Vertrauen und Vertrauenswürdigkeit

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

Vertrauenswürdigkeitstechnologie
→ Abgrenzung

- **Vertrauenswürdigkeitstechnologien** haben das Ziel, mit intelligenten Cyber-Sicherheitsarchitekturen, -konzepten und -funktionen dafür zu sorgen, dass die **digitalen Aktivitäten transparent und nachvollziehbar umgesetzt werden** können. Dadurch soll das Vertrauen der Nutzer erhöht werden.

- **Beispiele von Vertrauenswürdigkeitstechnologien**:
  - Security Kernel, Isolierung- und Separierungstechnologien (Trusted Computing, Zero Trust)
  - Zentraler Vertrauensdienst: Public Key-Infrastrukturen
  - Dezentraler Vertrauensdienst: Blockchain-Technologien
  - Self-Sovereign Identity (SSI) … EU-ID, EU-Wallet …

→ These:

*In der **Digitalisierung** ist **Vertrauenswürdigkeit notwendig** und **nachweisbar.***

Vertrauen

→ Grundsätzlich

- Status Quo:
  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**.

- Folge:
  Das macht den **Menschen Angst und schränkt sie in ihrer Handlungsfähigkeit ein.**

- **Lösung:**
  Vertrauen trägt zur **Komplexitätsreduzierung** bei, weil durch Vertrauen die **subjektive Überzeugung der Richtigkeit von Handlungen** manifestiert wird.

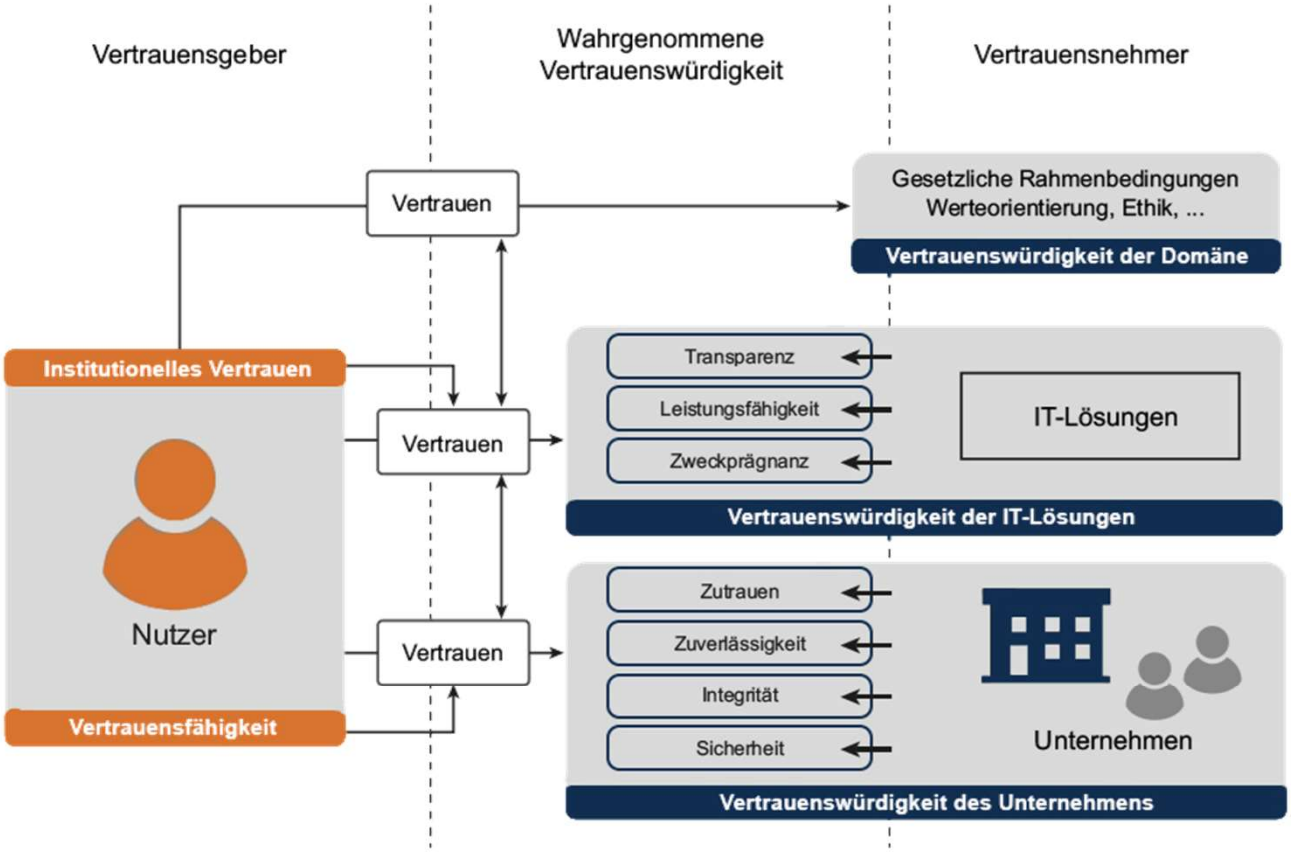
Vertrauenswürdigkeit

→ **Zunehmende Notwendigkeit**

- ***Wichtig:*** **Nutzer wollen Vertrauen können.**
  Aus diesem Grund müssen Unternehmen alles tun, damit es dem Nutzer möglich ist, ihrer **IT-Lösung** sowie auch dem **Unternehmen** zu **vertrauen – das bedeutet, vertrauenswürdig agieren.**

- ***Fazit:***
  Vertrauenswürdigkeit schafft Akzeptanz und damit **loyale Kunden.**

Das Vertrauenswürdigkeitsmodell



Vertrauenswürdigkeits-Agenda

→ Aspekt: Transparenz der IT-Lösung

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

- **Was bedeutet Transparenz und wie kann sie erreicht werden?**

- ***Beipackzettel-Cyber-Sicherheit***
- *Darstellung von Zertifikaten*

Vertrauenswürdigkeits-Agenda

→ Aspekt: Leistungsfähigkeit der IT-Lösung

- Die **Leistungsfähigkeit** einer IT-Lösung ist das, was der **Nutzer unmittelbar** erfassen und in der Regel eigenständig **kontrollieren** kann.
- Anhand welcher Kriterien kann ein Unternehmen die Leistungsfähigkeit des Produktes offensichtlich demonstrieren?

- *Bedienbarkeit*
- *Interoperabilität*
- ***Leistungsfähigkeit der Cyber-Sicherheitsmechanismen***

Vertrauenswürdigkeits-Agenda

→ Aspekt: Zweckprägnanz der IT-Lösung

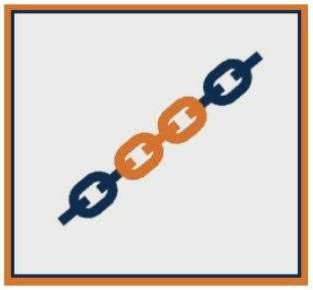
- Die Zweckprägnanz manifestiert sich im **Verwendungszweck der IT-Lösung,** dies bedeutet, dass vorab die **Entwicklung von Funktionen** sowie die **Intention** der IT-Lösung **zielgenau definiert** werden müssen.
- Wie wichtig ist die Zweckprägnanz aus Sicht der Nutzer und was können Unternehmen in diesem Bereich falsch machen?

- ***Geschäftsmodell***
- *Neue Features*

Vertrauenswürdigkeits-Agenda

→ Aspekt: Zutrauen zum Unternehmen

- Zutrauen ist ein erstes **relevantes Kriterium für den Aufbau von Vertrauenswürdigkeit von Unternehmen**.
- Wie kann **Zutrauen** im Hinblick auf die Funktionalität erzeugt werden – worüber müssen Unternehmen verfügen, damit der Nutzer vertrauen kann?



- ***Mitarbeiter***
- *Qualitätsstandards*
- *Betriebsmittel*
- ***Ausgaben für Cyber-Sicherheit***

Vertrauenswürdigkeits-Agenda

→ Aspekt: Zuverlässigkeit des Unternehmens

- IT-Lösungen führen nur Prozesse aus, die seitens der **Nutzer gewünscht** sind, beziehungsweise **die er erwartet** und dies sehr **verlässlich**.
- Wie können Unternehmen demonstrieren, dass sie grundsätzlich im besten Sinne der Nutzer handeln?

- *Kooperativ Handeln*
- ***Verantwortlich Handeln***

Vertrauenswürdigkeits-Agenda

→ Aspekt: Integrität des Unternehmens

- Es werden alle Faktoren der Vertrauenswürdigkeit und hier insbesondere die **ethischen Dimensionen** beachtet.
- Wie ist es Unternehmen möglich zu zeigen, dass sie generell dazu bereit sind, die Normen und Werte der Gesellschaft zu berücksichtigen?

- *Rechenschaftspflicht*
- ***Schutz der Privatsphäre***
- ***Keine eingeschränkte Cyber-Sicherheit***

Vertrauenswürdigkeits-Agenda

→ Aspekt: Sicherheit des Unternehmens

- Aufzeigen, dass Unternehmen alle Maßnahmen ergreifen, um ihre Kunden zu schützen.
- Was muss hier getan werden seitens der Unternehmen?

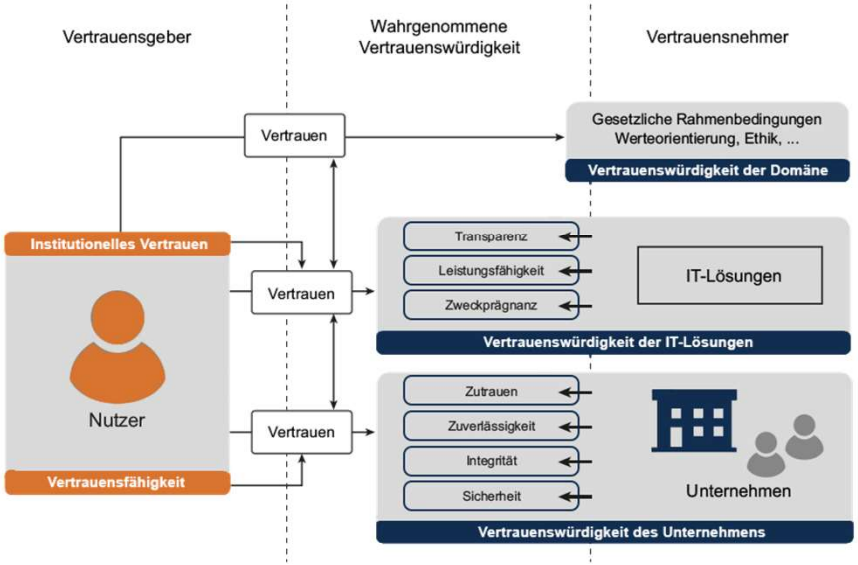
- *Darstellung der verwendeten Cyber-Sicherheitsmaßnahmen*
- *Zertifizierung des Unternehmens und deren IT-Lösung*
- ***Regelmäßige Überprüfung der IT-Lösungen des Unternehmens***
- ***Cyber-Sicherheitsstrategie***

Vertrauenswürdigkeit der Domänen

→ Übersicht & Beispiele

- Kollaborativ mit Herstellern und weiteren Stakeholdern wie Staat, Politik, Nutzer, Wissenschaft oder Anwendungsunternehmen gesellschaftliche Wertevorstellungen umsetzen, um eine gesamte Branche respektive Domäne vertrauenswürdig zu entwickeln.

  - Schaffung von Rahmenbedingungen
  - Motivierung von Öko-Systemen
  - Etablieren eines „Stand der Technik“



Vertrauenswürdigkeit von Herstellerunternehmen

→ Anwenderstudie: Transparenz der IT-Lösung (1)

- Im Zusammenhang mit der **Transparenz** sehen die Anwender es als besonders essenziell an, dass sie über die möglichen **Restrisiken** der IT-Lösung informiert werden.

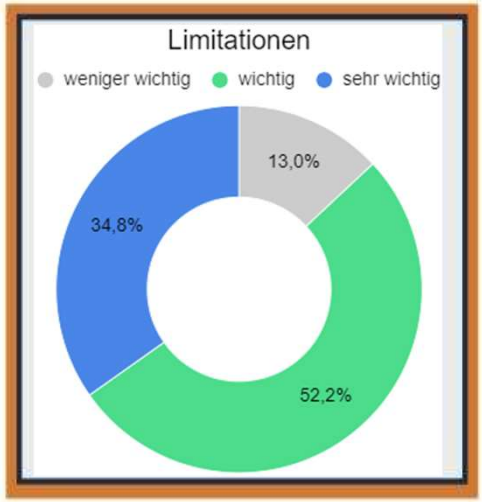
Die größte Relevanz haben die folgenden Kriterien:

- Aufklärung über **Restrisiken**
- Darstellung der **Cyber-Sicherheitsmaßnahmen**
- Darstellung der **Sicherheitszertifikate**

Vertrauenswürdigkeit von Herstellerunternehmen

→ Anwenderstudie: Leistungsfähigkeit der IT-Lösung (2)

- Bei der **Leistungsfähigkeit** erwarten die Anwenderunternehmen an erster Stelle eine detaillierte Leistungsbeschreibung und ggf. eine ausführliche Anleitung sowie die entsprechenden Informationen zu **Limitationen** der IT-Lösung.



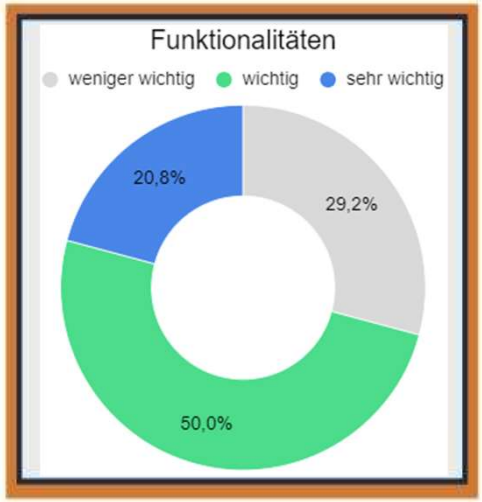
Die größte Relevanz haben die folgenden Kriterien:

- Aufklärung über **Limitationen**
- Bereitstellung von **Kontrollwerkzeugen**
- Bereitstellung einer **detaillierten Anleitung**

Vertrauenswürdigkeit von Herstellerunternehmen

→ Anwenderstudie: Zweckprägnanz der IT-Lösung (3)

- Die **Zweckprägnanz** – also der Einsatzzweck der IT-Lösung – muss aus Sicht der Anwenderunternehmen exakt dargestellt, die jeweilige **Funktionalität** auf einem hohen Abstraktionslevel beschrieben werden.



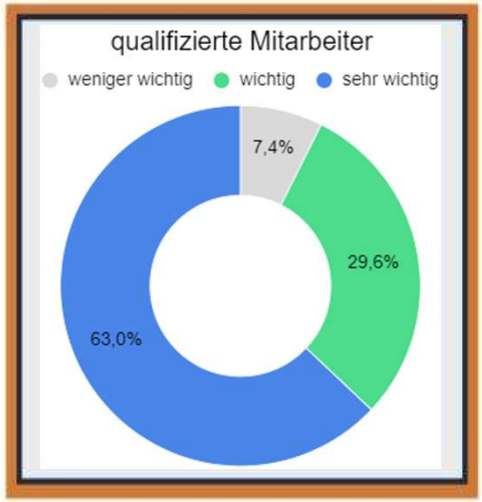
Die größte Relevanz haben die folgenden Kriterien:

- Darstellung der **Funktionalitäten** inkl. des **Verwendungszwecks**
- Transparente Darstellung der **Verarbeitung von Nutzerinformationen**

Vertrauenswürdigkeit von Herstellerunternehmen

→ Anwenderstudie: Zutrauen zum Unternehmen (1)

- In Bezug auf den Aspekt **Zutrauen** war besonders markant, dass **qualifizierte Mitarbeiter** und **Qualitätsstandards** von den Studienteilnehmern als wichtigstes Kriterium ausgewählt wurde, als Basis für die Herstellung von qualitativ hochwertigen IT-Lösung.



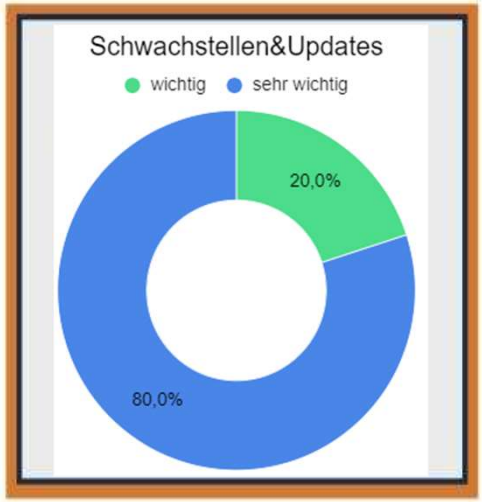
Die größte Relevanz haben die folgenden Kriterien:

- **Qualifizierte Mitarbeiter** im Entwicklungsteam
- Einhaltung von **hohen Qualitätsstandards** in der Entwicklung

Vertrauenswürdigkeit von Herstellerunternehmen

→ Anwenderstudie: Zuverlässigkeit des Unternehmens (2)

- Als Nachweis der **Zuverlässigkeit** dient, dass die IT-Lösung **kontinuierlich funktionsfähig** ist. Hierzu gehört auch, dass sie zeitnah über **Schwachstellen informiert** und ihnen **schnellstmöglich** entsprechende **Updates** zur Verfügung gestellt werden.



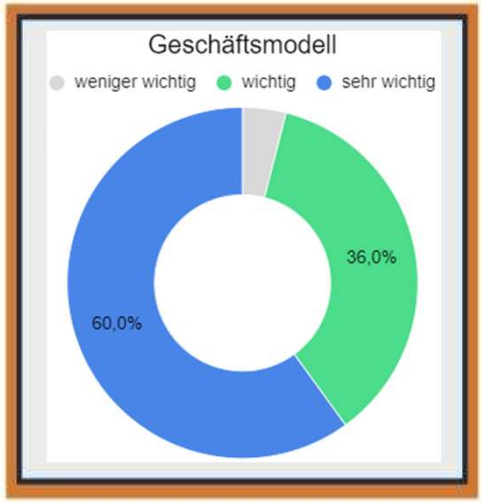
Die größte Relevanz haben die folgenden Kriterien:

- Schnelle Bereitstellung von **Sicherheits-Updates**
- **Kontinuierliche Funktionsfähigkeit** der IT-Lösung
- Informieren über potentielle **Angriffsmöglichkeiten**

Vertrauenswürdigkeit von Herstellerunternehmen

→ Anwenderstudie: Integrität des Unternehmens (3)

- Die **Integrität** eines Unternehmens ist aus Sicht der Anwender eng mit der **Transparenz** des Herstellers verknüpft – hier wird in erster Linie eine **Offenlegung** des **Geschäftsmodells** als sehr wichtig erachtet.



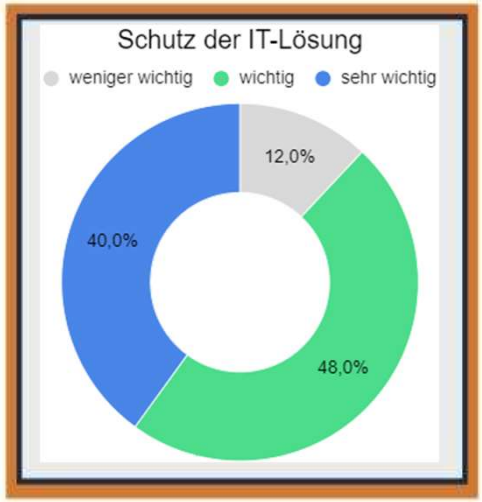
Die größte Relevanz haben die folgenden Kriterien:

- Transparente **Darstellung des Geschäftsmodells**
- Informieren über **eingeschränkte IT-Sicherheit**
- Einhaltung der **DSGVO-Konformität**

Vertrauenswürdigkeit von Herstellerunternehmen

→ Anwenderstudie: Sicherheit des Unternehmens (4)

- Im Kontext der **Unternehmenssicherheit** steht die langfristige **IT-Sicherheitsstrategie** an erster Stelle, aber auch **Maßnahmen** zur kontinuierlichen **Schwachstellen-Erkennung** betrachten die Anwender bei Unternehmen als fundamental.



Die größte Relevanz haben die folgenden Kriterien:

- **Schutz der IT-Lösung**
- Langfristige **Cyber-Sicherheitsstrategie**
- Kontinuierliche **Überprüfung auf Schwachstellen**

Vertrauenswürdigkeit von Herstellerunternehmen

→ Anwenderstudie: positive Keywords

Die am häufigsten genannten **positiven** Keywords können unter den folgenden **Oberbegriffen** zusammengefasst werden:

- ✓ Kunden-Referenzen
- ✓ Transparente Kommunikation
- ✓ Ganzheitliches Informationssicherheitskonzept
- ✓ Nachweise durch unabhängige Dritte
- ✓ DSGVO-Konformität

Vertrauenswürdigkeit von Herstellerunternehmen

→ Anwenderstudie: negative Keywords

Die am häufigsten genannten **negativen** Keywords können unter den folgenden **Oberbegriffen** zusammengefasst werden:

- ✘ Nichtbeachtung von IT-Sicherheit
- ✘ Unzureichender Support
- ✘ Nichtbeachtung von Datenschutz
- ✘ Intransparenz
- ✘ Unseriöses Marketing

Vertrauen und Vertrauenswürdigkeit

→ Zusammenfassung / 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.

- *Das von uns angestrebte **Ziel:*** Aufbau einer **Vertrauenswürdigkeits-Plattform**

  ➔ basierend auf der Darstellung der **wahrgenommenen Vertrauenswürdigkeit** niedergelegt in einer **Vertrauenswürdigkeits-Agenda**

  ➔ in Verbindung mit einem **hochwertigen Reputationssystem** sowie

  ➔ einem anerkannten **Vertrauenswürdigkeits-Index**.

Vertrauenswürdigkeit *ist* ***nachweisbar*** *und* ***notwendig****,*
da der ***Aufbau von Vertrauen*** *der Schlüssel* ***zum Erfolg***
von ***IT- und IT-Sicherheitsunternehmen*** *ist.*

Prof. Dr. (TU NN)

Norbert Pohlmann

Professor für Cyber-Sicherheit *und*

Leiter des Instituts für Internet-Sicherheit - if(is)

Literatur

→ Auswahl

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
https://norbert-pohlmann.com/artikel/vertrauenswuerdigkeit-schafft-vertrauen/

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 u. künstliche Intelligenz – Wer macht die Spielregeln für die KI?", IT & Production/Zeitschrift für erfolgreiche Produktion, TeDo Verlag, 2019

Glossar Cyber-Sicherheit: https://norbert-pohlmann.com/glossar-cyber-sicherheit/vertrauenswuerdigkeit/

N. Pohlmann: **Lehrbuch „Cyber-Sicherheit",** Springer Vieweg Verlag, Wiesbaden 2022

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