Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Vertrauen und Vertrauenswürdigkeit

Prof. Dr. (TU NN)
Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet-sicherheit.

Vertrauen u. Vertrauenswürdigkeit
→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- Einleitung
- Vertrauenswürdigkeitsmodell
- Vertrauenswürdigkeit der IT-Lösung
- Vertrauenswürdigkeit des Unternehmens
- Vertrauenswürdigkeit von Domänen
- Zusammenfassung

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Vertrauen u. Vertrauenswürdigkeit
→ Inhalt

- **Ziele und Ergebnisse der Vorlesung**
- Einleitung
- Vertrauenswürdigkeitsmodell
- Vertrauenswürdigkeit der IT-Lösung
- Vertrauenswürdigkeit des Unternehmens
- Vertrauenswürdigkeit von Domänen
- Zusammenfassung

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Ziele und Ergebnisse der Vorlesung
→ Vertrauen u. Vertrauenswürdigkeit

- Gutes Verständnis dafür was **Vertrauen** und **Vertrauenswürdigkeit** ist.

- Erlangen der Kenntnis, was eine **wahrgenommenen Vertrauenswürdigkeit** für einen Nutzer bedeutet und wie damit Vertrauen zu angebotenen IT-Lösungen, zum Unternehmens (Hersteller …) und für die entsprechende Domäne aufgebaut werden kann.

- Verstehen, wie Vertrauen bei den Nutzern mithilfe von **Vertrauenswürdigkeit** umgesetzt werden kann und welche **Vorteile das für Hersteller** hat.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Vertrauen u. Vertrauenswürdigkeit
→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- **Einleitung**
- Vertrauenswürdigkeitsmodell
- Vertrauenswürdigkeit der IT-Lösung
- Vertrauenswürdigkeit des Unternehmens
- Vertrauenswürdigkeit von Domänen
- Zusammenfassung

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

→ **These:**

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

Daher ist es für DE- und EU-Unternehmen essenziell, sich über den ***Aufbau von Vertrauen*** *sowohl international als auch gegen internationale Unternehmen* ***nachhaltig zu positionieren****.*

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Vertrauen / Vertrauenswürdigkeit
→ Grundsätzlich

- **Vertrauen** bezeichnet die **subjektive Überzeugung** der **Richtigkeit von Handlungen**.
- **Vertrauen reduziert die Komplexität**, dadurch ist der Nutzer auch in einer *ungewissen* oder *unsicheren* Situation handlungsfähig.
- Dies kommt vor allem dann zum tragen, wenn der **Ausgang seiner 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.
- Die **Darstellung** der **Vertrauenswürdigkeit** der IT-Lösungen im Einzelnen sowie des Unternehmens insgesamt schafft **Vertrauen beim Nutzer**.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Interpersonales = institutionelles → 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 andere **Vertrauenswürdigkeitskriterien** nutzen, um **Nutzer** in die Lage zu versetzen, ihre **grundsätzliche Vertrauensfähigkeit** auf IT-Lösungen zu übertragen.
- Das **institutionelle Vertrauen** ist das **Ergebnis der 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 **Vertrauenswürdigkeit der Domäne** *(positiv)* beeinflusst werden *(siehe Modell).*

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Vertrauen und Vertrauenswürdigkeit
→ Notwendigkeit

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

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

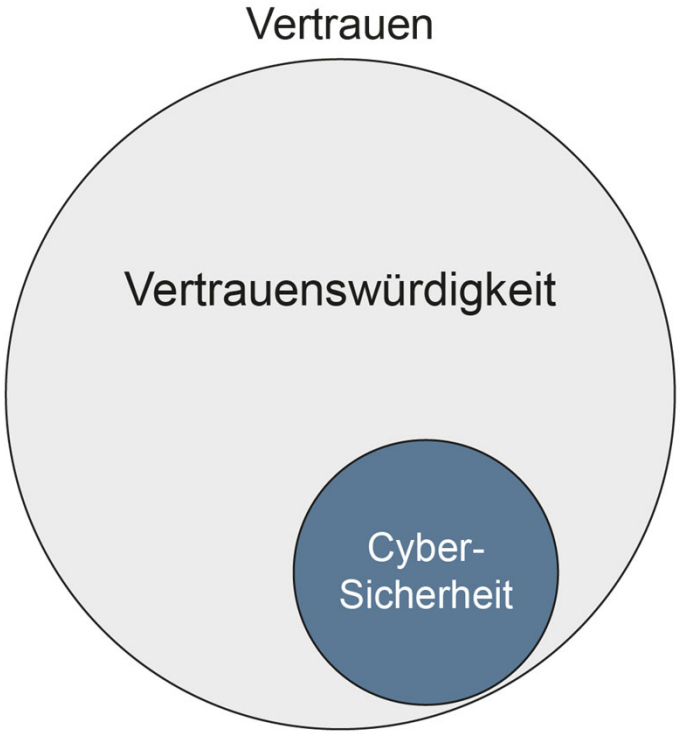
- Aus diesem Grund müssen Unternehmen alles tun, damit es einem Nutzer möglich ist einer **IT-Lösung** und dem **Unternehmen,** das diese herstellt, zu **vertrauen**.

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

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Vertrauen, Vertrauenswürdigkeit → und Cyber-Sicherheit

- **Vertrauen bedeutet,** das Unternehmen den Nutzern eine **Vertrauensgrundlage dahingehend bieten**, eine IT-Lösung trotz bestehender Risiken nutzen zu können.
- Die Umsetzung und Darstellung von **Cyber-Sicherheit** ist *ein* **wichtiger Bestandteil bei der Darstellung** der **Vertrauenswürdigkeit**, aber nicht der einzige.



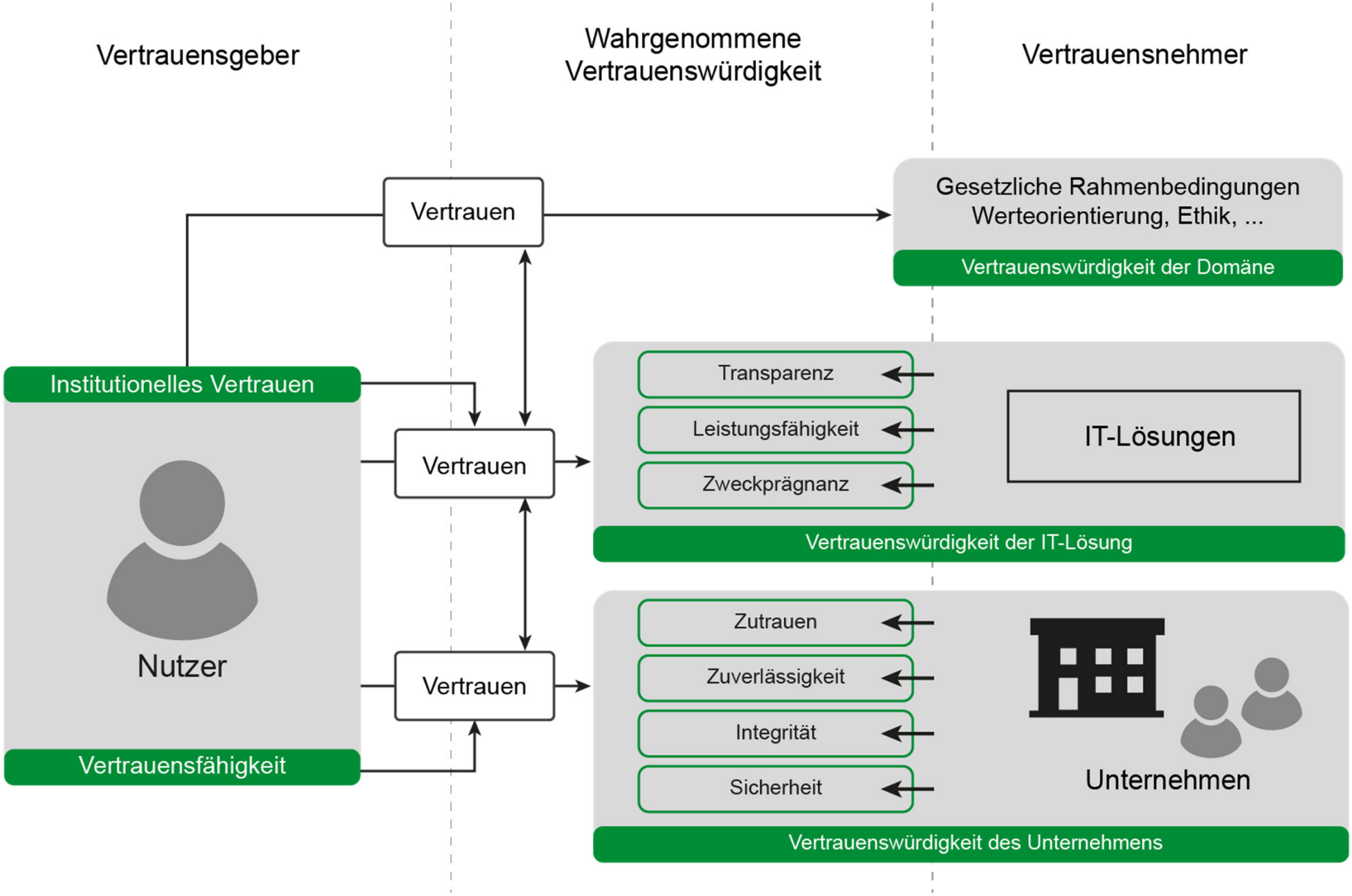
© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Vertrauen u. Vertrauenswürdigkeit
→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- Einleitung
- **Vertrauenswürdigkeitsmodell**
- Vertrauenswürdigkeit der IT-Lösung
- Vertrauenswürdigkeit des Unternehmens
- Vertrauenswürdigkeit von Domänen
- Zusammenfassung

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Vertrauenswürdigkeitsmodell
→ Übersicht



© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Vertrauenswürdigkeitsmodell
→ Definitionen von Begriffen (1/6)

Vertrauen, **Vertrauensgeber** und **Vertrauensnehmer**:

- Vertrauen bezeichnet unter anderem **die subjektive Überzeugung** der **Richtigkeit von Handlungen**.
- Grundsätzlich ist Vertrauen notwendig zur **Reduzierung von Komplexität** und immer dann erforderlich, wenn der Nutzer mit einer ungewissen oder unsicheren Situation konfrontiert wird oder der Ausgang seiner Handlung risikobehaftet sein kann.
- Das „Zulassen können“ des **Vertrauensgebers (Nutzer)** einem **Vertrauensnehmer (Unternehmen)** zu vertrauen, bedeutet daher die Bereitschaft den jeweiligen Vertrauensnehmer nicht infrage stellen zu wollen und sich damit einem bestimmten Risiko auszusetzen.
- Insbesondere bei IT-Lösungen ist ein wichtiger Aspekt, dass Vertrauen beim Nutzer in erster Linie aufgrund der Vertrauenswürdigkeit eines Unternehmens und/oder deren IT-Lösungen entstehen kann – also dadurch, dass Unternehmen als Vertrauensnehmer mit verschiedenen Maßnahmen eine **Vertrauensgrundlage schaffen**.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Vertrauenswürdigkeitsmodell
→ Definitionen von Begriffen (2/6)

Institutionelles Vertrauen: *(Teil 1)*

- Eine Grundvoraussetzung dafür, dass Menschen IT-Lösungen nutzen, ist das Versprechen eines Mehrwerts.
- Das bedeutet im Umkehrschluss, wenn für die Nutzer kein Wertzuwachs durch deren Einsatz entsteht, sind sie kritischer in ihrer Beurteilung und dadurch weniger bereit, sich auf das jeweilige Produkt per se zu verlassen.
- Darüber hinaus müssen Unternehmen weitere Maßnahmen ergreifen, um Nutzer in die Lage zu versetzen, ihre grundsätzliche Vertrauensfähigkeit auf IT-Lösungen zu extendieren.
- Das kann ermöglicht werden, indem es gelingt, interpersonales Vertrauen – also das Vertrauensverhältnis, das aufgrund bestimmter eigener Kriterien zwischen Menschen entsteht – auf IT-Lösungen zu übertragen.
- Dabei ist es wichtig zu beachten, dass im Verhältnis zwischen zwei Personen Vertrauen aufgrund der Fähigkeit zur Empathie aufgebaut wird und die individuell relevanten Kriterien direkt nachprüfbar sind.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Vertrauenswürdigkeitsmodell
→ Definitionen von Begriffen (3/6)

Institutionelles Vertrauen: *(Teil 2)*

- Diese Option ist in Bezug auf IT-Lösungen nicht gegeben, allein unter dem Aspekt, dass sich deren **Verhalten** beziehungsweise **Funktionsweise nicht** unbedingt **nachprüfen lässt**.
- Das **institutionelle Vertrauen** ist das **Ergebnis der erfolgreichen Transferleistung**, also inwieweit Nutzer fähig und auch dazu bereit sind, ihr Vertrauen auf Institutionen wie etwa Unternehmen zu übertragen.
- Dieses Vertrauen kann in erster Linie durch das Unternehmen selbst, über die IT-Lösung sowie auch über die Vertrauenswürdigkeit der Domäne (positiv) beeinflusst werden.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Vertrauenswürdigkeitsmodell
→ Definitionen von Begriffen (4/6)

Wahrgenommene Vertrauenswürdigkeit:

- Vertrauenswürdigkeit basiert auf der Annahme, dass es möglich ist, sich auf etwas Bestimmtes verlassen zu können.
- Im Regelfall beruht die wahrgenommene Vertrauenswürdigkeit auf offensichtlichen Funktionalitäten der IT-Lösung und Maßnahmen des Unternehmens, die dem Nutzer als Vertrauensgeber entweder aufgrund des ersten Eindrucks oder aus eigener Erfahrung oder über Dritte bekannt sind.
- Daran wird deutlich, dass es für **Unternehmen** zunehmend **wichtig** wird, **eine Vertrauensgrundlage zu schaffen**, indem sie relevante Aspekte der Vertrauenswürdigkeit sowohl für die IT-Lösung als auch das Unternehmen **explizit darstellen**, damit die Nutzer **Vertrauen aufbauen** können.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Vertrauenswürdigkeitsmodell
→ Definitionen von Begriffen (5/6)

Vertrauensfähigkeit:

- Grundsätzlich ermöglicht diese Personen oder auch Unternehmen zu vertrauen beziehungsweise ihnen etwas zuzutrauen.
- Basierend auf der individuellen Prägung eines Menschen oder dessen Vorerfahrung ist die Fähigkeit dazu unterschiedlich dominant.
- In diesem Sinne hat die **wahrgenommene Vertrauenswürdigkeit** einen **Einfluss** auf die **Vertrauensfähigkeit des Nutzers** und kann sich positiv auf diese auswirken.

Unternehmen:

- Sind Hersteller oder Anbieter von IT-/Sicherheits-Technologien, -Produkten oder -Diensten, die auch als IT-Lösungen zusammengefasst werden.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Vertrauenswürdigkeitsmodell
→ Definitionen von Begriffen (6/6)

Nutzer:

- Darunter sind im Allgemeinen alle Nutzer von IT-/Sicherheits-Technologien, -Produkten oder -Diensten subsummiert, also auch Anwenderunternehmen.

IT-Lösung:

- Im Kontext der Cyber-Sicherheit ist eine IT-Lösung eine allgemeine Anwendung mit entsprechenden **Cyber-Sicherheitsmechanismen** oder ein **Cyber-Sicherheitssystem**.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Vertrauenswürdigkeitsmodell
→ Wichtige Punkte

- **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.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

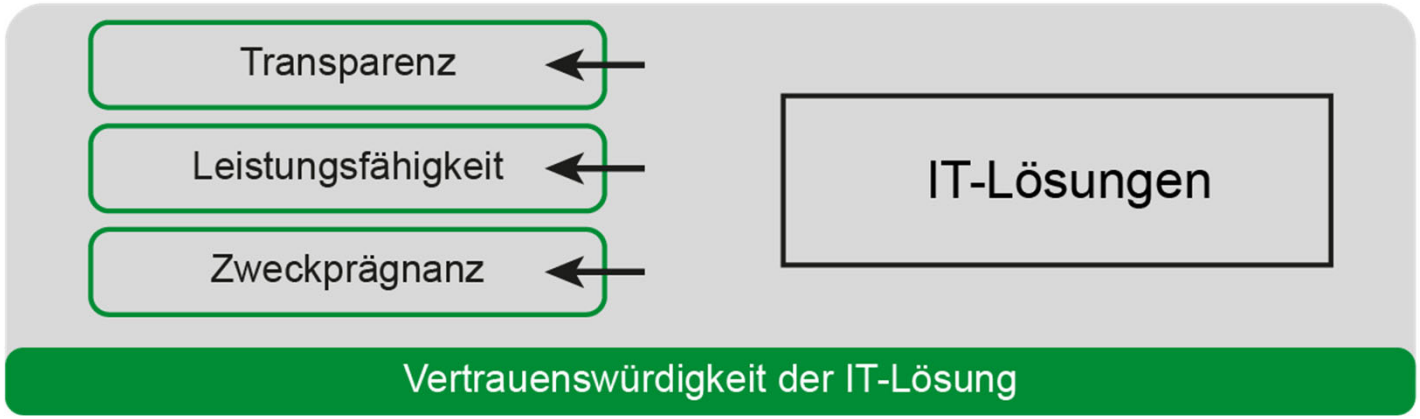
Vertrauen u. Vertrauenswürdigkeit
→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- Einleitung
- Vertrauenswürdigkeitsmodell
- **Vertrauenswürdigkeit der IT-Lösung**
- Vertrauenswürdigkeit des Unternehmens
- Vertrauenswürdigkeit von Domänen
- Zusammenfassung

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Vertrauenswürdigkeit der IT-Lösung
→ Übersicht

Wahrgenommene Vertrauenswürdigkeit



- **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.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

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

- Für den Nutzer ist es aufgrund der zunehmend intelligenten Angriffe und komplexeren Cyber-Sicherheitsmechanismen zunehmend 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 Transparenz:

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

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

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

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 Leistungsfähigkeit:

- ***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)*.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

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

- Die Zweckprägnanz manifestiert sich im **Verwendungszweck der IT-Lösung**.

- Für Unternehmen bedeutet dies, dass bei der Entwicklung von **Funktionen** sowie die **Intention** der IT-Lösung **zielgenau definiert** sind.

Beispiele für Zweckprägnanz:

- ***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.*

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

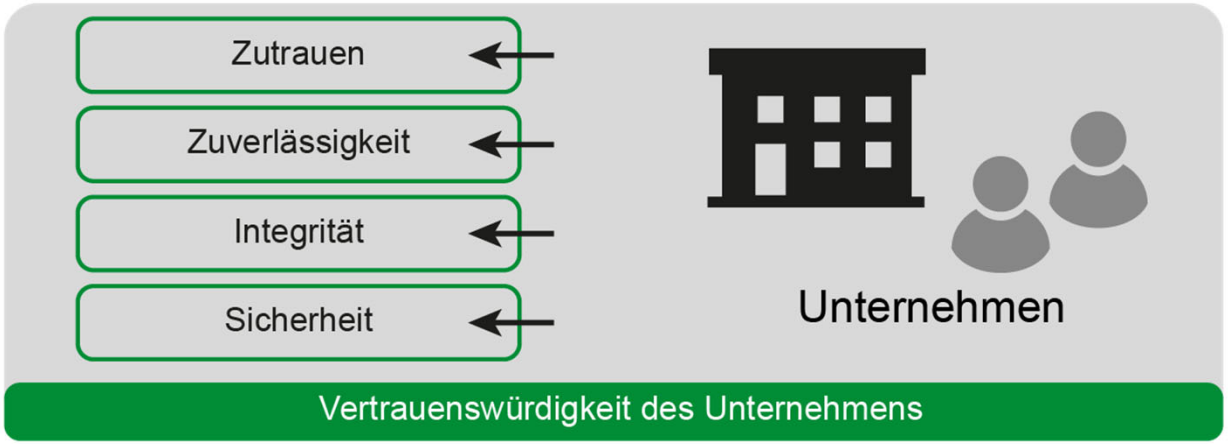
Vertrauen u. Vertrauenswürdigkeit
→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- Einleitung
- Vertrauenswürdigkeitsmodell
- Vertrauenswürdigkeit der IT-Lösung
- **Vertrauenswürdigkeit des Unternehmens**
- Vertrauenswürdigkeit von Domänen
- Zusammenfassung

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Vertrauenswürdigkeit des Unternehmens → Übersicht

Wahrgenommene Vertrauenswürdigkeit



- **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**.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

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 Zutrauen:

- ***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 / 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**.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

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 Zuverlässigkeit:

- ***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.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

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 Integrität:

- ***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.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Vertrauenswürdigkeit des Unternehmens → Aspekt: Sicherheit des Unternehmens

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

Beispiele für Sicherheit:

- ***Darstellung der verwendeten Cyber-Sicherheitsmaßnahmen:*** Aufzeigen, was sie tun, um die IT-Lösung und ihr Unternehmen zu schützen.
- ***Zertifizierung der IT-Lösung/Unternehmen:*** Die **Zertifizierung** der IT-Lösung aber auch des Unternehmens ist eine wichtige **Maßnahme zur Vertrauensbildung**.
- ***Regelmäßige Überprüfung der Produkte 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.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

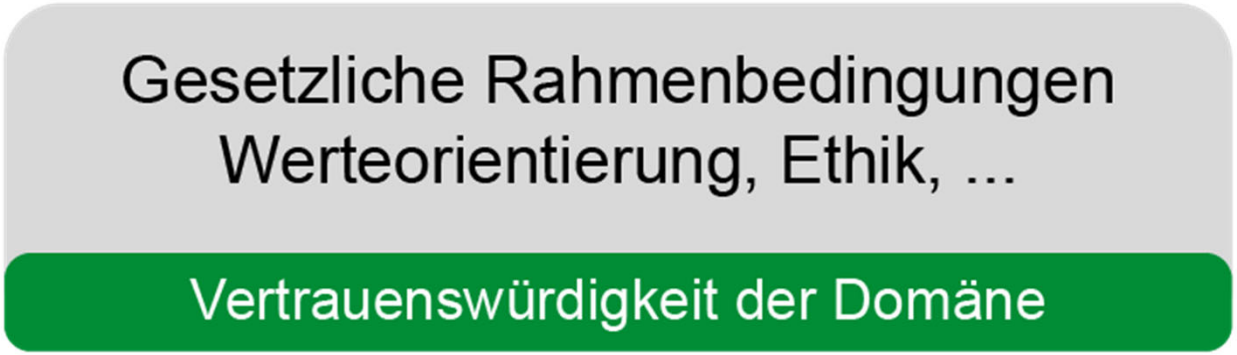
Vertrauen u. Vertrauenswürdigkeit
→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- Einleitung
- Vertrauenswürdigkeitsmodell
- Vertrauenswürdigkeit der IT-Lösung
- Vertrauenswürdigkeit des Unternehmens
- **Vertrauenswürdigkeit von Domänen**
- Zusammenfassung

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Vertrauenswürdigkeit von Domänen
→ Übersicht

Wahrgenommene Vertrauenswürdigkeit



- **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.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Vertrauenswürdigkeit von Domänen
→ Beispiele für Domänen

- ***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:*** Self-Sovereign Identities (SSI), GAIA-X … **Souveräne Technologie**, die unseren **Wertevorstellungen** entsprechen.

- ***Etablierung eines gemeinsamen Vertrauenssiegels:*** Gütesiegel helfen den Unternehmen, ihre Vertrauenswürdigkeit darzustellen.
  Ein Beispiel für ein **Vertrauenssiegel ist „IT Security – Made in Germany“**.

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

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Vertrauen u. Vertrauenswürdigkeit
→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- Einleitung
- Vertrauenswürdigkeitsmodell
- Vertrauenswürdigkeit der IT-Lösung
- Vertrauenswürdigkeit des Unternehmens
- Vertrauenswürdigkeit von Domänen
- **Zusammenfassung**

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

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.

- Anhand des **Vertrauenswürdigkeitsmodells** ist es möglich, die **Vertrauenswürdigkeit** der *IT-Lösung*, eines *Unternehmens* sowie der *Domäne* zu **dokumentieren**.

- *Das von uns angestrebte **Ziel***
  Der Aufbau eines **Vertrauenswürdigkeitssystems** basierend auf der Darstellung der **wahrgenommenen Vertrauenswürdigkeit** in Verbindung mit einem **hochwertigen Reputationssystem** sowie einem anerkannten **Vertrauenswürdigkeitsindex**.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Vertrauen *und* Vertrauenswürdigkeit

***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

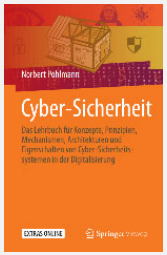
Professor** für **Informationssicherheit
Leiter** des **Instituts für Internet-Sicherheit - if(is)
Vorstandsmitglied** des **Verbands der Internetwirtschaft - eco
Vorstandsvorsitzender** des **Bundesverbands IT-Sicherheit - TeleTrusT

if(is) internet-sicherheit.

Anhang / Credits

Wir empfehlen

- **Cyber-Sicherheit**
  Das **Lehrbuch** für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung“, Springer Vieweg Verlag, Wiesbaden 2022
  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/

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Literatur

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/

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen