TeleTrusT
Pioneers in IT security.

Fachhochschule Gelsenkirchen

# Sichere Online-Anbindung

## → Status und Anforderungen

**Prof. Dr. Norbert Pohlmann**

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

if(is) internet-sicherheit.

# Inhalt

- **Motivation**
- **IT-Sicherheit heute:**
  **→ Eine kritische Bewertung**
- **Wichtige IT-Sicherheitsaspekte**
  - **VPN**
  - **Beweissicherung**
- **Ausblick**

# IT-Sicherheit u. Vertrauenswürdigkeit → Motivation

- **Veränderung, Fortschritt, Zukunft**
  - Entwicklung zur **vernetzten Informations- und Wissensgesellschaft.**

- **IT-Sicherheit ist eine sich verändernde Herausforderung**
  - Das Internet geht über alle Grenzen und Kulturen hinaus!
  - Zeit und Raum werden überwunden!
  - Immer schnellere Entwicklung und Veränderung in der IT.
  - Die Nutzer müssen immer wieder neues Wissen erwerben, wie sie sich angemessen verhalten können.
  - Die zu schützenden Werte steigen ständig.
  - Die Werte, die wir schützen müssen, ändern sich mit der Zeit.
  - Die Angriffsmodelle innovieren und Angreifer werden professioneller.
  - IT-Sicherheitsmechanismen werden komplexer, intelligenter und verteilter.
  - **Mit der Zeit werden die Sicherheitsprobleme immer größer!**

# IT-Sicherheit heute
## → Eine kritische Bewertung (1/7)

- **Webserver Sicherheit**
  - Schlechte Sicherheit auf den Webservern / Webseiten
  - Heute wird Malware hauptsächlich über Webseiten verteilt
  - Viele Webseiten sind nicht sicher aufgebaut!
  - Patches werden nicht oder sehr spät eingespielt


- **Gründe**
  - Firmen geben kein Geld für IT-Sicherheit aus! (Funktionalität und Design sind wichtiger)
  - Mitarbeiter haben keine Zeit (Geld)
  - Verantwortliche kennen das Problem nicht!

# IT-Sicherheit heute
## → Eine kritische Bewertung (2/7)

- **Computer-Sicherheit**
  - Die **Software-Qualität** der Betriebssysteme und Anwendungen sind **nicht „sicher“ genug!**
  - **Schwache Erkennungsrate** bei Anti-Malware Produkten -> nur 75 bis 90%!
  - **Jeder 25. Computer hat Malware!**

  - **Die Nutzer und deren Computer sind nicht gut genug vorbereitet!**
    - Erwerb von Computern
    - Ausstattung der Computer
    - Betrieb der Computer

# IT-Sicherheit heute
## → Eine kritische Bewertung (3/7)

- **Identity Management**
  - Passworte, Passworte, Passworte, …
    sind das Mittel zur Authentiktion  im Internet!
  - Identifikationsbereiche liegen im Unternehmens- und Kundenumfeld, nicht international!
  - Föderationen sind noch nicht verbreitet genug!

- **Lösungen**
  - **nPA** (Neue Personalausweis
    mit Authentikationsfunktion)


  - **Gesundheitswesen**
    - Elektronische **Gesundheitskarte**
    - Elektronischer **Heilberufsausweis**

# IT-Sicherheit heute
## → Eine kritische Bewertung (4/7)

- **Soziale Netzwerke**
  - Internet-Nutzer können sich über Soziale Netzwerke sehr schnell neues Wissen aneignen und Informationen beschaffen.
  - Vertrauliche Informationen sollen nicht eingestellt und besprochen werden!
  - Die Rechte der Betreiber sind nicht angemessen! (siehe AGBs → können alles mit den eingestellten Inhalten machen!)
  - Die angebotenen Schutzmechanismen sind nicht klar und qualitativ nicht gut genug!

# IT-Sicherheit heute
## → Eine kritische Bewertung (5/7)

- **Datensammler (z.B. Google-Health, MS Health Vault, …)**
  - **Patientenakte für sechs Milliarden Menschen**
    - Gesundheitliche Beschwerden,
    - Krankheiten,
    - Medizinische Behandlungen,
    - …

  - **Informationen**
    - Ärzte
    - Medikamente
    - Gesundheitsrelevante Themen
  - **Herausforderungen, Probleme**
    - Internationale, privatwirtschaftliche Unternehmen
    - Datenschutz (Anforderung, Kultur, Gesetze, …)

# IT-Sicherheit heute
## → Eine kritische Bewertung (6/7)

- **E-Mail Sicherheit**
  - ***Wenig verschlüsselte E-Mails*** (<4 %)
    (S/MIME, PGP, …)
  - ***Wenig Signaturen unter E-Mails*** (<6 % )
    (Finanzbereich deutlich mehr)
  - ***Spam***-Anteil größer als 95 %
    (in der Infrastruktur – siehe ENISA-Studie)
  - ***Keine Beweissicherung***
  - ***Nicht zuverlässig*** *(*Zustellung, E-Mail-Adresse, ….)

- **Was kommt in der Zukunft?**
  - **DE-Mail**
    - SSL-Verschlüsselung zwischen den Gateways, Zustell-Garantie
    - Verpflichtende Authentifizierung, Sichere Dokumentenablage
  - **epost - Deutschen Post AG**
    - Hybridmodell

# IT-Sicherheit heute
## → Eine kritische Bewertung (7/7)

- **Internet-Nutzer**
  - Internet-Nutzer müssen die Gefahren des Internets kennen, sonst schaden sie sich und anderen!
  - ***Umfrage BITKOM:***
    Jeder dritte **Internet-Nutzer** ***schützt sich nicht angemessen***!
    - ***keine*** Personal Firewall
    - ***keine*** Anti-Malware
    - gehen ***sorglos*** mit E-Mails und Links um
    - usw.
  - ***Studie „Messaging Anti-Abuse Working Group“:***
    57 Prozent der Befragten haben schon einmal ***Spam-Mails geöffnet*** oder einen ***darin enthaltenen Link angeklickt***.

# IT-Sicherheit heute
## → Lösungsansätze

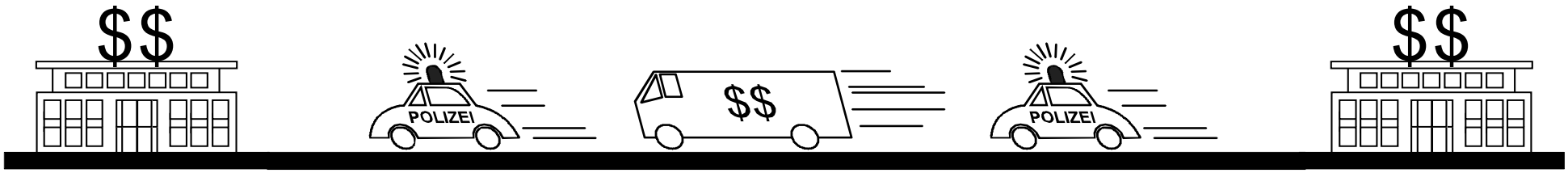
**Der Level an IT-Sicherheit und Vertrauenswürdigkeit unserer IT-Systeme ist heute ungenügend!**

**Lösungsansätze:**

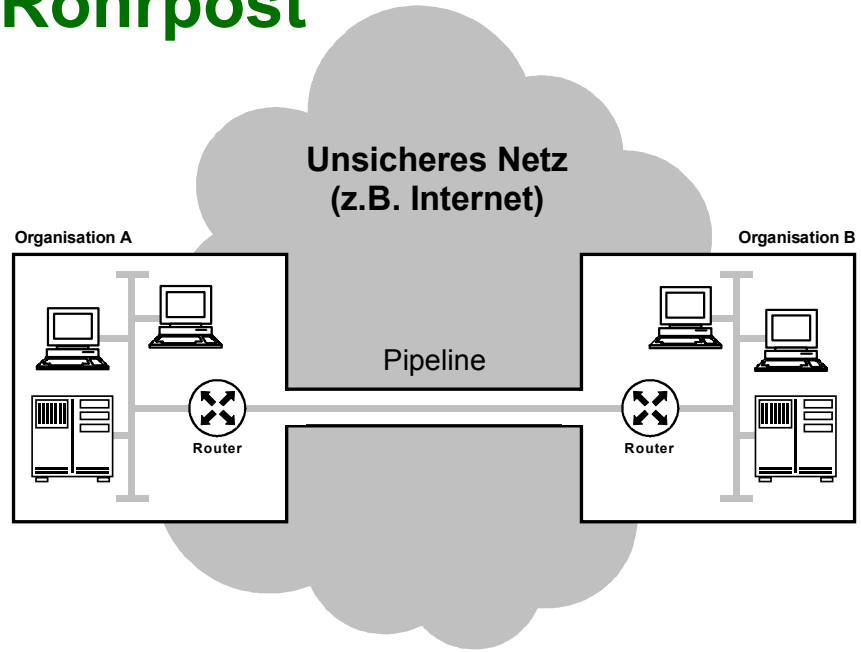
- **Herstellerverantwortung**
- **Regulierte Anwendungen / Dienste**
- **Höhere Internet-Kompetenz für die Nutzer**

# Virtual Private Network (VPN)
## → Analogien

- **Sicherheitstransporter**




- **Pipeline und Rohrpost**

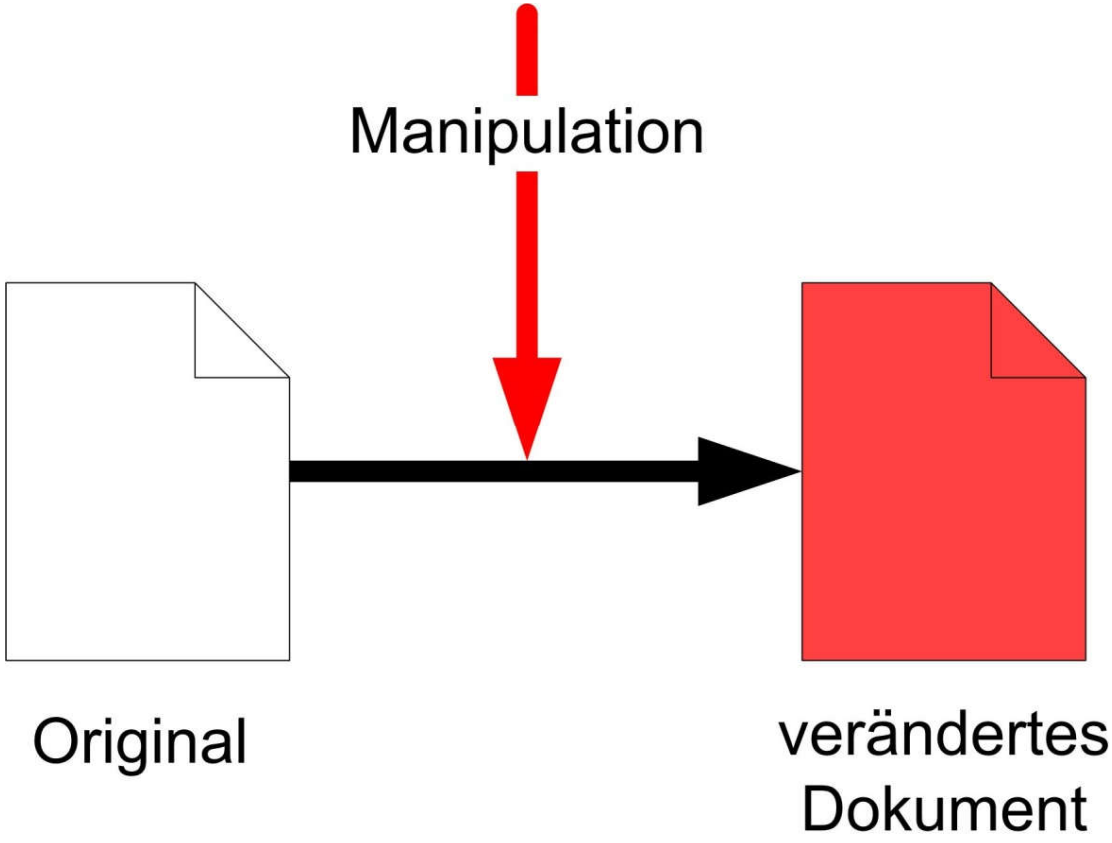


# Virtual Private Network (VPN)
## → Idee und Sicherheitsmechanismen

- **Grundsätzliche Idee bei Virtual Private Networks (VPNs):**
  - offene Kommunikationsinfrastruktur, z.B. Nutzung des Internets
    - kostengünstig,
    - weltweit verfügbar **UND**
  - **Allen Bedrohungen und Risiken sinnvoll entgegenwirken**

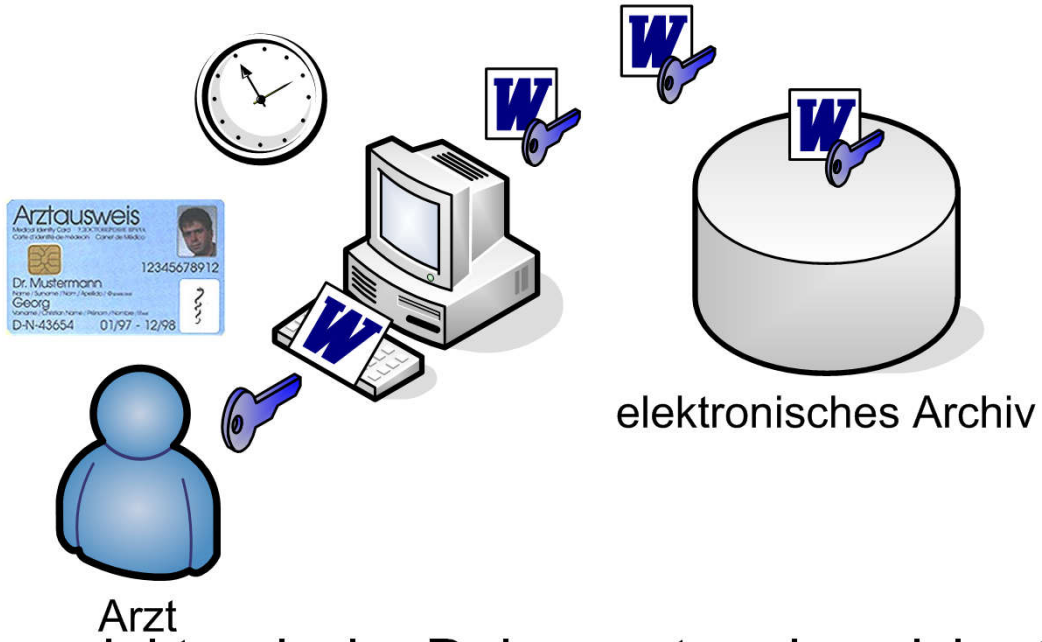
- **Sicherheitsmechanismen von VPNs**
  - **Verschlüsselung** (schützt Vertraulichkeit)
  - **Authentikation** (gewährleistet Eindeutigkeit des Benutzers)
  - **MAC-Funktionen** (sorgen für die Unversehrtheit der Daten)
  - **Tunneling** (verschleiert Datentransfer)
  - **Firewalling** (schützt Netzwerkressourcen)

# Beweissicherung
## → Was ist ein verändertes Dokument?




- Die **Beweissicherheit** soll zeigen, **dass** ein Dokument und wenn, **was,** in einem Dokument verändert wurde.

# Beweissicherung
## → Elektronische Signatur

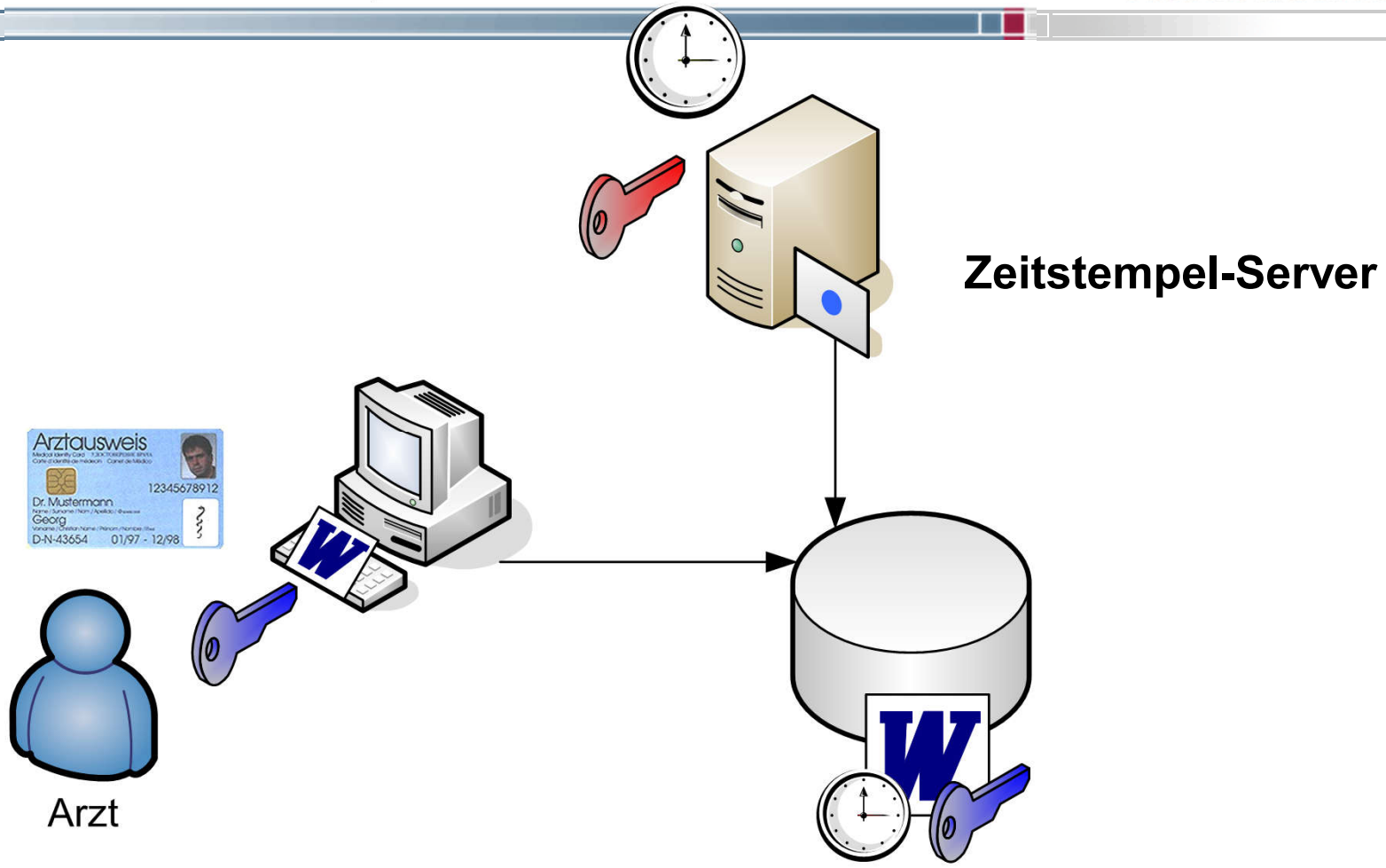



- Der Arzt signiert das elektronische Dokument und speichert dieses in einem elektronischen Archiv (z.B. mit der **Health Professional Card** – **HPS**).
- Für die Beweissicherheit muss die **Revisionssicherheit des Archivs** gewährleistet sein.
- Kann der Administrator des Systems Daten verändern, kann er dies auch im Auftrag des Arztes tun (i.d.R. sehr aufwendig)
- Wird das Dokument von einem anderen als dem Arzt verändert, wird dies durch die elektronische Signatur sicher erkannt.

# Beweissicherung
## → Anforderungen an elektronisches Archiv

- Ordnungsmäßigkeit
- Vollständigkeit
- Sicherheit des gesamten Verfahrens
- Schutz vor Veränderung und Verfälschung
- Sicherung vor Verlust
- Nutzung nur durch Berechtigte
- Einhaltung der Aufbewahrungsfristen
- Dokumentation des Verfahrens
- Nachvollziehbarkeit
- Prüfbarkeit

# Beweissicherung
## → Archiv mit Zeitstempelfunktion




- Die Dokumente werden in diesem Szenario noch mit einem **eindeutigen Zeitstempel** versehen.
- Dieser Zeitstempel kann nicht von einem System Administrator verändert werden.

# Beweissicherung
## → Zusammenfassung

- Es gibt technische und organisatorische Sicherheitsmechanismen, wie die
  - **elektronische Signatur,**
  - **elektronischer Zeitstempel** und
  - **revisionssichere Archivierung,**

  die eine Beweissicherung von veränderten Dokumenten möglich machen.

- Die **Umsetzung** dieser Sicherheitsmechanismen in die Praxis noch **nicht sehr weit verbreitet**.

# Online-Anbindung
# → Zusammenfassung

- Wir müssen etwas tun,
  um unsere Zukunft **sicherer** und **vertrauenswürdiger** zu gestalten.

- Dazu brauchen wir einen **Quantensprung**
  - in der **Sicherheitstechnologie**,
  - in der **Vorgehensweise** und
  - in der **Zusammenarbeit** mit anderen.

- Die Zukunft beginnt jetzt, also lassen Sie uns anfangen!

TeleTrusT
Pioneers in IT security.

Fachhochschule Gelsenkirchen

# Sichere Online-Anbindung

## → Status und Anforderungen

## Vielen Dank für Ihre Aufmerksamkeit
## Fragen ?

**Prof. Dr. Norbert Pohlmann**

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

if(is) internet-sicherheit.