Westfälische Hochschule

Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Security Awareness

Prof. Dr. (TU NN)

Norbert Pohlmann

Professor** für **Cyber-Sicherheit** und **Leiter** des **Instituts für Internet-Sicherheit – if(is), Westfälische Hochschule, Gelsenkirchen

Vorstandsvorsitzender Bundesverband IT-Sicherheit - TeleTrusT

Vorstand im Verband der Internetwirtschaft - eco

if(is)
internet-sicherheit.

Social Engineering
→ Beschreibung

- **Social Engineering** ist eine ***Beeinflussung auf zwischenmenschlicher Ebene*** mit dem Ziel, bei **Personen** ***bestimmte Verhaltensweisen zu initiieren***, die diese eigentlich **nicht durchführen wollen**.

- **Social Engineers**
  - **spionieren** das persönliche Umfeld ihres Opfers aus,
  - **täuschen Identitäten vor** *oder*
  - nutzen Verhaltensweisen wie **Autoritätshörigkeit** aus,

  um z.B. **vertrauliche Informationen** wie Passworte, Kreditkarteninformationen, Patentinformationen oder auch unbezahlte Dienstleistungen **zu erlangen**.

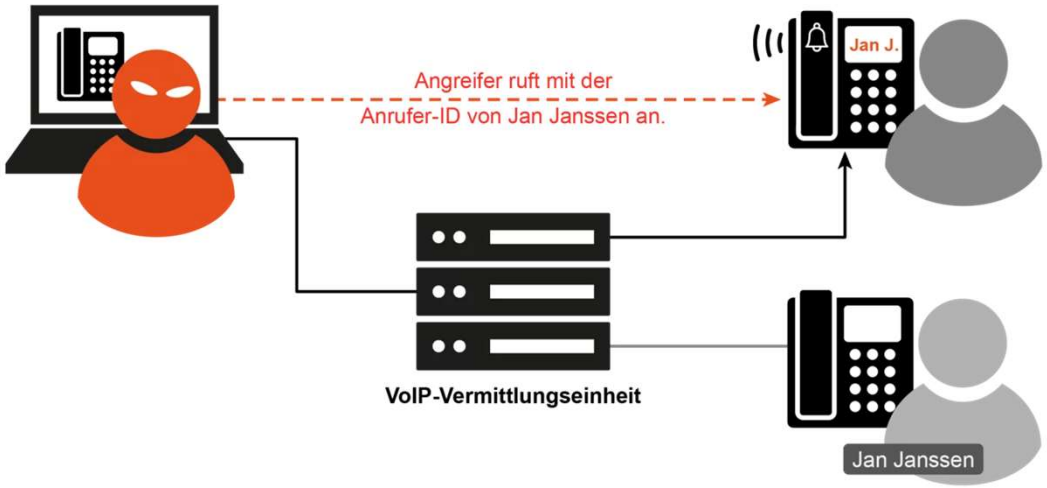
- Häufig dient Social Engineering dem **Eindringen in ein fremdes IT-System**, um vertrauliche Daten einzusehen, zu manipulieren oder alles zu verschlüsseln (Ransomware-Angriff).
- Oft wird dieser Vorgang auch **Social Hacking** genannt.

ChatGPT – KI in allen Ausprägungen
→ Fortschrittliches Social Engineering

- Die Tatsache, dass ChatGPT **menschenähnliche Texte formuliert** macht Betrug mittels **Social Engineering** wesentlich **einfacher** (Spear-Phishing).

- In Kombination mit *KI-generierten* **Bilder von Personen**, ***Audio-Imitationen*** und **Deepfake-Videos** stehen den Angreifern Techniken zur Verfügung, um moderne Social Engineering-Ansätze sehr gut und einfach umzusetzen.

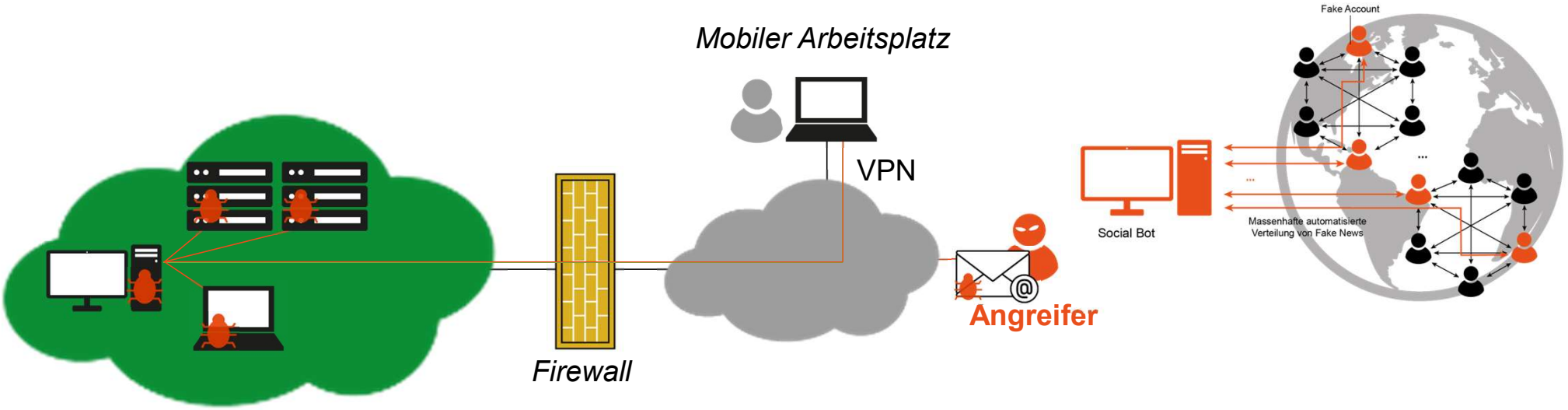
- Ideal für **CEO-Angriffe**.



Anrufer-ID-Spoofing

Social Engineering
→ Erster Schritt - Advanced Persistent Threat (APT)

Angreifer erlangt VPN-Zugang mithilfe von ***Social Engineering*** / ***Phishing*** / ***Malware***
*(Typischer Angriffsvektor: **Ransomware**)*



Social Engineering
→ Beispiele von speziellen Methoden / Begriffe

- **Pretexting**
  - Das besondere an Pretexting ist die **kreative Art und Weise des Angreifers**.
  - Der Angreifer nutzt einen erfundenen Vorwand (“Pretext”) oder interessante Geschichten, um einen Menschen dazu bewegen, Dinge zu tun, die er normalerweise nicht macht.
  - Psychologische Tricks, die Angreifer nutzen, um beim Pretexting das Vertrauen des Opfers zu gewinnen, sind zum Beispiel als **Autoritätsperson aufzutreten** oder **fürsorglich und helfend zu agieren**.
  - Dabei wird das Opfer auf einer **emotionalen Ebene** angesprochen.
  - Der Angreifer spielt eine überzeugende Rolle, der das Opfer ungerechtfertigterweise Glauben schenkt. Beispiele: Enkeltrick, Heiratsschwindel, Kryptowährungs-Betrug …
- **Doxing**
  - Unter Doxing wird grundsätzlich das **intensive und systematische internetbasierte Zusammentragen** und unter anderem die anschließende Veröffentlichung **sensibler privater Daten** verstanden.
  - Ziele sind auch, die privaten Informationen für einen Social Engineering Angriff zu verwenden oder die betroffene Person **zu beeinflussen**, **einzuschüchtern**, **zu erpressen**, **zu mobben**.

Social Engineering
→ Einschätzung

- Also Social Engineering nutzt unsere ***menschlichen Unzulänglichkeiten*** aus, um unsere Unternehmen und deren IT-Systeme anzugreifen!

- **Psychologische Tricks** sind z.B. die Ausnutzung von **Autoritätshörigkeit, Panikmache**, **Druck machen** oder **Angst auslösen**.

- Wichtig ist noch festzuhalten, dass **Social Engineering sehr erfolgreich** umgesetzt wird, d.h. wir fallen darauf herein und die **Social Hacker** haben **viel Erfahrungen** und sind in der Regel auch **sehr gut vorbereitet**.

- **Schäden von Social Engineering Angriffe:**
  - **CEO-Betrug** (Schaden nur in den USA)
    - 2,3 Milliarden US-Dollar Schaden durch CEO-Betrugsmasche
    - 17.000 Opfer
  - **Ransomware** (Schaden nur in Deutschland)
    - Mehr als 20 Milliarden Euro

Security Awareness
→ Beschreibung (1/2)

- **Security Awareness** bedeutet **Sicherheitsbewusstsein**

- Sicherheitsbewusstsein ist das ***Wissen*** und die ***Einstellung***, die Mitarbeiter einer Organisation zum **Schutz der IT einer Organisation** mit allen ihren Werten ***besitzen***.
  - **Wissen**
    - über die **Werte** einer Organisation, die zu schützen sind,
    - den **Schutzbedarf** der Werte
    - **Bedrohungen**, die auf diese Werte wirken,
    - organisatorische **Regelungen**, die einzuhalten sind,
    - richtige Nutzung von **IT-Sicherheitsmaßnahmen** zum Schutz der Werte,
    - usw.

  - **Einstellung**
    - bedeutet, dieses **Wissen zu verinnerlichen** und **zum Schutz der Organisation** ***aktiv*** umzusetzen.

Security Awareness
→ Beschreibung (2/2)

- In der Regel beinhaltet Security Awareness ***verschiedene Schulungsmaßnahmen***, um Mitarbeiter einer Organisation für Themen rund um die Sicherheit der IT-Systeme zu sensibilisieren, auch für die Gefahren von Social Engineering.

- **Ziel** ist es, die durch Mitarbeiter *verursachten* **Gefahren für die IT-Sicherheit** zu **minimieren**.

- Also ***Security Awareness*** soll die Mitarbeiter auch ***davor schützen auf Social Hacking reinzufallen!***

- **Security Awareness Markt:**
  - 2023 war der Markt 5.6 Milliarde Dollar groß.
  - Wachstum auf **10 Milliarden Dollar bis 2027** (15 % Wachstum im Jahr)

Der Mensch im Mittelpunk
→ Social Engineering/Security Awareness

Sowohl **Security Awareness** sowie **Social Engineering** ***adressieren uns als Menschen***, nur beide Aspekte wollen genau das **Gegenteil** erreichen.

Resilienz

Viel Erfahrung und sehr gute Vorbereitung

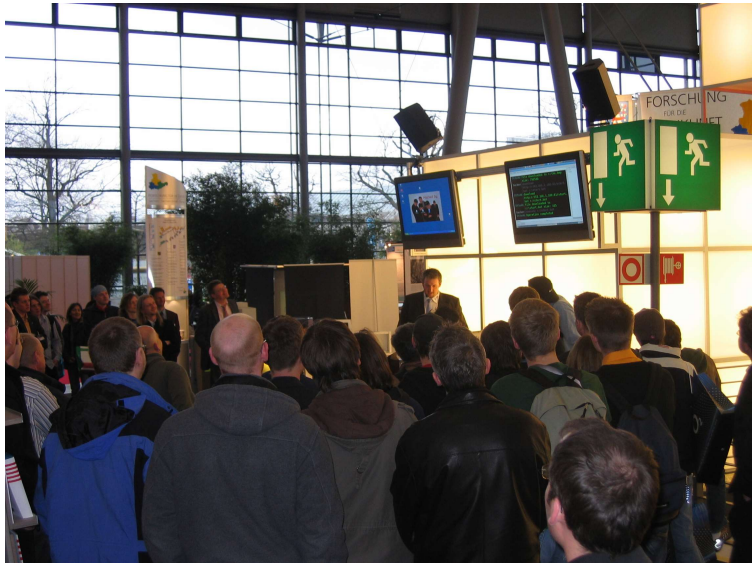
Selbstlernangebot IT-Sicherheit - SecAware

→ das kostenlose Selbstlernangebot, nicht nur für Hochschulen

- SecAware ist ein **maßgeschneidertes Online-Selbstlernangebot**, das ca. 750.000 Studierenden und ca. 50.000 akademischem Personal in NRW mit essenziellem Wissen und Fertigkeiten im Bereich IT-Sicherheit ausstatten soll.
- Projektpartner:
  Institut für Internet-Sicherheit – if(is) – **Kompetenz: IT-Sicherheit**
  Institut für Digitalisierung von Arbeits- u. Lebenswelten – **Kompetenz: Didaktik**
- **20 Themen** (weitere folgen in den nächsten 2 ½ Jahren):
  (Spear)-Phishing, Passwörter, MFA, Social Engineering, Fake Websites, Verschlüsselung, Netzwerke, Backup, Updates, Social Media, Messenger, Heimarbeitsplatz …
- Vierklang aus **Videos**, **Quizzes**, **interaktiven Elementen** und **Zusatzmaterial**
- Auch auf dem **Marktplatz IT-Sicherheit** kostenlos verfügbar:
  https://it-sicherheit.de/ratgeber/selbstlernangebot-it-sicherheit/

SecAware nrw

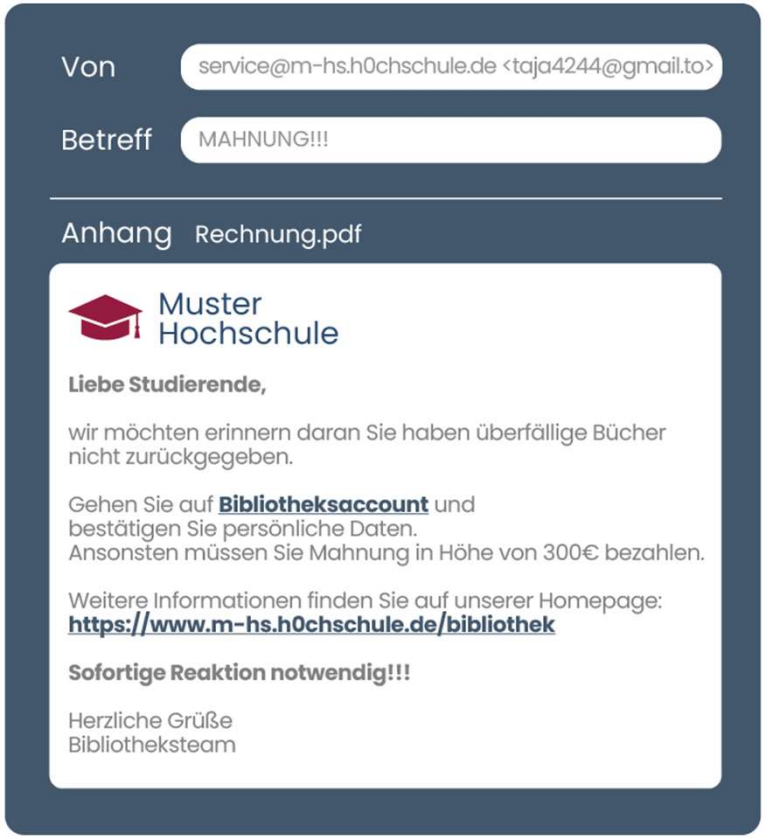
Live Hacking & Cyber Security Shows
→ Mit Unterhaltung Sicherheitsbewusstsein schaffen



- **600+** Live Hacking & Cyber Security Shows mit 12 unterschiedlichen Hackern vom Institut für Internet-Sicherheit - if(is) umgesetzt.
- Es wird aufgezeigt, wie **Hacker arbeiten**, **denken** und **vorgehen**, um Daten zu stehlen, Prozesse zu stören und Schaden zu verursachen.
- Ein **Zusammenspiel** zwischen dem **naiven Nutzer** und dem **erfolgreichen Hacker**.

Die Grenzen der Awareness
→ Beispiel Spear-Phishing-E-Mail

- Die **Unterscheidung** zwischen einer **Business**- und **Spear-Phishing-E-Mail** wird immer schwerer.
  - Durch KI perfekte Auswertung von Inhalten (Input Soziale Netze)
  - Durch ChatGPT perfekte Texterstellung (perfekt angepasste Tonalität, in jeder Sprache)
  - …

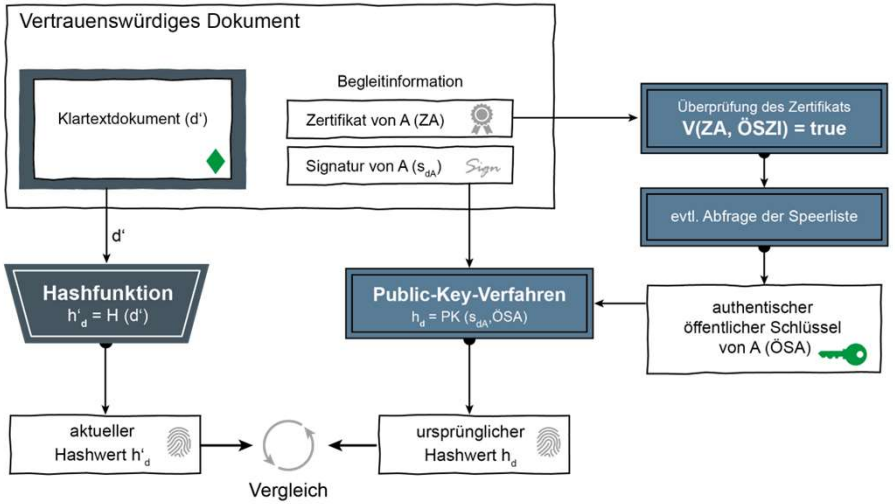


(Alte Spear-Phishing-E-Mail)

Die Grenzen der Awareness
→ Digitale Signaturen helfen

- Wir sollten Business-E-Mails **digital unterschreiben**.
- Dann kann der Empfänger sehr einfach feststellen, vom wem die E-Mail kommt.

  → **Das entlastet uns Nutzer sehr.**



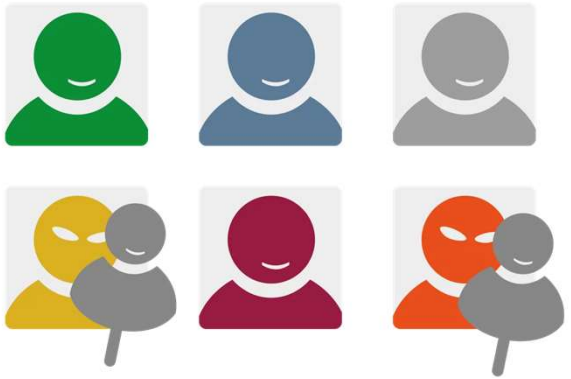
- Wir benötigen immer **mehr IT-Sicherheitstechnologie**, damit wir als Nutzer in der Lage sind, sicherheitsbewusst unsere Aufgaben risiko-ärmer umsetzen zu können.

  → Nur, diese **IT-Sicherheitstechnologie** müssen dann auch **richtig genutzt** werden.

  → Dies muss als ein **neuer Schwerpunkt** im Rahmen von Security Awareness umgesetzt werden.

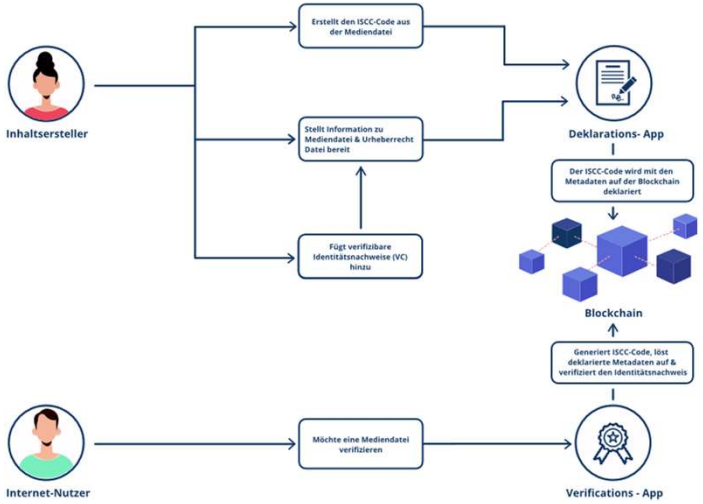
Zukünftige Herausforderungen
→ Beispiele

- **Deepfake in Videokonferenzen**
  - Identifikation / Authentifikation der Teilnehmer bei einer Videokonferenzen
    - eIDAS könnte helfen



- **Fake News**
  - Deklaration von Nachrichten (Signatur, Zertifikate, Rechte …)
  - Projekt: Trust Media

    https://trust-media.it/



Westfälische Hochschule

Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Security Awareness

Wir brauchen sicherheitsbewusste Nutzer!

Wir brauchen aber immer IT-Sicherheitstechnologien, die die Nutzer unterstützen.

Prof. Dr. (TU NN)

Norbert Pohlmann

Professor** für **Cyber-Sicherheit** und **Leiter** des **Instituts für Internet-Sicherheit – if(is), Westfälische Hochschule, Gelsenkirchen

Vorstandsvorsitzender Bundesverband IT-Sicherheit - TeleTrusT

Vorstand im Verband der Internetwirtschaft - eco

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.

Glossar Cyber-Sicherheit

https://norbert-pohlmann.com/category/glossar-cyber-sicherheit/

Cyber-Sicherheit GLOSSAR

It‘s all about Trust!

https://vertrauenswürdigkeit.com/

Quellen Bildmaterial

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

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/

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/

Literatur

N. Pohlmann, S. Schmidt: „Der Virtuelle IT-Sicherheitsberater – Künstliche Intelligenz (KI) ergänzt statische Anomalien-Erkennung und signaturbasierte Intrusion Detection“, IT-Sicherheit – Management und Praxis, DATAKONTEXT-Fachverlag, 05/2009

D. Petersen, N. Pohlmann: "Ideales Internet-Frühwarnsystem", DuD Datenschutz und Datensicherheit – Recht und Sicherheit in Informationsverarbeitung und Kommunikation, Vieweg Verlag, 02/2011

M. Fourné, D. Petersen, N. Pohlmann: “Attack-Test and Verification Systems, Steps Towards Verifiable Anomaly Detection“. In Proceedings der INFORMATIK 2013 - Informatik angepasst an Mensch, Organisation und Umwelt, Hrsg.: Matthias Horbach, GI, Bonn 2013

U. Coester, N. Pohlmann: „Verlieren wir schleichend die Kontrolle über unser Handeln? Autonomie hat oberste Priorität“, BI-SPEKTRUM Fachzeitschrift für Business Intelligence und Data Warehousing, 05-2015

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: „Künstliche Intelligenz und Cybersicherheit – Diskussionsgrundlage für den Digitalgipfel 2018“ https://norbert-pohlmann.com/app/uploads/2018/12/Künstliche-Intelligenz-und-Cybersicherheit-Diskussionsgrundlage-für-den-Digitalgipfel-2018-Prof.-Norbert-Pohlmann.pdf

N. Pohlmann: „Künstliche Intelligenz und Cybersicherheit - Unausgegoren aber notwendig“, IT-Sicherheit – Fachmagazin für Informationssicherheit und Compliance, DATAKONTEXT-Fachverlag, 1/2019

U. Coester, N. Pohlmann: „Wie können wir der KI vertrauen? - Mechanismus für gute Ergebnisse“, IT & Production – Zeitschrift für erfolgreiche Produktion, Technik-Dokumentations-Verlag, Ausgabe 2020/21

D. Adler, N. Demir, N. Pohlmann: „Angriffe auf die Künstliche Intelligenz – Bedrohungen und Schutzmaßnahmen“, IT-Sicherheit – Mittelstandsmagazin für Informationssicherheit und Datenschutz, DATAKONTEXT-Fachverlag, 1/2023

P. Farwick, Pohlmann: „Chancen und Risiken von ChatGPT – Vom angemessenen Umgang mit künstlicher Sprachintelligenz“, IT-Sicherheit – Mittelstandsmagazin für Informationssicherheit und Datenschutz, DATAKONTEXT-Fachverlag, 4/2023

N. Pohlmann: Lehrbuch „Cyber-Sicherheit“, Springer Vieweg Verlag, Wiesbaden 2022
Druckausgabe (ISBN 978-3-658-36242-3) und eBook (ISBN 978-3-658-36243-0).

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