



**Westfälische  
Hochschule**

Gelsenkirchen Bocholt Recklinghausen  
University of Applied Sciences

# **Eine strategische Sichtweise auf die sich verändernden IT-Sicherheitsprobleme**

Prof. Dr. (TU NN)

**Norbert Pohlmann**

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

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

- **Internet und IT-Sicherheit**  
(Situation, Problemfelder, Herausforderungen)
- **Prinzipielle IT Sicherheitsstrategien**  
(Fokussierung, Vermeiden, Entgegenwirken, Erkennen)
- **Technologien und Vorgehensweise**  
(spotuation, Xign, ...)
- **Fazit und Ausblick**

- **Internet und IT-Sicherheit**  
(Situation, Problemfelder, Herausforderungen)
- **Prinzipielle IT Sicherheitsstrategien**  
(Fokussierung, Vermeiden, Entgegenwirken, Erkennen)
- **Technologien und Vorgehensweise**  
(spotuation, Xign, ...)
- **Fazit und Ausblick**

# Internet und IT-Sicherheit

## → Situation

- Wir entwickeln uns zur einer **Internet-Gesellschaft** (*Informationsquelle, eCommerce, eGovernment, ..., eAssistenten, ..., Industrie 4.0, Internet der Dinge, ...*)
- Viele lokale Dienste werden **an das Internet gebunden** (*intelligente Analysen → Internetkonnektivität*)
- **Private- und Unternehmensdaten** „lagern“ immer häufiger **im Internet** (*zentrale Speicherung → Internetkonnektivität*)
- Die IT und IT-Sicherheitstechnologien sind nicht sicher und vertrauenswürdig genug (**Widerstandsfähigkeit**)!
- Professionelle **Hacker greifen alles erfolgreich an!**
- Das **Risiko wird immer größer**, die Schäden auch!



# Was sind die Problemfelder?

## → 1. Privatheit und Autonomie

### Verschiedenen Sichtweisen

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



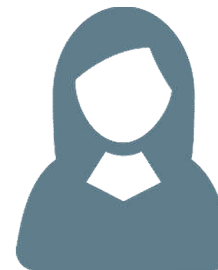
**Geschäftsmodelle**  
„Bezahlen mit persönlichen Daten“



# Privatheit / Autonomie



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



**Nutzer:** Autonomie im Sinne der Selbstbestimmung

# Was sind die Problemfelder?

## → 2. Wirtschaftsspionage



ca. 51 Milliarden € Schaden pro Jahr

# Wirtschaftsspionage



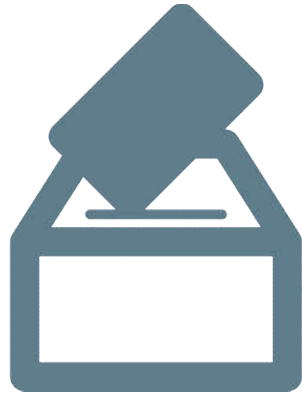
Zum Vergleich:

Internet-Kriminalität: ca. 100 Millionen € pro Jahr  
(Online Banking, DDoS, ...)



# Was sind die Problemfelder?

## → 3. Cyberwar



Umsetzung von politischen Zielen  
→ Einfach und „preiswert“

Cyberwar



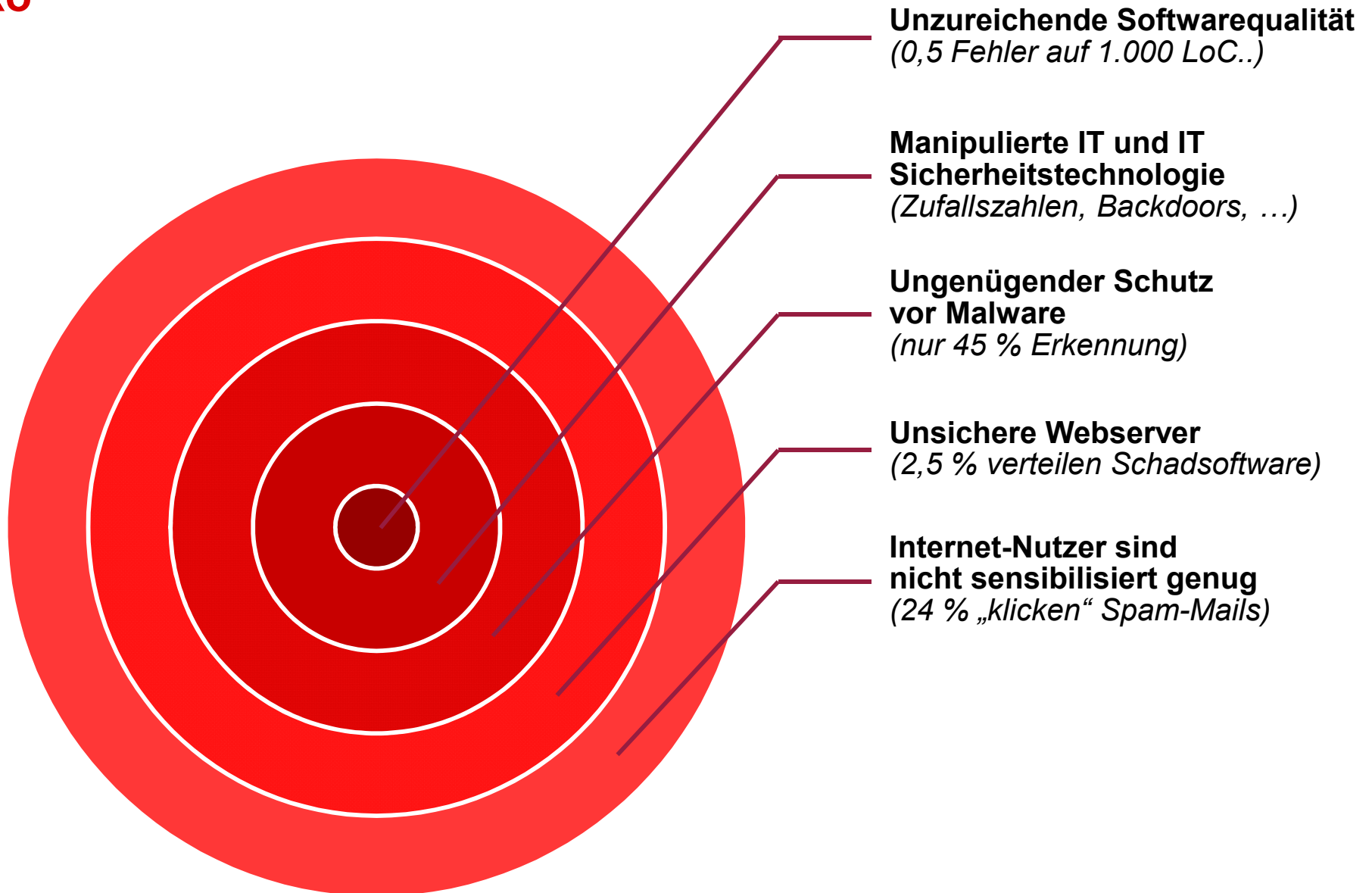
Angriffe auf Kritische Infrastrukturen  
z.B. Stromversorgung, Wasserversorgung, ...



# IT-Sicherheit

## → Die größten Herausforderungen

### Risiko



# Aktuelle Herausforderungen → mit aktuellen Risiken

- **Kein internationales Identity Management**  
*(Passworte für die Authentifikation im Internet, ...)*
- **Neue Gefahren** durch mobile Geräte  
*(BYOD, Masse statt Klasse, Tracking, Verlust/Diebstahl, ...)*
- **Ein zu hohes Risiko** bei der Kommunikation  
*(E-Mail, Web, Chat, ...)*
- **Cloud Computing** ist eine große **Herausforderung**  
*(Session Hijacking, Ort der Speicherung, ...)*
- ...





# Internet und IT-Sicherheit

## → Evaluierung der Situation

- **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 innovative Ansätze** im Bereich der Internet-Sicherheit, um das Risiko für unsere Gesellschaft auf ein angemessenes Maß zu reduzieren

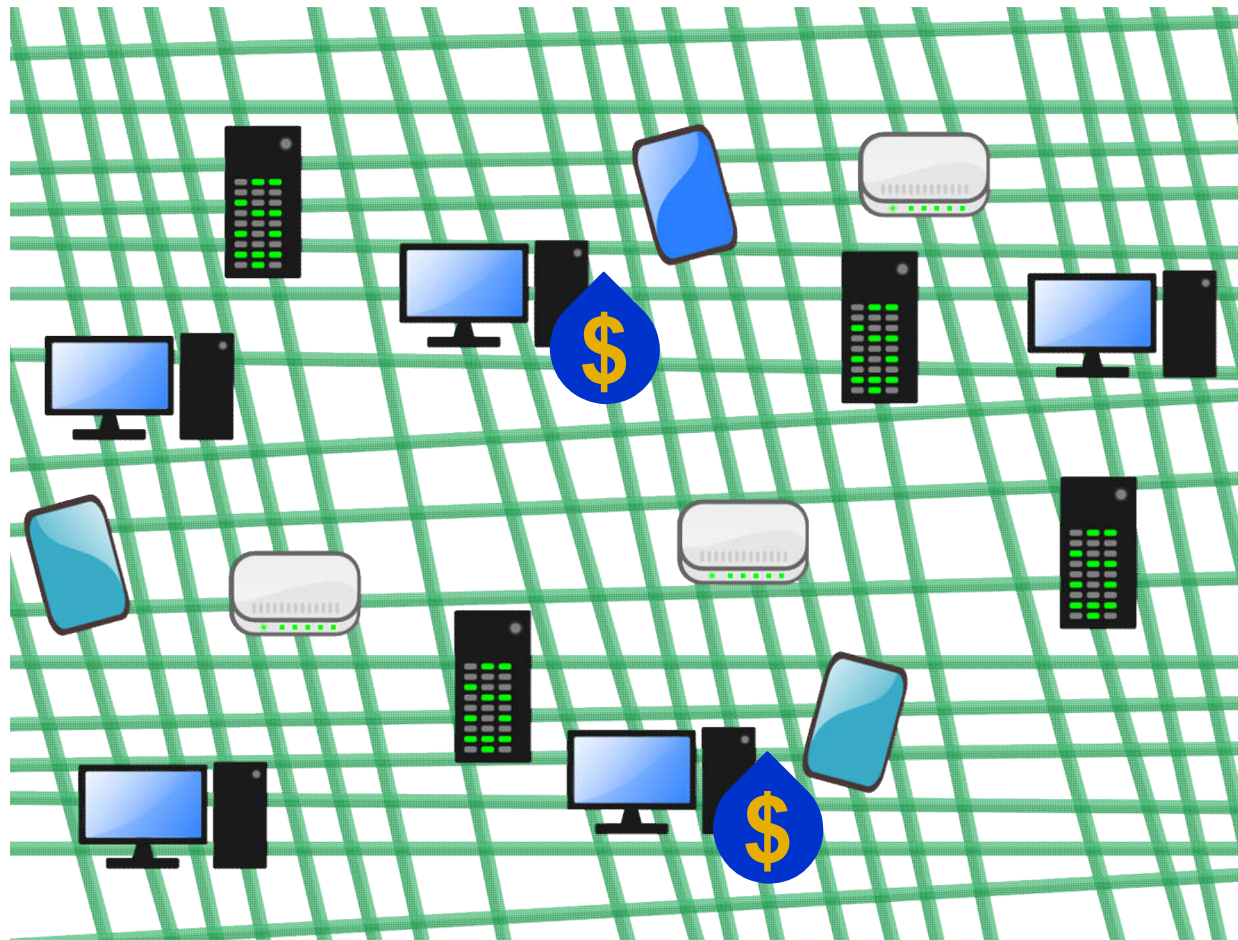


- **Internet und IT-Sicherheit**  
(Situation, Problemfelder, Herausforderungen)
- **Prinzipielle IT Sicherheitsstrategien**  
(Fokussierung, Vermeiden, Entgegenwirken, Erkennen)
- **Technologien und Vorgehensweise**  
(spotuation, Xign, ...)
- **Fazit und Ausblick**

# Prinzipielle IT Sicherheitsstrategien

## → Fokussierung

- Im Schnitt sind nur ca. **5 %** aller vorhandenen Daten in Unternehmen **besonders schützenswert**.



- Aber **welche Daten** sind besonders schützenswert und wie können diese **angemessen geschützt** werden?

# Prinzipielle IT Sicherheitsstrategien

## → Vermeiden von Angriffen – (1)

- **Generell gilt: Das Prinzip der digitalen Sparsamkeit.**  
→ So wenig Daten generieren wie möglich, so viele wie nötig.
- **Keine Technologie und Produkte mit Schwachstellen verwenden**  
(z.B. Browser, Betriebssysteme, Internet-Dienste, ...)

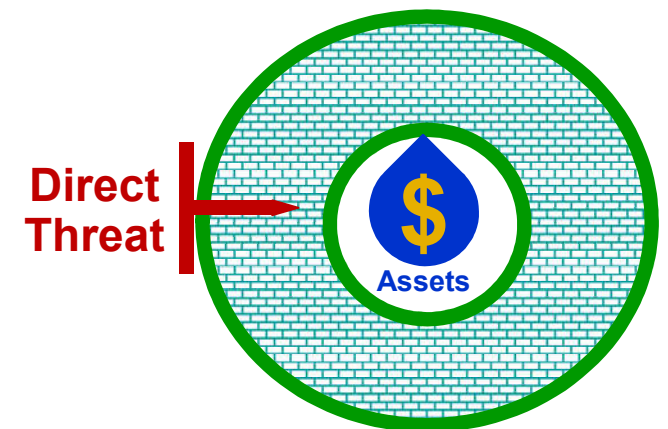


- **Bewertung der Vermeidung**
  - **Vermeidung von Angriffen ist die beste IT-Sicherheitsstrategie!**
  - **Ist nur begrenzt umsetzbar, wenn wir IT mit allen Vorteilen nutzen wollen!**

# Prinzipielle IT Sicherheitsstrategien

## → Entgegenwirken von Angriffen – (2)

- Meist verwendete IT-Sicherheitsstrategie
- Beispiele, bei denen ein hoher Nachholbedarf besteht:
  - **Verschlüsselungssicherheitssysteme**  
(Datei-, Festplatten-, E-Mail-Verschlüsselung, VPN-Systeme, SSL, ...)
  - **Authentikationsverfahren**  
(Challenge-Response, globale Identität, Föderation, ...)
  - **Vertrauenswürdige IT-Systeme**  
(Security Kernel, Isolierung u. Separierung, ..)
  - ...

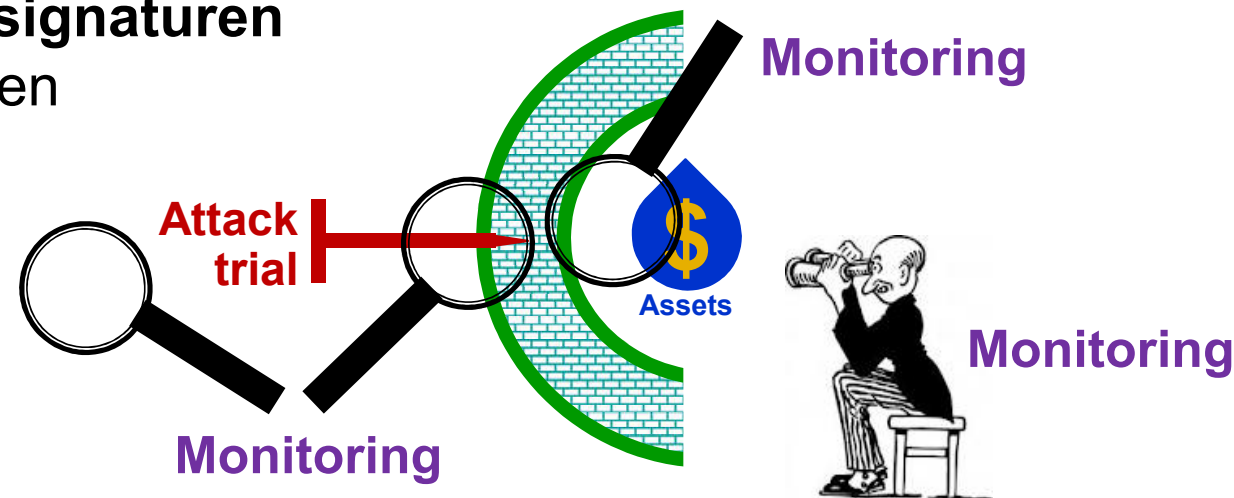


- **Bewertung des Entgegenwirkens**
  - Eine naheliegende IT-Sicherheitsstrategie
  - **Leider stehen zurzeit nicht genug *wirkungsvolle* und *vertrauenswürdige* IT-Sicherheitstechnologien, -lösungen und -produkte zur Verfügung oder sind im Einsatz**

# Prinzipielle Sicherheitsstrategien

## → Erkennen von Angriffen – (3)

- **Erkennen** von Angriffen, denen nicht entgegengewirkt werden kann
- Angriffe erkennen und versuchen, den Schaden so schnell wie möglich zu minimieren (APT)
- Generell IT-Sicherheitssysteme, die Warnungen erzeugen, wenn Angriffe mit Hilfe von **Angriffssignaturen** oder **Anomalien** erkannt werden



- **Bewertung des Erkennens**
  - Die IT-Sicherheitsstrategie, Erkennen von Angriffen, ist sehr hilfreich, hat aber definierte Grenzen

- **Internet und IT-Sicherheit**  
(Situation, Problemfelder, Herausforderungen)
- **Prinzipielle IT Sicherheitsstrategien**  
(Fokussierung, Vermeiden, Entgegenwirken, Erkennen)
- **Technologien und Vorgehensweise**  
(spotuation, Xign, ...)
- **Fazit und Ausblick**

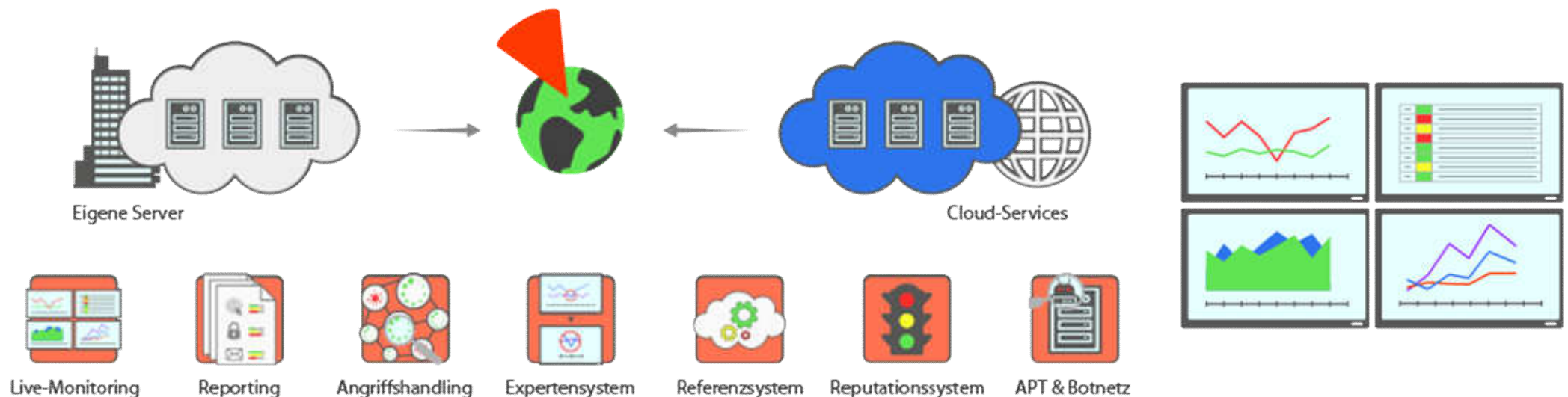
# Bewusstsein für den eigenen Schutzbedarf → Angemessenheit

- Für Bedrohungen existieren immer „Gegenmaßnahmen“ (Strategien)
  - Sichere Passwörter, Displaysperren, Verschlüsselung, ...
- Wir können keine 100%ige Sicherheit erreichen
  - Unmöglich, denn z.B.: Software hat immer ausnutzbare Fehler
  - Gerät man unbewusst ins Visier eines Angreifers, ist es eine Frage des Aufwands
  - Angreifer hat meist „endlos Zeit“ und einen großen Werkzeugkasten
- **Realistisches und gewolltes Ziel:**  
**Die Hürde für den Angreifer sollte maximal hoch ein!**

# Landkarte für's Netzwerk

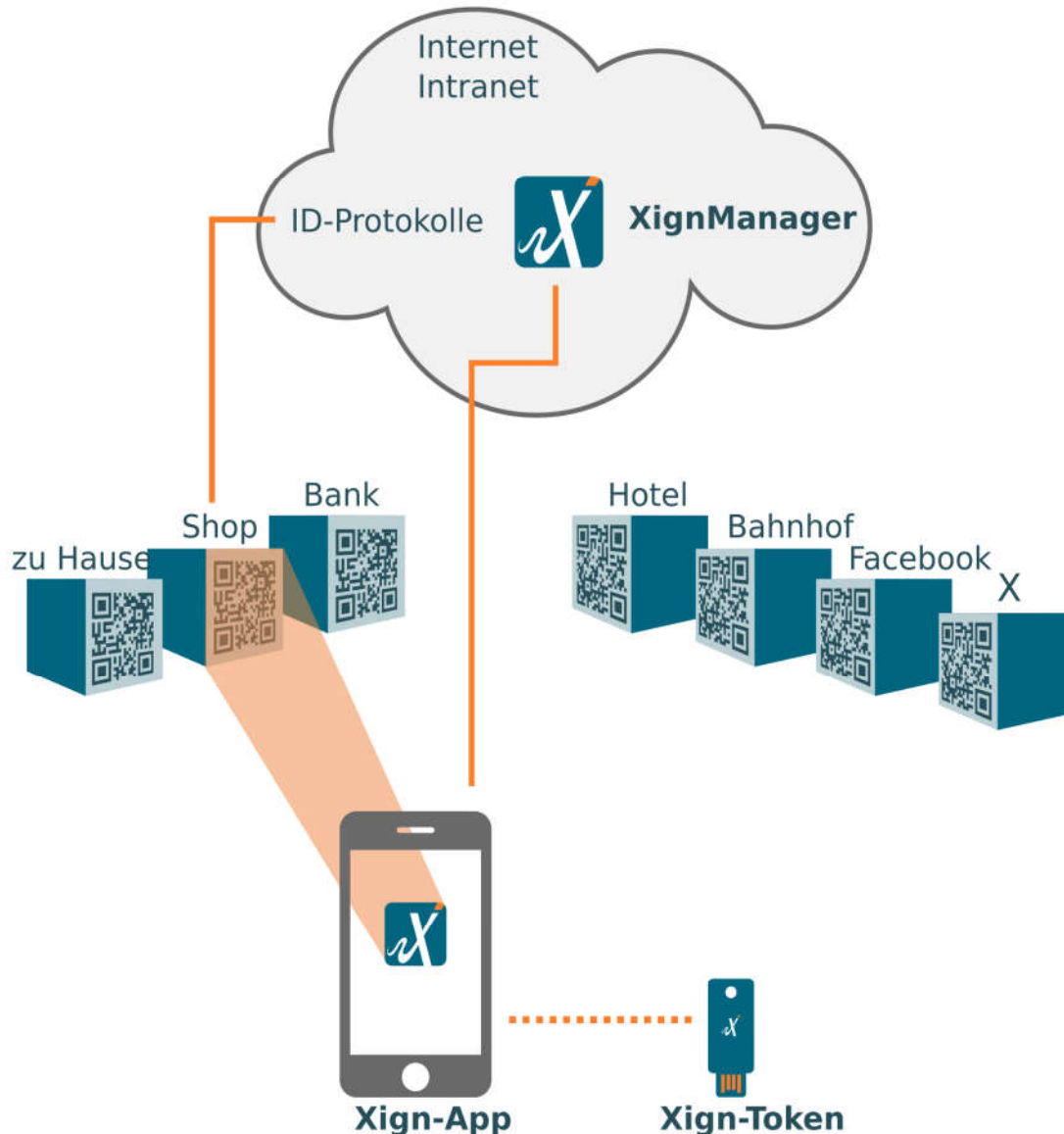
## → spotuation

- Wie wäre es, Sie könnten eine persönliche Landkarte aller Systeme/Netzwerke erzeugen?
- Sie könnten jeden Zeitpunkt speichern und miteinander vergleichen!
- Sie hätten Kennzahlen zur IT-Sicherheit Ihres Unternehmens!
- Daten wären dabei **vollständig, Datenschutzkonform & unter Ihrer eigenen Kontrolle!**



# Identifikation/Authentifikation - Signatur

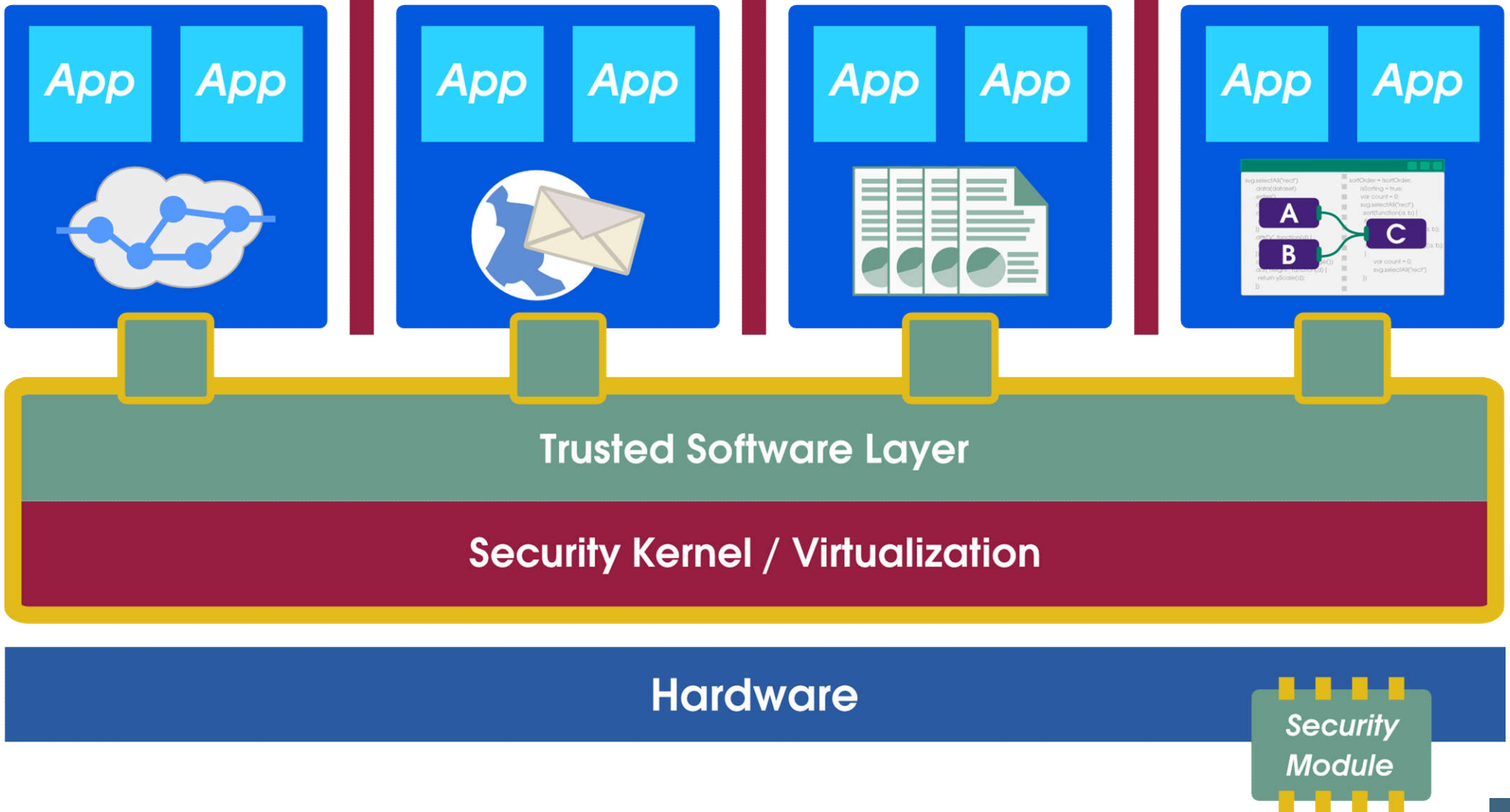
## → Xign



- Eine Registrierung, viele Anwendungen & Märkte
- Datenschutz & Datensicherheit Made in Germany
- Nicht trackbar
- Einfach, schnell & benutzerfreundlich

# Proaktive IT-Sicherheitssysteme

## → Vertrauenswürdige Basis: Konzept (1/5)

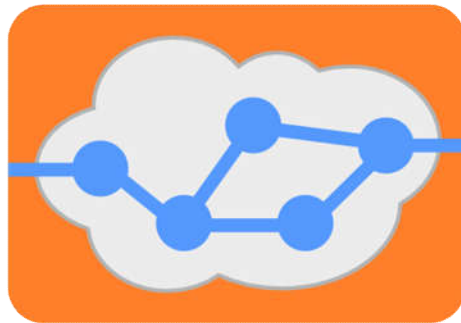


# Proaktive IT-Sicherheitssysteme

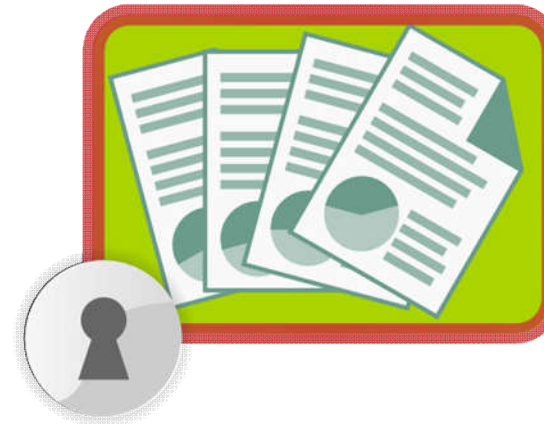
## → Vertrauenswürdige Basis: Konzept (2/5)

**Aufteilung in verschiedene virtuelle Maschinen  
( unterschiedliche Aufgaben und Sicherheitsbedarfe – 1 )**

Internet



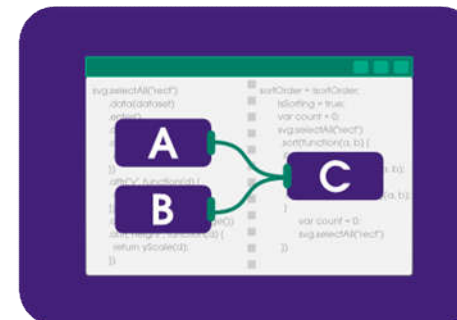
Office



Browser  
E-Mail



Development

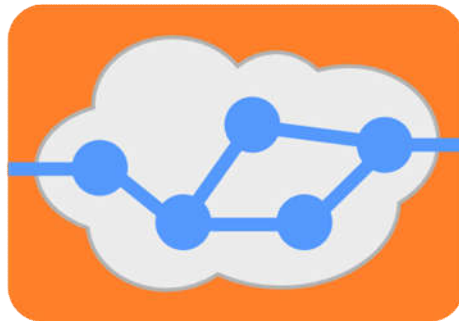


# Proaktive IT-Sicherheitssysteme

## → Vertrauenswürdige Basis: Konzept (3/5)

Aufteilung in verschiedene virtuelle Maschinen  
( unterschiedliche Aufgaben und Sicherheitsbedarfe – 2 )

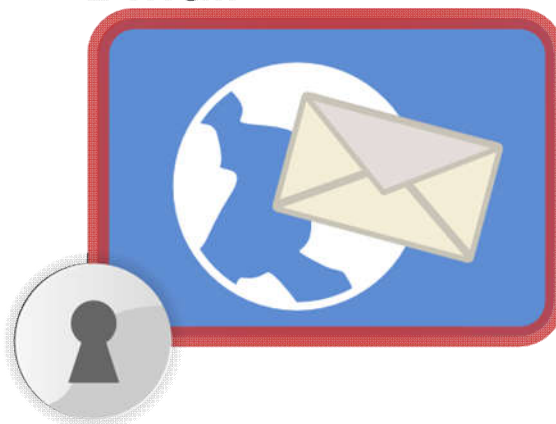
Internet



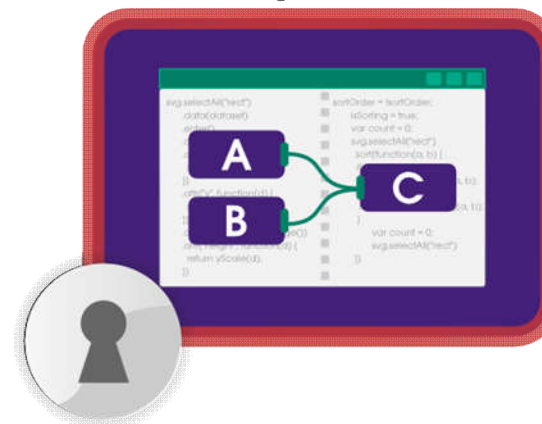
Office



Browser  
E-Mail



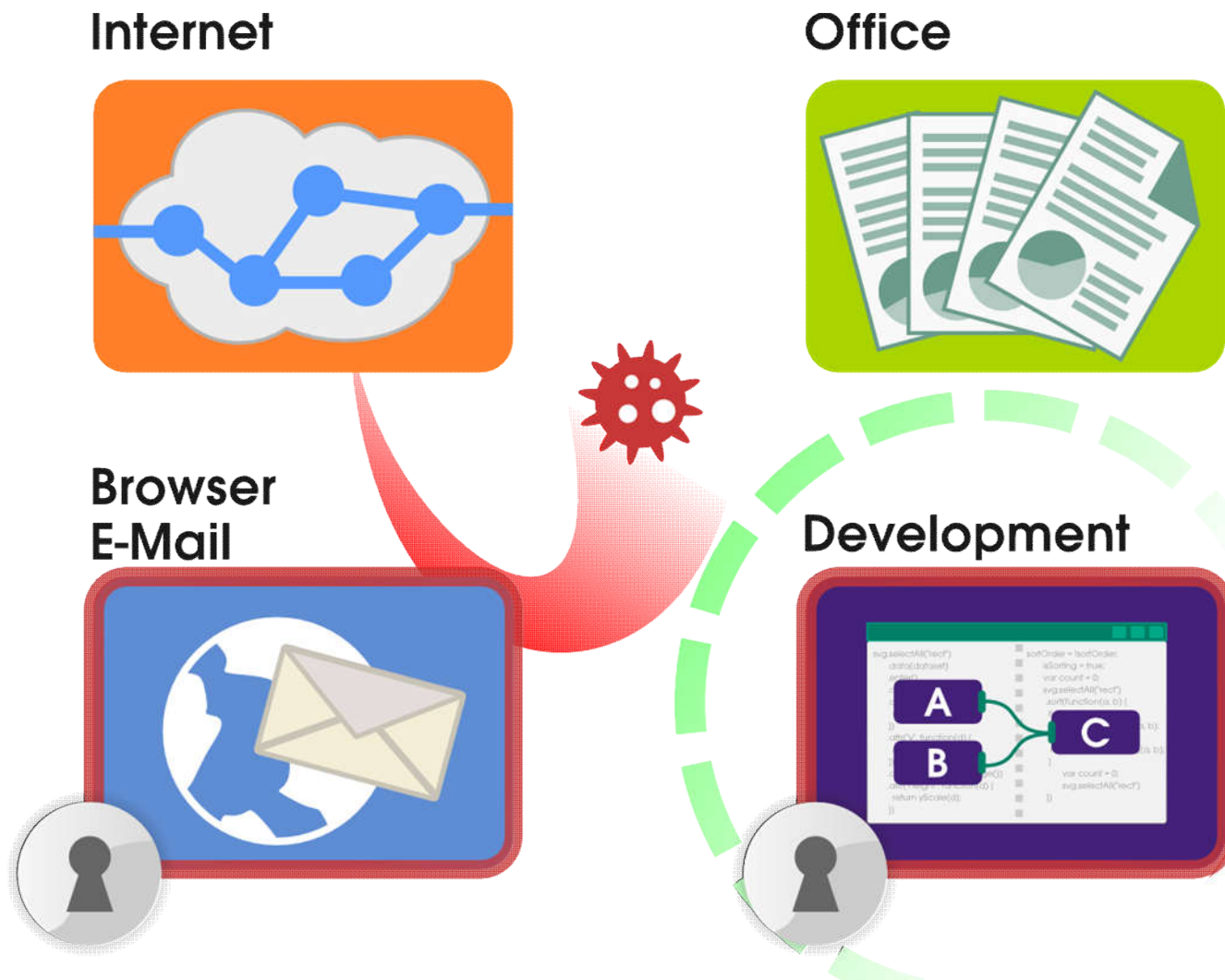
Development



# Proaktive IT-Sicherheitssysteme

## → Vertrauenswürdige Basis: Konzept (4/5)

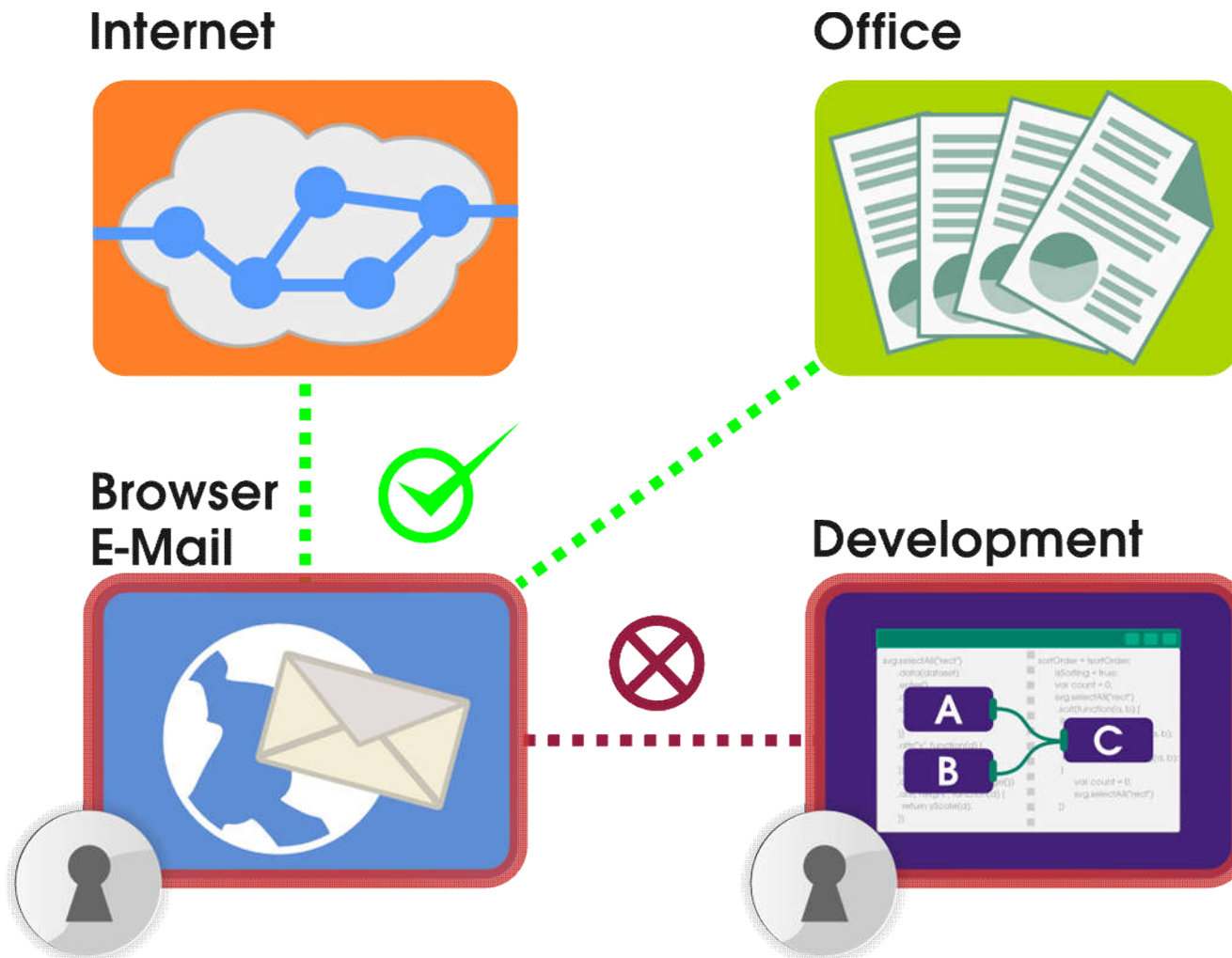
Wichtige Daten werden besonders  
in separaten, isolierten virtuellen Maschinen geschützt



# Proaktive IT-Sicherheitssysteme

## → Vertrauenswürdige Basis: Konzept (5/5)

Security Policies und ein Enforcement System sorgen für mehr Sicherheit und Vertrauenswürdigkeit



# Verschlüsselung

## → Schreiben Sie weniger Postkarten

- Konkurrenten, Staaten, Kriminelle, ... haben Begehrlichkeiten
- Vertrauenswürdiger Kommunikation bedeutet:  
Weniger Raum für Manipulationen und Spionage, Nachweisbarkeit, Vertraulichkeit
- **Praxis:**
  - Festplattenverschlüsselung
  - HTTPS überall anbieten & einfordern!
  - Datenverbindungen per VPN schützen (Standorte, öffentl. WLAN, ...)
  - E-Mails verschlüsseln
  - Instant-Messaging nur Ende-zu-Ende verschlüsselt nutzen
  - Plattformen für kollaborative Arbeit nicht auf fremden Servern
  - Datensparsamkeit & Mitarbeiterschulungen

# Cloud [sprich: Klaut] → Seien Sie misstrauisch

- Cloud-Dienste: ca. 80% der Anbieter kommen aus den USA
- Andere Länder, andere Sitten, andere Rechtslage
- Man kann sicher sein: Private Daten sind hier **nicht** mehr privat

10.04.2014 19:39

240

## Dropbox-Nutzer empört über Berufung von Condoleezza Rice

Die ehemalige US-Außenministerin der Ära Bush sitzt nun im Verwaltungsrat des Cloud-Dienstes. Nutzer zeigen sich fassungslos und rufen zum Boykott auf.

# Drop Dropbox



- **Unternehmen haben gegenüber Mitarbeitern und Kunden (→ Gesellschaft) eine große Verantwortung**
- Wer den Schaden hat, braucht für den Spott nicht zu sorgen. ;)
- Seien Sie anderen einen Schritt voraus, und setzen Sie auf angemessene und hochwertige IT-Sicherheit
- Wenn Sie „keine Ahnung“ haben, fragen Sie jemanden! (der qualifiziert ist)
- Guter Rat muss nicht teuer sein, schlechter Rat kann jedoch sehr teuer werden

- **Internet und IT-Sicherheit**  
(Situation, Problemfelder, Herausforderungen)
- **Prinzipielle IT Sicherheitsstrategien**  
(Fokussierung, Vermeiden, Entgegenwirken, Erkennen)
- **Technologien und Vorgehensweise**  
(spotuation, Xign, ...)
- **Fazit und Ausblick**

# Wie geht es weiter in der IT-Sicherheit?

## → Fazit und Ausblick

- Klar ist, dass wir uns **zurzeit nicht angemessen** gegen die professionellen Hacker **schützen** können!
- **Die 5 % unserer wichtigen und wertvollen Daten müssen wir wirkungsvoll schützen (Vertrauenswürdige IT-Systeme, Verschlüsselungssicherheitssysteme, ...), um Schaden zu verhindern!**
- Wir müssen unseren eignen Schutzbedarf kennen.
- **Wir müssen passende IT-Sicherheitsprodukte einsetzen, um unser Risiko zu steuern.**



**Westfälische  
Hochschule**

Gelsenkirchen Bocholt Recklinghausen  
University of Applied Sciences

# **Eine strategische Sichtweise auf die sich verändernden IT-Sicherheitsprobleme**

**Wir haben ein großes Problem,  
das sehr viel Aufmerksamkeit verlangt!**

Prof. Dr. (TU NN)

**Norbert Pohlmann**

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

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

## Wir empfehlen unsere kostenlose App securityNews

- Kostenlose App vom Institut für Internet-Sicherheit
- Aktuelle Sicherheitshinweise für Smartphone, Tablet, PC und Mac
- Warnung vor Sicherheitslücken in Standardsoftware, dank Schwachstellenampel
- Konkrete Anweisungen für Privatanwender und Unternehmen



securityNews



## Quellen Bildmaterial

Eingebettete Piktogramme:

- Institut für Internet-Sicherheit – if(is)
- Icon made by Freepik from [www.flaticon.com](http://www.flaticon.com)

„Internet of Things“ Darstellung:

<http://blog.surveyanalytics.com/2014/09/top-5-infographics-of-week-internet-of.html>

## Besuchen und abonnieren Sie uns :-)

### WWW

<https://www.internet-sicherheit.de>

### Facebook

<https://www.facebook.com/Internet.Sicherheit.ifis>

### Twitter

<https://twitter.com/ifis>

### Google+

<https://plus.google.com/107690471983651262369/posts>

### YouTube

<https://www.youtube.com/user/InternetSicherheitDE/>

## IT-Sicherheitsstrategie für Deutschland

Wirkungsklassen von IT-Sicherheitsmaßnahmen für unterschiedliche Schutzbedarfe

Ein Aspekt der IT-Sicherheitsstrategie für DE

<https://www.internet-sicherheit.de/downloads/publikationen-vortraege/dokumente-2015.html>