



**Westfälische
Hochschule**

Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Cyber-Sicherheitsstrategien

→ zur Reduzierung der Risiken für Unternehmen

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

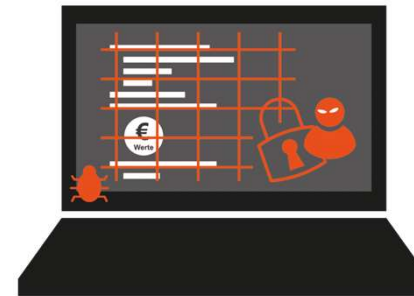
→ Einschätzung

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

Lage der IT-Sicherheit in DE 2022

→ 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.*

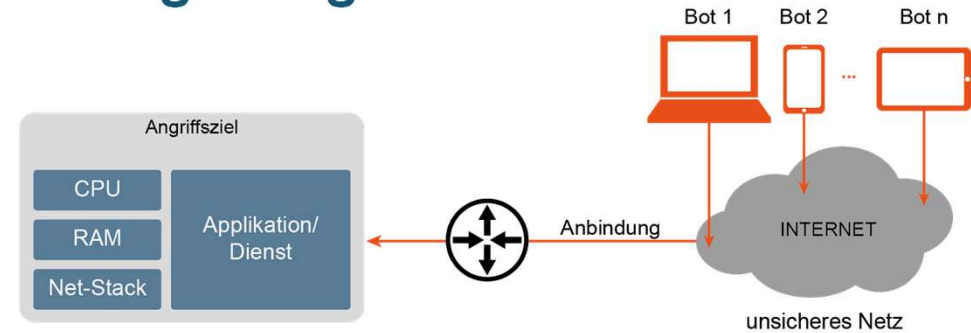


- **Big Game Hunting**, die Erpressung umsatzstarker Unternehmen mit verschlüsselten und exfiltrierten Daten, **hat weiter zugenommen.**
- *Aber nicht nur Unternehmen sind Ziel von Ransomware-Angriffen.*
- Mit dem **folgeschweren Angriff auf eine Landkreisverwaltung** in Sachsen-Anhalt wurde **wegen 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.



- *Zahl der Schwachstellen in Software steigt um 10 Prozent.*

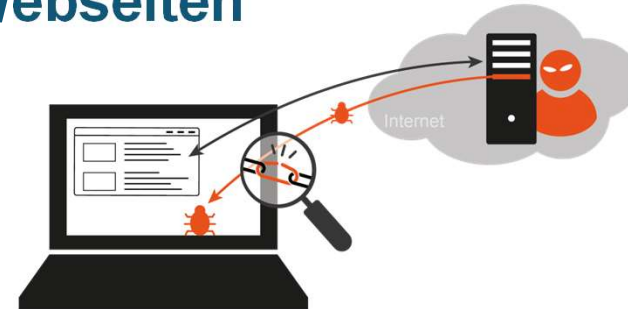
Je höher die Investition in IT-Sicherheit, je geringer der Schaden (BSI-Studie).

- *24 Mrd. Euro Schaden nur Ransomware in DE in 2021*
- **Durchschnittliche Lösegeldzahlung** in allen Bereichen liegt bei **812.360 Dollar**.
- *Durchschnittliche Lösegeldzahlung bei **Fertigungsunternehmen** liegt bei **2.036.189 Dollar**.*
- **90 Prozent der Unternehmen** wurden durch einen **Ransomware-Angriff** in ihrer **Betriebsfähigkeit beeinträchtigt**.
- ***1,4 Mio. durchschnittliche Kosten für die Behebung der Angriffs-Folgen***
- **1 Monat** durchschnittlich benötigte Zeit bis zur kompletten **Wiederherstellung** nach einem Angriff
- *Bei **Fertigungsunternehmen** sehen wir **einen mindestens zweimonatigen Produktionsstillstand** (bis zu 12 Monaten).*

Angriffsvektoren

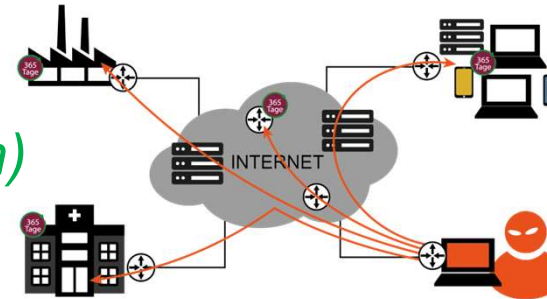
→ Beispiele

- Malware-Infiltration über manipulierte Webseiten



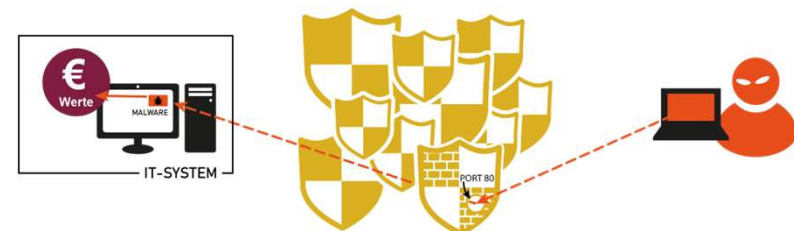
- Malware-Infiltration über schadhafte E-Mail-Anhänge

Social Engineering <> **Security Awareness**
(technische Maßnahmen)



- Mehrstufiger Angriff auf die IT-Infrastruktur von Unternehmen (APT)

Schwachstellen, Passwörter, Rechte ...



Entwicklung der Digitalisierung

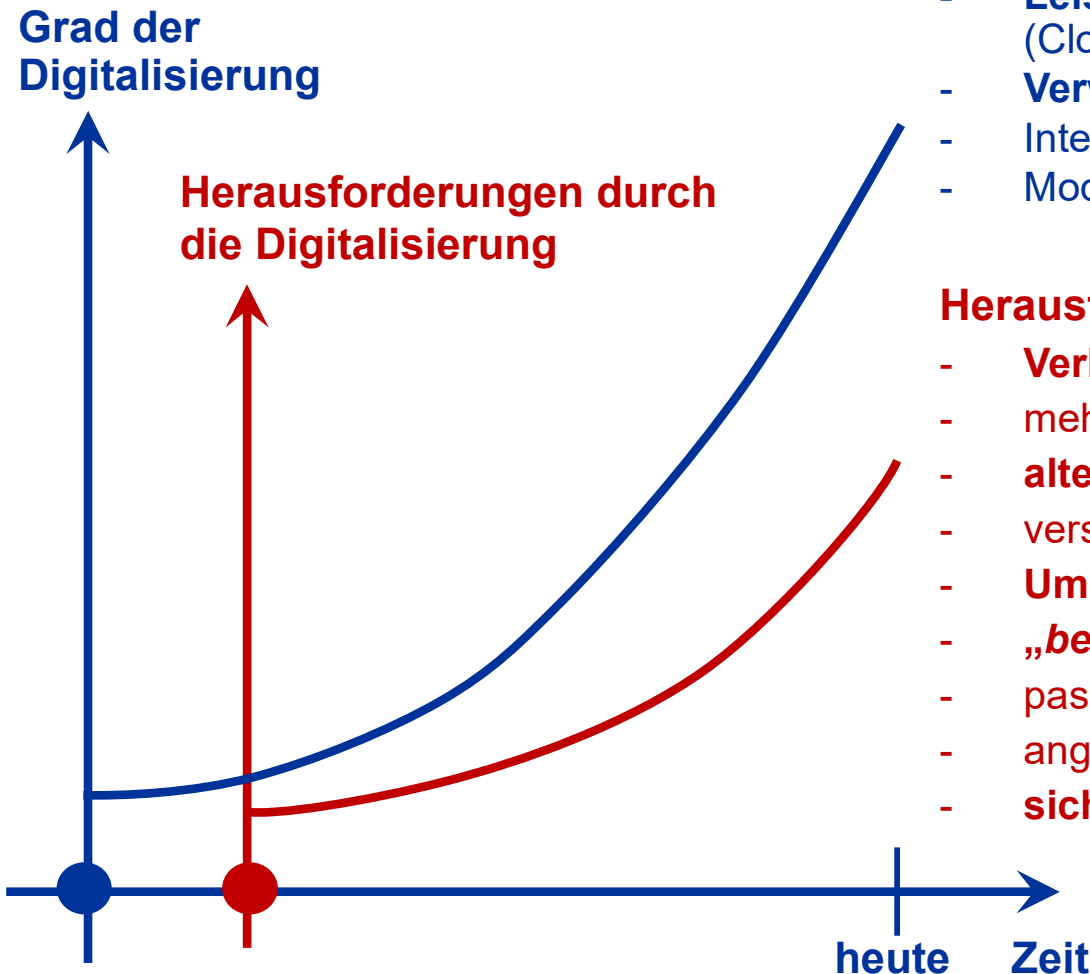
→ Erfolgsfaktoren und Herausforderungen

Erfolgsfaktoren der Digitalisierung (Beispiele)

- **Kommunikationsinfrastruktur** (5G, Glasfaser, NB, CUG ...)
- **Smarterheit 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%)



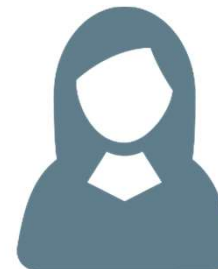
Geschäftsmodelle
„Bezahlen mit persönlichen Daten“



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

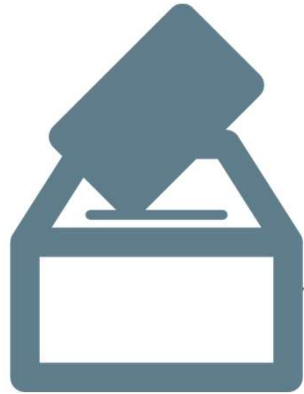


Zum Vergleich:
Internet-Kriminalität: ca. 100+ Millionen €
pro Jahr
(Online Banking ...)



Was sind die Herausforderungen?

→ 3. Cyberwar



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

Cyberwar



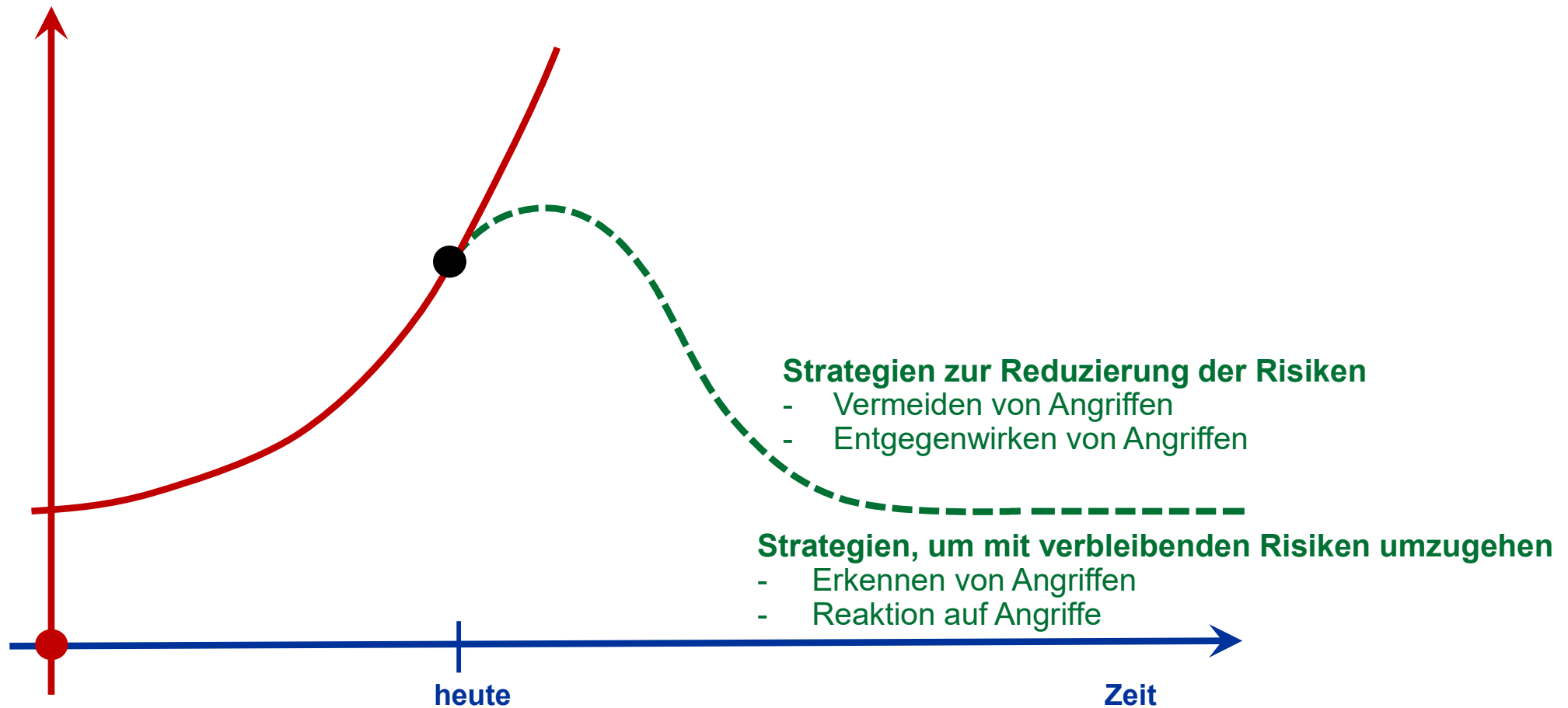
Angriffe auf Kritische Infrastrukturen
z.B. Stromversorgung, Wasserversorgung ...



Cyber-Sicherheitsstrategien

→ Übersicht

Risiko durch die Digitalisierung



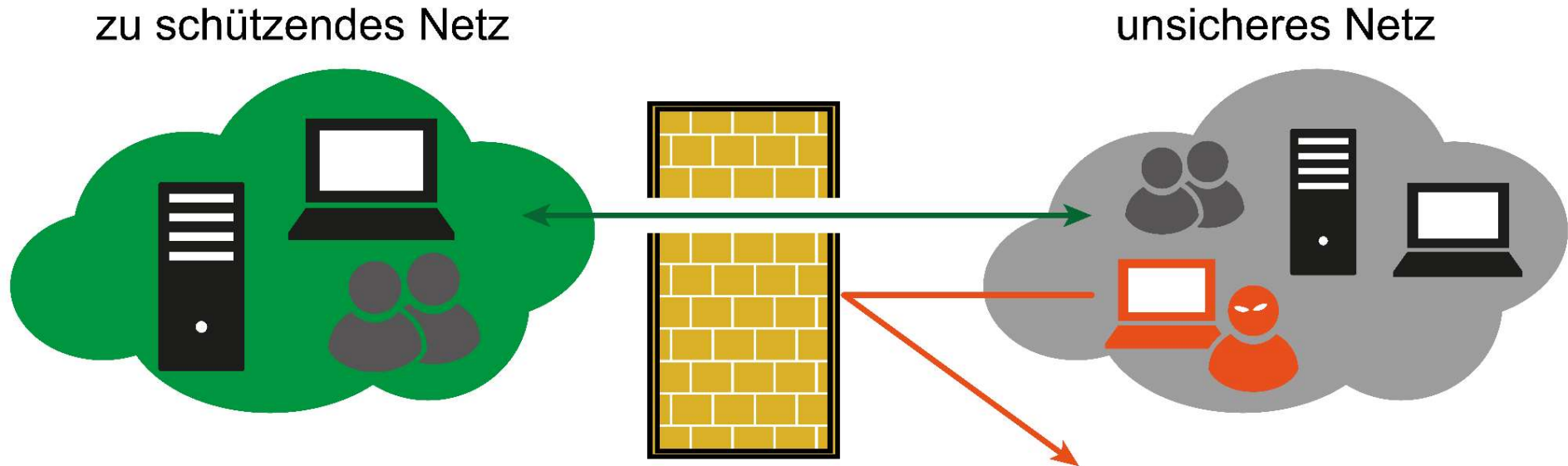
- Mit Hilfe der Vermeidungsstrategie wird eine **Reduzierung der Angriffsfläche** und damit die **Reduzierung der Risiken** erreicht.
- Die Herausforderung besteht darin, **die IT so einzurichten**, dass das Unternehmen **alles wirklich *Notwendige*** für das Business **umsetzen** kann, aber **alles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

Cyber-Sicherheitsmechanismen

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



Sicherheitskonzept → Firewall-System



Kommunikationsmodell

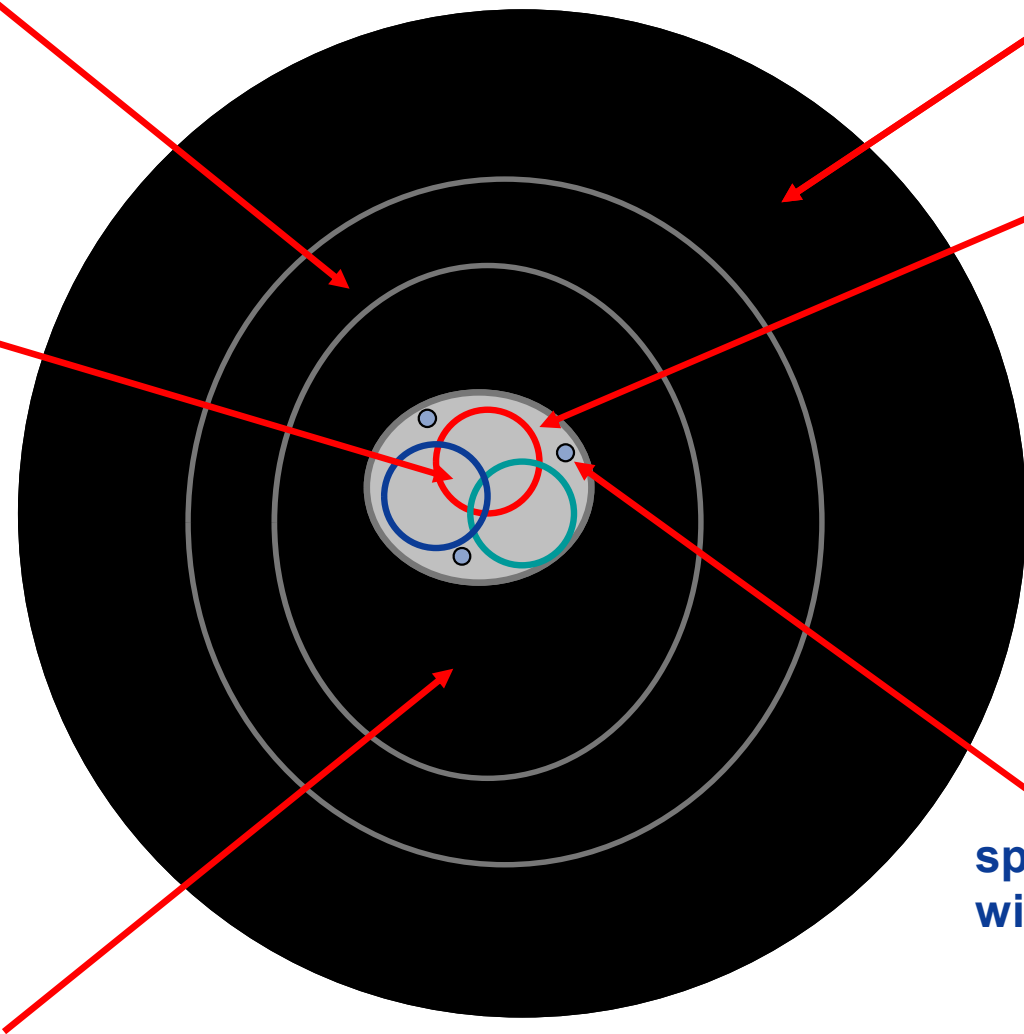
→ Reduzierung des Schadensrisikos

Einschränkung der erlaubten Protokolle

Protokolle, die nicht erlaubt sind

Kommunikations-
Profile

zeitliche
Einschränkung



spezielle Anwendungen,
wie z.B. SMTP

Einschränkung der erlaubten IT-Systeme (Transmitter, Receiver)

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 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 geht aber in der Regel deutlich weiter.

- 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*)



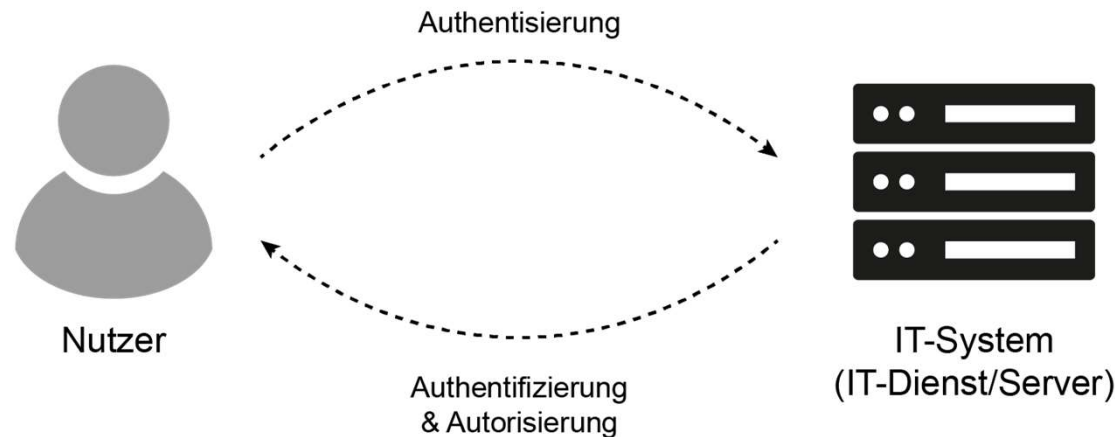
Aktive Verschlüsselung

→ 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**.

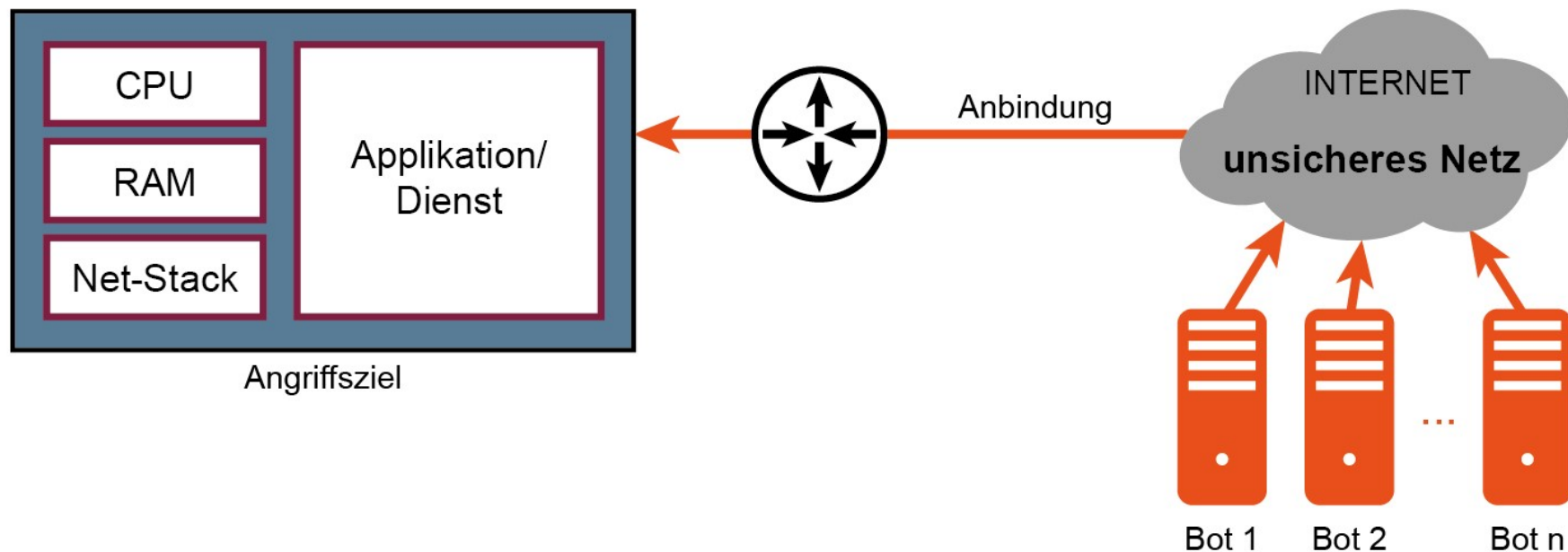
DDoS-Angriffe

→ Ziel: Gezielte Überlastung

Ziel eines DDoS-Angriffes:

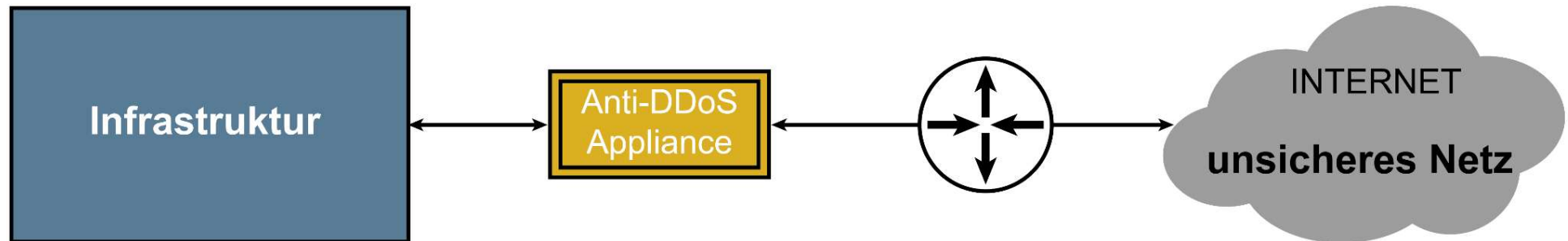
Ausgesuchte IT-Systeme koordiniert mit einer großen Last spezieller Anfragen durch **Erschöpfung** der verfügbaren Ressourcen

- CPU
 - RAM
 - Bandbreite
- lahmzulegen



Abwehrstrategien

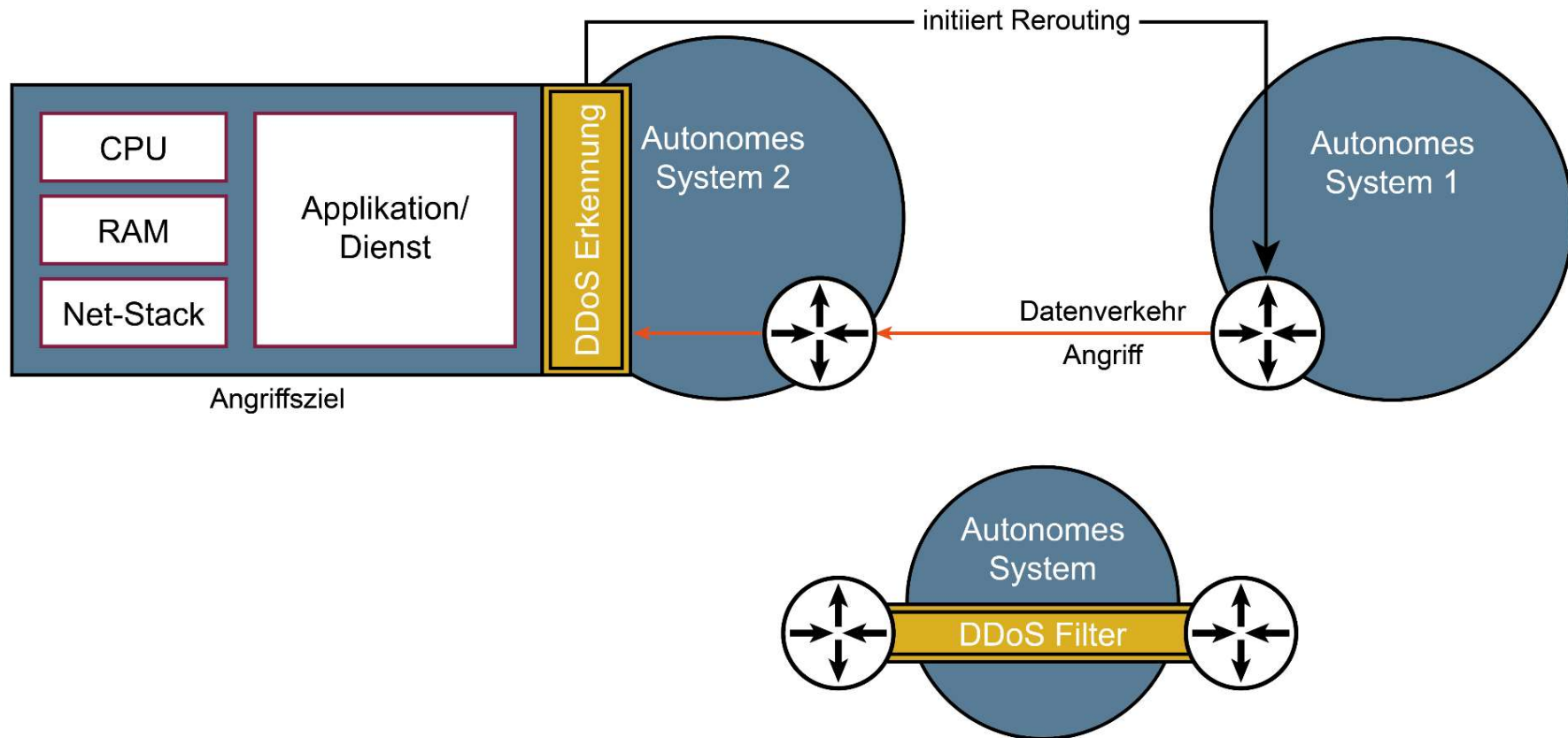
→ On-Site: Anti-DDoS Appliance



Abwehrstrategien

→ Off-Site: Traffic-Scrubbing-Netze

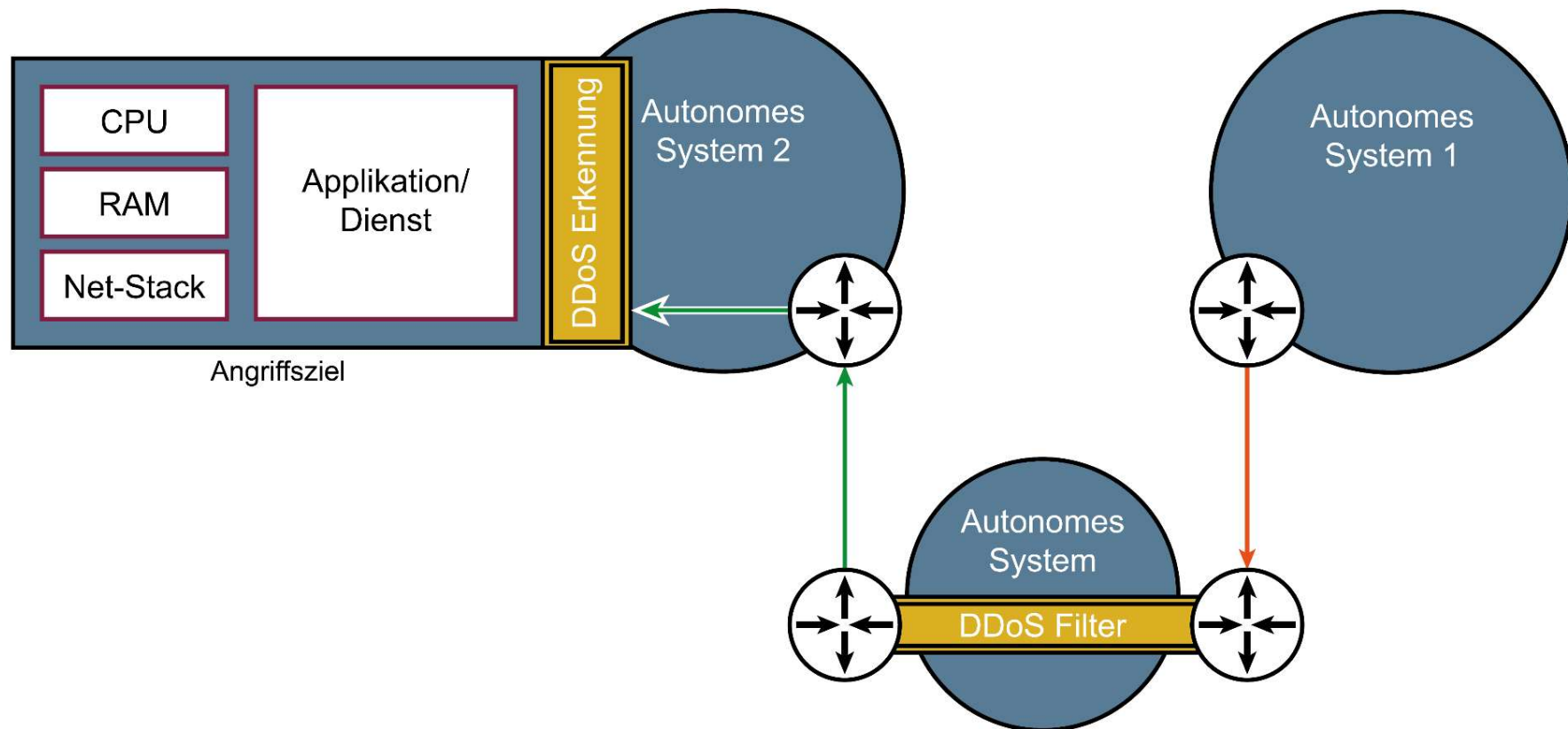
- **Der Schutzmechanismus:**
Die Filtertechnik steht bei einem DDoS-Angriff im Hot-Standby.



Abwehrstrategien

→ Off-Site: Traffic-Scrubbing-Netze

- Nur wenn der DDoS-Erkennungsfiler 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

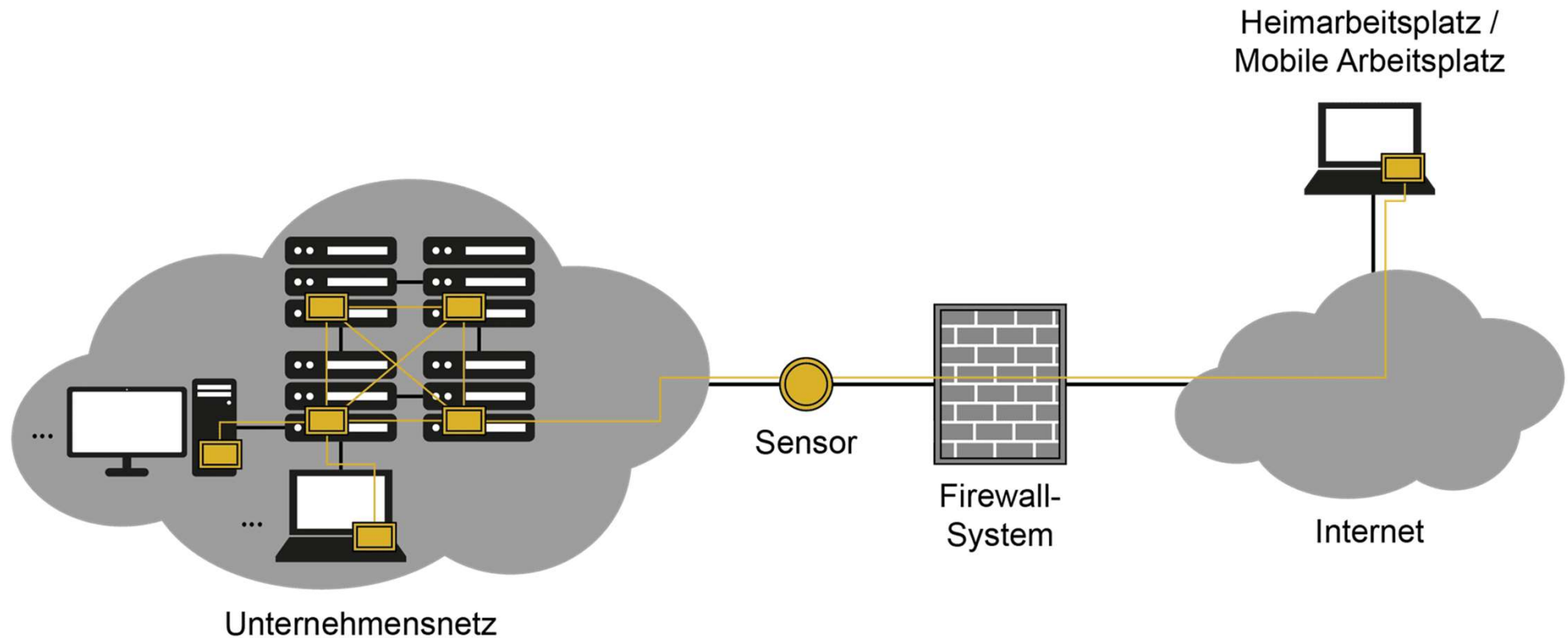
- Proaktive Sicherheitsmechanismen machen IT-Systeme robuster und vertrauenswürdiger.
- Hier spielen **Sicherheitsplattformen** auf der Basis von **intelligenten kryptographischen Verfahren** eine wichtige Rolle.
(**Vertrauenswürdige Basis**)

„ESP-Strategie“

Verhindern, dass man überhaupt ins Schleudern kommt



Zero Trust → Prinzipien

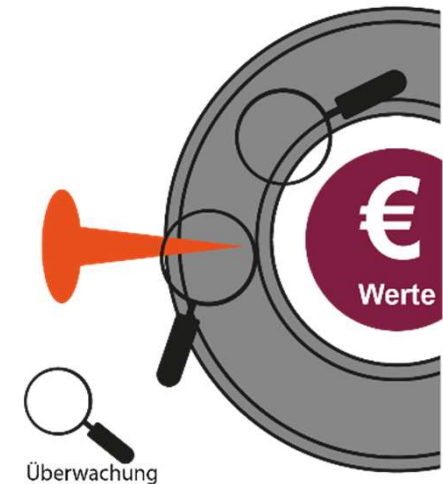


Gegen **mehrstufige Angriffe** auf die IT-Infrastruktur
von Unternehmen (APT)

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.



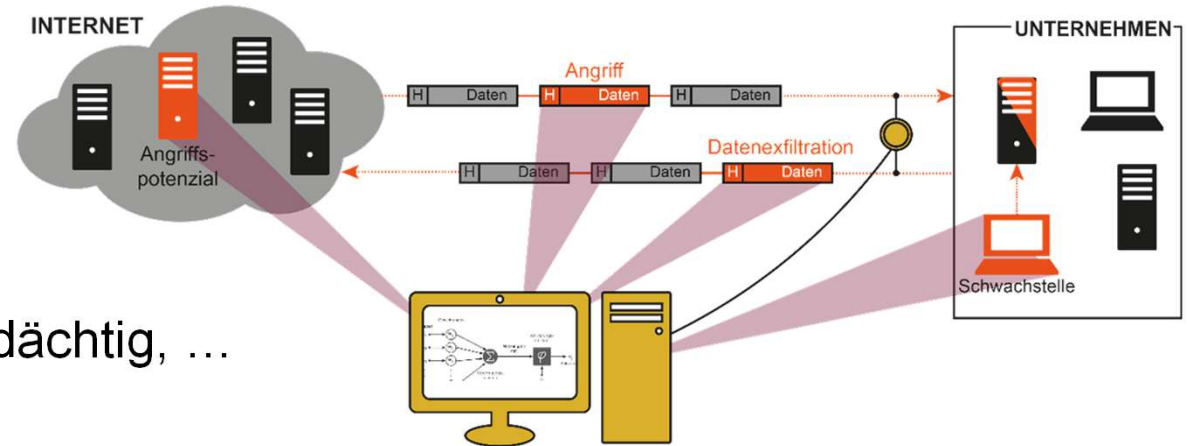
Cyber-Sicherheitsmechanismen

- **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, ...

- 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**

IT-Sicherheit

→ 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

Cyber-Sicherheitsstrategien

→ zur Reduzierung der Risiken für Unternehmen

***IT-Sicherheit
wird in der Zukunft immer wichtiger***

Prof. Dr. (TU NN)

Norbert Pohlmann

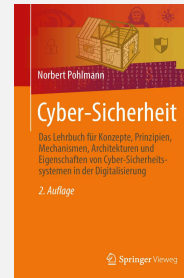
*Professor für Informationssicherheit und
Leiter des Instituts für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen*

if(is)
internet-sicherheit.

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>



Master Internet-Sicherheit

<https://it-sicherheit.de/master-studieren/>



Glossar Cyber-Sicherheit

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



It's all about Trust!

<https://vertrauenswuerdigkeit.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/>

M. Hesse, N. Pohlmann: „Kryptographie (I bis VII): Von der Geheimwissenschaft zur alltäglichen Nutzenanwendung“, 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.

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 Cybersecurity – **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

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