Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Cyber-Sicherheitsstrategien

Prof. Dr. (TU NN)
Norbert Pohlmann

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

if(is) internet-sicherheit.

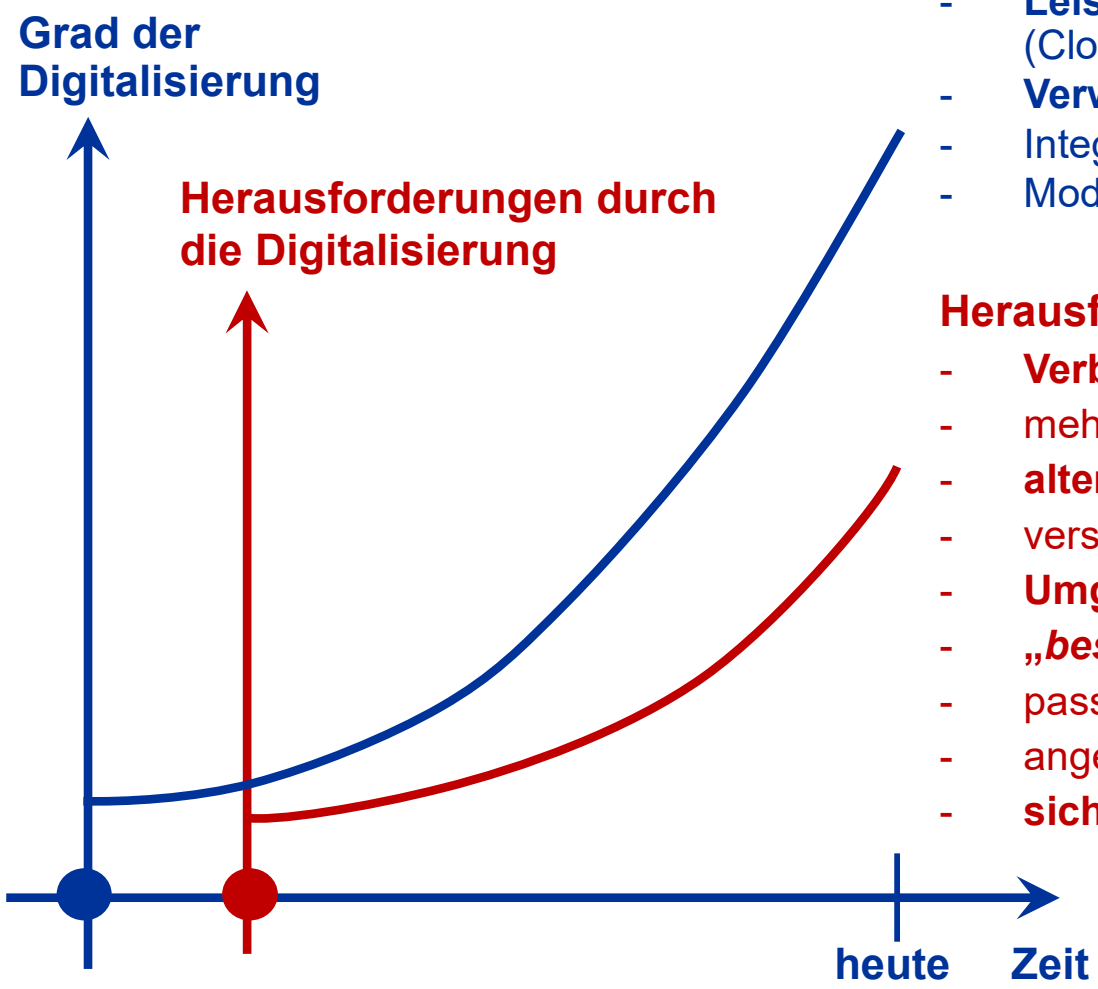
Cyber-Sicherheitslage
→ Einschätzung

- ***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… mehr Software … mehr Verbindungen … Supply-Chain… Facebook-Problem…)*
    - **Angriffsfläche wird größer**
  - *Die **Methoden der Angreifer** werden **ausgefeilter***
    - **Kriminelles-Ökosysteme**
  - ***Angriffsziele** werden **kontinuierlich lukrativer** (Digitalisierung)*
    - **mehr digitale Werte**

Entwicklung der Digitalisierung
→ Erfolgsfaktoren und Herausforderungen



Erfolgsfaktoren der **Digitalisierung** (Beispiele)

- **Kommunikationsinfrastruktur** (5G, Glasfaser, NB, CUG …)
- Smartheit der Endgeräte (Watch, Phone, Book/Pad, IoT …)
- **Leistungsfähigkeit zentraler IT-Systeme** (Cloud, Edge-Computing, Hyperscaler ...)
- **Verwendung von KI** (ML …)
- Integration in IT-Prozesse und IT-Systeme (echtzeitorientiert+)
- Moderne Benutzerschnittstellen (Sprache, Gestik …)

Herausforderungen Cyber-Sicherheit (Beispiele)

- **Verbesserung der Softwarequalität**
- mehr Schutz vor Malware, unsichere Webseiten, …
- **alternativen zu Passwörtern (MFA)**,
- verschlüsselte E-Mails, Kommunikation (IPSec, TLS …)
- **Umgang mit der Komplexität der IT-Systeme**, …
- **„*bessere*“ IT-Sicherheitsarchitekturen**
- passenden Level IT-Sicherheit (z.Z. nicht „Stand der Technik“)
- angemessene Verfügbarkeit
- **sichere Hardware** (Sicherheitsmodule in den Komponenten)

Was sind die Herausforderungen?
→ 1. Privatheit und Autonomie

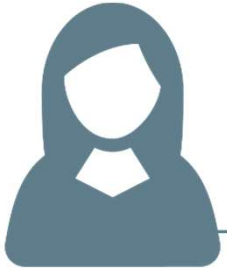
Verschiedenen Sichtweisen

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

Geschäftsmodelle „Bezahlen mit persönlichen Daten“

Privatheit / Autonomie

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



Nutzer: Autonomie im Sinne der Selbstbestimmung

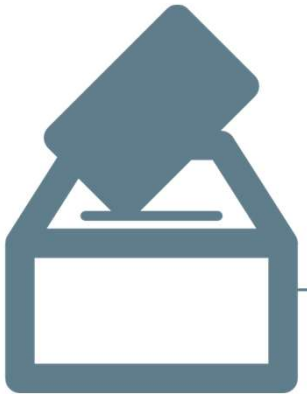
Was sind die Herausforderungen?
→ 2. Wirtschaftsspionage

ca. 220 Milliarden € Schaden pro Jahr

Wirtschaftsspionage

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

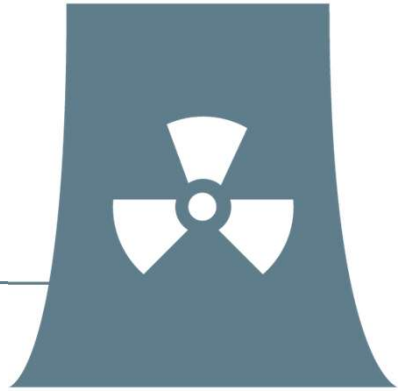
Was sind die Herausforderungen?
→ 3. Cyberwar



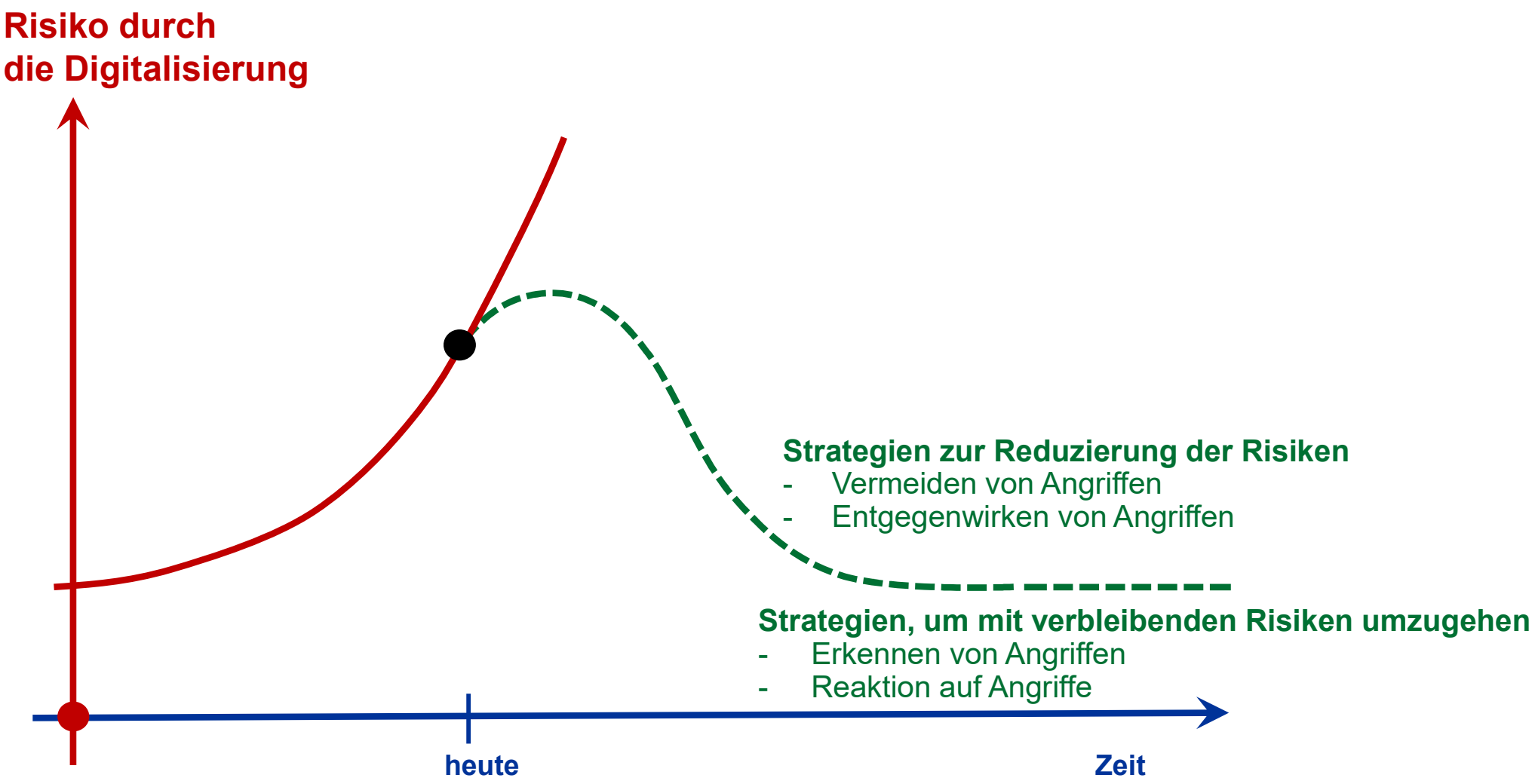
Umsetzung von politischen Zielen
→ „einfach“ und „preiswert“

Cyberwar

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



Cyber-Sicherheitsstrategien
→ Übersicht



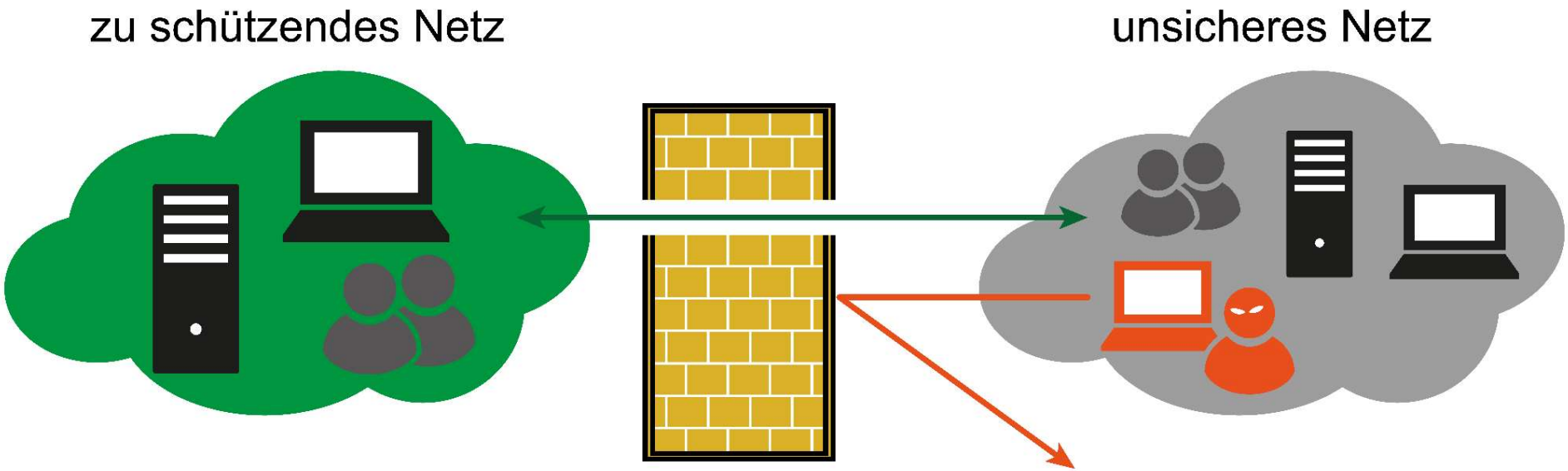
Prinzipielle IT-Sicherheitsstrategien
→ Vermeiden von Angriffen

- Mit Hilfe der Vermeidungsstrategie wird eine **Reduzierung der Angriffsfläche** und damit die **Reduzierung der Risiken** erreicht.
- Die Herausforderung besteht darin, **die IT so einzurichten**, dass das Unternehmen **alles wirklich *Notwendige*** für das Business **umsetzen** kann, aber **alles andere *aktiv* vermieden wird**.

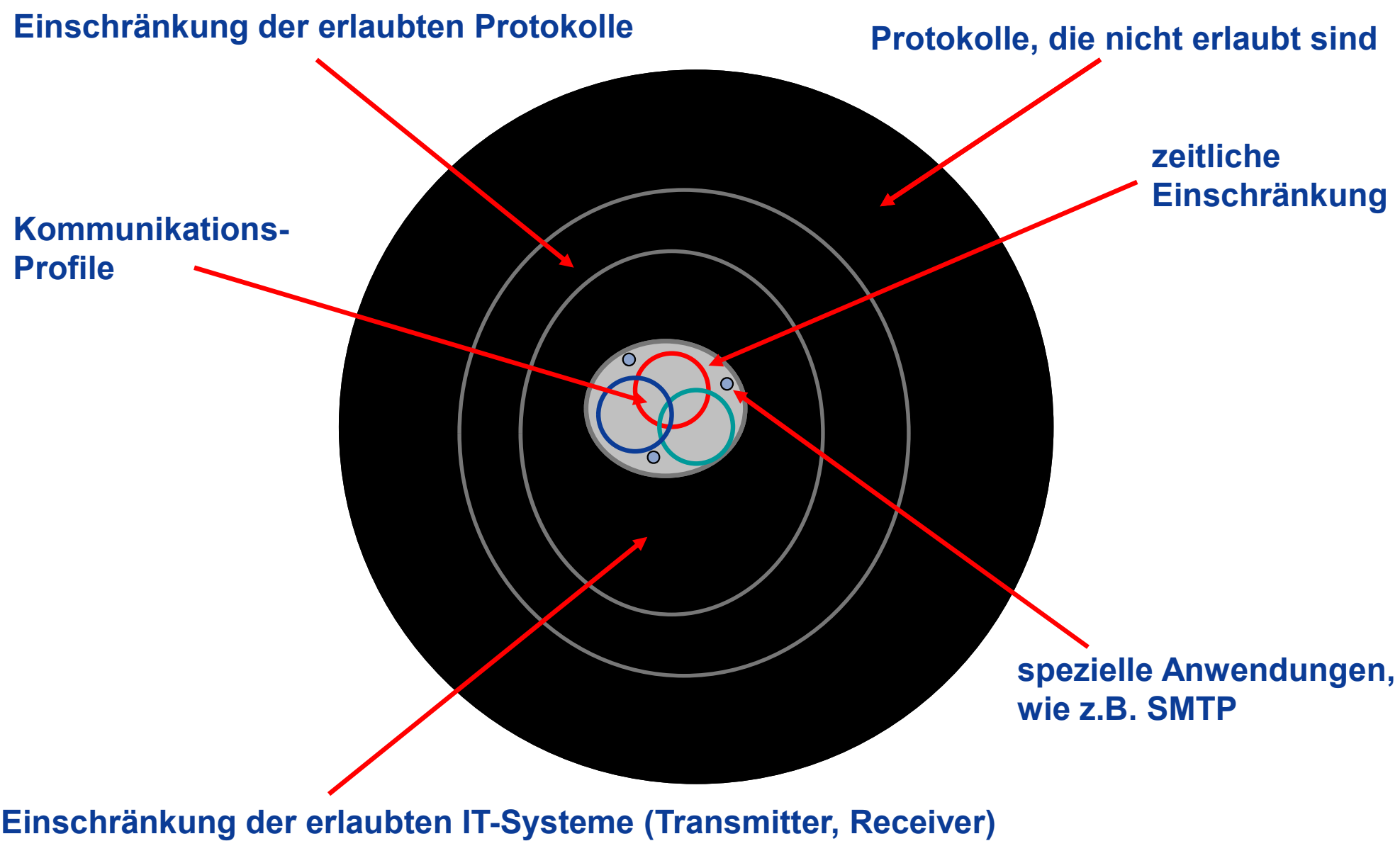
Cyber-Sicherheitsmechanismen

- ***Digitale Datensparsamkeit***
- ***Fokussierung*** *(ca. 5 % sind besondere schützenswert)*
- ***Nur sichere IT-Technologien, -Produkte und -Dienste verwenden***
- ***Reduzierung von IT-Möglichkeiten*** *(SW, Rechte, Kommunikation …)*
- ***Sicherheitsbewusste Mitarbeiter***

Sicherheitskonzept
→ Firewall-System



Kommunikationsmodell
→ Reduzierung des Schadensrisikos



Social Engineering
→ Beschreibung (1/2)

- **Social Engineering** ist eine ***zwischenmenschliche Beeinflussung*** mit dem Ziel, bei Personen ***bestimmte Verhaltensweisen hervorzurufen***, wie zum Beispiel, die **Personen zur Preisgabe von vertraulichen Informationen zu bewegen**.

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

  um **geheime Informationen** oder unbezahlte Dienstleistungen **zu erlangen**.

- Häufig dient Social Engineering dem Eindringen in ein fremdes IT-System, um vertrauliche Daten einzusehen.

- Oft wird dieser Vorgang auch **Social Hacking** genannt.

Social Engineering
→ Beschreibung (2/2)

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

- Wichtig ist auch 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**.

- **Durch ChatGPT effizientere Angriffe möglich**

Security Awarness
→ Beschreibung (1/2)

- **Security Awarness** 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 Awarness
→ Beschreibung (2/2)

- In der Regel beinhaltet Security Awarenes ***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 geht aber in der Regel deutlich weiter.

Prinzipielle IT-Sicherheitsstrategien
→ Entgegenwirken von Angriffen

- Das Entgegenwirken von Angriffen ist die meistverwendete Cyber-Sicherheitsstrategie, um das vorhandene Risiko zu minimieren und damit Schäden zu vermeiden.
- Dazu werden Cyber-Sicherheitsmechanismen verwendet, die eine **hohe Wirkung** gegen **bekannte Angriffe** zur Verfügung stellen und damit die Werte angemessen schützen.

Cyber-Sicherheitsmechanismen

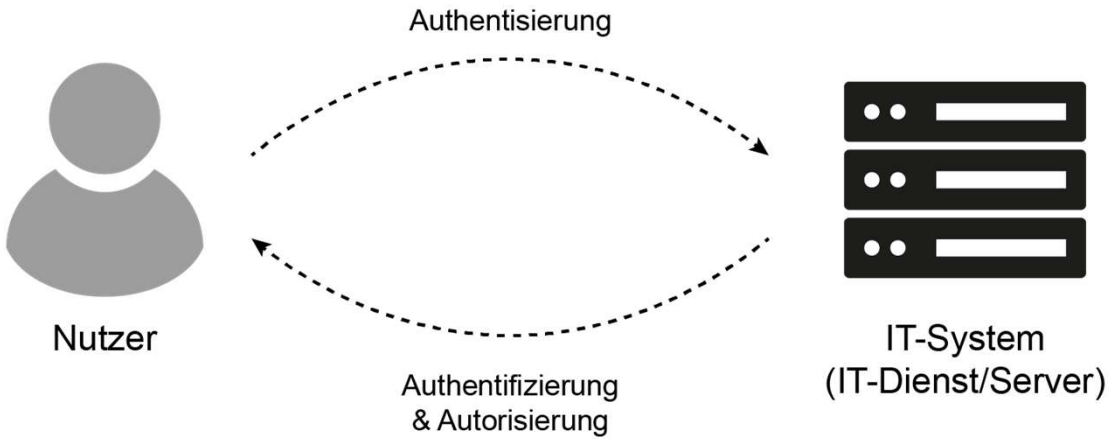
- ***Verschlüsselung*** *(in Motion, at Rest, in Use)*
- ***Multifaktor-Authentifikationsverfahren***
- ***Anti-Malware-Lösungen*** *(neue Konzepte)*
- ***Anti-DDoS-Verfahren*** *(gemeinsame Strukturen)*
- ***Zero Trust-Prinzipien*** *(TCB, Virtualisierung, Authentifikation aller Entitys …)*
- ***Confidential Computing*** *(Basis CPU, Daten/Code verschlüsselt/überprüft)*
- ***Digitale Signaturverfahren*** */ Zertifikate (E-Mail, SSI …) – PKI, BC*
- ***Hardware-Sicherheitsmodule*** *(Smartcard, TPM, HSM, Smartphone)*

Aktive Verschlüsselung
→ Wichtige Aspekte

- Verschlüsselung für einen **nachhaltigen Schutz der Daten (Kommunikation, Speicherung und Verarbeitung)**
  - **IPSec** (weniger als 1%), **TLS** (80 %)… *(Kommunikation)*
  - **E-Mail-Verschlüsselung** (weniger als 5%) , **Chat** ... *(Kommunikation)*
  - Festplatten-, Datei-Verschlüsselung … *(Speicherung)*
  - Confidential Computing *(Verarbeitung)*

- **Voraussetzungen:**
  - **Vertrauenswürdige Verschlüsselungstechnologie**
    (Keine Backdoors, starke Zufallszahlen, korrekte Implementierung …)
    → *Sehr leistungsstarke IT-Sicherheitsindustrie in D*
    → *IT Security made in Germany*
  - **Vertrauenswürdige IT-Sicherheitsinfrastruktur**
    (PKI mit RA und CA; Root-Zertifikate, …)

Identifikation und Authentifikation
→ Die Herausforderung



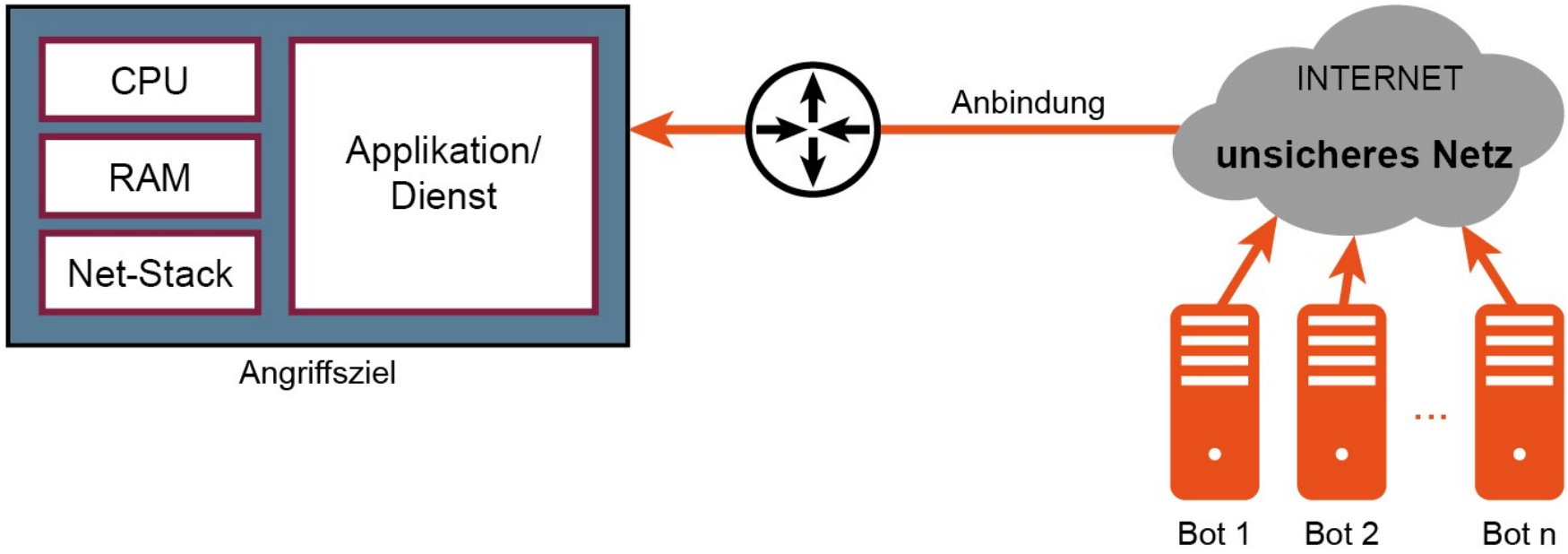
- **Authentisierung:** (Sichtweise Nutzer)
  Der **Nutzer** authentisiert sich gegenüber einem IT-System (Endgerät, Server, IT-Dienst, Cloud, …), indem er einen **Nachweis *(Wissen, Besitz, Sein)*** über seine **digitale Identität**, zum Beispiel den Nutzernamen (E-Mail-Adresse), **erbringt**.

- **Authentifizierung:** (Sichtweise IT-System)
  Das **IT-System** (Endgerät, Server, IT-Dienst, Cloud, …) **überprüft den Nachweis**, um die **Echtheit der digitalen Identität** eines Nutzers im Rahmen der Authentifizierung **festzustellen**.

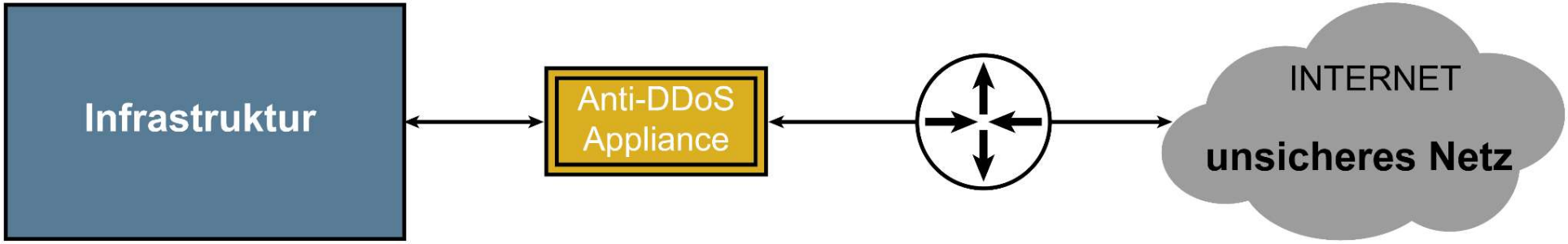
- **Autorisierung:** (Sichtweise IT-System)
  Wenn die Echtheit der digitalen Identität eines Nutzers erfolgreich verifiziert werden konnte, kann das IT-System (Endgerät, Server, IT-Dienst, Cloud, …) dem **Nutzer definierte Rechte einräumen**.

DDoS-Angriffe
→ Ziel: Gezielte Überlastung

Ziel eines DDoS-Angriffes:
Ausgesuchte IT-Systeme koordiniert mit einer großen Last spezieller Anfragen durch **Erschöpfung** der verfügbaren Ressourcen
- CPU
- RAM
- Bandbreite
lahmzulegen

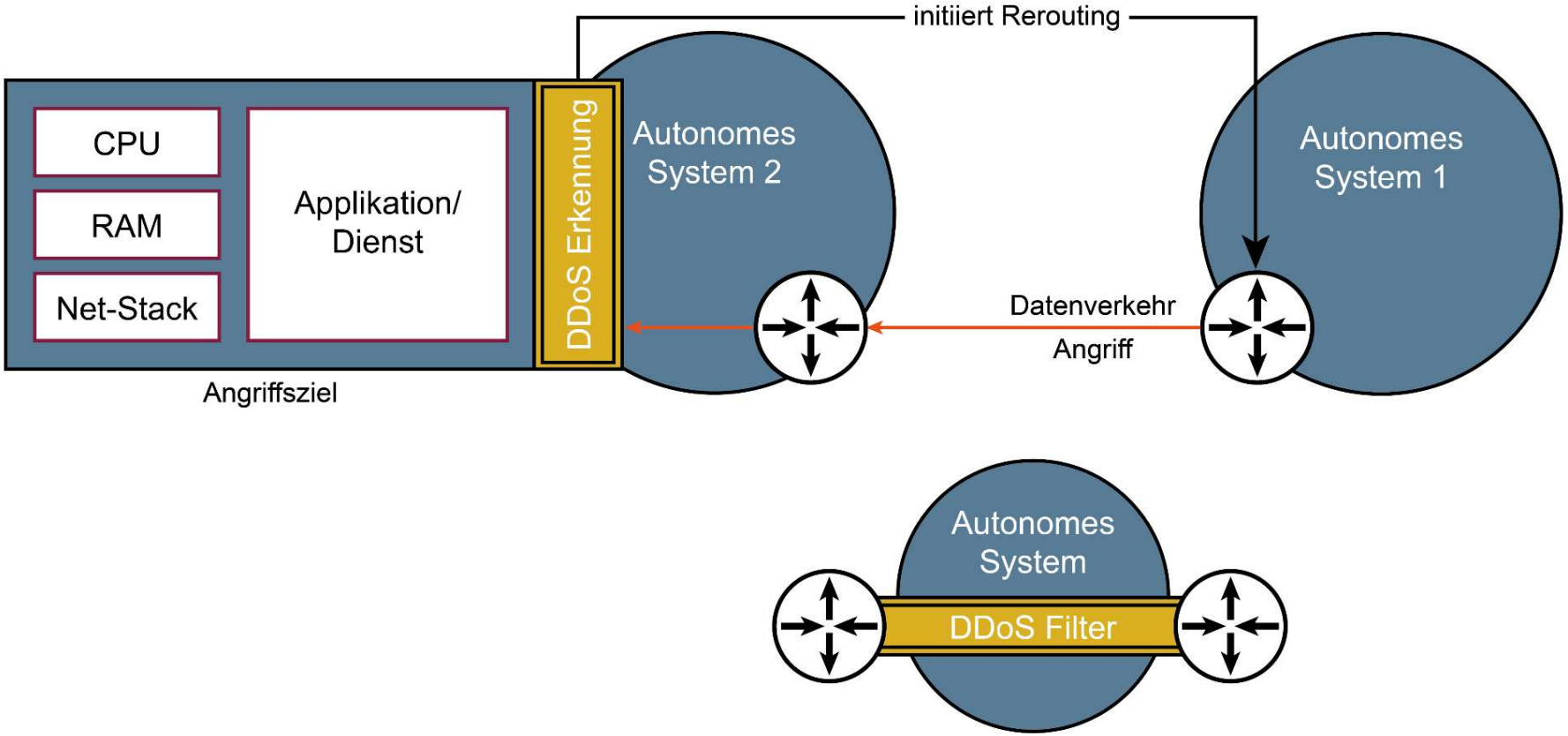


Abwehrstrategien
→ On-Site: Anti-DDoS Appliance



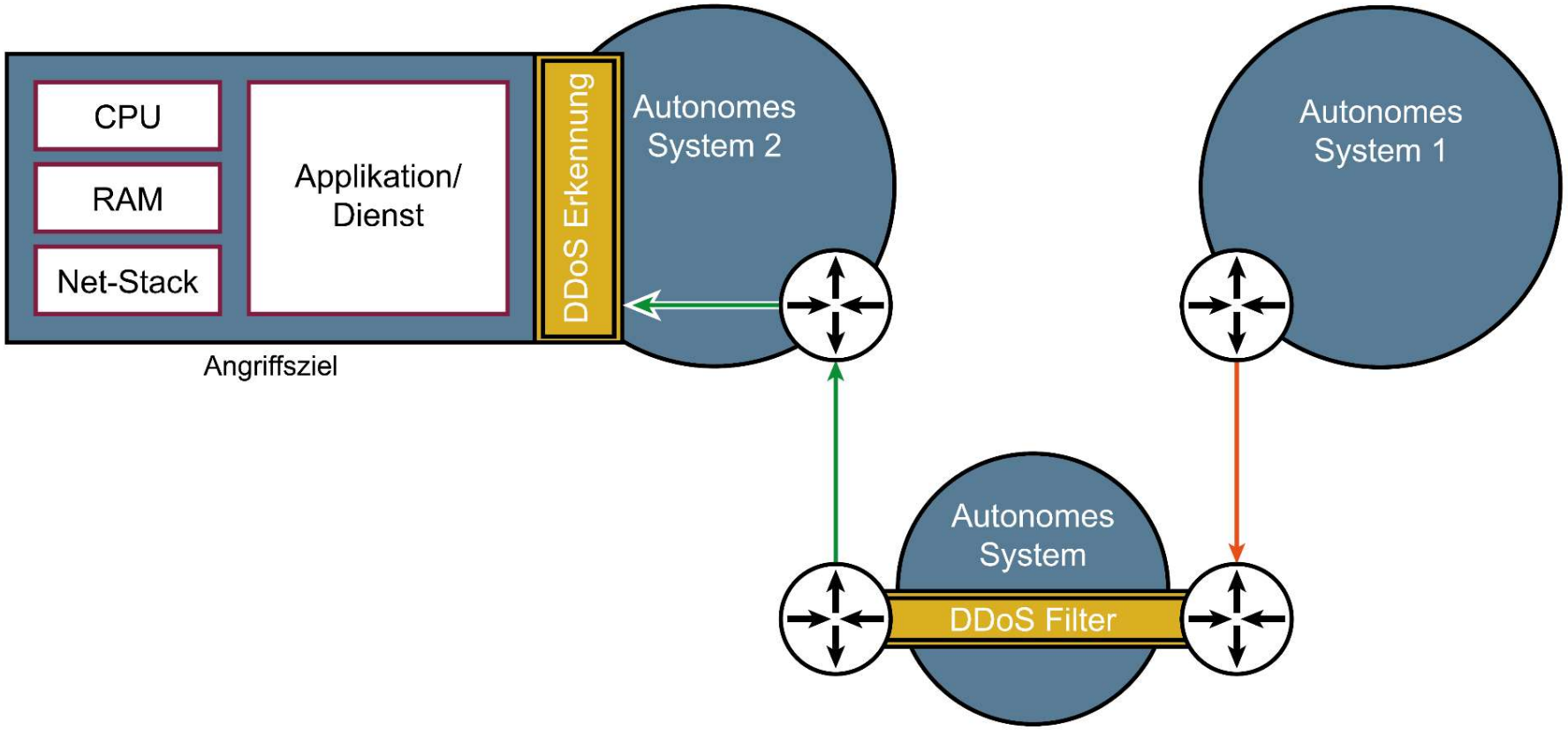
Abwehrstrategien
→ Off-Site: Traffic-Scrubbing-Netze

- **Der Schutzmechanismus:**
  Die Filtertechnik steht bei einem DDoS-Angriff im Hot-Standby.



Abwehrstrategien
→ Off-Site: Traffic-Scrubbing-Netze

- Nur wenn der DDoS-Erkennungsfilter einen Angriff feststellt, wird der Datenverkehr per Netz-Announcement über das Filternetz geroutet.



Paradigmenwechsel

→ Mehr proaktive statt reaktive IT-Sicherheit (1/2)

Reaktive IT-Sicherheitssysteme

- Bei reaktiven IT-Sicherheitssystemen rennen wir den **IT-Angriffen hinterher**!

- Das bedeutet, ***wenn*** wir einen **Angriff erkennen**, ***dann*** versuchen wir uns so schnell wie möglich zu **schützen**, um den Schaden zu reduzieren.

- **Beispiele für reaktive Sicherheitssysteme sind:**
  - *Firewall-Systeme*
  - *Intrusion Detection*
  - *Anti-Malwareprodukte*
  - *Anti-Spam /-Phishing, …*

„Airbag-Methode“

Wenn‘s passiert, soll es weniger „weh tun“

Paradigmenwechsel

→ Mehr proaktive statt reaktive IT-Sicherheit (2/2)

Proaktive Sicherheitssysteme

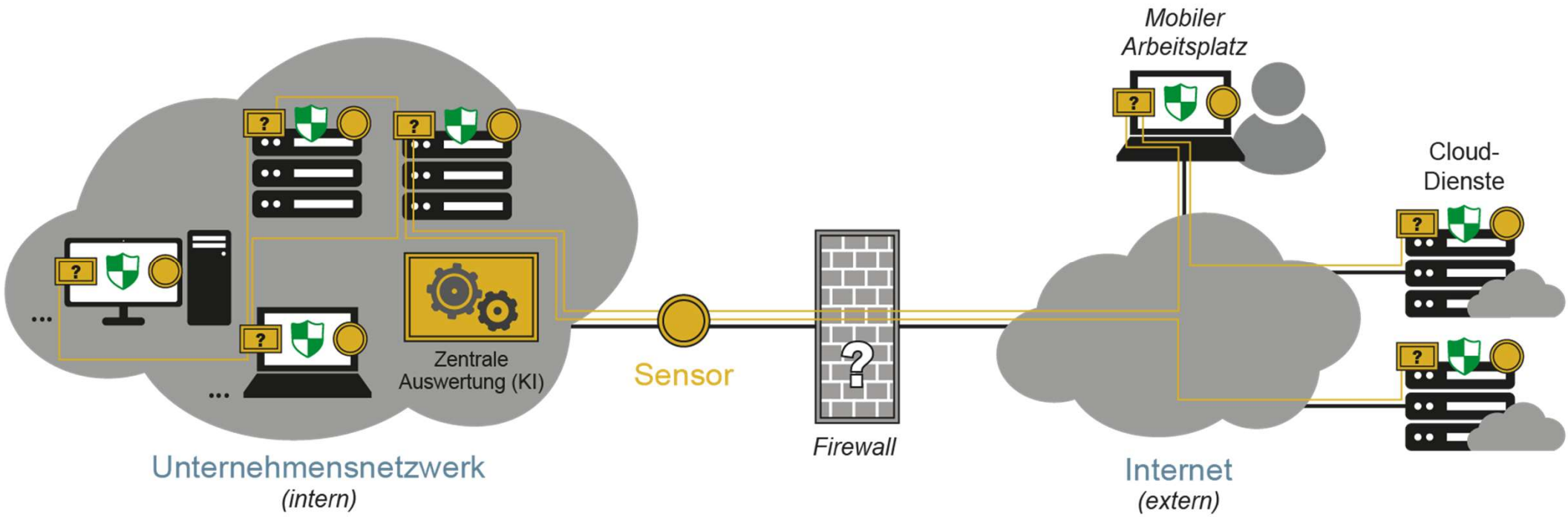
- Proaktive Sicherheitsmechanismen machen IT-Systeme robuster und vertrauenswürdiger.
- Hier spielen **Sicherheitsplattformen** auf der Basis von **intelligenten kryptographischen Verfahren** eine wichtige Rolle.

(Vertrauenswürdige Basis)

„ESP-Strategie“

Verhindern, dass man überhaupt ins Schleudern kommt

Zero Trust
→ Prinzipien



Gegen **mehrstufige Angriffe** auf die IT-Infrastruktur
von Unternehmen (APT)

Prinzipielle Sicherheitsstrategien
→ Erkennen von Angriffen

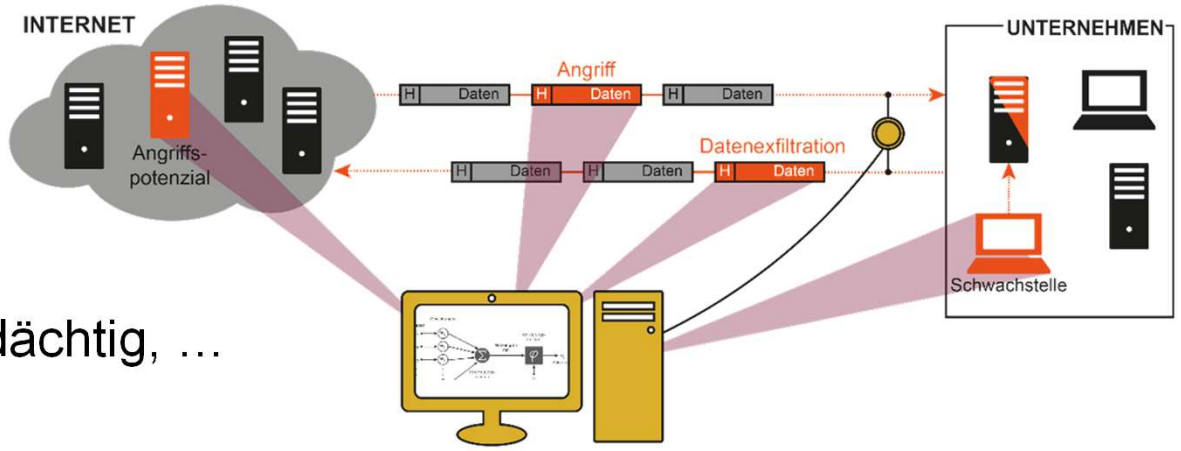
- Wenn Angriffen nicht vollständig entgegengewirkt werden oder eine Vermeidung nicht ausreichend die Angriffsfläche reduzieren kann, dann bleibt noch die Strategie, **Angriffe zu erkennen** und zu versuchen, den Schaden so schnell wie möglich zu minimieren.
- Hier ist die Idee, dass in einem definierten Bereich (IT- und Kommunikationsinfrastruktur, Endgeräte, …) nach **Angriffssignaturen** oder **Anomalien** gesucht wird.

Cyber-Sicherheitsmechanismen

- ***Frühwarn- und Lagebildsysteme***
- ***Bewertung von sicherheitsrelevanten Ereignissen (Priorisierung)*** *- KI*

Künstliche Intelligenz
→ und IT-Sicherheit

- Erhöhung der **Erkennungsrate** von **Angriffen**
  - Netzwerk, IT-Endgeräte, …
  - adaptive Modelle
  - Unterschied: normal und verdächtig, …



- **Unterstützung / Entlastung** von **Cyber-Sicherheitsexperten**
  - Erkennen von **wichtigen** sicherheitsrelevanten Ereignissen *(Priorisierung)*
  - **(Teil-)Autonomie** bei Reaktionen, … Erhöhung der Resilienz, …

- **Verbesserungen** von bestehenden **Cyber-Sicherheitslösungen**
  - KI leistet einen Beitrag zu einer erhöhten Wirkung und Robustheit
  - Z.B.: Risikobasierte und adaptive Authentifizierung

- **Weitere Bereiche:** Erkennung von Malware, Spam, Fake-News, usw. sichere Softwareentwicklung, IT-Forensik, Threat Intelligence, …

Prinzipielle Sicherheitsstrategien
→ Reaktion auf Angriffe

- Wenn Angriffe erkannt werden, sollte so schnell wie möglich mit passenden Aktionen reagiert werden, die den **Schaden** im optimalen Fall noch **verhindern** oder zumindest die Höhe **reduzieren**.

Cyber-Sicherheitsmechanismen

- ***Automatisierte Reaktion*** *(Firewall, E-Mail-Dienst …) - KI*
- ***Digitale Forensik*** *(Maßnahmen optimieren, Schwachstellen schließen)*
- ***Definition von Befugnissen, Informationsflüsse, Entscheidungsprozess und Kommunikationsstrategien***
- ***Notfallplanung***

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Self-Sovereign Identity als Treiber einer dezentralen Revolution

→ Ein europäisches Ökosystem für eine souveräne digitale Zukunft.

Prof. Dr. (TU NN)
Norbert Pohlmann

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

Self-Sovereign Identity
→ Motivation

- Derzeit **dominieren im Cyber-Raum** zentrale ID-Provider wie Google, Facebook und Apple die **Verwaltung von Identitätsdaten** bei sehr vieler IT-Dienste weltweit.

- Diese Situation schafft eine **große Abhängigkeit der Gesellschaft**, **Unternehmen** und **Nutzer** in Bezug auf den **Fortgang der Digitalisierung**.

- (Monopolistischen) ID-Provider nutzen **sensible personenbezogenen Daten** für eigene Werbezwecke oder stellen diese weiteren Unternehmen zur Verfügung, um damit **Geld zu verdienen**.

- Das **schwächt die Privatsphäre der Nutzer** und hat Folgen bezüglicher der **Akzeptanz für unsere digitale Zukunft**.

- Self-Sovereign Identity (SSI) wird helfen, **diese Probleme** zu lösen und ist **ein Digitalisierungsbeschleuniger** für unsere Gesellschaft.

Self-Sovereign Identity
→ Grundsätzliche Idee

- Self-Sovereign Identity oder abgekürzt SSI soll dazu beitragen, die **digitale Zukunft in Deutschland** und in der **EU** souverän, sicherer und vertrauenswürdiger zu gestalten.

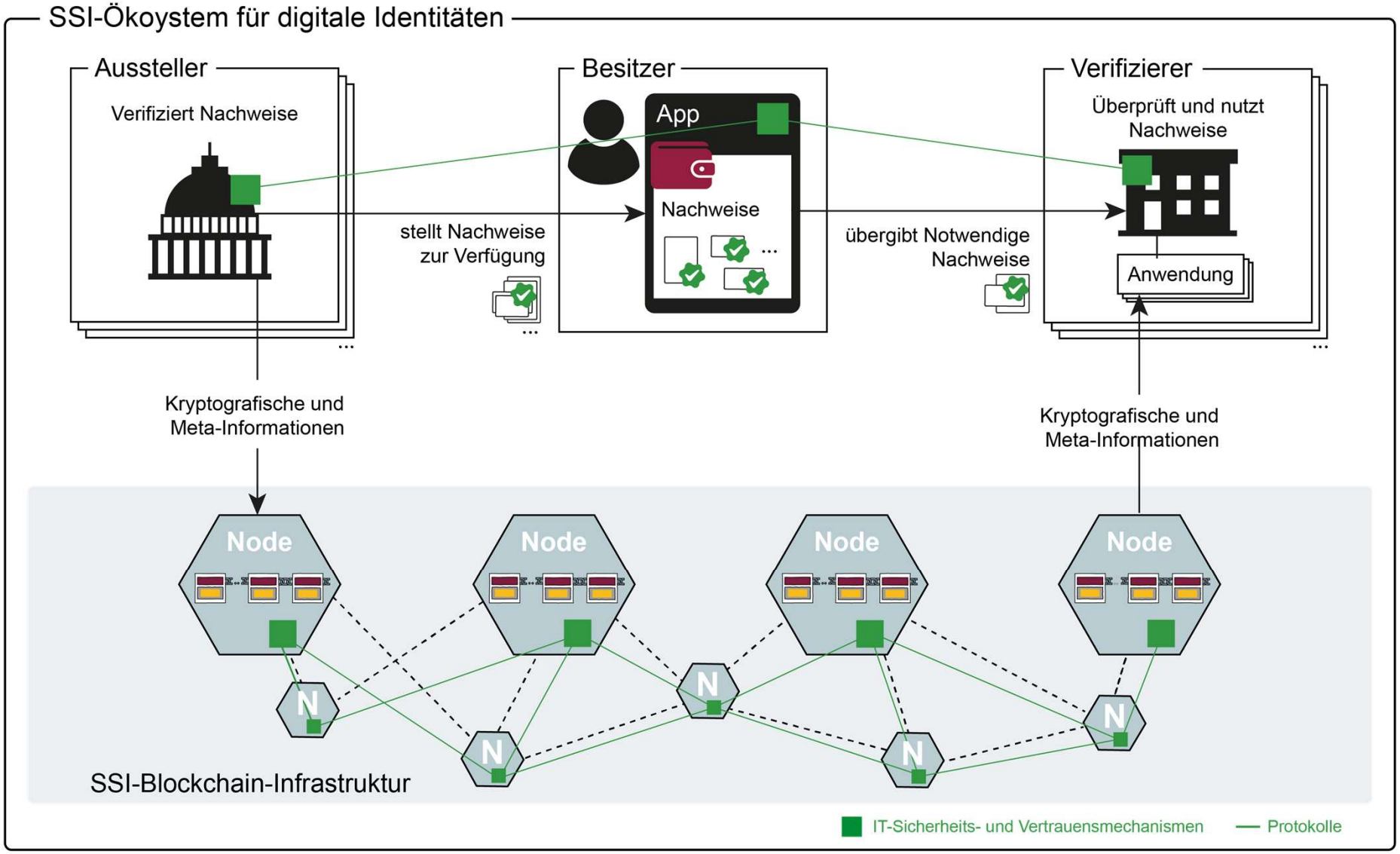
- Die Idee ist, dass **Nutzer wie Bürger oder Mitarbeiter** ihre digitalen Identitäten und weitere digitale Nachweise **selbstbestimmt verwalten** und deren **Weitergabe eigenständig kontrollieren**.

- Diese digitalen Nachweise sind durch Anwendungen, die die Informationen in den digitalen Nachweisen in ihren Prozessen benötigen, **automatisiert verifizier- und verarbeitbar**.

- Das schafft **mehr Datenschutz** und einen **höheren Grad an Digitalisierung** in vielen Prozessen.

Self-Sovereign Identity
→ Architektur

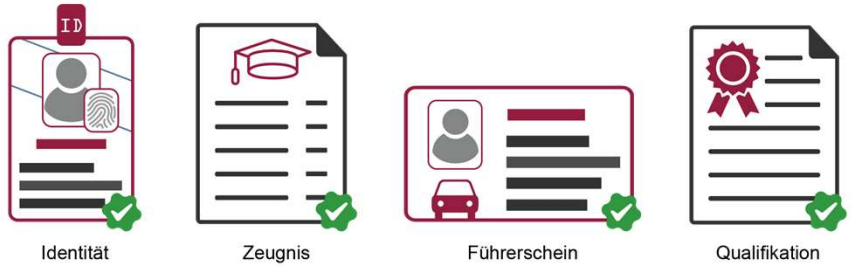
- Im SSI-Ökosystem spielen **drei Akteure eine Rolle**, die gemeinsam einen Vertrauensdienst – die SSI-Blockchain-Infrastruktur - nutzen.



Self-Sovereign Identity
→ Aussteller von digitalen Nachweisen

Aussteller stellen verifizierbare digitale Nachweise aus und sind:

- **Einwohnermeldeamt**, Straßenverkehrsamt, **Schulen- und Hochschulen**, Unternehmen, **Berufsverbände**, Behörden, **Qualifizierungsorganisationen**, TÜVs oder **weitere Unternehmen,** die hier ein Geschäftsmodell für sich sehen.



Verifizierbare digitale Nachweise:

- **Bescheinigungen der Identität** (wie Personalausweis, Firmen-/Dienstausweis …),
- **Führerscheine** (für Auto oder Motorrad …),
- **Zeugnisse** (wie Abitur, Bachelor, Master, Promotionsurkunden …),
- **Bestätigungen** (zum Beispiel Teilnahmebestätigung, Buchungsbestätigung, Echtheitsbestätigung, Impfbestätigung …)
- **Befugnisse** (wie Amtsbefugnis, Aufenthaltsbefugnis …),
- **Qualifikationen** (zum Beispiel Weiterbildungsnachweise, Personenzertifikate …),
- **Mitgliedsausweise** (für Fitnessstudien, Vereine, ADAC und so weiter),
- **Kundenkarten** (wie Bonuskarten, Vielfliegerprogramme …)
- und vieles mehr

Self-Sovereign Identity
→ Besitzer oder Nutzer

- Ein Besitzer oder Nutzer hat in der Regel auf seinem **mobilen Endgerät** eine entsprechende **SSI-App** mit einem **digitalen Portemonnaie**, die sogenannte **SSI-Wallet** in der die verifizierbaren digitalen Nachweise sicher gespeichert sind.

- Es ist auch möglich, als Alternative oder Ergänzung zur App einen Cloud-Agent zu nutzen.

- Die **Nutzer** können alle **verifizierbaren digitalen Nachweise** von den entsprechenden **Ausstellern anfordern**, wenn sie dazu eine Berechnung haben und in ihre **SSI-Wallet sicher ablegen**.

- Damit sind sie in der Lage, **selbstbestimmt** und **souverän** diese verifizierbaren **digitalen Nachweise** oder **bestimmte Attribute** oder **Teile daraus** den entsprechenden Anwendungen **zur Verfügung zu stellen**.

- Dies sollten die Nutzer nur dann tun, wenn die Anwendung die Inhalte der **digitalen Nachweise** wirklich **für die Umsetzung der eigentlichen Aufgabenstellung benötigen**.

Self-Sovereign Identity
→ Zero-Knowledge-Proof (1/3)

- Ein weiteres wichtiges **Feature für den Schutz der Privatheit** und **Souveränität des Nutzers** wird mithilfe von sogenannten **Zero-Knowledge-Proof** umgesetzt.

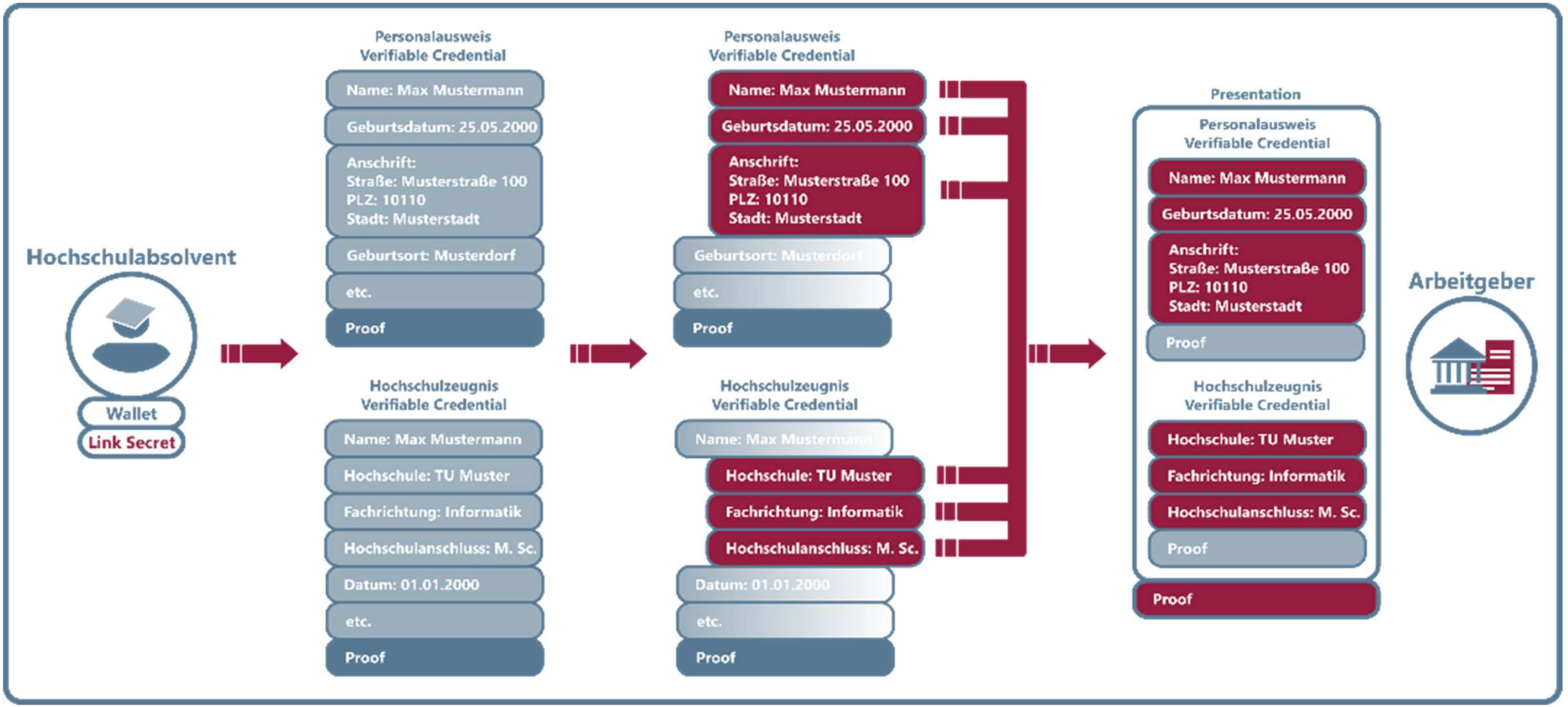
- Damit ist es möglich, sicher und vertrauenswürdig nur **bestimmte Attribute anonym** oder **Teile** aus den Nachweisen **zu beweisen**.
  - Das der Nutzer über **18 Jahre alt** ist
  - Das der Nutzer **zu einem bestimmten Unternehmen gehört**
  - Das der Nutzer schon **zweimal gegen Corona geimpft** worden ist

- Diese **Attribute** oder **Teile** aus digitalen Nachweisen **können bewiesen werden**, **ohne weitere** und für die Anwendung nicht wichtigen **Informationen** zur Verfügung zu stellen.

- Der **Zero-Knowledge-Proof** hilft in vielen Fällen, **Datenschutzaspekte** einfach und wirkungsvoll umzusetzen, weil nur bestimmte Attribute überprüft werden, ohne datenschutzrelevante Informationen übertragen zu müssen.

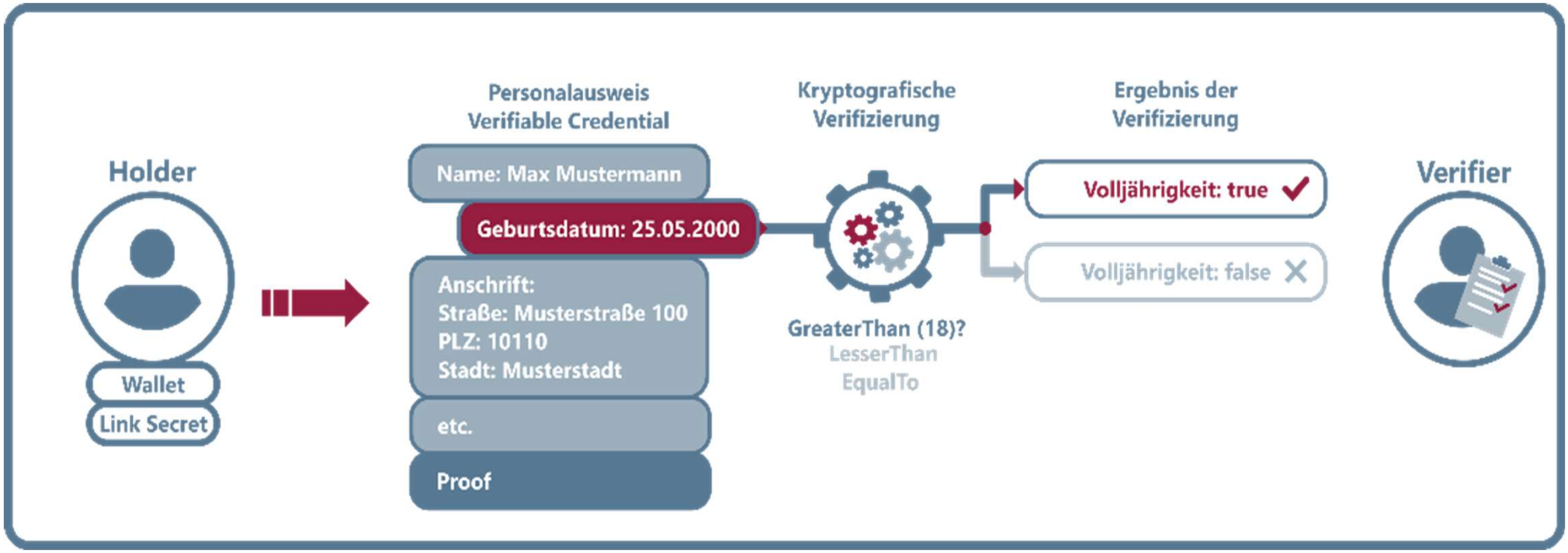
Self-Sovereign Identity
→ Zero-Knowledge-Proof (2/3)

Gezielte Informationsweitergabe durch **Selective Disclosure**



Self-Sovereign Identity
→ Zero-Knowledge-Proof (3/3)

Nachweis der Volljährigkeit mithilfe von **Predicate Proofs**



Self-Sovereign Identity
→ Verifizierer oder Anwendungen

- Anwendungen, die die **digitalen Nachweise** für ihre spezielle Aufgabenstellung benötigen, bekommen diese oder **Teile davon** oder nur Aussagen über **bestimmte Attribute** von den Nutzern **unter definierten Rahmenbedingungen** zur Verfügung gestellt.
- Diese können von der Anwendung vollkommen automatisiert, in einem digitalisierten Prozess sicher und eindeutig verifiziert und bearbeitet werden.
- Damit wird eine höhere Sicherheit bei der Nutzung von Nachweisen erzielt.
- Bei physischen Nachweisen müssen oft ungeschultes Personal die Verifikation mit allen Fehlern umsetzen.
- **Bei den Anwendungen entsteht der größte Vorteil**, weil die Prozesse mithilfe der digitalen Nachweise **automatisiert** und damit **effizient** und **kostengünstig** umgesetzt werden.

Self-Sovereign Identity
→ Blockchain-Infrastruktur

- Damit die **digitalen Nachweise verifiziert** werden können, brauchen wir einen **Vertrauensdienst**.
- Eine **moderne Blockchain-Infrastruktur** ist für die **Souveränität** und die **Skalierbarkeit** des SSI-Ökosystems besonders gut geeignet *(Konsortium)*.
- Das bedeutet, die Akteure sind auf der Basis dieses dezentralen Blockchain-Netzwerks in der Lage, die **Echtheit**, den **Ursprung** als auch die **Unversehrtheit** der digitalen Nachweise **zu überprüfen**, ohne dass die SSI-Blockchain die Nutzer oder die ausgestellten digitalen Nachweise kennt.
- Im SSI-Ökosystem können und werden **mehrere unterschiedliche SSI-Blockchain-Netzwerke** im Sinne Network-of-Networks eingebunden sein.
- Das macht das Ökosystem skalierbar und effizient bei der Umsetzung in verschiedenen Bereichen.
- Beispiele von möglichen verschiedenen SSI-Blockchain-Netzwerken sind: Government, Banken, Smart City, Industrie-Branchen, Gesundheitswesen … und das in verschiedenen Ländern wie Bundesländer, EU-Länder.
- Alle zusammen bieten **als Ganzes** einen **einheitlichen Vertrauensdienst**.

Self-Sovereign Identity
→ Beispiel: Auto-Anmietung

- Wer schon einmal ein Auto gemietet hat, kennt die folgende Situation:
- **Der Mitarbeitende des Autovermieters** braucht eine gefühlte Ewigkeit, um Ausweis, Führerschein, Kreditkarte, Reservierung und Gutscheine zu prüfen und **die Daten im PC zu erfassen**.
- Mit **Self-Sovereign Identity (SSI)** würde **dieser Vorgang** wesentlich **vereinfacht** und dadurch **erheblich verkürzt**:
- Am Schalter angekommen, wird ein QR-Code vom Kunden gescannt.
- Anschließend werden die digitalen Nachweise vom Kunden freigegeben und ein Vertrag digital signiert – danach erfolgt die Übergabe der Autoschlüssel.
- Quasi **simultan** und **automatisiert** laufen die **Prozesse sicher** und **vertrauenswürdig** im Hintergrund ab.
- Ein schönes Beispiel, welchen **Effekt SSI bei der Digitalisierung** hat.
  - Der Auto-Vermieter hat ein sehr **hohes Einsparungspotenzial**, weil alles automatisiert abläuft.
  - Der Kunde bekommt sein Auto sehr viel schneller und muss **nicht lange warten**.

Self-Sovereign Identity
→ Weitere Aspekte

Gesellschaftliche Relevanz

- Digitalisierung: hoher gesellschaftlicher Relevanz *(zu viele nicht effiziente Prozesse)*.
- **Problem:** Unternehmen nutzen persönlichen Daten wirtschaftlich.
- Das **Recht auf Privatsphäre** gilt als Grundrecht und ist in allen modernen Demokratien verankert. Wird aber **im Cyber-Raum** zurzeit **nicht wirklich berücksichtigt.**
  → Das SSI-Ökosystem löst das Problem

Wirtschaftliche Relevanz

- Händisch durchgeführte Abläufe und vorhandene Medienbrüche.
- Die Umsetzung von digitalen Identitäten und Nachweisen hat einen hohen wirtschaftlichen Nutzen. Laut der MGI Studie 3 bis 4 Prozent des BIP (2030)
  → 3 % in Deutschland im Jahr 2020 wären 100 Mrd. Euro gewesen.

Technologische Souveränität

- Ist ein zunehmend wichtiger Faktor *(Wertschöpfungsanteil: IT, Internet und Daten)*
- Wie brauchen unabhängige Gestaltungsmöglichkeiten (*Schlüsselbranchen: gezielter Kompetenzaufbau und Schlüsseltechnologien entwickelten).*
- **SSI-Technologien ist ein Schlüsselbereich** *(größere Autonomie in Bezug auf die Nutzung und Verwertung von persönlichen Daten)*
  → höheren Gard an Digitalisierung

Self-Sovereign Identity
→ Zusammenfassung

- Das SSI-Ökosystem **löst Abhängigkeiten von Monopolisten** und gibt uns die **Freiheit**, die digitale **Zukunft unabhängiger** und damit erfolgreicher zu gestalten.
- **Self-Sovereign Identity (SSI)** sorgt als **Digitalisierungsbeschleuniger** für **eine schnellere, sichere 2und vertrauenswürdige Digitalisierung**.
- Die **Nutzer** können **selbstbestimmt** ihre Identitätsdaten und weitere digitale Nachweise an Anwendungen weitergeben.
- Das schafft einen **hohen Grad an Privatsphäre**, an **werteorientierter IT** und **-Diensten** und damit eine **hohe Akzeptanz für die digitale Zukunft**.

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Self-Sovereign Identity als Treiber einer dezentralen Revolution

Wir brauchen ein souveränes europäische Ökosystem für Identitätsdaten

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.

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Identifikation und Authentifikation

Prof. Dr. (TU NN)
Norbert Pohlmann

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

Identifikation und Authentifikation
→ Identifikation (1/2)

- Die Identifikation ist die **Überprüfung** eines vorgelegten, **kennzeichnenden Merkmals**, zum Beispiel des Nutzernamens oder allgemein der Identität.
- Eine **Person** wird **weltweit eindeutig** durch die Angabe der Attribute **Vorname**, **Nachname**, **Geburtsort** und **Geburtstag** identifiziert.
- In Deutschland wird die Eindeutigkeit der Identifikation durch die Regularien der Standesämter garantiert.
- Im **Cyber-Raum** handelt es sich zum Beispiel bei der Identifikation um die Feststellung der **digitalen Identität** einer Person (Nutzer).
- Als **digitale Identität** – kennzeichnendes Merkmal – wird in der Regel der **Nutzername** (Name oder E-Mail-Adresse der Person) verwendet.
- Mit einer digitalen Identität lassen sich Nutzer in einem IT-System eindeutig zuordnen und identifizieren.
- Eine Person kann abhängig vom Kontext und den dadurch erforderlichen Attributen auch mehrere digitalen Identitäten besitzen.

Identifikation und Authentifikation
→ Identifikation (2/2)

- Eine **Identifikation** muss immer innerhalb eines **Systems** (Organisation) abgesprochen sein, damit sie **eindeutig** ist.
- Ein **System** kann die **Weltbevölkerung** sein, die **Bürger in Deutschland**, die Kunden eines Webshops, die **Mitglieder eines sozialen Netzwerks** wie Facebook usw.
- Damit eine solche Absprache mit verschiedenen Nutzern zustande kommt, müssen klar definierte Regeln bezüglich der Identifikation eingehalten werden.
- Beispiel:
  - CCITT »Recommendation« X.509 bzw. ISO 9594-8
    (Ein Konzept eindeutiger, kennzeichnender Namen oder »distinguishing identifier«)

Identifikation
→ Beispiele von digitalen Identitäten

- **E-Mail-Adresse -** Nutzername ist eine E-Mail-Adresse
  Dies hat den Vorteil, dass von aktiven E-Mail-Adressen international keine Doppelungen auftreten können.
  Das heißt, dass die E-Mail-Adresse einer Person weltweit ein eindeutiges kennzeichnendes Merkmal ist.
  Die E-Mail-Adressen mit ihren entsprechenden Domänen werden als Baumstruktur verwaltet und sind daher eindeutig. rainer.maier@gmx.de gibt es nur ein Mal. Möchte ein zweiter Rainer Maier eine E-Mail-Adresse bei GMX haben, könnte er zum Beispiel rainer.maier2@gmx.de wählen.
- **Freie Wahl**
  Der Nutzer kann selbst einen Nutzernamen auswählen, zum Beispiel rmaier oder MickyMaus.
  Das IT-System muss dann prüfen, ob der gewählte Nutzername in diesem IT-System nicht schon vergeben ist. Wenn ja, muss der Nutzer einen anderen Namen finden, der noch nicht vergeben ist.
- **Das IT-System bestimmt**
  Es ist aber auch möglich, dass das IT-System den Nutzernamen bestimmt und dem Nutzer mitteilt.

Identifikation und Authentifikation
→ Authentifikation (1/2)

- **Authentifikation** bezeichnet einen **Prozess**, in dem **überprüft** wird, ob „jemand“ oder „etwas“ **echt** ist.
- Daher bedeutet **Authentifikation** die Verifizierung (**Überprüfung**) der Echtheit beziehungsweise **der Identität**.
- Die Überprüfung des Personalausweises einer Person ist eine solche Authentifikation in der realen Welt.
- Ein Prüfer kann, mithilfe eines Personalausweises, das Aussehen einer Person mit dem Lichtbild vergleichen.
- Im **Cyber-Raum** wird bei der Authentifikation mit der Erbringung eines oder mehrere **Nachweise** bestätigt, ob es sich um die Person (Nutzer) mit der **angegebenen** und **behaupteten digitalen Identität** handelt.
- Damit wird die **Echtheit der digitalen Identität** eines Nutzers **festgestellt**.

Identifikation und Authentifikation
→ Authentifikation (2/2)

- Was muss und kann z.B. identifiziert und authentisiert werden?
  - **Nutzer,** wie Personen, Prozesse, Instanzen und weitere Entitäten.
  - **Medien,** wie Notebooks, Smartphones, Smartwatches, Serversysteme, Cyber-Sicherheitssysteme, Security Token usw.
  - **Nachrichten,** wie E-Mails, Dateien, Java-Applets, Datenpakete usw.

Klassen von Authentifizierungsverfahren → Übersicht

- Es werden **verschiedene Klassen** von Authentifizierungsverfahren unterschieden, wie der **Nachweis der Echtheit** der **digitalen Identität** überprüft wird.

- Bei den verschiedenen Klassen spielen **unterschiedliche Aspekte** eine Rolle und es müssen **diverse Charakteristika** berücksichtigt werden.

Klassen von Authentifizierungsverfahren → Wissen

Bei dieser Klasse von Authentifizierungsverfahren wird über einen **Nachweis** der Kenntnis von **Wissen** die **Echtheit eines Nutzers** überprüft.

Beispiele von Wissen: Passwort, PIN, Antwort auf eine bestimmte Frage (Sicherheitsfrage) usw.

Charakteristika von Wissen:

- Das Wissen kann vergessen werden (insbesondere nach einer Feier).
- Das Wissen kann dupliziert, verteilt, weitergegeben und verraten werden.
- Das Wissen kann in vielen Fällen erraten werden (Social Engineering, Wörterbuchangriff, …).
- Das Wissen kann beim Eintippen mitgelesen oder mithilfe eines Keyloggers (Malware) im Endgerät ausgelesen werden.
- Einmal abgefangenes Wissen gilt als kompromittiert, wenn es auch für weitere Dienste genutzt wird.
- Die Preisgabe von Wissen kann kompromittiert werden (Androhung von Gewalt).
- Die Mitführung von Wissen erfordert in der Regel keine praktischen Hilfsmittel (Passwortmanager).

Klassen von Authentifizierungsverfahren → Besitz

Verwendung eines **Besitztums als Nachweis** für das Authentifizierungsverfahren ist eine weitere Klasse.

Beispiele für Besitz: Neuer Personalausweis, SIM-Karte im Smartphone, Hardware-Sicherheitsmodule (Smartcard, USB-Stick …) usw.

In der Regel wird der **Besitz von geheimen Schlüsseln** mithilfe von Challenge-Response-Verfahren nachgewiesen, die in den Sicherheitsmodulen sicher gespeichert sind.

Charakteristika von Besitz:

- Das Besitztum ist mit Kosten verbunden (Hardware).
- Das Besitztum muss mitgeführt werden (umständlich).
- Das Besitztum kann verloren gehen (kein Zugang mehr).
- Das Besitztum kann gestohlen werden (kein Zugang mehr).
- Das Besitztum kann übergeben oder weitergereicht werden (jemand anderes kann zugreifen).

Klassen von Authentifizierungsverfahren → Sein

Bei dieser Klasse von Authentifizierungsverfahren muss der **Nutzer** als Nachweis **gegenwärtig sein**.

Beispiele von Sein: Biometrische Merkmale wie Fingerabdruck, Gesichtsgeometrie, Iris, Tippverhalten DNA usw.

Charakteristika von Sein:

- Biometrische Merkmale werden durch Personen immer mitgeführt.
- Biometrische Merkmale können nicht an andere Personen weitergegeben werden.
- Verfahren zur Erkennung von biometrischen Merkmalen können keine 100 %-Aussagen treffen, sondern nur mit einer gewissen Wahrscheinlichkeit die Echtheit von Personen abschätzen.
- Eine Lebenderkennung kann erforderlich sein (damit zum Beispiel ein künstlicher Fingerabdruck oder abgeschnittener Finger zurückgewiesen wird)
- Ein biometrisches Merkmal ist im Laufe der Zeit oder durch Unfälle veränderlich und damit schlechter erkennbar.
- Bestimmten Personengruppen fehlt das biometrische Merkmal.
- Ein biometrisches Merkmal kann nicht ersetzt werden (Problem, wenn diese „gestohlen“ werden können).

Klassen von Authentifizierungsverfahren → Weitere unterstützende Faktoren

Es können noch weitere **unterstützende Faktoren** für die **Beurteilung der Echtheit** des Nutzers herangezogen werden.

Beispiele für weitere unterstützende Faktoren: Vergangene Transaktionen des Nutzers (**Reputation**), verwendete Endgeräte und Software des Nutzers (**Technologie**), **Standort** und **Zeit** des Authentisierungsprozesses.

Charakteristika weiterer unterstützender Faktoren:

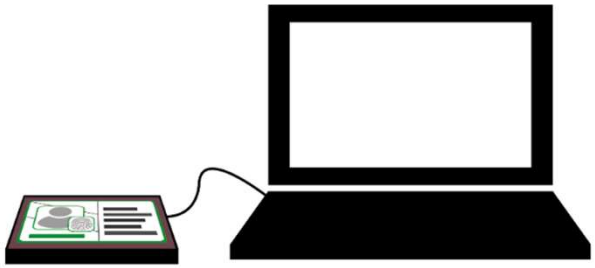
- Die Reputation des Nutzers ist ein Indiz, wie er sich zukünftig verhalten wird.
- Die genutzte Technologie gibt einen Hinweis, ob es sich um den Nutzer handelt und wie das Angriffspotenzial des Endgeräts eingeschätzt werden kann.
- Der Standort gibt geografische und netzbasierte Informationen über das Vertrauensniveau des Orts (sichere oder unsichere Umgebung).
- Mit dem Zeitpunkt des Zugriffs kann geprüft werden, ob das natürliche Verhaltensmuster passt.

Identifikationsverfahren
→ eID Verfahren des Personalausweises

Beim eID-Verfahren des elektronischen Personalausweises (ePA) handelt es sich um ein Identifikationsverfahren, bei dem sich der Besitzer des Ausweisdokuments gegenüber einem Dienstanbieter identifizieren und als legitimer Eigentümer authentifizieren kann.

Ablauf des eID-Verfahrens

- Aufbau einer Verbindung zwischen Nutzer und Dienstanbieter.
- Übermittlung des **Berechtigungszertifikats** und der dienstanbieterspezifischen Informationen an die AusweisApp des Nutzers.
- Annehmen oder ablehnen der Berechtigungen gemäß Berechtigungszertifikat beziehungsweise Einschränkung der Berechtigungen.
- Bestätigung der erteilten Berechtigungen durch Eingabe der eID-PIN.
- Auslesen der freigegebenen Daten des ePA.



Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Identifikation und Authentifikation

Prof. Dr. (TU NN)
Norbert Pohlmann

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

Cyber-Sicherheit
→ Zusammenfassung

- Die **Cyber-Sicherheitsprobleme** im Cyberraum **sind größer** denn je und **wachsen weiter an.**

- **Cyber-Sicherheit** ist für unsere **Digitalisierung wichtig**, um die Zukunft sicher und vertrauenswürdig gestalten zu können.

- **Cyber-Sicherheitsstrategien** helfen auf verschiedenen Ebenen und Phasen, **Risiken zu reduzieren** und **verbleibende Risiken zu managen.**

Marktplatz
→ IT-Sicherheit

www. it-sicherheit.de
Der Marktplatz IT-Sicherheit

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Cyber-Sicherheitsstrategien

Cyber-Sicherheit
wird in der Zukunft immer wichtiger

Prof. Dr. (TU NN)
Norbert Pohlmann

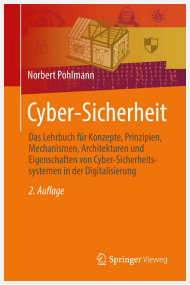
***Professor** für **Informationssicherheit** und*
Leiter** des **Instituts für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen

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

***Professor** für **Informationssicherheit** 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 Informationssicherheit *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 des 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 ca. 40)

60+ Drittmittelprojekte
mit Unternehmen / Behörden

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

54 Forschungsprojekte
BMBF 20, BMWK 10, BMDV 1, EU 4, NRW 15, BMI 4 …

4 Start-ups aus dem if(is)
finally safe; XignSys, TrustCerts, aware7

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 City, -Car, -Traffic
- Cloud, Fog, Edge Computing
- Mobile Security
- Botnetz-Erkennung
- Vertrauenswürdigkeit