Security for Future Services in Next Generation Networks

Prof. Dr. Norbert Pohlmann

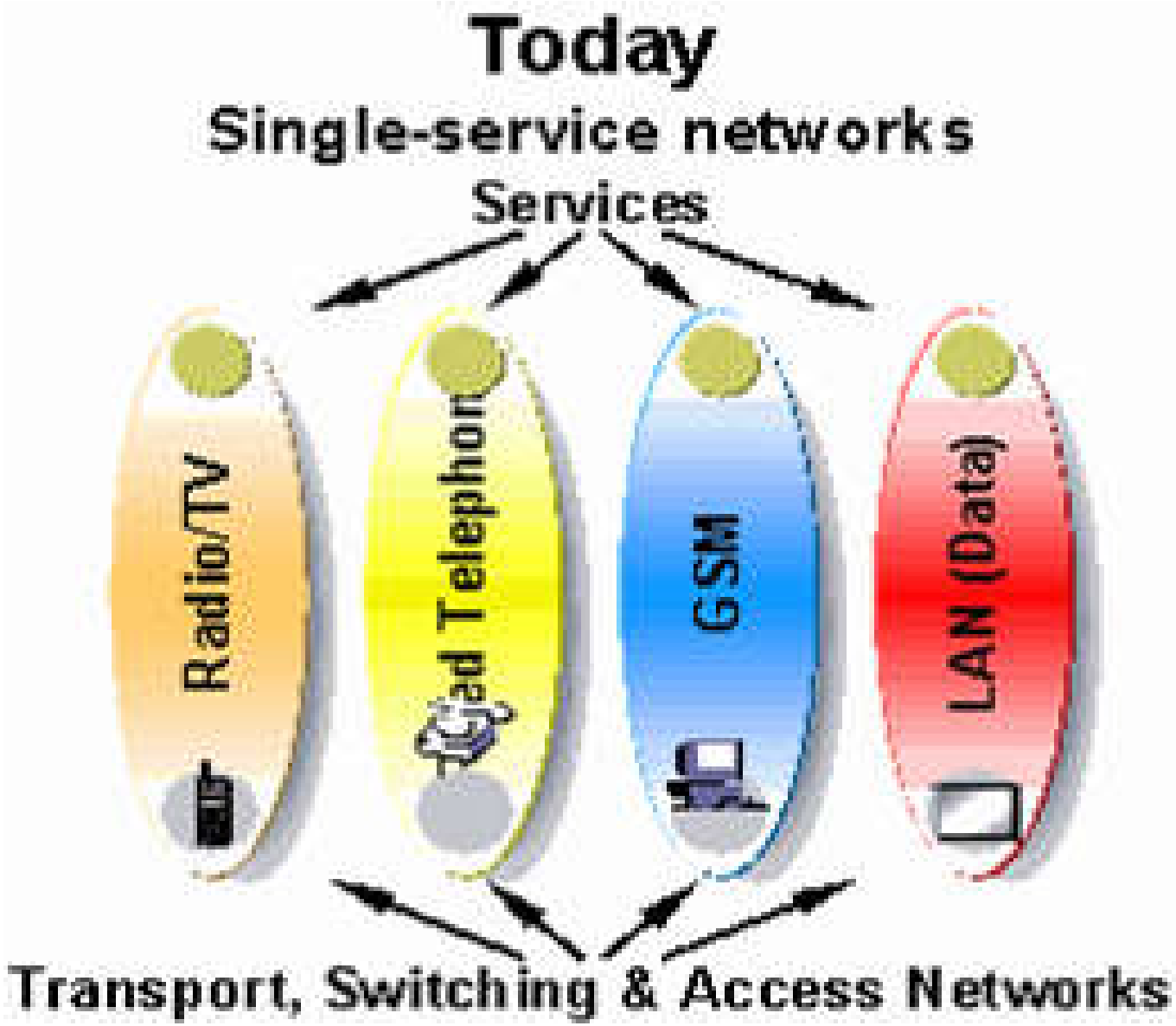
Institut für Internet-Sicherheit
http://internet-sicherheit.de
Fachhochschule Gelsenkirchen

Next Generation Network
→ Ausgangspunkt

- Wir entwickeln uns zunehmend zu einer **vernetzten Wissens- und Informationsgesellschaft**.
- **Verlässlichkeit und Vertrauenswürdigkeit** von Informations- und Kommunikationstechnik spielen hier eine besondere Rolle.
- Die Kommunikationsnetze und die darauf aufbauenden Dienste sind sehr schnell gewachsen und bilden **eine der wichtigsten Infrastrukturen** in unserer modernen Gesellschaft.
- Die angebotenen Dienste haben enorme Vorteile gebracht und es besteht in Zukunft noch ein **sehr großes Potenzial**, Geschäftsprozesse rationaler abzuwickeln und weitere Geschäftsfelder zu erschließen.
- In den letzten Jahren ist die Bedeutung von **Sicherheitsproblemen** in diesem Bereich nicht kleiner, sondern **größer geworden**.
- Jetzt besteht die größte Herausforderung darin, für eine **notwendige und passende Vertrauenswürdigkeit** des Next Generation Network zu sorgen.

© Prof. Dr. Norbert Pohlmann, Institut für Internet-Sicherheit (ifis), FH Gelsenkirchen

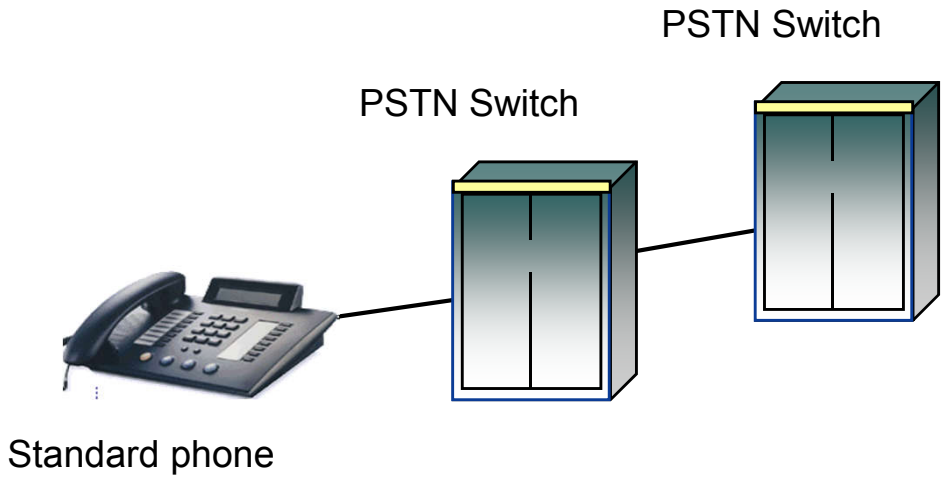
Network
→ Heute



© Prof. Dr. Norbert Pohlmann, Institut für Internet-Sicherheit (ifis), FH Gelsenkirchen

Wie sehen die Netze heute aus?

- Jedem Netz ist in der Regel ein **eigener Dienst** zugeordnet.
- Die **Netzintelligenz ist überwiegend hardwaremäßig** mit jeweils eigener Technologie realisiert.
- Es gibt nur **wenige Schnittstellen** und der Kunde erhält alles aus einer Hand.
- **Sicherheit ist oft implizit erzielbar**.
- Beispiel: Authentikation →“Trust by Wire”



© Prof. Dr. Norbert Pohlmann, Institut für Internet-Sicherheit (ifis), FH Gelsenkirchen

Next Generation Network
→ Multimedia Service

© Prof. Dr. Norbert Pohlmann, Institut für Internet-Sicherheit (ifis), FH Gelsenkirchen

Next Generation Network
→ Charakteristiken

- Ein Netz, das auf der **Paket-Technologie** basiert und jede Art von Informationen transportieren kann
- Ein Multi-Service Netz, das **Sprache, Daten und Video** unterstützt
  → mehr Bandbreite, Realzeitanwendungen
- Ein Netz, das **interaktive Echtzeit-Kommunikation** ermöglicht
  → mehr Zuverlässigkeit, Ausfallsicherheit
- Ein Netz mit differenzierter **Qualität (QoS)** für verschiedene Dienste und Anwendungen
  → Service-Differenzierung
- **Permanente Erreichbarkeit** in ausreichender Qualität
- **Web-Technologie** für das Management, auch für Kunden
- Offene Plattformen, **offene Service-Schnittstellen**
- Ein **ALL IP Netz** für multimediale Dienste

© Prof. Dr. Norbert Pohlmann, Institut für Internet-Sicherheit (ifis), FH Gelsenkirchen

Next Generation Network
→ Sicherheitsherausforderungen von NGN

- Mit neuen technischen Möglichkeiten wachsen auch die Risiken.
- Es werden in zukünftigen Kommunikationsnetzen mehr sensitive Daten generiert.
  → **Datenschutz**
- Offene Schnittstellen ermöglichen einen freieren Zugriff auf Daten von Dritten.
  → **Zugriffschutz**
- Die neuen Dienste erfordern den Austausch sensibler Daten zwischen unterschiedlichen Parteien.
  → **Medienschutz**

© Prof. Dr. Norbert Pohlmann, Institut für Internet-Sicherheit (ifis), FH Gelsenkirchen

Next Generation Network
→ Sicherheitsanforderungen: allgemein

- Neue Notwendigkeiten durch elektronische Geschäftsprozesse
  → eine **passende Vertrauenswürdigkeit**, damit das Potenzial ausgeschöpft werden kann
- Wir wollen schon genutzte Dienste weiterhin verlässlich und vertrauenswürdig nutzen können
- Vertrauenswürdigkeit/Sicherheit als **Enabler**, weitere neue Dienste über das Netz der Zukunft motivieren zu können
- **Neue Strategien** durch offene Systeme
  → Von der „Perimeter Security“ zur Server- und Anwendungssicherheit

© Prof. Dr. Norbert Pohlmann, Institut für Internet-Sicherheit (ifis), FH Gelsenkirchen

Next Generation Network
→ Sicherheitsanforderungen: speziell

- Sicherer Zugang zu NGN
  - Zugriffssicherheit für Breitband (DSL, usw.)
  - AAA (Authentication, Authorization und Accounting) für mobilen Zugriff
- Vertraulichkeit von Medien (Verschlüsselung)
- Verbindlichkeit von Geschäftsprozessen (digitale Signatur)
- Quality of Service (Verfügbarkeit von Diensten)
- Sicherheit für Quality of Service
  (missbräuchliche Nutzung höherer Qualitäten)
- Sichere Managementinfrastruktur
- Usw.

© Prof. Dr. Norbert Pohlmann, Institut für Internet-Sicherheit (ifis), FH Gelsenkirchen

Next Generation Network
→ Ziele für NGN-Sicherheit

- **Skalierbare** Sicherheitslösungen
- **Maßgeschneiderte** Sicherheitslösungen in Abhängigkeit von den Sicherheitsanforderungen
- **Benutzerfreundliche** Sicherheitslösungen
  → Die gleiche Benutzerschnittstelle für alle Zugriffe
- Gleiche und **standardisierte** Sicherheitslösungen für alle Produkte, Anwendungen und Dienste

© Prof. Dr. Norbert Pohlmann, Institut für Internet-Sicherheit (ifis), FH Gelsenkirchen

Sicherheitsmechanismen für NGN
→ Identity Management

- **Motivation**
  - Jeder Benutzer hat eine Vielzahl von Benutzernamen und Passwörtern
  - Diese sich zu merken ist schwierig, eine Mehrfachverwendung ist unsicher

- **Ziel**
  - Mit einem Benutzernamen und einem Passwort (und einem SmartToken) den Zugang zu allen Diensten schaffen

- **Technologien**
  - *SingleSignOn*
    - Softwareverwaltung auf der Client-Seite
  - *1-Button-Klick-Through Technologie*
    - Einheitliche kryptographische Authentikation, z.B. Client-SSL-Authenikation mit SmartToken
  - *Liberty Alliance Technologie*
    - Mehrere Service Provider bilden einen „Circle of Trust“ (global Login und Logout)

© Prof. Dr. Norbert Pohlmann, Institut für Internet-Sicherheit (ifis), FH Gelsenkirchen

Sicherheitsmechanismen für NGN
→ E-Mail Verlässlichkeit

- **Motivation**
  - Spam, Viren und Co.
    - Viren: 2,9 %
    - Spam: 61,5 %
  - Es werden nur 4,3 % der E-Mail verschlüsselt und nur 6% signiert!
  - IP-Adressen haben wir nicht im Griff
    (Spammer schalten und walten, wie sie wollen)

- **Ziel**
  - Höhere Verlässlichkeit der E-Mail-Anwendung

- **Technologien**
  - Mehr Ordnung, mehr Verantwortung der Betreiber
  - Schwarze / Weiße Listen
  - Digitale Signatur und Verschlüsselung

© Prof. Dr. Norbert Pohlmann, Institut für Internet-Sicherheit (ifis), FH Gelsenkirchen

Sicherheitsmechanismen für NGN
→ Web Service Security

- **Motivation**
  - Ein **Web Service** ist ein Softwaresystem, das entworfen wurde, um eine interoperable Maschine-zu-Maschine Interaktion über ein Netzwerk zu ermöglichen.
  - Web Service kann die Dienste dynamisch lokalisieren und binden, es existiert eine lose Kopplung zwischen Provider und Consumer sowie eine Interoperabilität.

- **Ziel**
  - Passende und einfache Sicherheitstechnologie.

- **Technologien (W3C)**
  - XML Signature, XML Encryption
  - XKMS - XML Key Management Specification
    - XML Key Registration Service (X-KRSS)
    - XML Key Information Service (X-KISS).

© Prof. Dr. Norbert Pohlmann, Institut für Internet-Sicherheit (ifis), FH Gelsenkirchen

Next Generation Network
→ TeleTrusT

- **Hilfestellungen bei organisationsübergreifenden Sicherheitsmechanismen**

- **ISIS-MTT**
  - Spezifikation, Testkonzeption, Testbed
  - Grundlage für interoperable PKI-Systeme
  - Mit T7 e.V. und dem BMWA

- **European-Bridge-CA**
  - Brücke des Vertrauens zwischen PKIs

© Prof. Dr. Norbert Pohlmann, Institut für Internet-Sicherheit (ifis), FH Gelsenkirchen

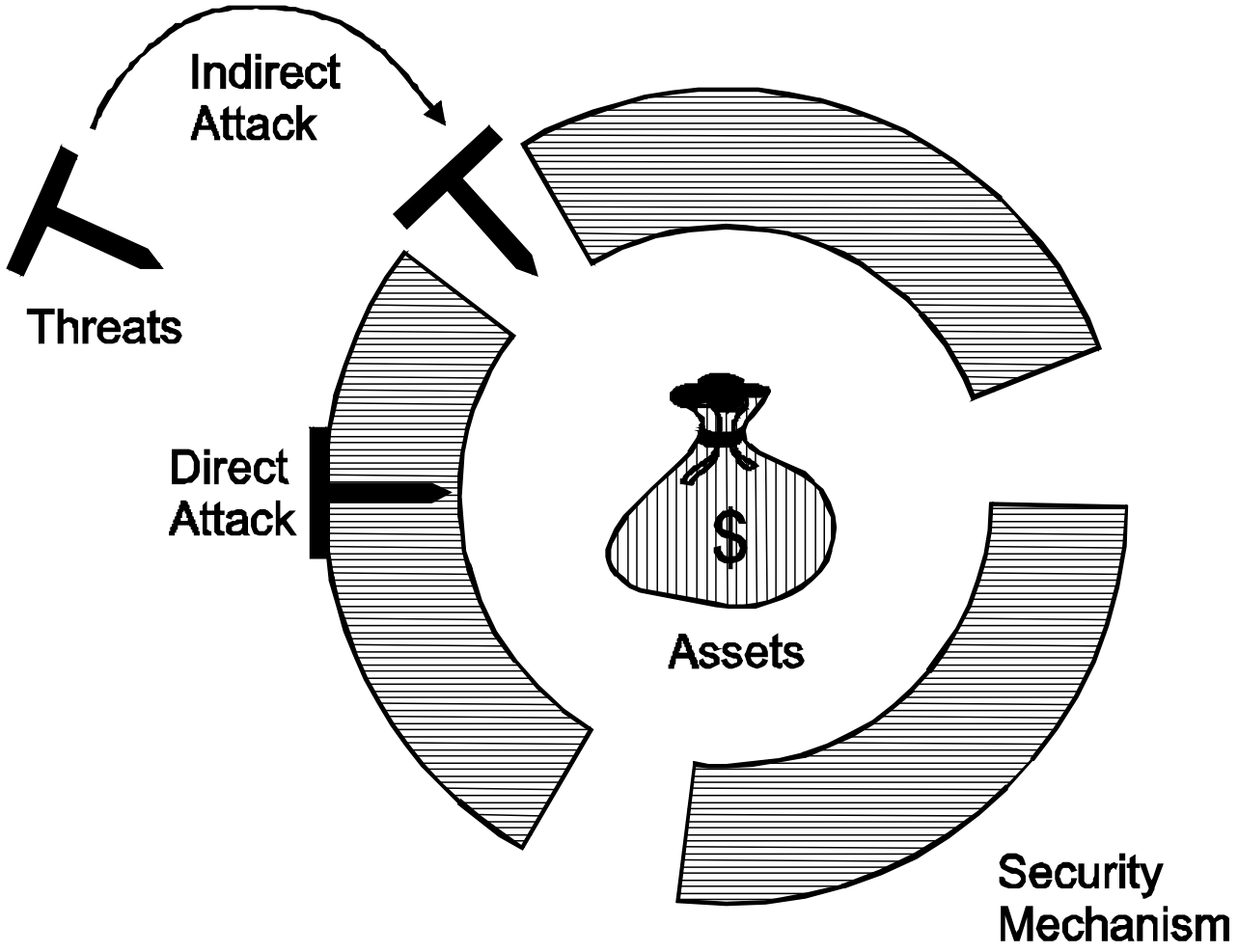
Sicherheitsmechanismen für NGN
→ Weitere Themen in der Zukunft

- **SPIT (SPam over Internet Telephony):**
  Reklameterror übers Internettelefon
  - bei Spit-Attacken wird es sich aus Kostengründen eher um Audio-Werbenachrichten handeln als um Live-Anrufe aus Call-Centern
  - Laut US-Magazin „New Scientist“ schafft es ein entsprechend programmierter Computer, bis zu 1000 Anschlüsse pro Minute anzurufen und gesprochene Reklame abzuladen

© Prof. Dr. Norbert Pohlmann, Institut für Internet-Sicherheit (ifis), FH Gelsenkirchen

Sicherheit und Vertrauenswürdigkeit
→ Wirksamkeit von Sicherheitssystemen

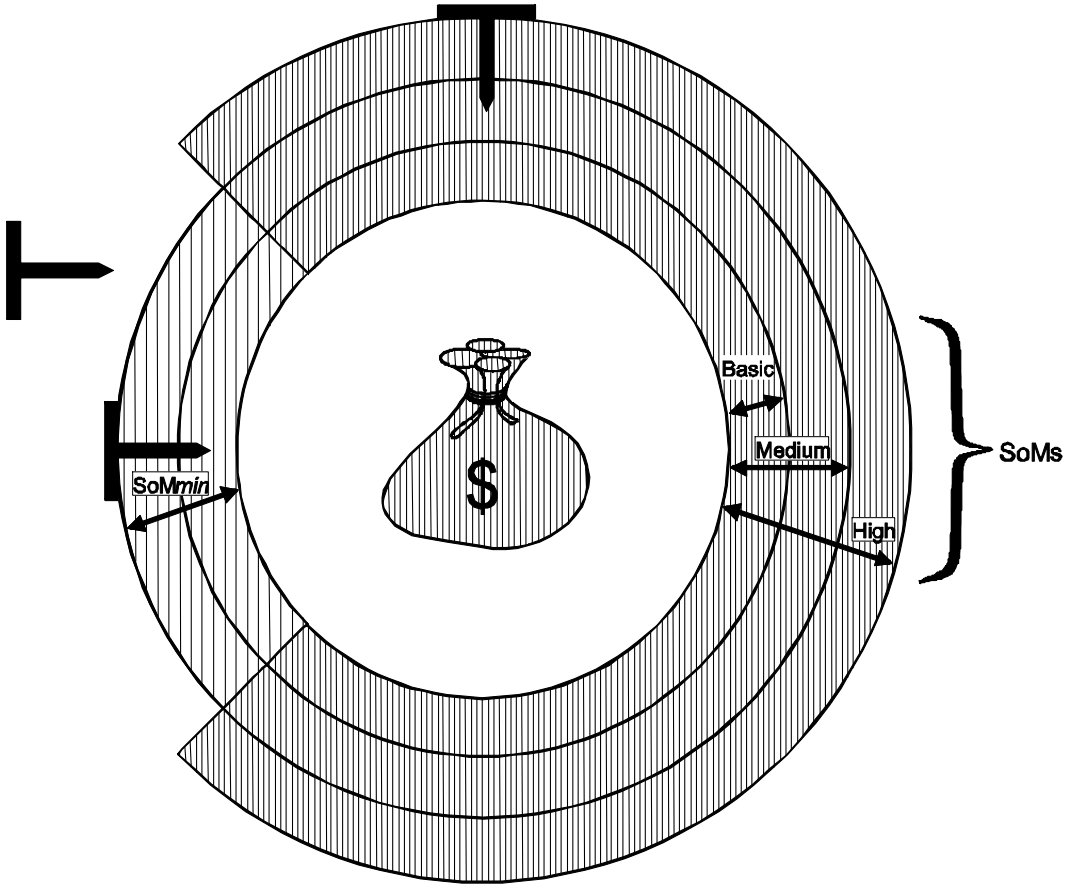
- Für die Beurteilung von Sicherheitssystemen ist ein wichtiges Kriterium, ob die Sicherheitssysteme auch tatsächlich geeignet sind, den realen Angriffen entgegen zu wirken.



© Prof. Dr. Norbert Pohlmann, Institut für Internet-Sicherheit (ifis), FH Gelsenkirchen

Sicherheit und Vertrauenswürdigkeit
→ Stärke von Sicherheitsmechanismen

- Ein wichtige Größe für die Bewertung von Sicherheitsmechanismen ist die Stärke des Sicherheitsmechanismus, die notwendig ist, um allen Angriffen erfolgreich entgegenzuwirken.



- Kriterien für die Bewertung der Stärke sind:
  - Fachkenntnisse (Laie, kenntnisreiche Person, Experte)
  - Ressourcen (Zeit, Ausstattung)
  - Gelegenheit (allein, mit Anwender, mit Systemverwalter)

© Prof. Dr. Norbert Pohlmann, Institut für Internet-Sicherheit (ifis), FH Gelsenkirchen

Sicherheit und Vertrauenswürdigkeit
→ Korrektheit der Sicherheitsmechanismen

institut für internet-sicherheit.

- Korrektheit der Sicherheitsmechanismen
  - Korrekt implementiert
  - Vertrauen in die Korrektheit

- IT-Systeme sind nur sicher, wenn
  - die Wirksamkeit
  - die Stärke und
  - die Korrektheit

  angemessen vorhanden sind.

© Prof. Dr. Norbert Pohlmann, Institut für Internet-Sicherheit (ifis), FH Gelsenkirchen

Sicherheit und Vertrauenswürdigkeit
→ Was heißt Vertrauenswürdigkeit?

- **Sicherheit** in dem Sinne, dass wir IT-Produkte und Lösungen risikoärmer nutzen können.
- **Zutrauen**, dass die Hersteller, die Netz- und Serviceprovider eine verlässliche und sichere IT-Technologie zur Verfügung stellen, was in der jungen Vergangenheit in der IT-Branche nicht optimal geschehen ist.
- Mit **Zuverlässigkeit** ist gemeint, dass die IT-Produkte und Lösungen nur die Dinge tun, die gewünscht sind, und das möglichst 100% zuverlässig.
- **Gewissheit**, dass sich jemand um die Sicherheitsfragen und die anderen Aspekte der Vertrauenswürdigkeit kümmert.
- **Glaubwürdigkeit** in die Aussagen, die gemacht werden, und in die Aktivitäten, die im Bereich der IT getan werden, um mehr Sicherheit, mehr Vertrauenswürdigkeit zu erlangen.
- Weitere Aspekte der Vertrauenswürdigkeit sind z.B.: Aufrichtigkeit, Pflichtbewusstsein, Gewissenhaftigkeit und vor allem Verantwortlichkeit.

© Prof. Dr. Norbert Pohlmann, Institut für Internet-Sicherheit (ifis), FH Gelsenkirchen

Security for Future Services in Next Generation Networks

Vielen Dank für Ihre Aufmerksamkeit

Fragen ?

Prof. Dr. Norbert Pohlmann

Institut für Internet-Sicherheit
http://internet-sicherheit.de
Fachhochschule Gelsenkirchen

institut für internet-sicherheit.