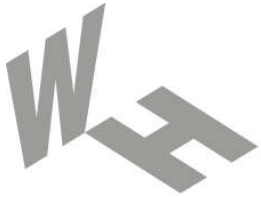


Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

# Security:
# Zu komplex für Angriffe *oder* digital außer Kontrolle?


Prof. Dr. (TU NN)
**Norbert Pohlmann**

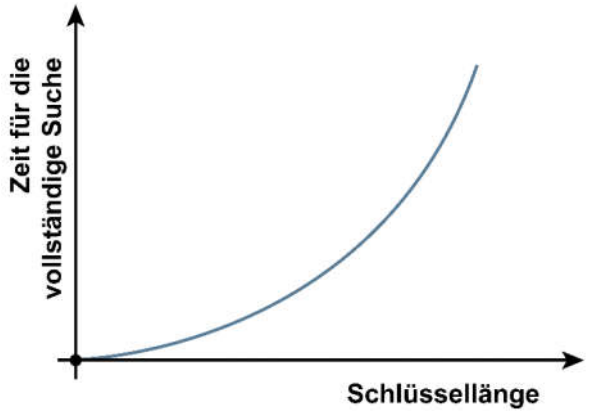
Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
**http://www.internet-sicherheit.de**


if(is)
internet-sicherheit.

# **Komplexität** ist **IT-Sicherheit** → **Kryptographie (1/2)**

- **Kryptographie** spielt eine **besondere Rolle** bei vielen wichtigen **Cyber-Sicherheitssystemen** (Verschlüsselung, Signatur, Hashfunktionen, …).
- Die **Sicherheit von Kryptographie** hängt von der **Geheimhaltung der Schlüssel** ab.
- **Angriffsmethode:** Vollständige Suche (Brute-Force-Methode) besteht im Wesentlichen im Ausprobieren aller möglichen Schlüsselkombinationen.
- **Praktische Sicherheit:** Es ist zwar theoretisch möglich, jedes Kryptosystem zu brechen, praktisch wird dazu jedoch so viel **Rechnerkapazität** benötigt, dass dieser Weg aussichtslos erscheint und deswegen nicht umgesetzt werden kann.

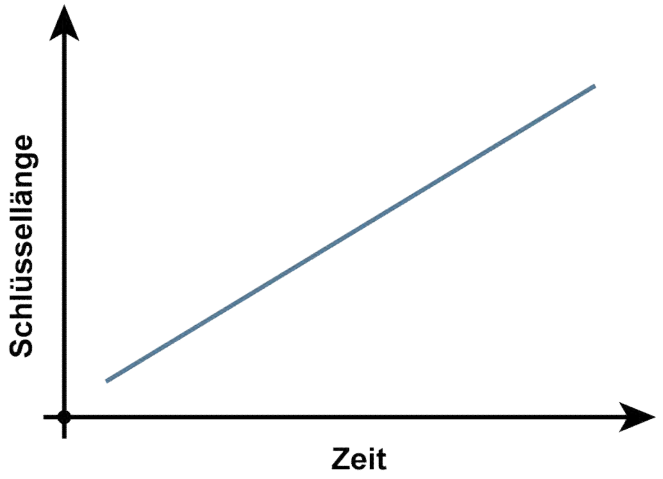
| **Schlüssellänge** in Bits | **Anzahl der möglichen Schlüssel** | **Aufwand**, den richtigen Schlüssel zu finden, in Jahren. (Annahme dieser Betrachtung: 1.000.000.000 Versuche in der Sek.) |
|---|---|---|
| 8 | 256 | 0,00000 |
| 40 | 1.099.511.627.776 | 0,00002 |
| 56 | 72.057.594.037.927.900 | 1,14 |
| 64 | 1,84E+19 | 292,47 |
| 128 | 3,40E+38 | 5.391.448.762.278.160.000.000 (länger als das Universum bisher existiert) |
| 192 | 6,27E+57 | 9,95E+40 |
| 256 | 1,16E+77 | 1,83E+60 |




**Komplexitätsklasse exponentiell $O(2^n)$**

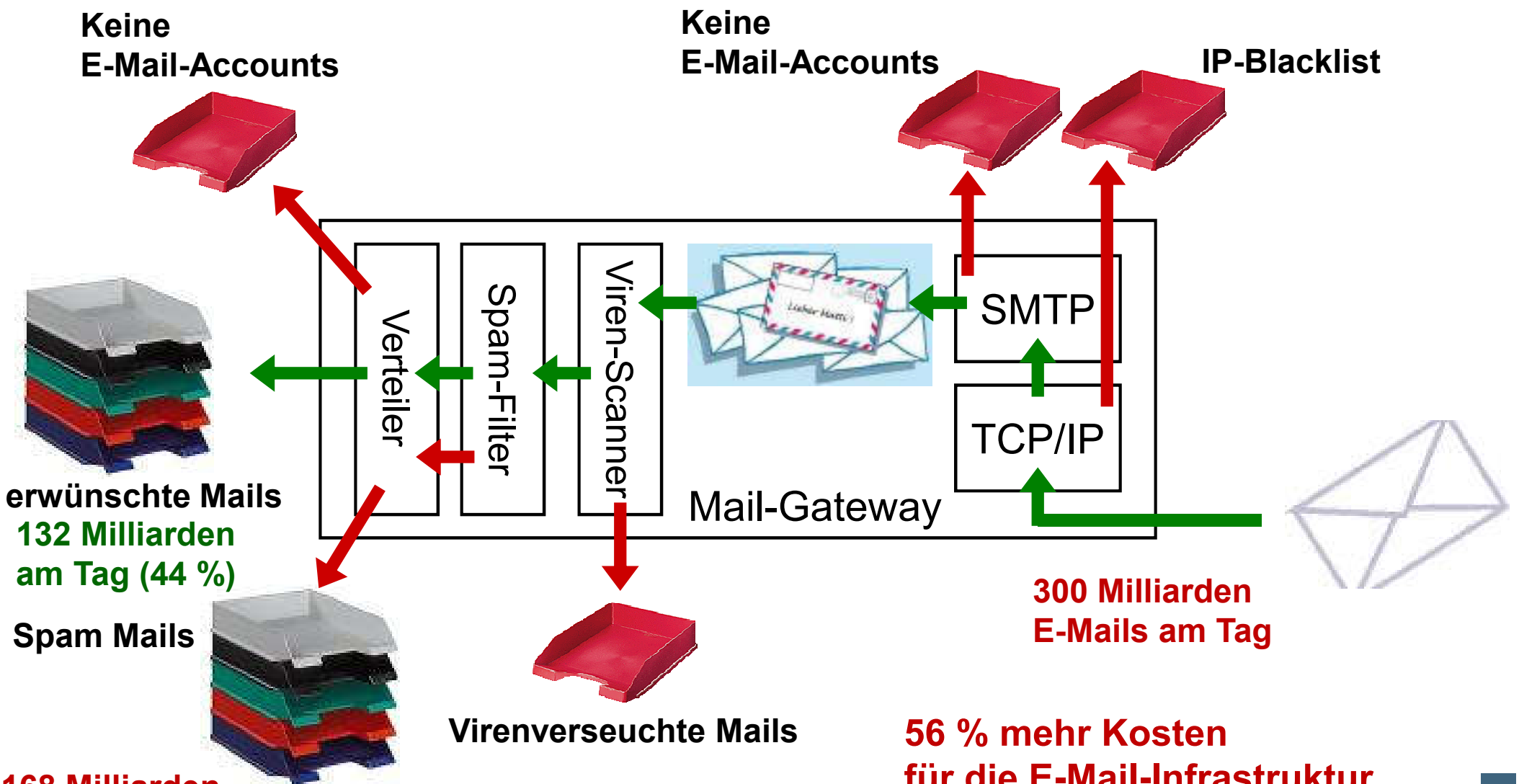
# Komplexität ist IT-Sicherheit → Kryptographie (2/2)

- **Ein Wettlauf um die Sicherheit**
  - **Mehr Rechnerkapazität** bedeutet, **weniger Sicherheit!**
  - Da die **Rechnerkapazität** ständig wächst, müssen auch die **Schlüssellängen / Verfahren von Zeit zu Zeit angepasst werden**.
  - Der **Aufwand ist sehr hoch** und die Zeit für eine **Umstellung ist recht lange**.

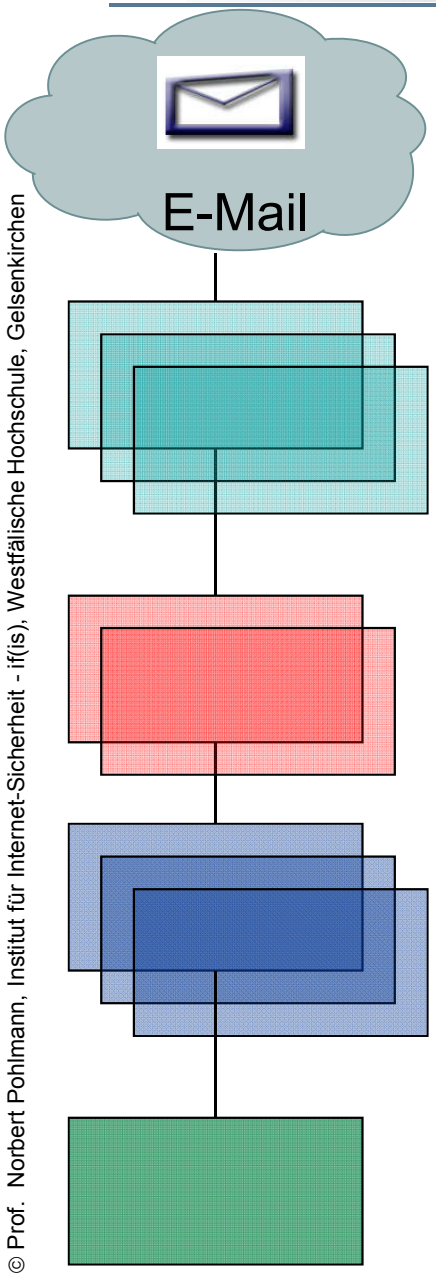



- **Quantencomputer:** Das Damoklesschwert der Kryptographie
  - **Shors Algorithmus:** macht asymmetrische Verfahren unbrauchbar!
  - **Grover Algorithmus:** halbiert die Schlüssellänge von symmetrischen Verfahren!
  - **Lösung:** Post-Quanten-Kryptographie (ist in der NIST-Auswahl, muss eingeführt werden)

# Komplexität E-Mail
## → Spam



# Anti-Spam-Techniken
## → Das Ebenen-Modell




### Ext. E-Mail-Gateway / E-Mail-Proxy als Teil einer Firewall

- Checks auf IP-Ebene (IP-Adresse)
  - **Blacklists** (RBLs, Dynamische-/Dial-Up-IP, open relay, ...)
  - IP Reputation System
  - **Frequenzmessung**
- Checks auf SMTP-Ebene
  - Überprüfen der HELO-Angabe
  - Überprüfen der Absender-E-Mail-Adresse (Black-/White-/Greylist)
  - Existenz der Empfänger-E-Mail-Adresse (DB, Verzeichnisdienst)

1

### Spam-Filter

- Checks auf E-Mail-Ebene
  - Wortliste, Hash/Signatur, …
- …

2

### Viren-Filter

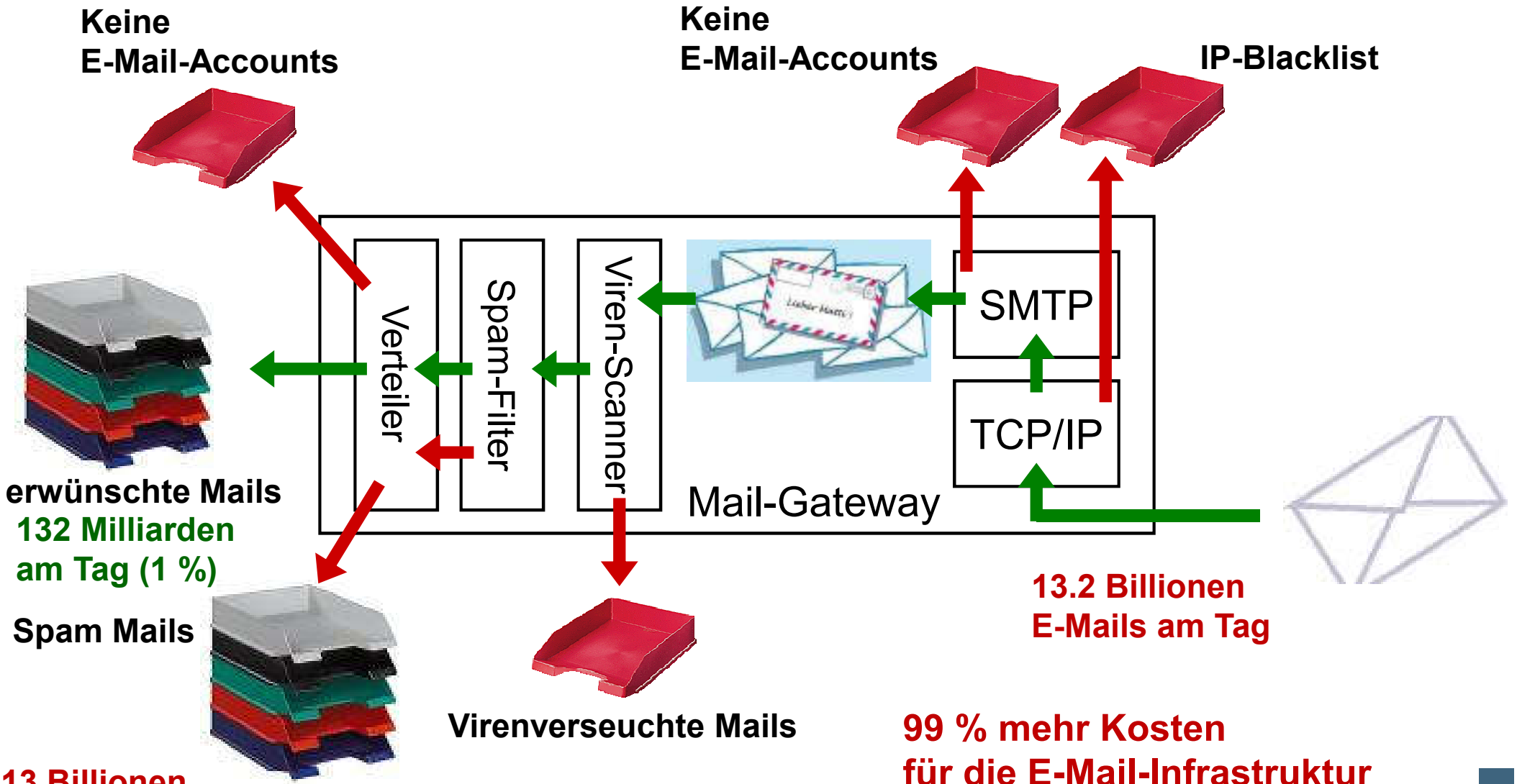
- Checkt E-Mails und Anhänge auf Virenbefall

3

### Interner E-Mail-Server

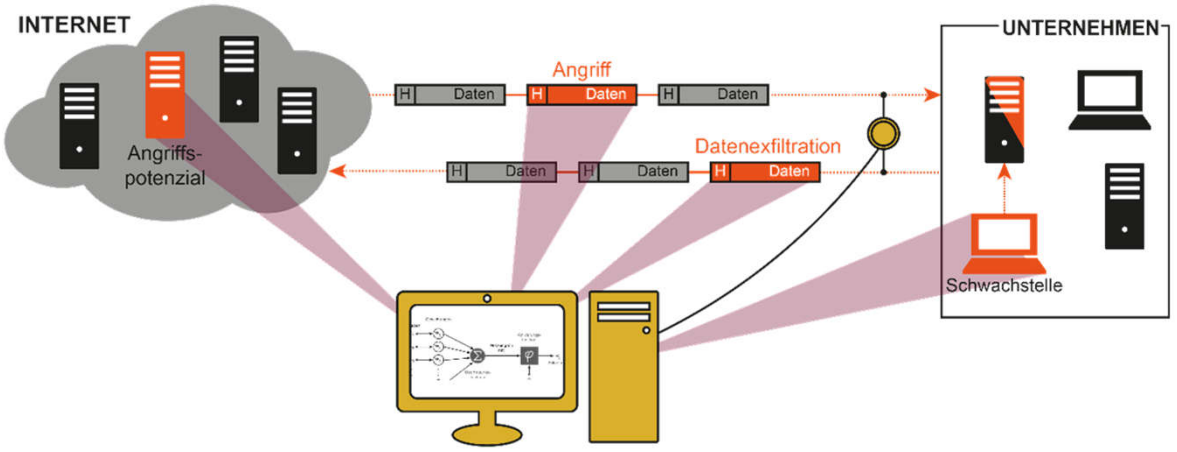
Ressourcenverbrauch

# Komplexität E-Mail
## → Spam ohne Ebene 1



# Komplexität eine Herausforderung → für die IT-Sicherheit (1/3)

## Kommunikationslagebild (Angriffserkennung)




- **Ziele**
  - Erkennen von Angriffen
  - Analyse u. Auswertung der Angriffe und Angriffspotentiale
  - Übersicht u. Bewertung der Kommunikationslage

- **Komplexität (Reduktion) für die Nutzung von KI**
  - Kombination in IP-Pakten (~1000 Byte) = 1,7E+2408
  - Kombination IP+TCP Header (320 Bit) = 2,1E+95
  - Spezialsensor: 4.000.000 mögliche Kommunikationsmerkmale
  - 20.000 bis 120.000 + 50% werden genutzt
  - Ca. 3.000 repräsentieren alle (Zusammenhänge: Architektur, Modelle, …)
  - Wichtigsten davon, um abnormales Verhalten zu identifizieren

# Komplexität eine Herausforderung → für die IT-Sicherheit (2/3)

## Komplexität von Angriffen und deren Einschätzung

- **30.893.191** Angriffe am Tag bei der Telekom (29.06.19)
- 5 bis 10 davon sind relevant, leider ist unklar, welche!
- Es werden sehr viele Hundertschaften von Cyber-Sicherheitsexperten benötigt
  - Sehr teuer (Mangelware)
  - Stehen nicht zur Verfügung (es gibt nicht genug)

- **KI: Unterstützung / Entlastung** von **Cyber-Sicherheitsexperten**
  - Erkennen von **wichtigen** sicherheitsrelevanten Ereignissen *(Priorisierung)*
    - KI analysiert die Angriffsdaten und ermittelt Prioritäten
  - **(Teil-)Autonomie** bei Reaktionen, … Erhöhung der Resilienz, …
    - Reduktion von Angriffsflächen
      (Business läuft weiter, Schäden werden reduziert)

# Komplexität eine Herausforderung → für die IT-Sicherheit (3/3)

**Verbesserungen** von bestehenden **Cyber-Sicherheitslösungen**

- KI leistet einen Beitrag zu einer erhöhten Wirkung und Robustheit
- Z.B.: Risikobasierte und adaptive Authentifizierung

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

# Security:
# Zu komplex für Angriffe *oder* digital außer Kontrolle?

## Mit KI für Cyber-Sicherheit in die 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.

# Anhang / Credits

## Wir empfehlen

- **Kostenlose App securityNews**




- **7. Sinn im Internet (Cyberschutzraum)**
  https://www.youtube.com/cyberschutzraum


- **Master Internet-Sicherheit**
  https://it-sicherheit.de/master-studieren/


## Besuchen und abonnieren Sie uns :-)

**WWW**
https://www.internet-sicherheit.de

**Facebook**
https://www.facebook.com/Internet.Sicherheit.ifis

**Twitter**
https://twitter.com/_ifis

**YouTube**
https://www.youtube.com/user/InternetSicherheitDE/

**Prof. Norbert Pohlmann**
https://norbert-pohlmann.com/

## Quellen Bildmaterial

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

## 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/