



**Westfälische
Hochschule**

Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Vorlesung: Grundlagen der IT-Sicherheit (ITS)

Prof. Dr. (TU NN)

Norbert Pohlmann

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

if(is)
internet-sicherheit.

- **Einordnung**
- **Lernziele**
- **Vorlesungsinhalt**
- **Themen für Ausarbeitungen und Vorträge (Übung)**
- **Praktikum**
- **Unterlagen / Literatur**

- **Einordnung**
- Lernziele
- Vorlesungsinhalt
- Themen für Ausarbeitungen und Vorträge (Übung)
- Praktikum
- Unterlagen / Literatur

Grundlagen der IT-Sicherheit

→ Einordnung (1/2)

■ Zielgruppe:

- Pflichtmodul für Bachelor-Studiengang Informatik,
- Studienrichtung **Praktische Informatik**
- Wahlpflichtmodul für Bachelor-Studiengang Informatik,
- Studienrichtung **Technische Informatik**
- Wahlpflichtmodul für Bachelor-Studiengang **Medieninformatik**
- Wahlpflichtmodul Bachelor-Studiengang **Wirtschaftsinformatik**

■ Stundenumfang:

- 4 SWS (2 Vorlesungen + 1 Übung + 1 Praktikum)

Grundlagen der IT-Sicherheit

→ Einordnung (2/2)

■ Voraussetzungen:

- Rechnernetze 1 oder Netzwerke
- Betriebssysteme
- Die Vorlesung kann aber auch ohne diese Vorkenntnisse sinnvoll gehört werden!

- Einordnung
- **Lernziele**
- Vorlesungsinhalt
- Themen für Ausarbeitungen und Vorträge (Übung)
- Praktikum
- Unterlagen / Literatur

- Gutes Verständnis von möglichen Angriffen und geeigneten Gegenmaßnahmen in der IT
- Erlangen der Kenntnisse über den Aufbau, die Prinzipien, die Architektur und die Funktionsweise von Sicherheitskomponenten und -systemen
- Sammeln von Erfahrungen bei der Ausarbeitung und Präsentation von neuen Themen aus dem Bereich IT-Sicherheit
- Gewinnen von praktischen Erfahrungen über die Nutzung und die Wirkung von Sicherheitssystemen
- Erleben der Notwendigkeit und Wichtigkeit der IT-Sicherheit

- Einordnung
- Lernziele
- **Vorlesungsinhalt**
- Themen für Ausarbeitungen und Vorträge (Übung)
- Praktikum
- Unterlagen / Literatur

Grundlagen der IT-Sicherheit

→ Vorlesungsinhalt (1/4)

- **Einführung:**
 - IT-Sicherheit als Wirkungs- und Handlungszusammenhang
 - Sicherheitsbedürfnisse
 - Bedrohungen
 - Angriffe
 - Schadenskategorien
 - Eintrittswahrscheinlichkeiten

Grundlagen der IT-Sicherheit

→ Vorlesungsinhalt (2/4)

- **Kryptographie und technologische Grundlagen für Schutzmaßnahmen:**
 - Private-Key-Verfahren
 - Public-Key-Verfahren
 - Kryptoanalyse
 - Hashfunktionen
 - Schlüsselgenerierung
- **Sicherheitsmodule**
 - SmartCards
 - TPM
 - high-security und high-performance Lösungen

Grundlagen der IT-Sicherheit

→ Vorlesungsinhalt (3/4)

- **Authentifikationsverfahren:**
 - Grundsätzliche Prinzipien
 - Algorithmen
 - Verfahren

- **ID - Management**
 - Idee
 - Ziel
 - Konzepte

- **Neue Personalausweis (nPA)**
 - Idee
 - Ziel
 - Konzepte

Grundlagen der IT-Sicherheit

→ Vorlesungsinhalt (4/4)

- IT und Internet Frühwarnsysteme (Grundlagen)
 - Idee
 - Ziel
 - Konzepte

- Einordnung
- Lernziele
- Vorlesungsinhalt
- **Themen für Ausarbeitungen
und Vorträge (Übung)**
- Praktikum
- Unterlagen / Literatur

Grundlagen der IT-Sicherheit

→ Themen für Ausarbeitungen u. Vorträge

- Ausarbeitungen und Vortrag sind Voraussetzung für die Klausur!
- **Mögliche Themen sind z.B.:**
 - Neue Schwachstellen
 - Neue Bedrohungen
 - Neue Angriffe
 - Neue Sicherheitsmechanismen
 - Veränderungen im Internet
 - ...
 - Die 10 größten Probleme im Internet: genauer Beschreibung und Diskussion, warum sie ein Problem sind, und wie groß der potentielle Schaden ist
 - ...
 - weitere Themen, für die Sie sich interessieren, nach Absprache

- Einordnung
- Lernziele
- Vorlesungsinhalt
- Themen für Ausarbeitungen und Vorträge (Übung)
- **Praktikum**
- Unterlagen / Literatur

Grundlagen der IT-Sicherheit

→ Praktikum

- Das Praktikum ist Voraussetzung für die Klausur!
- Themen des Praktikums sind:
 - **Analysen mit dem IAS (und/oder Alternativaufgabe)**
in einer Kleingruppe (2-3 Pers.) mit Ausarbeitung der Ergebnisse
- Das Praktikum findet im Raum **A4.1.07** statt
- Zur Teilnahme bitte bei Moodle anmelden

- Einordnung
- Lernziele
- Vorlesungsinhalt
- Themen für Ausarbeitungen und Vorträge (Übung)
- Praktikum
- **Unterlagen / Literatur**

Grundlagen der IT-Sicherheit

→ Unterlagen

- Folien stelle ich als PDF zur Verfügung
- Web-Server: <https://www.internet-sicherheit.de/downloads/lehrmaterialien.html>
 - Username: student2003
 - Passwort: fuzzy25

- N.Pohlmann: „**Firewall-Systeme - Sicherheit für Internet und Intranet, E-Mail-Security, Virtual Private Network, Intrusion Detection-System, Personal Firewalls**“, 5. aktualisierte und erweiterte Auflage, ISBN 3-8266-0988-3, MITP-Verlag, Bonn 2002
- M.a Campo, N.Pohlmann: „**Virtual Private Network (VPN)**“, 2. aktualisierte und erweiterte Auflage, ISBN 3-8266-0882-8; MITP-Verlag, Bonn 2003
- G.Simmons(Hrsg.): „**Contemporary Cryptology - The Science of Information Integrity**“, IEEE Press, New York
- F.P.Heider, D. Kraus, M. Welschenbach: „**Mathematische Methoden der Kryptoanalyse**“, Vieweg Verlag 1985
- A. Beutelspacher, „**Geheimsprachen**“, 1997, Beck'sche Verlagsanstalt
- B. Schneier, „**Applied Cryptography**“, „**Secrets&Lies**“, „**Practical Cryptography**“, John Wiley & Sons
- Klaus Schmeh, „**Kryptographie und PKIs im Internet**“, 2001, dpunkt
- C.Langenbach, O. Ulrich (Hrsg.): „**Elektronische Signaturen - Kulturelle Rahmenbedingungen**“ einer technischen Entwicklung, Springer Verlag, Berlin
- und sehr viele mehr

Grundlagen der IT-Sicherheit

→ Zeitschriften

- DuD Datenschutz und Datensicherheit – Recht und Sicherheit in Informationsverarbeitung und Kommunikation, Vieweg Verlag
- KES - Kommunikations- und EDV-Sicherheit, SecMedia Verlag
- Network Computing - CMP-WEKA Verlag
- GIT - Sicherheit + Management - Magazin für Safety und Security, GIT Verlag
- IT-Sicherheit - Praxis der Daten- und Netzsicherheit, DATAKONTEXT-Fachverlag
- Information Security Bulletin – Deutsche Ausgabe, Fachzeitschrift für Führungskräfte im IT-Sicherheitsbereich, CHI Publishing Ltd.
- WIK – Zeitschrift für die Sicherheit der Wirtschaft, SecMedia Verlag
- www.bsi.de, www.teletrust.de, www.bridge-ca.org, www.regtp.de, ...



**Westfälische
Hochschule**

Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Vorlesung: Grundlagen der IT-Sicherheit

**Vielen Dank für Ihre Aufmerksamkeit
Fragen ?**

Prof. Dr. (TU NN)

Norbert Pohlmann

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

if(is)
internet-sicherheit.