



**Westfälische  
Hochschule**

Gelsenkirchen Bocholt Recklinghausen  
University of Applied Sciences

# **Paradigmenwechseln in der Cyber Security**

→ Wie schützen wir uns in der Zukunft?

Prof. Dr. (TU NN)

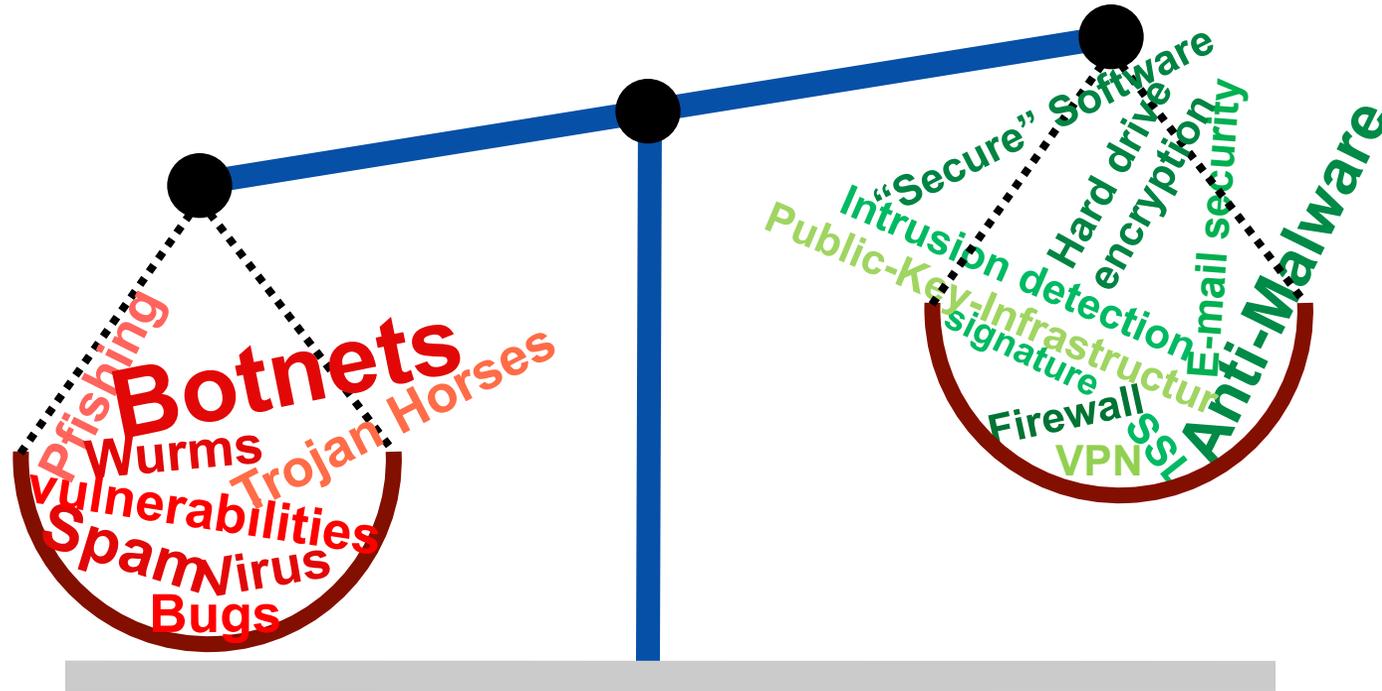
**Norbert Pohlmann**

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

**if(is)**  
internet-sicherheit.

# Cyber Security

## → Situation



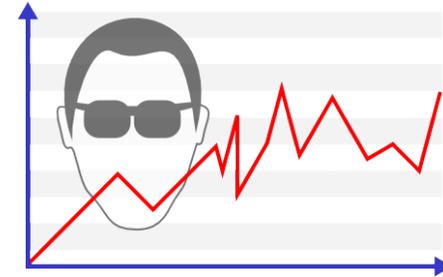
- Professionelle Hacker greifen alles erfolgreich an!
- NSA und Co. sammeln alle Daten und werten fleißig aus!
- Wir haben zurzeit zu viele ungelöste IT-Sicherheitsprobleme

# Cyber Security

## → Problemfelder

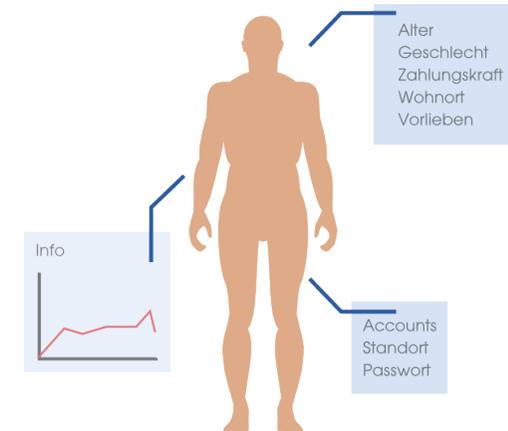
### ■ Wirtschaftsspionage

- 50 Milliarden Euro Schaden im Jahr
- Können wir uns als Wissensgesellschaft nicht leisten!



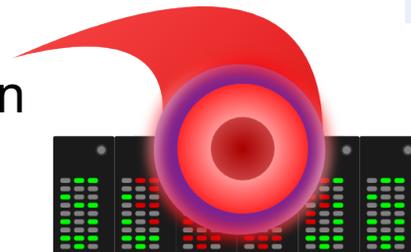
### ■ Der Wert der Privatsphäre

- Eine **Gesellschaft**, die wirtschaftlich und politisch auf die **Eigenverantwortlichkeit des Einzelnen** setzt, muss umgekehrt das **schützen**, was den einzelnen als Sozialwesen und als Wirtschaftsfaktor ausmacht:
  - einerseits seine **persönliche Integrität**,
  - andererseits seinen **materiellen Besitz**.



### ■ Cyber War

- Angriffe auf Kritische Infrastrukturen
- Umstieg auf alternative Energien
- prinzipielle höhere Angreifbarkeit



# Cyber Security

## → Die größten Herausforderungen

### IT Sicherheitsprobleme

Smart Everything  
bringt neue Angriffsvektoren

Zu viele Schwachstellen  
in Software

Cloud  
Computing  
ist eine  
Herausforderung

Internet-Nutzer sind  
nicht sensibilisiert genug

# Risk

Manipulierte IT und IT  
Sicherheitstechnologie

Ungenügender Schutz  
vor Malware

Geschäftsmodell:  
„Bezahlen mit persönlichen Daten“

Unsichere Webserver  
im Feld

Ein zu hohes Risiko bei der  
E-Mail Kommunikation

heute

## Snowden

Neue Gefahren  
durch mobile Geräte

Kein internationales  
Identity Management

Zeit

# Cyber Security

## → Evaluierung

- **Wir kennen die IT-Sicherheitsprobleme**, doch die heute vorhandenen und genutzten IT-Sicherheitssysteme und IT-Sicherheitsmaßnahmen **reduzieren das IT-Sicherheitsrisiko nicht** ausreichend!
- Es handelt sich um ein globales Problem
- Die zukünftigen Angriffe werden die heutigen **Schäden** noch deutlich überschreiten.
- **Wir brauchen Paradigmenwechsel** in der IT und IT-Sicherheit, um das Risiko für unsere Gesellschaft auf ein angemessenes Maß zu reduzieren

# Paradigmenwechsel – (1)

## → Mehr **Verschlüsselung** statt **offen**

- Verschlüsselung für einen nachhaltigen Schutz der Daten (Kommunikation und Speicherung)
  - **IPSec** (jedes 125. IP-Paket – 60%), **SSL/TLS** (jedes 7. IP-Paket – 90%)
  - E-Mail-Verschlüsselung (jede 20. E-Mail), ...
  - Festplatten-, Datei-Verschlüsselung, ...
- **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, ...)

# Paradigmenwechsel – (2)

→ Mehr **Vertrauenswürdigkeit** statt **Gleichgültigkeit**

## ■ Produkthaftung

Software und Hardware arbeiten besser zusammen und Sicherheitsprobleme werden einfacher identifiziert und behoben.



## ■ Evaluierung / Zertifizierung (BSI, ENISA, ISO 27001, eco, ...)

Unabhängige und qualifizierte Organisationen prüfen (verbessern) die Qualität und Vertrauenswürdigkeit von IT und IT Sicherheit in Produkten und Lösungen.



## ■ IT-Security Made in Germany

Qualitätssiegel für vertrauenswürdige IT-Sicherheitslösungen  
(Unternehmenshauptsitz in Deutschland, keine Backdoors, Datenschutz, ...)



# Paradigmenwechsel – (3)

→ 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 – (3)

→ 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



# Paradigmenwechsel – (3)

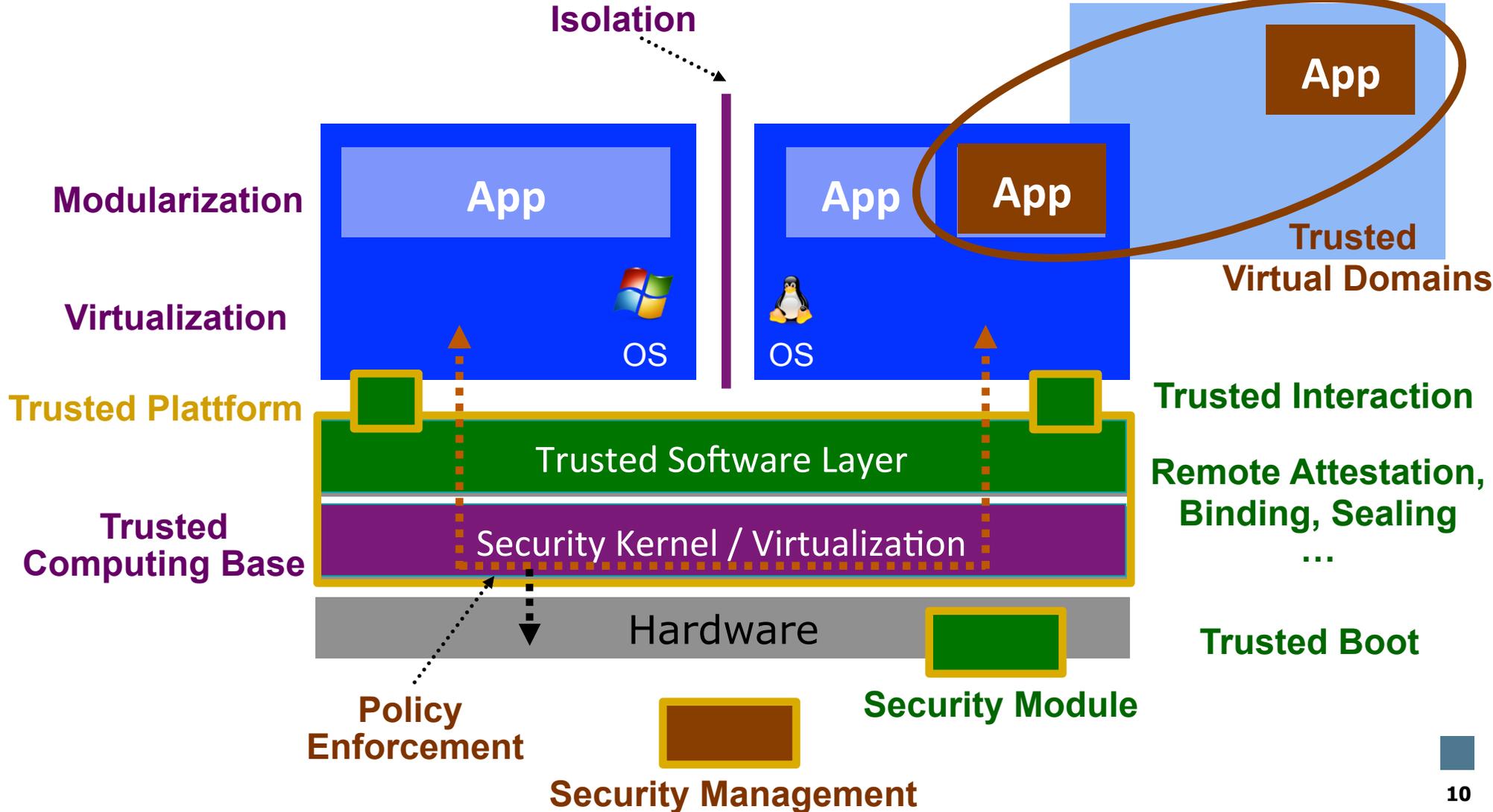
→ Vertrauenswürdige Basis

*Robustness/Modularity*

*Trusted Process*

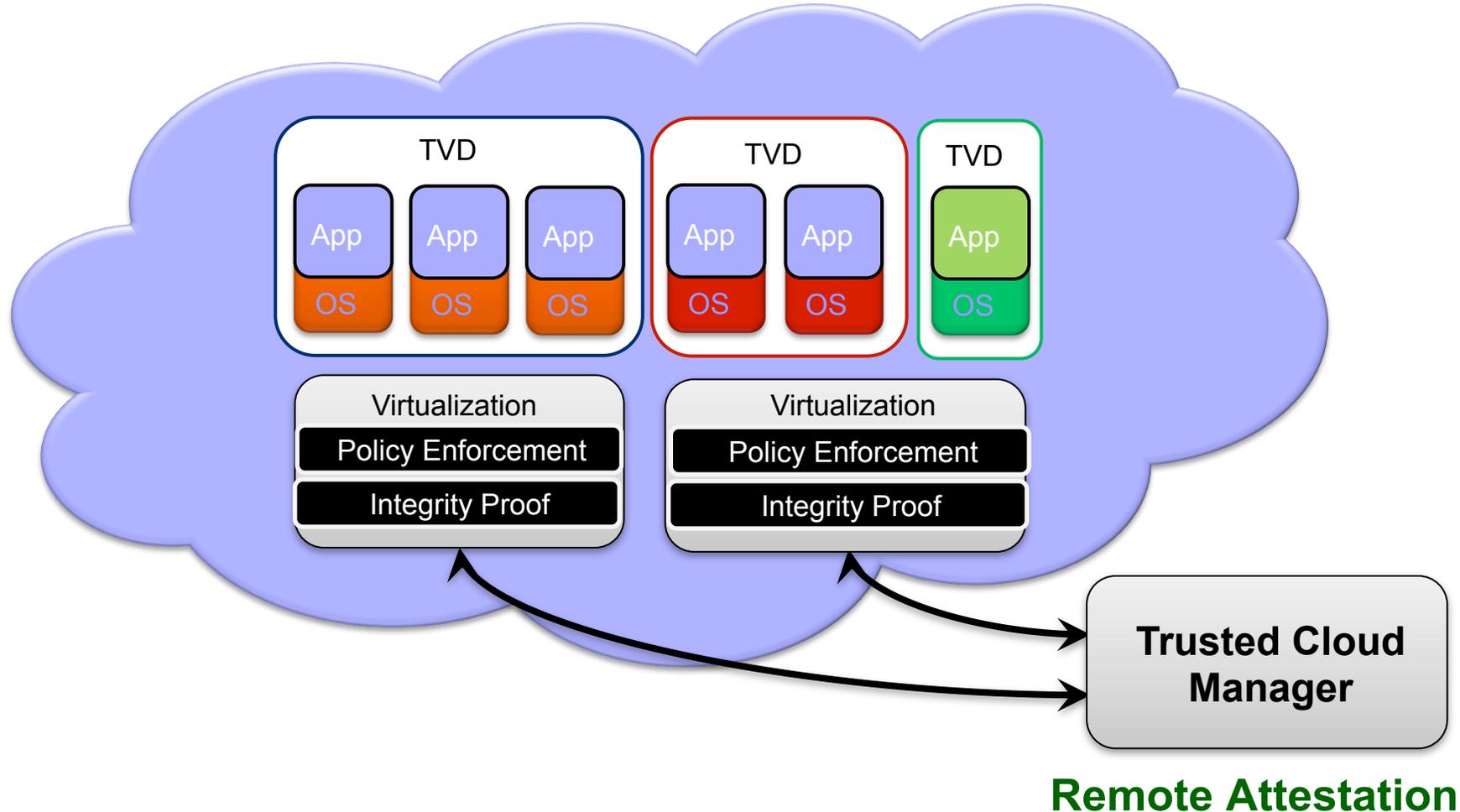
*Integrity Control*

Isolation



# Paradigmenwechsel – (3)

## → Vertrauenswürdige Cloud Rechner

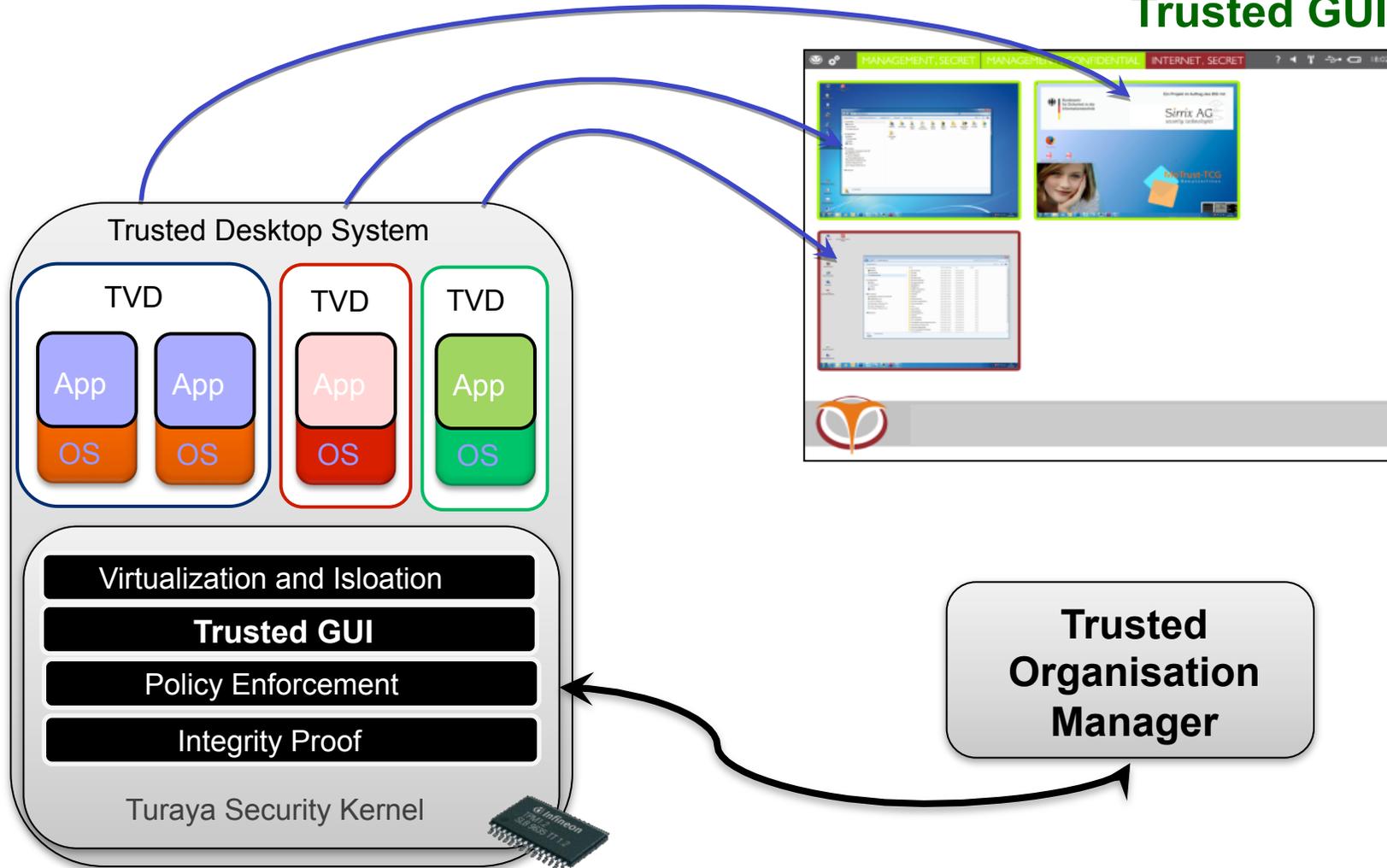


TVD = Trusted Virtual Domains

# Paradigmenwechsel – (3)

## → Vertrauenswürdige Endsysteme

### Trusted GUI

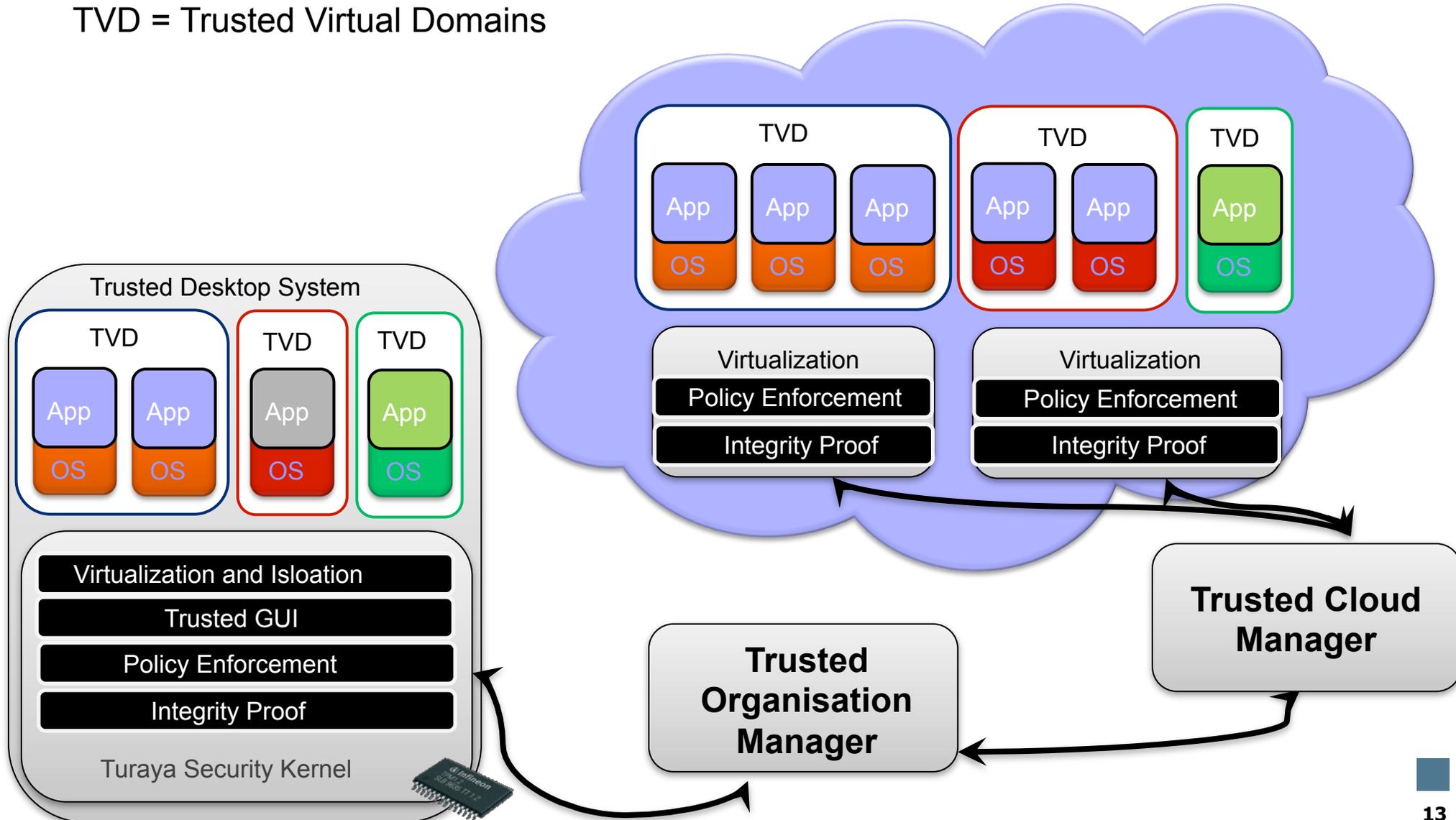


TVD = Trusted Virtual Domains

# Paradigmenwechsel – (3)

## → Proaktive Cloud Sicherheit

TVD = Trusted Virtual Domains



# Paradigmenwechsel – (4)

→ Mehr **Objekt-** statt **Perimeter-Sicherheit** (1/3)

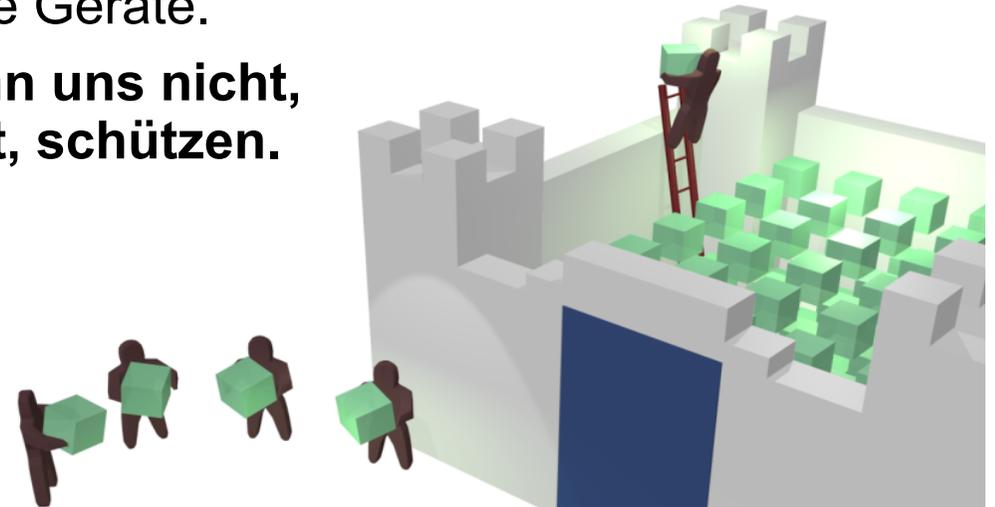
## ■ **Perimeter-Sicherheit (Abschottung „Netz“)**

### ■ **Abwehrmodell:**

- Schützt eine Anzahl von Computern und Netzwerken mit der Hilfe von Firewall-Systemen, VPNs, Intrusion Detection, usw.
- Annahme: Die Computer und das Netz sind fest installiert.

### ■ **Bewertung:**

- Die moderne Geschäftswelt nutzt flexible und verteilte mobile Geräte.
- **Perimeter-Sicherheit kann uns nicht, wie in der Vergangenheit, schützen.**



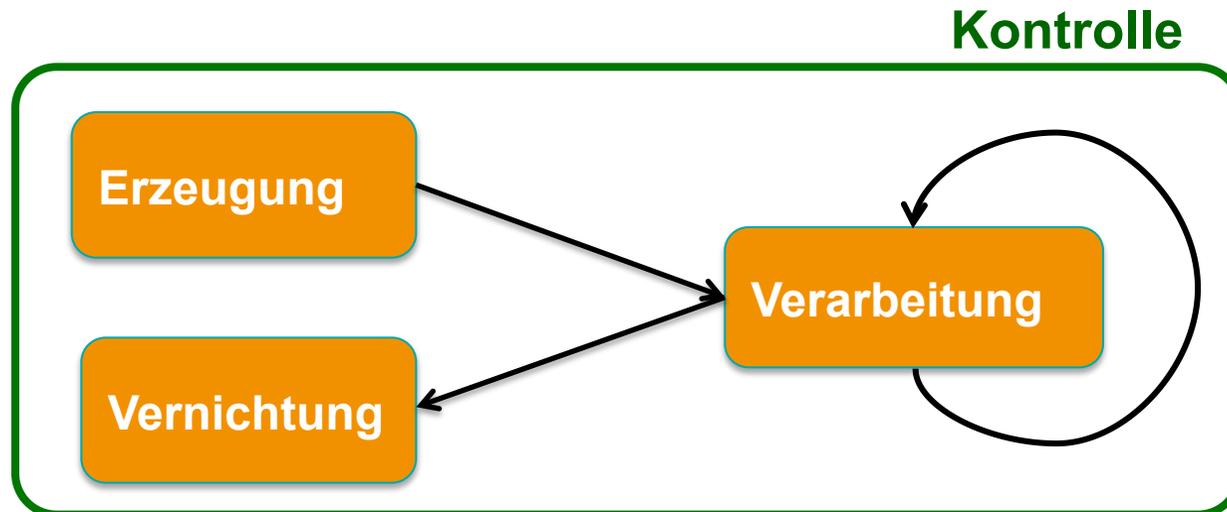
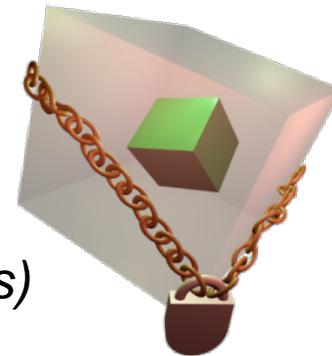
# Paradigmenwechsel – (4)

→ Mehr **Objekt-** statt **Perimeter-Sicherheit** (2/3)

## ■ Objekt-Sicherheit (Informationsflusskontrolle)

- **Idee:** Domänenorientierte Objektsicherheit, bei der die Objekte mit Rechten versehen werden, die definieren, wer sie in welcher IT-Umgebung wie nutzen darf.

- *Object Lifecycle Protection*
- *Distributed Policy Enforcement (even on foreign systems)*



# Paradigmenwechsel – (5)

→ Mehr **Zusammenarbeit** statt **Separation**

**Ungleichgewicht bei Angreifern und Verteidigern im Internet**



**Kooperation hilft das Ungleichgewicht zu überwinden.**

# Cyber Security

## → Zusammenfassung

- **Bewertung der IT-Sicherheit**
  - Die **Angriffsmodelle** innovieren und **Angreifer** werden **professioneller**.
  - Wir kennen die IT-Sicherheitsprobleme, aber **heutige IT-Sicherheitsmaßnahmen** reduzieren das IT-Sicherheitsrisiko **nicht ausreichend!**
- **Wir brauchen Paradigmenwechsel in der IT-Sicherheit, um in der Zukunft das Internet sicherer und vertrauenswürdig nutzen zu können!**
  - Mehr **Verschlüsselung** (*statt offen*)
  - Mehr **Vertrauenswürdigkeit** (*statt Gleichgültigkeit*)
  - Mehr **proaktive IT-Sicherheit** (*statt aktive IT-Sicherheit*)
  - Mehr **Objekt-Sicherheit** (*statt Perimeter-Sicherheit*)
  - Mehr **Zusammenarbeit** (*statt Separation*)
  - ...



**Westfälische  
Hochschule**

Gelsenkirchen Bocholt Recklinghausen  
University of Applied Sciences

# **Paradigmenwechseln in der Cyber Security**

→ Wie schützen wir uns in der Zukunft?

**Mit der Hilfe von Paradigmenwechsel!**

Prof. Dr. (TU NN)

**Norbert Pohlmann**

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

**if(is)**  
internet-sicherheit.



**Westfälische  
Hochschule**

Gelsenkirchen Bocholt Recklinghausen  
University of Applied Sciences

# Nachwuchs gewinnen, Talente binden

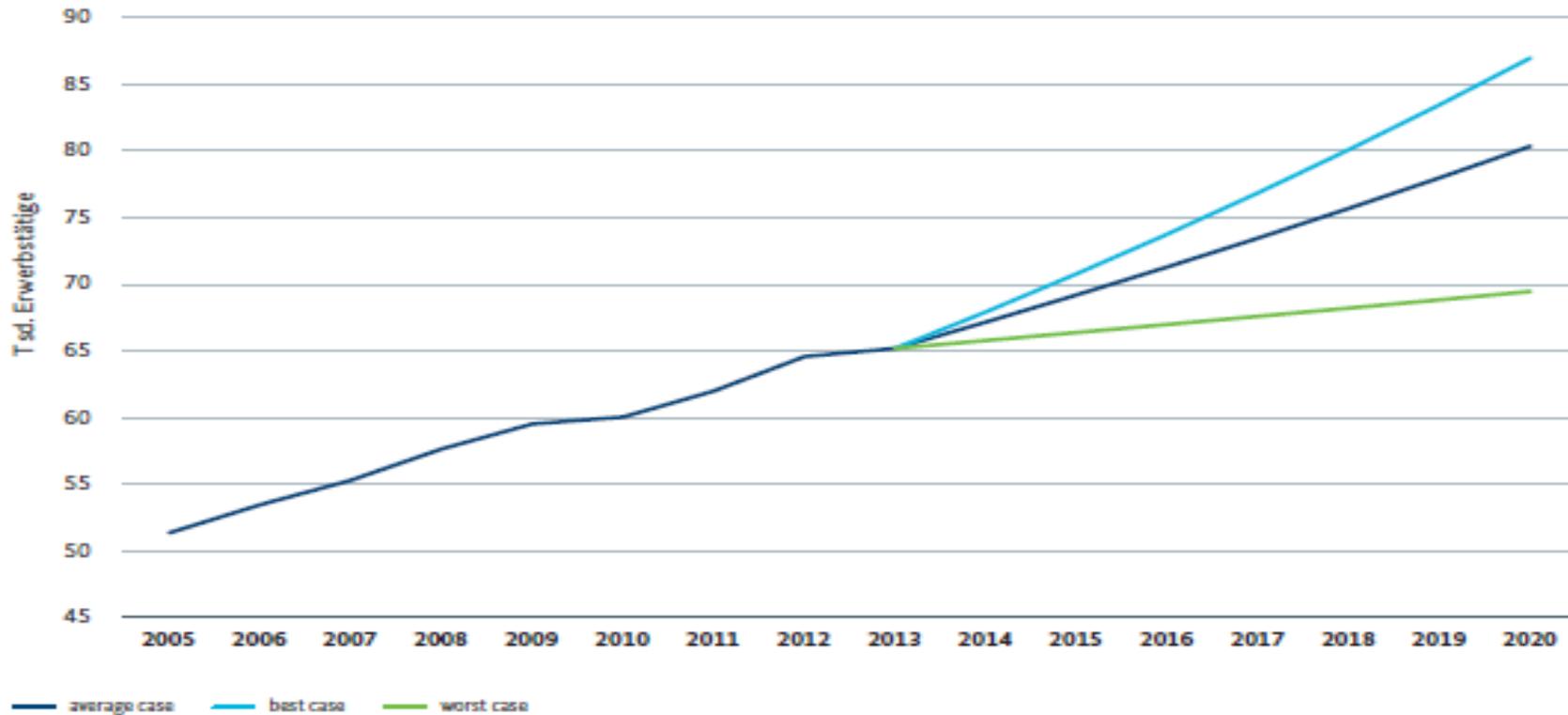
Prof. Dr. (TU NN)

**Norbert Pohlmann**

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

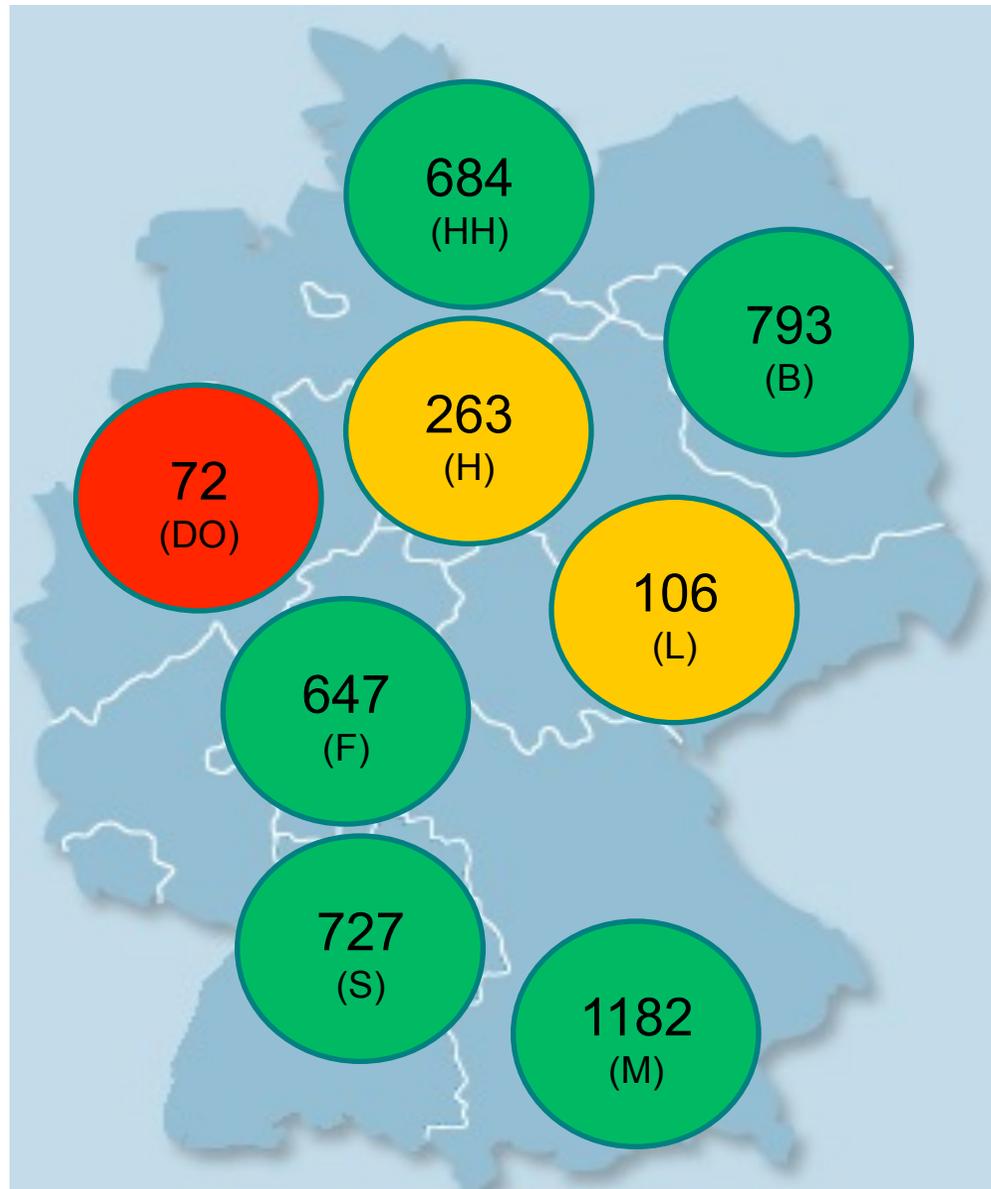
**if(is)**  
internet-sicherheit.

# Entwicklung Arbeitnehmeranzahl → Deutschland



- Bis 2020 werden **zwischen 5.000 und 30.000 neue Fachkräfte** in der IT-Sicherheit benötigt
- Anstieg von 2005 bis 2013: ~ 25%
- **Anstieg von 2005 bis 2020: ~ 70% („best case“)**

# IT-Sicherheit: Stellenangebote



<b>Frankfurt:</b>	<b>647</b>
Dortmund:	72
<b>München:</b>	<b>1.182</b>
<b>Stuttgart:</b>	<b>727</b>
Hannover:	263
<b>Hamburg:</b>	<b>684</b>
Leipzig:	106
<b>Berlin:</b>	<b>793</b>
<b>Gesamt „Marktplatz IT-Sicherheit“:</b>	<b>17.588</b>
	<b>Stellenangebote</b>

# Cyber Security Challenge

- **Junge Menschen (Cyber Security Talente)** für die Cyber Security begeistern, um die Zukunft **sicherer** und **vertrauenswürdiger** gestalten zu können
- Professionelle **IT-Sicherheitsexzellenz** in Deutschland **fördern**



Weitere Runden: Beginn Mai 2015 (Konferenz 15/16.09.15), Mai 2016, ...  
(aber zusätzlich mit einem europäischen Wettbewerb)

- **797 Teilnehmer der Online Challenge**
  - 765 (96 %) **männlich**
  - 32 ( 4 %) **weiblich**
  - 256 (32 %) **Schüler** - 42 (16 %) *aktiv*
  - 541 (68 %) **Studierende** - 133 (25 %) *aktiv*
- **Finalisten (10 Schüler und 10 Studierende)**
  - **Durchschnittsalter**
    - Studierende 23,5 Jahre
    - Schüler 17,4 Jahre
  - **Punktzahl in der Online Challenge**
    - Studierende 230 Punkte (maximal erreichbare Punkte)
    - Schüler 146,9 Punkte (ein Schüler hat auch maximale Punktzahl)



# Wie werden „Hacker“ ausgebildet?

## ■ Studium an Hochschulen



- Westfälische Hochschule Gelsenkirchen
- UNI Bochum, Darmstadt, München, Erlangen, ...
- FH Offenburg, Darmstadt, Albstadt-Sigmaringen, ...
- ...



## ■ Selbststudium



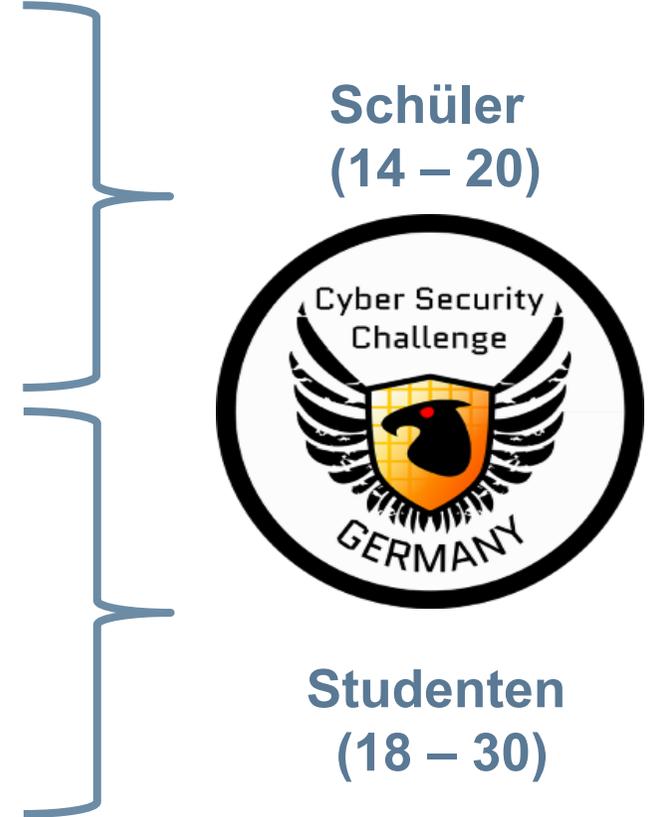
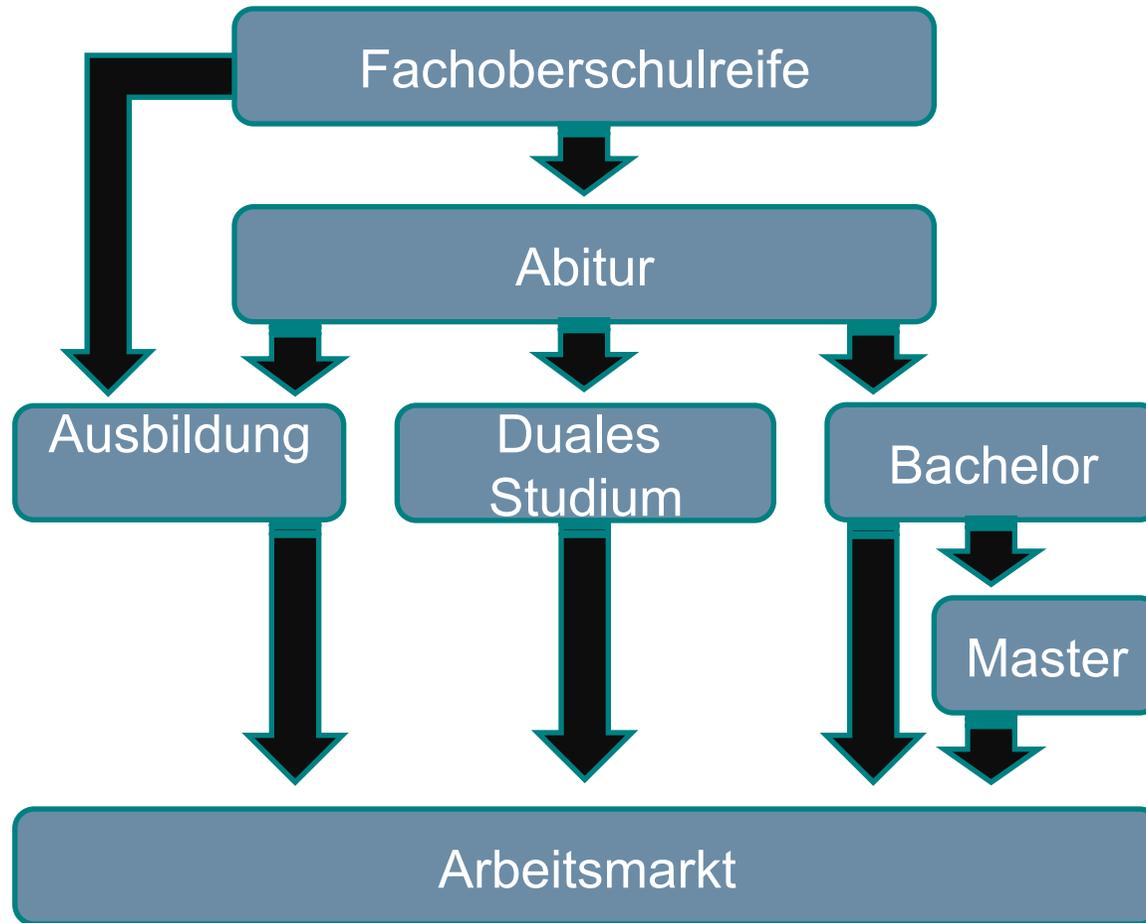
- Bücher
- Gruppen virtuell im Internet
- Zuhause in der Bude durch „learning by doing“
- ...

## ■ Praxis (Unternehmen, ...)



- Weiterbildungen
- Zertifizierungen, wie z.B. TISP, (ISC)<sup>2</sup>, ...
- Fernstudiengänge, ...
- ...

# Cyber Security: Ausbildungswege

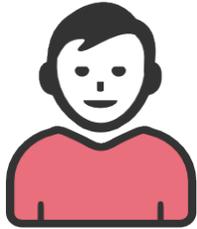


- Die **Cyber Security Challenge** findet auch „versteckte“ **Cyber Security Talente** sehr früh!

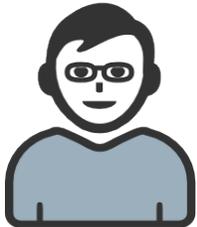
## Hochschulen

### Cyber Security Talente

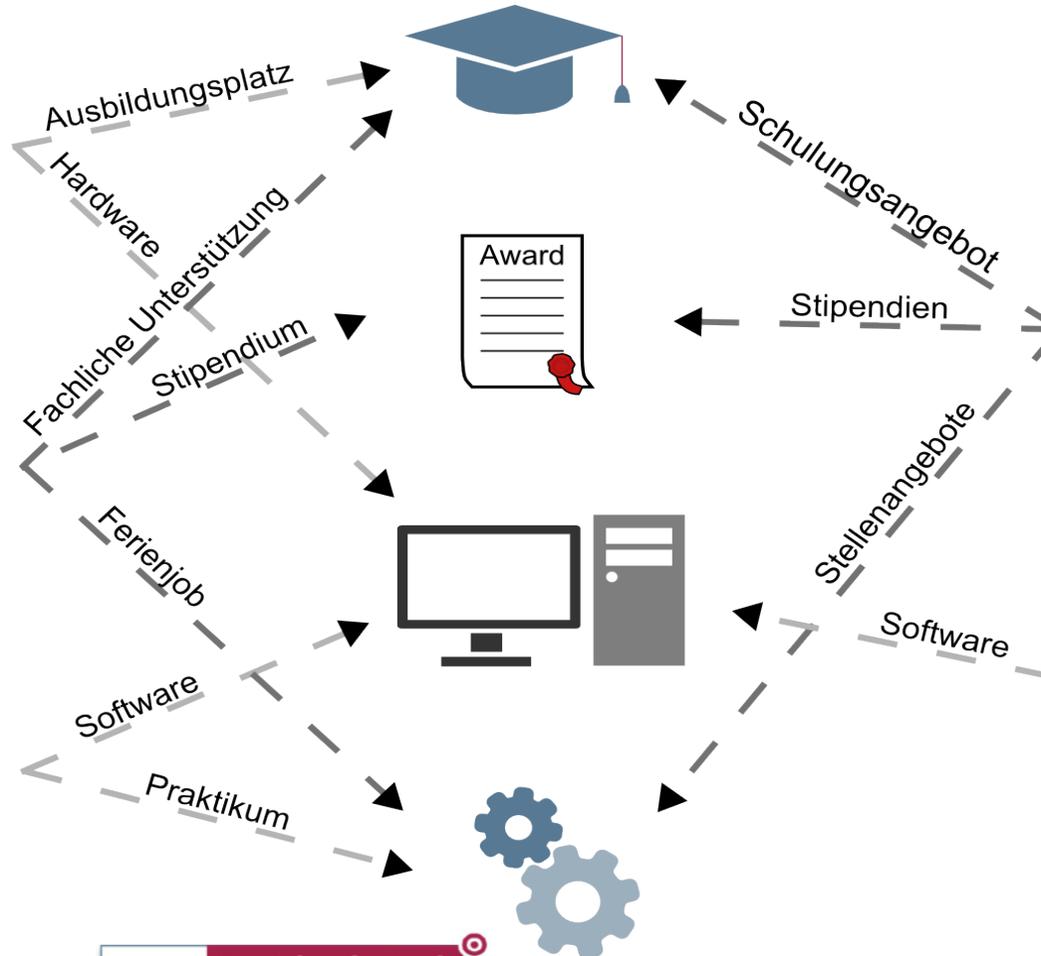
- Geld
- Aktion
- ...



- Sozial
- Freiheit
- ...



- Keller
- Ruhe
- ...



### Unternehmen, ...

- Bester Arbeitgeber DE
- Wollen mehr Sicherheit
- ...



- Zahle viel Geld
- Erwarte viel
- ...



**Westfälische  
Hochschule**

Gelsenkirchen Bocholt Recklinghausen  
University of Applied Sciences

# **Cyber Security Talente** **für mehr IT-Sicherheit und** **Vertrauenswürdigkeit in der Zukunft**

Prof. Dr. (TU NN)

**Norbert Pohlmann**

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

**if(is)**  
internet-sicherheit.