffen zu können.

Beispiele für die Transparenz einer IT-Lösung:

- ***Beipackzettel-Cyber-Sicherheit:*** Beschreiben, wie mithilfe von Cyber-Sicherheitsmechanismen in der IT-Lösung dafür gesorgt wird, die **Wahrscheinlichkeit** der verschiedenen **Angriffe** zu **reduziert** und aufzuzeigen, welche **Restrisiken** bestehen und wie der Nutzer damit **umgehen** kann.

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

Vertrauenswürdigkeit der IT-Lösung
→ Aspekt: Leistungsfähigkeit einer IT-Lösung

- Die **Leistungsfähigkeit** einer IT-Lösung ist das, was der **Nutzer unmittelbar** erfassen und in der Regel eigenständig **kontrollieren** kann.
- Daher ergeben sich daraus die **messbaren Kriterien** für dessen **Beurteilung**, inwieweit er sich bei der Erreichung des beabsichtigten Einsatzzwecks unterstützt fühlt und wie gut die **IT-Lösung** tatsächlich dafür **geeignet ist**.

Beispiele für die Leistungsfähigkeit einer IT-Lösung:

- ***Bedienbarkeit:*** Sind **Cyber-Sicherheitsmechanismen** und **-Management** für den Nutzer **einfach** und **intuitiv** zu bedienen *(Beschreiben, das sich z.B. die IT-Lösung in 5 Minuten sicher und vertrauenswürdig einrichten lässt)*.
- ***Leistungsfähigkeit der Cyber-Sicherheitsmechanismen*:** Z.B., wie stark **verringert** sich die **Leistungsfähigkeit** der IT-Lösung durch die **Verschlüsselung** der Daten *(Aufzeigen, dass es für den Nutzer nicht spürbar ist)*. Oder wie lange **benötigt** ein Angriffserkennungssystem von dem **Erkennen eines Angriffs bis zur Reaktion**, zum Beispiel dem Versenden eines Alarms oder einer automatischen Reaktion darauf *(Darstellen, das es schnell genug ist, um Schäden zu verhindern oder zu minimieren und welche Voraussetzungen zu schaffen sind)*.

Vertrauenswürdigkeit der IT-Lösung
→ Aspekt: Zweckprägnanz einer IT-Lösung

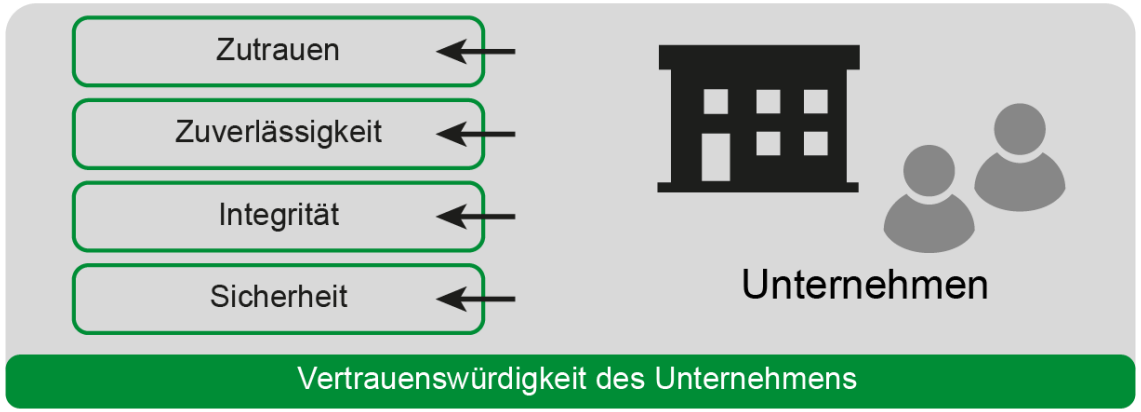
- Die Zweckprägnanz manifestiert sich im **Verwendungszweck der IT-Lösung**.
- Für Unternehmen bedeutet dies, dass die **Entwicklung von Funktionen** sowie die **Intention** der IT-Lösung **zielgenau definiert** sind.

Beispiele für die Zweckprägnanz einer IT-Lösung:

- ***Geschäftsmodell:*** Durch das Geschäftsmodell „Bezahlen mit persönlichen Daten“ können Unternehmen **sensitive Daten** ihrer Nutzer sammeln und diese für individualisierte Werbung **nutzen** und/oder an Dritte verkaufen, um Gewinn zu erzielen. *Die Intention des Unternehmens muss klar ersichtlich, also transparent dargestellt werden.*

- ***Neue Features:*** Das neue System von Apple (CSS), mit dem Daten auf dem iPhone anlasslos nach kinderpornografischem Material durchsucht werden sollen, hat zwar einen hohen gesellschaftlichen Wert, stellt aber für den **Nutzer** ein **Risiko** im Sinne seiner **Privatsphäre** und **Sicherheit** dar. *Neue Features sollten immer der Zweckprägnanz entsprechen. CSS hat nichts mehr mit dem eigentlichen Zweck zu tun.*

Vertrauenswürdigkeit des Unternehmens
→ Übersicht



- **Aspekte, die bei einem Unternehmen für das Aufbauen von Vertrauen eine Rolle spielen:** Zutrauen, Zuverlässigkeit, Integrität und Sicherheit
- Die **Vertrauenswürdigkeit des Unternehmens** spielt für unsere digitalen Zukunft zunehmend eine **wichtige Rolle** bei der Auswahl von IT-Lösungen.
- Durch die **Darstellung** der Aspekte der **wahrgenommenen Vertrauenswürdigkeit** kann der Nutzer prinzipiell **Vertrauen** zum Unternehmen **aufzubauen**.

Vertrauenswürdigkeit des Unternehmens
→ Aspekt: Zutrauen in ein Unternehmen

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

Beispiele für das Zutrauen in ein Unternehmen:

- ***Mitarbeiter:*** Aufzeigen der Qualifikationen der Mitarbeiter - Ausbildung *(z.B. **Master Internet-Sicherheit**)*, Qualifizierung und Weiterbildung *(z.B. **T.I.S.P.**)*.
- ***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 Cyber-Sicherheit:*** Ausgaben für Cyber-Sicherheit von den Ausgaben für Informationstechnologien offen legen, z.B. **6 bis 15% vom IT-Budget**.

Vertrauenswürdigkeit des Unternehmens
→ Aspekt: Zuverlässigkeit eines Unternehmens

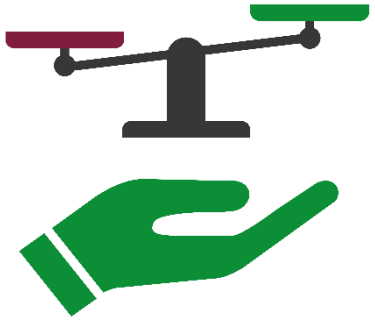
- IT-Lösungen führen nur Prozesse aus, die seitens der **Nutzer gewünscht** sind, beziehungsweise **die er erwartet** und dies sehr **verlässlich**.
- Das impliziert, dass **Unternehmen** grundsätzlich **wohlwollend** sind.
- Das bedeutet, dass sie im besten **Sinne ihrer Nutzer handeln**, sich also **an deren Bedürfnissen orientieren**, statt ihre eigenen Interessen besonders in den Mittelpunkt zu stellen.

Beispiele für die Zuverlässigkeit eines Unternehmens:

- ***Kooperativ handeln:*** Übernahme einer **Gesamtverantwortung** im **Schadensfall** oder **Rückrufaktionen** bei identifizierten Problemen.
  Sofortige Informationen bei gravierenden **Schwachstellen**.
- ***Verantwortlich handeln***: Überprüfung und **kontinuierliche Kontrolle** der Lieferketten.
  Ergreifen aller Maßnahmen, um **Betrugsprävention** im Sinne der Nutzer durchzuführen.

Vertrauenswürdigkeit des Unternehmens
→ Aspekt: Integrität eines Unternehmens

- Es werden alle Faktoren der Vertrauenswürdigkeit und hier insbesondere die **ethischen Dimensionen** beachtet.
- Das 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**.



Beispiele für die Integrität eines Unternehmens:

- ***Rechenschaftspflicht:*** Darstellung der **ethischen Grundsätze**, die ein Unternehmen einhalten will *(Fairness, Gerechtigkeit, Gleichheit, Solidarität …)*.
- ***Schutz der Privatsphäre:*** Sofortige **Löschung** von **Kundendaten**, wenn diese nicht mehr benötigt werden. Daten der Nutzer nicht für weitere wirtschaftliche Zwecke zu verwerten.
- ***Keine eingeschränkte Cyber-Sicherheit:*** Keine geschwächten Verschlüsselungen, Zufallszahlengeneratoren … keine Backdoors.
  Z.B. das TeleTrusT-Gütesiegel **„IT Security made in Germany“** deklarieren.

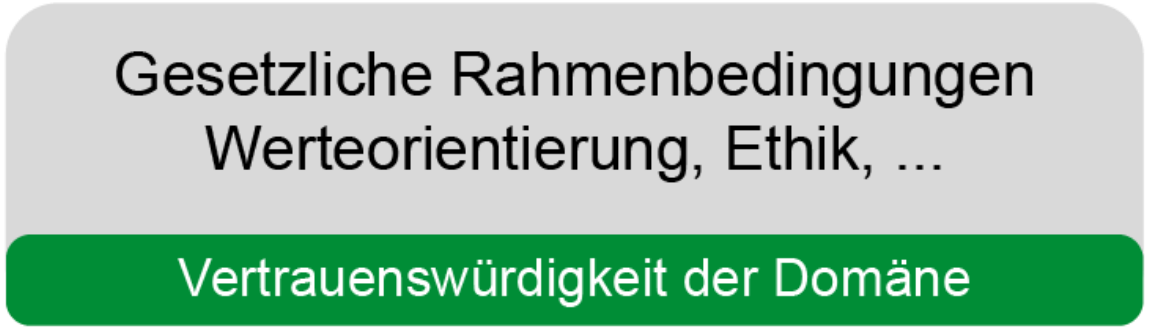
Vertrauenswürdigkeit des Unternehmens
→ Aspekt: Sicherheit des Unternehmens

- Aufzeigen, dass Unternehmen alles tun, um ihr Kunden zu schützen.

Beispiele für die Sicherheit des Unternehmens:

- ***Darstellung der verwendeten Cyber-Sicherheitsmaßnahmen:*** Aufzeigen, was sie tun, um die IT-Lösung und ihr Unternehmen zu schützen.
- ***Zertifizierung der IT-Lösung:*** Die **Zertifizierung** der IT-Lösung, aber auch des Unternehmens ist eine wichtige **Maßnahme zur Vertrauensbildung**.
- ***Regelmäßige Überprüfung der IT-Lösungen und des Unternehmens:*** Darstellen, wie **Schwachstellen aktiv** und **kontinuierlich** mit Penetrationstests / Red-Teams / Bug-Bounty-Programm **identifiziert** und so schnell wie möglich durch Updates **eliminiert** werden.
- ***Cyber-Sicherheitsstrategie:*** Vorstellen, wie mit **Vermeiden** und **Entgegenwirken** von IT-Angriffen die vorhandenen **Risiken reduziert** sowie mit **Erkennen** von und **Reaktion** auf IT-Angriffe die **verbleibenden Risiken gehändelt** werden.
- ***Ausgaben für Cyber-Sicherheit:*** Wie bei dem Aspekt Zutrauen - beschreiben, dass X % vom IT-Budget für Cyber-Sicherheit ausgegeben werden.

Vertrauenswürdigkeit der Domänen
→ Übersicht



- **Kollaborativ** mit anderen Herstellern und Stakeholdern (Staat, Politik, Nutzer, Wissenschaft, Anwendungsunternehmen …) gesellschaftliche **Werte kreieren** oder **Wertevorstellungen umsetzen**, um die gesamte Branche respektive Domäne vertrauenswürdig zu entwickeln.
- Durch die **Schaffung** einer **Vertrauenswürdigkeit der Domäne** kann eine erfolgreiche Einführung von **neuen Geschäftsmodellen** oder **IT-Lösungen** in der Domäne möglich werden.

Vertrauenswürdigkeit der Domänen
→ Beispiele

- ***Schaffung von Rahmenbedienungen:*** Der Staat schafft die Randbedingungen, indem Domänen-spezifisch vorgegeben wird, wie Unternehmen den Einsatz der IT-Lösungen zu gestalten haben (Datenschutz-Grundverordnung - DSGVO, IT-Sicherheitsgesetz, eIDAS …).

- ***Motivierung von Ökosystemen:*** EBCA, Self-Sovereign Identities (SSI), GAIA-X … **Souveräne Technologie**, die unseren **Wertvorstellungen** entsprechen.

- ***Etablierung eines gemeinsamen Gütesiegels:*** Gütesiegel helfen den Unternehmen, ihre Vertrauenswürdigkeit darzustellen.
  Beispiele für Gütesiegel sind **„IT Security – Made in Germany“** und **T.I.S.P.** von TeleTrusT.

- ***Schutzmechanismen des Staats:*** Ein Negativ-Beispiel ist die Anwendung des Bundestrojaners *(Schwächung der IT-Endgeräte aller Bürger und Unternehmen).*

Vertrauen und Vertrauenswürdigkeit
→ Zusammenfassung

- Das **Vertrauenswürdigkeitsmodell** stellt sehr gut dar, auf welchen Ebenen es Unternehmen möglich ist – durch entsprechendes **Handeln** und **Bereitstellung von Informationen** – ihre **wahrgenommene Vertrauenswürdigkeit** für ihre Kunden zu **erhöhen**.

- **Je höher die Vertrauenswürdigkeit** der *IT-Lösungen* und des *Unternehmens* ist, desto eher **kann Vertrauen bei den Nutzern entstehen**.

- Dieses ist notwendig, um eine **Akzeptanz bei den Nutzern** für die jeweils angebotene **IT-Lösung** zu erreichen.

- Die Darstellung der **Vertrauenswürdigkeit** von IT-Lösungen und Unternehmen stellt einen immer größeren **Wettbewerbsvorteil** dar.

"TeleTrusT-Konferenz 2021"

Berlin, 25.11.2021

Vertrauenswürdigkeit *ist der Schlüssel*
zum ***Erfolg*** *von IT- und IT-Sicherheitsunternehmen*

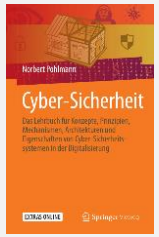
Prof. Dr. (TU NN)
Norbert Pohlmann
TeleTrusT-Vorstandsvorsitzender
Professor für Informationssicherheit und
Leiter des Instituts für Internet-Sicherheit - if(is)

Anhang / Credits
→ Übersicht

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Wir empfehlen

- **Cyber-Sicherheit**
  Das **Lehrbuch** für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung, Springer Vieweg Verlag, Wiesbaden 2019
  https://norbert-pohlmann.com/cyber-sicherheit/



- **7. Sinn im Internet (Cyberschutzraum)**
  https://www.youtube.com/cyberschutzraum

CYBER SCHUTZRAUM

- **Master Internet-Sicherheit**
  https://it-sicherheit.de/master-studieren/

(M) MASTER internet-sicherheit.

Besuchen und abonnieren Sie uns :-)

WWW
https://www.internet-sicherheit.de

Facebook
https://www.facebook.com/Internet.Sicherheit.ifis

Twitter
https://twitter.com/_ifis

https://twitter.com/ProfPohlmann

YouTube
https://www.youtube.com/user/InternetSicherheitDE/

Prof. Norbert Pohlmann
https://norbert-pohlmann.com/

Quellen Bildmaterial

Eingebettete Piktogramme:
- Institut für Internet-Sicherheit – if(is)

Der Marktplatz IT-Sicherheit

(IT-Sicherheits-) Anbieter, Lösungen, Jobs, Veranstaltungen und Hilfestellungen (Ratgeber, IT-Sicherheitstipps, Glossar, u.v.m.) leicht & einfach finden.
https://www.it-sicherheit.de/

if(is) internet-sicherheit.

Literatur
→ Auswahl

U. Coester, N. Pohlmann: „Vertrauen – ein elementarer Aspekt der digitalen Zukunft", DuD Datenschutz und Datensicherheit – Recht und Sicherheit in Informationsverarbeitung und Kommunikation, Vieweg Verlag, 2/2021
https://norbert-pohlmann.com/artikel/vertrauen-ein-elementarer-aspekt-der-digitalen-zukunft/

U. Coester, N. Pohlmann: „Artikelserie über Facetten der Künstlichen Intelligenz“

Warum Vertrauenswürdigkeit und KI unbedingt zusammengehören (Teil 1)
https://www.onpulson.de/63805/warum-vertrauenswuerdigkeit-und-ki-unbedingt-zusammengehoeren/

IT-Systeme: Warum Vertrauen für Unternehmen so wichtig ist (Teil 2)
https://www.onpulson.de/64428/it-systeme-warum-vertrauen-fuer-unternehmen-so-wichtig-ist/

Akzeptanz von IT-Lösungen – wie Vertrauen bei Anwendern entsteht (Teil 3)
https://www.onpulson.de/65619/akzeptanz-von-it-loesungen-wie-vertrauen-bei-anwendern-entsteht/

So lässt sich Vertrauenswürdigkeit für KI-basierte Anwendungen schaffen (Teil 4)
https://www.onpulson.de/65686/so-laesst-sich-vertrauenswuerdigkeit-fuer-ki-basierte-anwendungen-schaffen/

U. Coester, N. Pohlmann: „Diskriminierung und weniger Selbstbestimmung? Die Schattenseiten der Algorithmen“, tec4u, 12/17

U. Coester, N. Pohlmann: „Ethik und künstliche Intelligenz – Wer macht die Spielregeln für die KI?“, IT & Production – Zeitschrift für erfolgreiche Produktion, TeDo Verlag, 2019

N. Pohlmann: **Lehrbuch „Cyber-Sicherheit“,** Springer Vieweg Verlag, Wiesbaden 2019, ISBN 978-3-658-25397-4s

Weitere Artikel siehe: https://norbert-pohlmann.com/artikel/