Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Fakes, Malware, Security:
→ Können die Sicherheitslücken geschlossen werden?

Prof. Dr. (TU NN)
Norbert Pohlmann
Vorstandsmitglied eco – IT-Sicherheit
***Professor** für **Cyber-Sicherheit** und*
Leiter** des **Instituts für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen

if(is) internet-sicherheit.

Thesen
→ IT-Sicherheit

Wir können **nicht alle Sicherheitslücken** schließen!

Wir müssen ein **angemessenes Risiko** *erreichen*, um das **Vertrauen in die digitale Zukunft** zu erzielen.

Wenn wir bei der **zunehmenden Digitalisierung** nicht im passenden Umfang die **IT-Sicherheit beachten**, fällt und das auf die Füße.

Cyber-Sicherheitslage
→ Einschätzung

- ***Die Cyber-Sicherheitsprobleme werden immer größer***

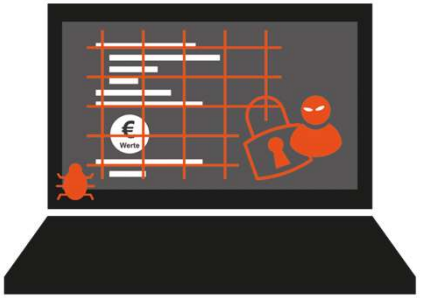
- **IT-Systeme** und **-Infrastrukturen** sind **nicht sicher genug konzipiert, aufgebaut, konfiguriert** und **upgedatete um den Angriffen intelligenter Hacker erfolgreich entgegenzuwirken.**

- **Weitere Herausforderungen mit der fortscheitenden Digitalisierung:**
  - *IT-Systeme und -Infrastrukturen werden **immer komplexer** (Steigerung der Abhängigkeiten… Supply-Chain… Facebook-Problem…)*
    - **Angriffsfläche wird größer**
  - *Die **Methoden der Angreifer** werden **ausgefeilter***
    - **Kriminelles-Ökosysteme**
  - ***Angriffsziele** werden **kontinuierlich lukrativer** (Digitalisierung)*
    - **mehr digitale Werte**

- ***Steigende Risiken führen zu höheren Schäden***

Lage der IT-Sicherheit in DE 2023
→ BSI-Bericht (1/2)

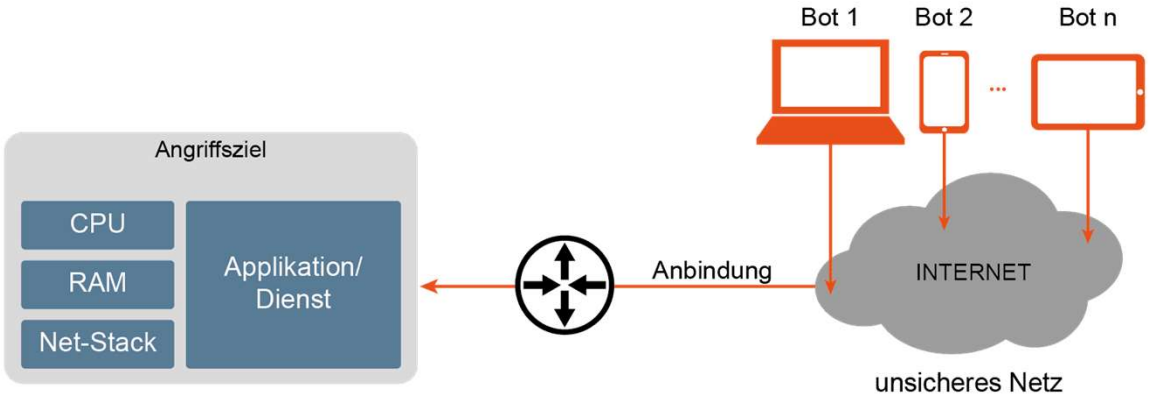
- Die bereits ***angespannte IT-Sicherheit-Lage*** spitzt sich weiter zu.
- **Die Bedrohung im Cyber-Raum ist so hoch wie nie.** ***„Alarmstufe Rot+“***
- *Ransomware ist die Hauptbedrohung, insbesondere für Unternehmen.*



- **Big Game Hunting,** die Erpressung umsatzstarker Unternehmen mit verschlüsselten und exfiltrierten Daten**, hat weiter zugenommen.**
- *Aber nicht nur Unternehmen sind Ziel von Ransomware-Angriffen.*
- Mit dem **folgenschweren Angriff auf eine Landkreisverwaltung** in Sachsen-Anhalt wurde **wegen eines Cyber-Angriffs der Katastrophenfall ausgerufen.**
  - *Bürgernahe Dienstleistungen waren über 207 Tage lang nicht oder nur eingeschränkt verfügbar.*

Lage der IT-Sicherheit in DE 2022
→ BSI-Bericht (2/2)

- **DDoS-Angriffe sind um 42 Prozent angestiegen.**
  (schwarzer Freitag)



- **Zahl der Schwachstellen in Software steigt um 10 Prozent.**
  (mehr Software durch die Digitalisierung, höher Identifizierung durch die kriminellen Organisationen …)

Die höhe der Schäden
→ IT-Sicherheitsbudget

- Je höher die Investition in IT-Sicherheit, je geringer der Schaden. (BSI-Studie)

- **Ausgaben für IT-Sicherheit:**
  - Die **Ausgaben für IT-Sicherheit** von den Ausgaben für Informationstechnologien liegen zurzeit bei **6,4 %**
  - Das **Ziel** sollte mindestens **10 %**, besser **15 %** sein.

Was sind die Herausforderungen?
→ 1. Privatheit und Autonomie

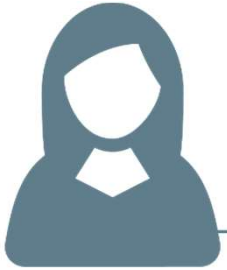
Verschiedene Perspektiven

Kulturelle Unterschiede
(Private Daten gehören den Firmen? US 76%, DE 22%)

Geschäftsmodell „Bezahlen mit persönlichen Daten“

Privatheit / Autonomie

Staat *(NSA, BND, …)*: Identifizieren von terroristischen Aktivitäten



Nutzer: Autonomie im Sinne der Selbstbestimmung

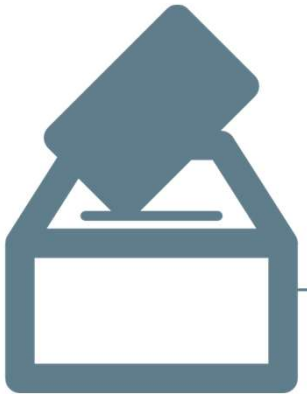
Was sind die Herausforderungen?
→ 2. Wirtschaftsspionage

ca. 220 Milliarden € Schaden pro Jahr

Wirtschaftsspionage

Zum Vergleich:
Internet-Kriminalität: ca. 100+ Millionen € pro Jahr
(Online Banking …)

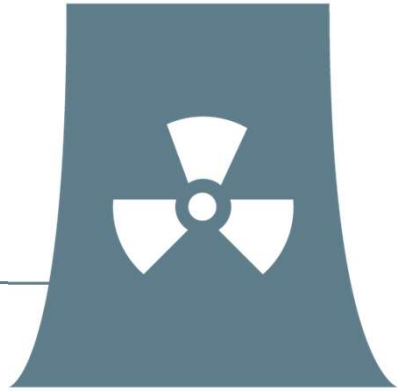
Was sind die Herausforderungen?
→ 3. Cyberwar



Umsetzung von politischen Zielen
→ „einfach“ und „preiswert“

Cyberwar

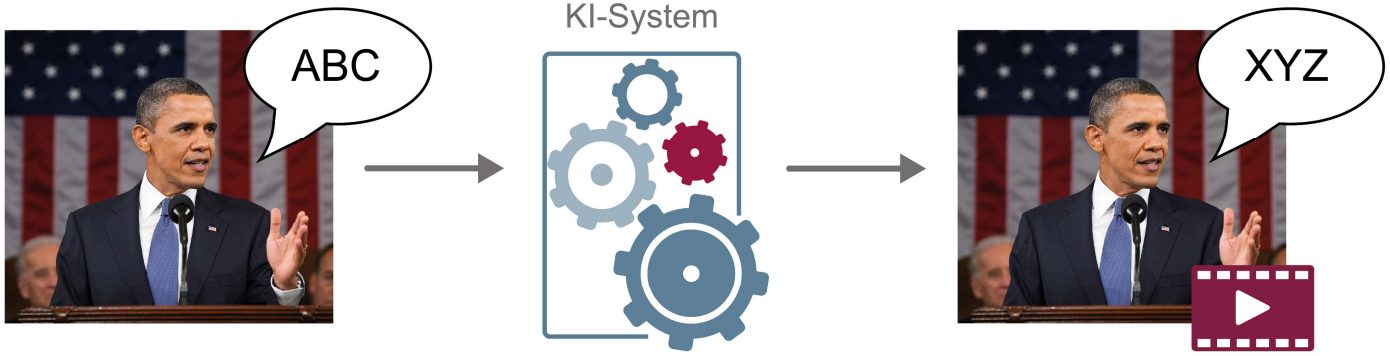
Angriffe auf Kritische Infrastrukturen
z.B. Stromversorgung, Wasserversorgung …



Deep-Fake
→ Gefahr Demokratie / hohes Sec-Risiko

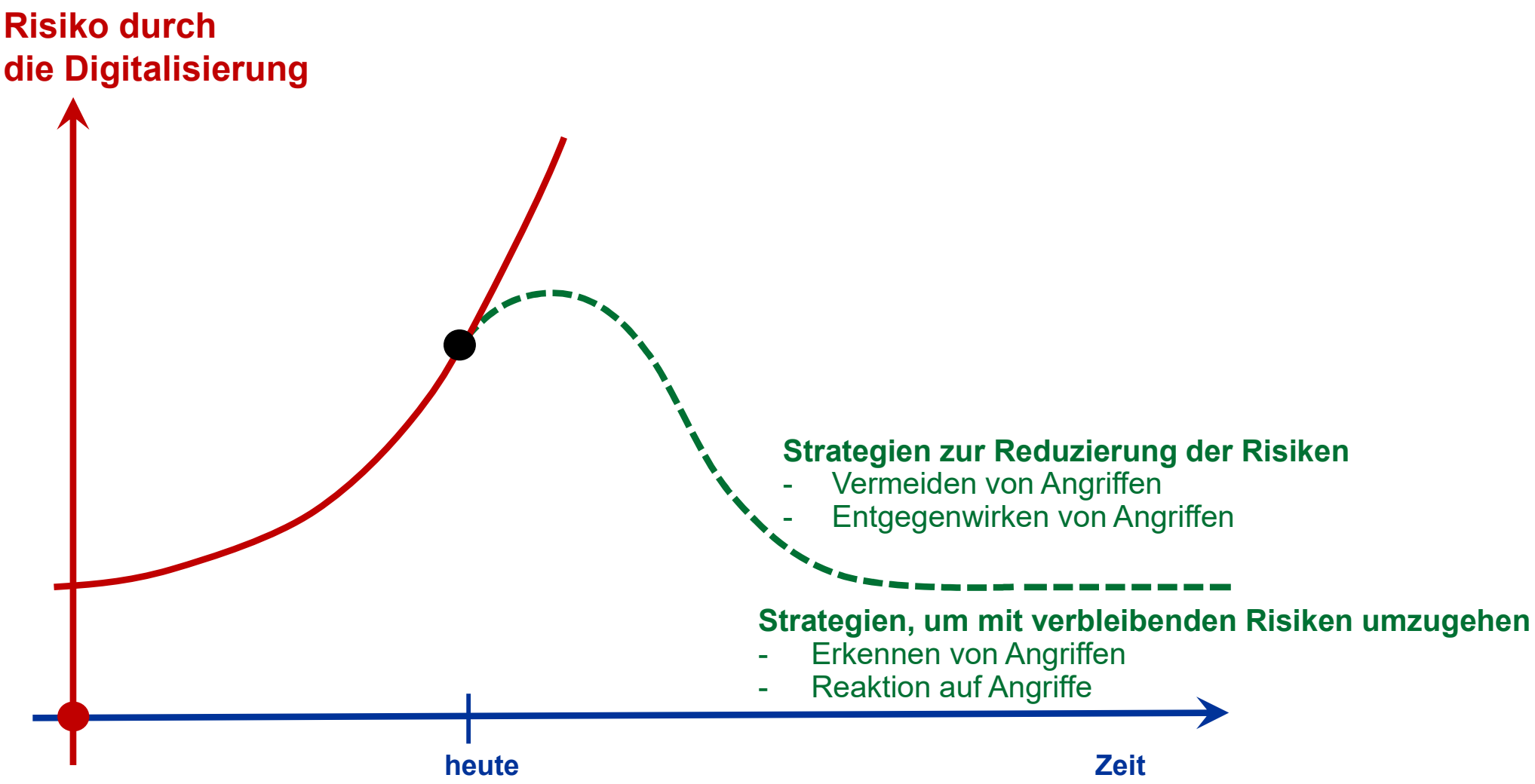
- **Bildgenerierende Systeme** können überzeugend mithilfe von **künstlicher Intelligenz (KI)** gestellte Videos (Deep-Fake-Video) erzeugen und damit Individuen oder ganze Personengruppen ***diffamieren***, zu ***Gewalt aufrufen*** und ***Chaos anstiften***.
  → Desinformationskampagnen und Cyber-Mobbing

- Ein normaler Nutzen kann ein Deep-Fake nicht von einem echten Video unterscheiden.



- Aber auch gefälschte Stimmen (**CEO-Fraud**) und Texte (**Phishing**)
  → Social Engineering

Cyber-Sicherheitsstrategien
→ Übersicht



Fakes, Malware, Security ...
→ Zusammenfassung

- Die **IT-Sicherheitsprobleme** werden **immer größer**
- **IT-Sicherheit** spielt mit dem **Grad der Digitalisierung** eine immer **größere Rolle**
- **Krisensituationen** verstärken die **Notwendigkeit** einer souveränen und vertrauenswürdigen **IT-Sicherheit**, insbesondere bei Kritischen Infrastrukturen.
- **IT-Sicherheitsstrategien** helfen auf verschiedenen Ebenen und Phasen, **Risiken zu reduzieren** und **verbleibende Risiken zu managen.**

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Fakes, Malware, Security:
→ Können die Sicherheitslücken geschlossen werden?

IT-Sicherheit
wird in der Zukunft immer wichtiger

Prof. Dr. (TU NN)
Norbert Pohlmann
Vorstandsmitglied eco – IT-Sicherheit
***Professor** für **Cyber-Sicherheit** und*
Leiter** des **Instituts für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen

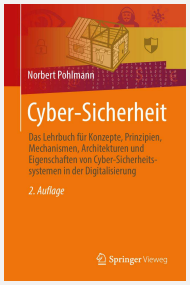
if(is) internet-sicherheit.

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/

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/

Quellen Bildmaterial

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

Literatur

M. Hesse, N. Pohlmann: „Kryptographie (I bis VII): Von der Geheimwissenschaft zur alltäglichen Nutzanwendung“, IT-Sicherheit & Datenschutz - Zeitschrift für rechts- und prüfungssicheres Datenmanagement, Vogel-Verlag, 06/2006

N. Heibel, M. Linnemann, N. Pohlmann: „Mehr Vertrauenswürdigkeit für Anwendungen durch eine Sicherheitsplattform", in "Trusted Computing - Ein Weg zu neuen IT-Sicherheitsarchitekturen”, Hrsg.: N. Pohlmann, H. Reimer; Vieweg-Verlag, Wiesbaden 2008

J. Fischer, N. Pohlmann: „Ein Quantum Bit. Quantencomputer und ihre Auswirkungen auf die Sicherheit von morgen“, IT-Sicherheit – Fachmagazin für Informationssicherheit und Compliance, DATAKONTEXT-Fachverlag, 1/2017

N. Pohlmann: „Wertschöpfung der Digitalisierung sichern - Vier Cybersicherheitsstrategien für den erfolgreichen Wandel in der IT“, IT-Sicherheit – Mittelstandsmagazin für Informationssicherheit und Datenschutz, DATAKONTEXT-Fachverlag, 1/2020

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/

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Institut für Internet-Sicherheit
→ Vorstellung und Übersicht

Prof. Dr. (TU NN)
Norbert Pohlmann
Vorstandsmitglied eco – IT-Sicherheit

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

if(is) internet-sicherheit.

Institut für Internet-Sicherheit
→ Prof. Norbert Pohlmann

Berufliche Erfahrungen: Unternehmer im Bereich IT-Sicherheit

- Geschäftsführender Gesellschafter der **KryptoKom** GmbH *(1988-1999)*
- Vorstandsmitglied der **Utimaco Safeware** AG *(1999-2003)*

Hauptamtliche Tätigkeiten: seit 2003

- **Informatikprofessor** für Cyber-Sicherheit *und*
- Geschäftsführender **Direktor des Instituts für Internet-Sicherheit** – if(is) an der Westfälische Hochschule

Ehrenämter:

- Vorstandsvorsitzender des **Bundesverbands IT-Sicherheit** – TeleTrusT
- Vorstandsmitglied des eco – **Verband der Internetwirtschaft** e.V.
- Vorstandsmitglied **EuroCloud** Deutschland_eco e.V.
- Mitglied des wissenschaftlichen Beirates der **GDD**
- Mitglied im Lenkungskreis Initiative „**IT-Sicherheit in der Wirtschaft**“ des BMWi
- Mitglied der Advisory Group der European Union Agency for Cypersecurity – **ENISA**
- …

Institut für Internet-Sicherheit
→ Übersicht

- Das Institut für Internet-Sicherheit - if(is) ist eine Fachbereich übergreifende, **wissenschaftliche Einrichtung der Westfälischen Hochschule,** im Fachbereich Informatik
- Gründung: 2005
- Wir haben uns zu dem **führenden Institut für Internet-Sicherheit** entwickelt!
- Seit WS10/11: **Master** „Internet-Sicherheit“
- Ca. 50 Mitarbeiter

- Unser **Ziel** ist es, einen Mehrwert an **Vertrauenswürdigkeit** und **Sicherheit** im Internet herzustellen.

Zahlen: 15+ Jahre if(is)

→ Übersicht

600+ Hacking-Shows
(mit 12 unterschiedlichen Hackern)

100 Forschungspartner
(Firmen/Behörden (65) und Hochschulen (35))

300+ Artikel / 400+ Vorträge / 30+ Bücher
(national und international)

150+ Fernsehauftritte
(Tagesschau/-themen, WDR, ZDF, SAT1, 3SAT, …)

200+ Abschlussarbeiten
(Diplom, Bachelor, Master und Promotionen)

200+ wissenschaftliche *und* studentische **Mitarbeiter** (zurzeit sind es mehr als 50)

60+ Drittmittelprojekte
mit Unternehmen / Behörden

150+ Zeitungsinterviews
(ZEIT, Focus, FAZ, Süddeutsche Zeitung, Handelsblatt, Welt, DPA, …)

53 Forschungsprojekte
(BMBF (20), BMWi (10), EU (4), NRW (15), BMI (4), …)

7 Cyber Security Challenges
Finden von IT-Sicherheitstalenten

Forschungsschwerpunkte im if(is) internet-sicherheit.

- Internet Frühwarnsysteme
- (Internet-)Kennzahlen-Sys.
- KI + Cyber-Sicherheit
- Zahlungssysteme und Banktransaktionen
- Blockchain
- Identity Management
- IoT Security
- Gesundheitswesen
- Vertrauenswürdige IT-Systeme
- Smart Grids, -Car, -Traffic
- Cloud, Fog, Edge Computing
- Mobile Security
- Botnetz-Erkennung