Firewall-Systeme

Ziele, Bedrohungen sowie Angriffsmethoden und prinzipielle Gegenmaßnahmen

Prof. Dr. Norbert Pohlmann
Fachbereich Informatik
Verteilte Systeme und Informationssicherheit

Fachhochschule Gelsenkirchen

Inhalt

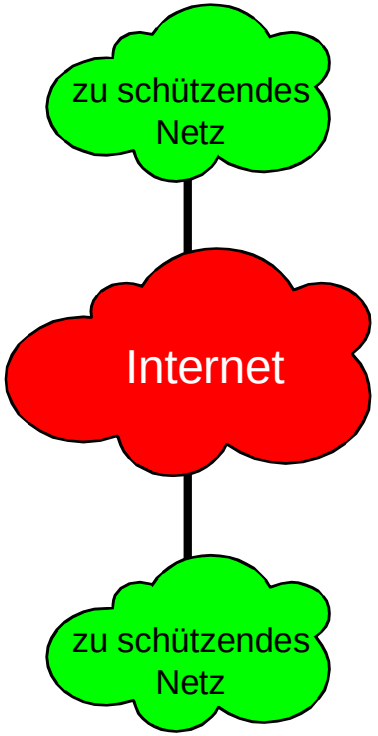
- Ziele
- Kommunikationsmodell
- Bedrohungen (Firewall-System)
- Definition eines Firewall-Elements
- Angriffsmethoden und prinzipielle Gegenmaßnahmen
- Zusammenfassung

Inhalt

- **Ziele**
- Kommunikationsmodell
- Bedrohungen (Firewall-System)
- Definition eines Firewall-Elements
- Angriffsmethoden und prinzipielle Gegenmaßnahmen
- Zusammenfassung

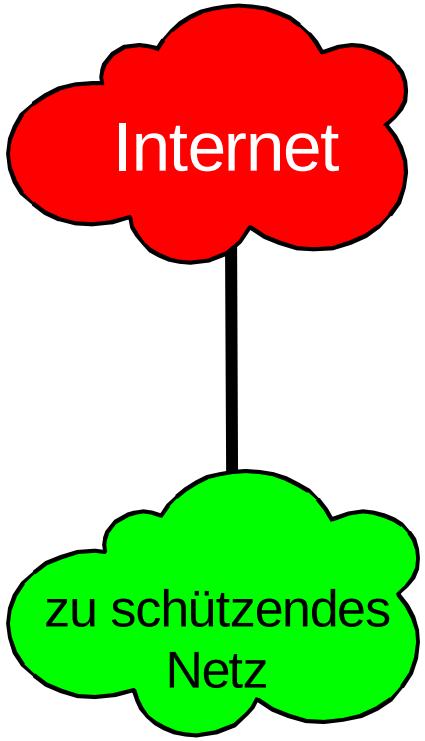
Ziele (Chancen)
→ Kommunikation über IP-Netze

- Einfacher und kostengünstiger Zugang
- Weltweites Netz
- Weite Verbreitung
- Einheitlicher Standard
- Günstig für internationale Verbindungen



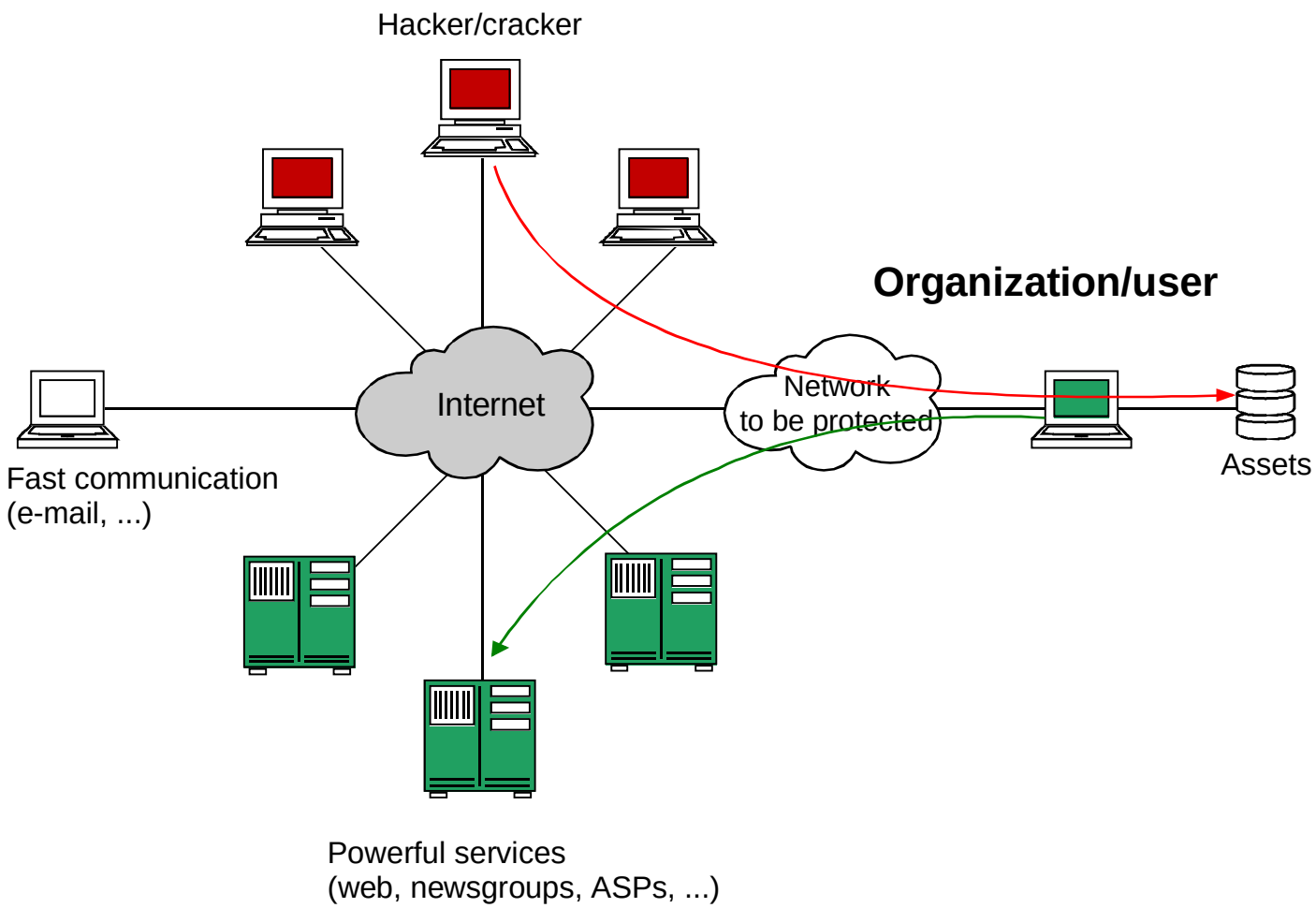
Ziele (Chancen)
→ TCP/IP-Dienste

- Elektronische Post (E-mail)
- Multimedia (World Wide Web)
- Dateien-Transfer (FTP)
- Weltweite Foren (News)
- Online-Ankopplung an Rechnersysteme
- Internet als weltweite Informationsquelle



Chance und Risiko
→ Zwei Seiten einer Medaille

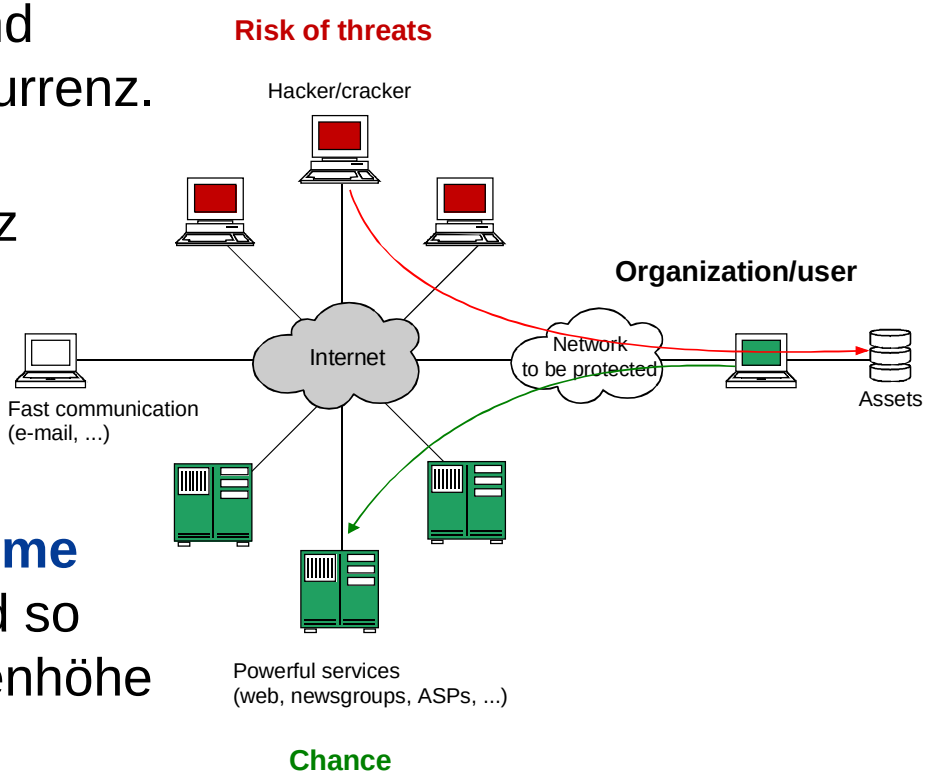
Risk of threats



Chance

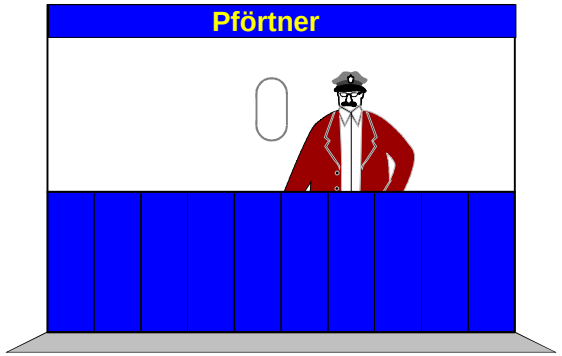
Ein öffentliches Netz ist keine Einbahnstraße

- High-Tech-Spione **stehlen** fremdes Know-How oder Strategiepläne und verkaufen sie lukrativ an die Konkurrenz.
- Hacker **brechen** in das lokale Netz von Firmen und Behörden ein und fälschen Daten oder schleusen falsche Informationen **ein**.
- Hacker können die **Rechnersysteme** einer Organisation **lahmlegen** und so wirtschaftliche Schäden in Millionenhöhe verursachen.

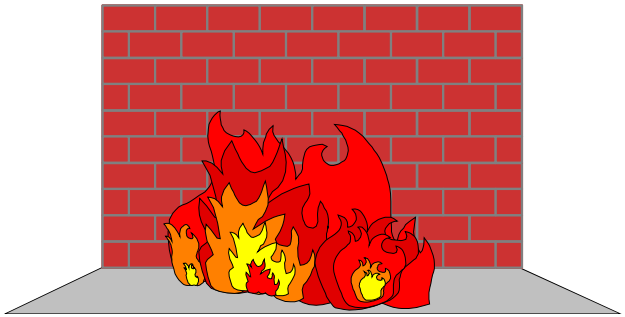


Analogien zu Firewall-Systemen

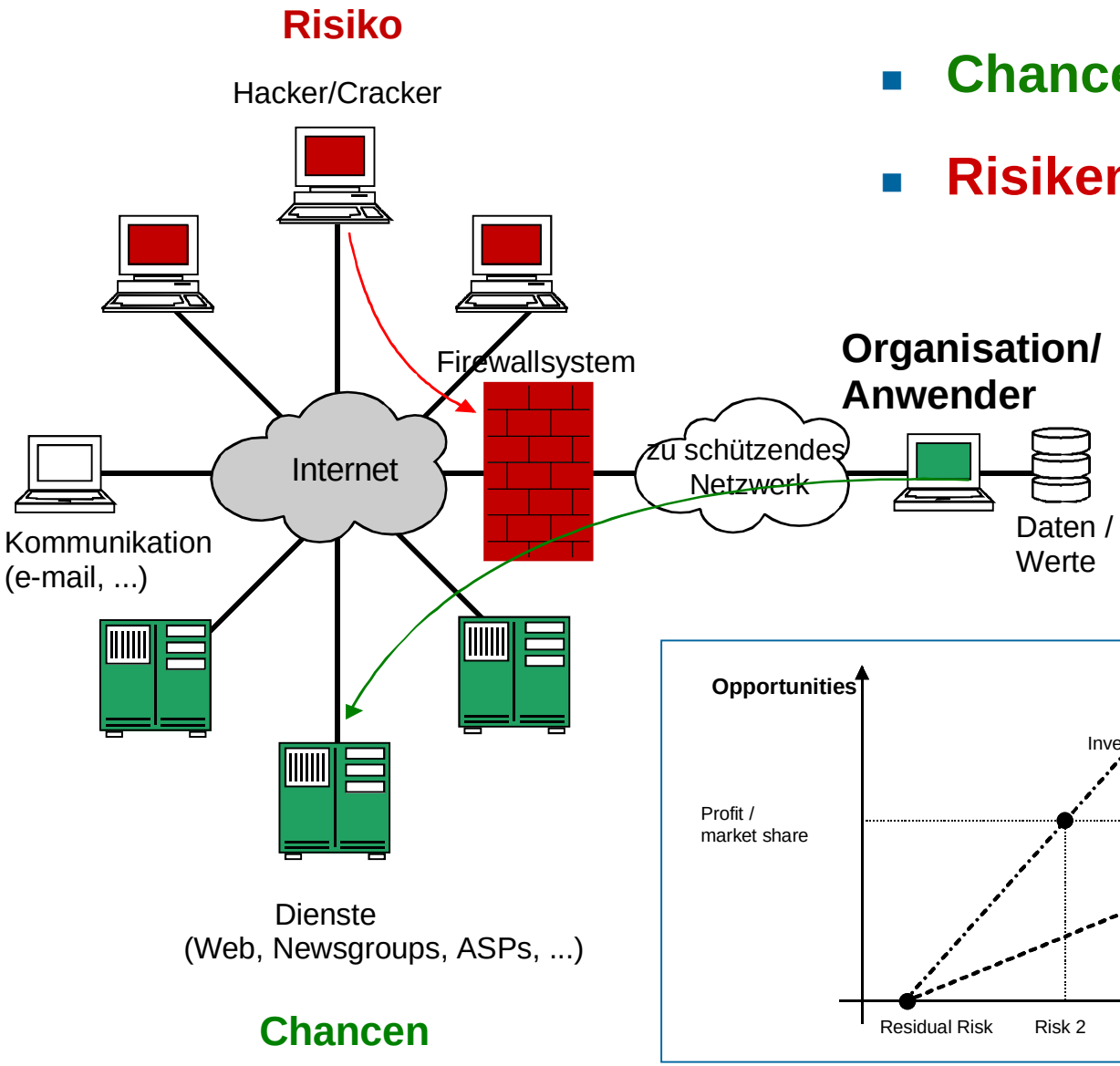
- **Pförtner**
  - schützt unsere Gebäude vor unbefugtem Eindringen
  - hält fest, wer uns besucht hat
  - kontrolliert, was herein und heraus geht



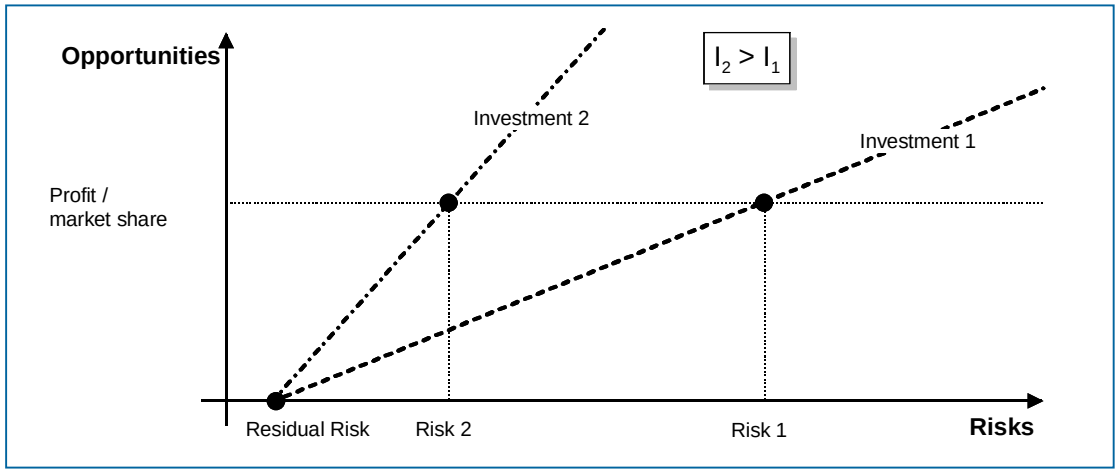
- **Brandmauer**
  - Abschottung bestimmter Abschnitte vor Gefahren
  - Schutz sensibler Bereiche vor Zerstörung



Idee eines Firewall-Systems

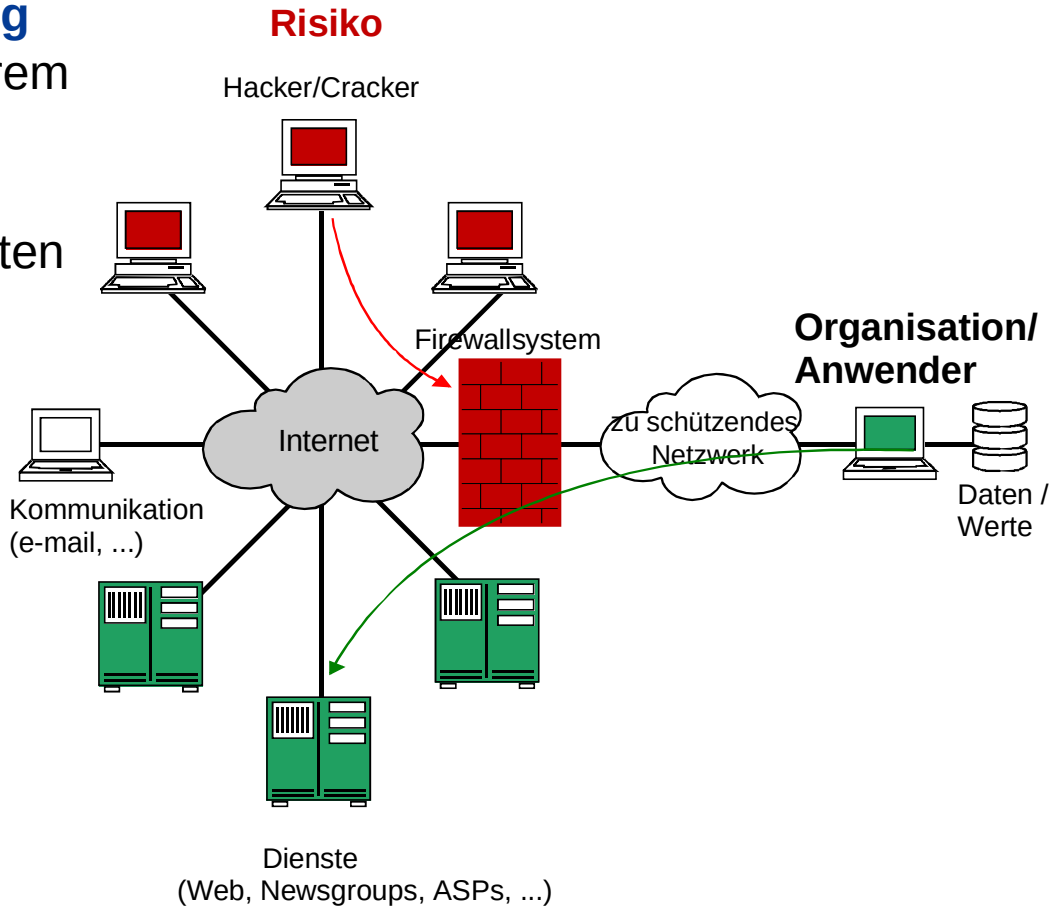


- **Chancen nutzen**
- **Risiken minimieren**



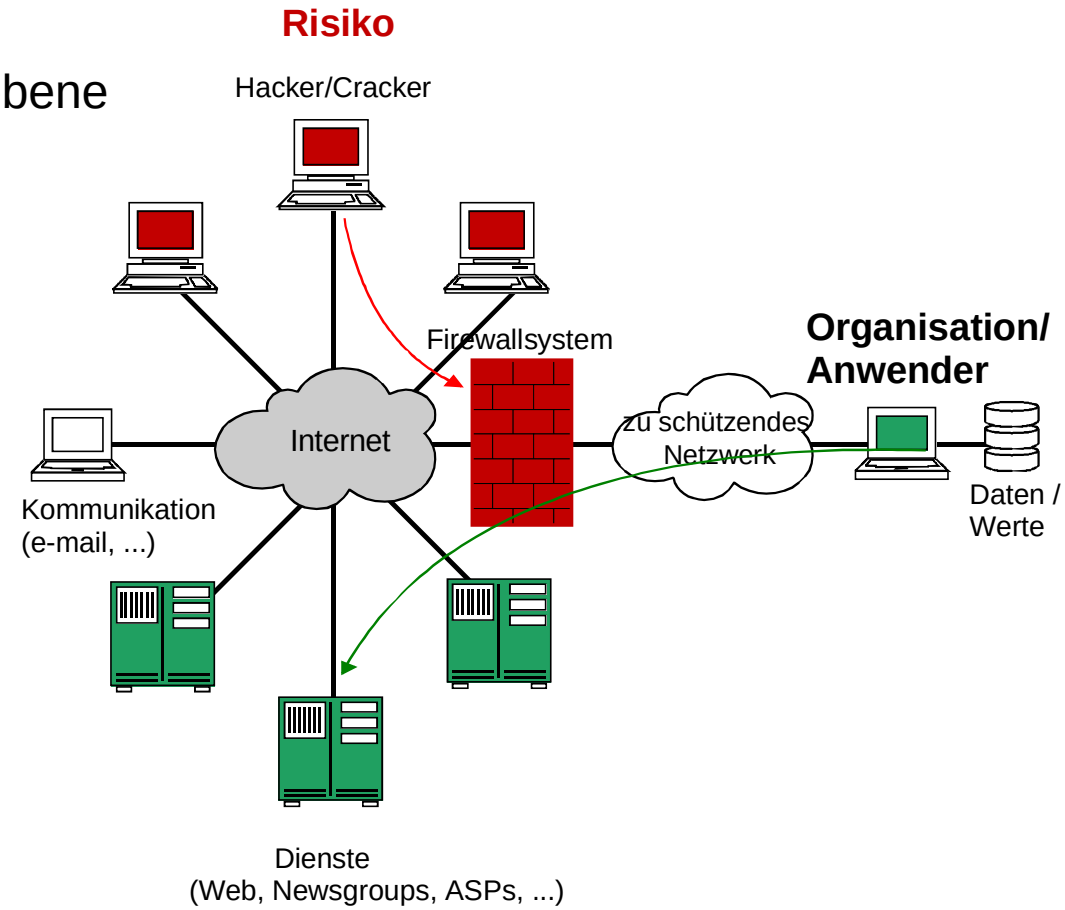
Ziele eines Firewall-Systems
→ Grundsätzlich

- Implementierung von Sicherheits-mechanismen, die den **Übergang** zwischen unsicherem und sicherem Netz **beherrschbar machen**
- **Analyse** der Kommunikationsdaten
- **Kontrolle** der Kommunikationsbeziehungen
- **Reglementierung** der Kommunikation
- **Protokollierung** sicherheitsrelevanter Ereignisse
- Eventuelle **Alarmierung** des Security-Administrators



Ziele eines Firewall-Systems
→ Sicherheitsfunktionen

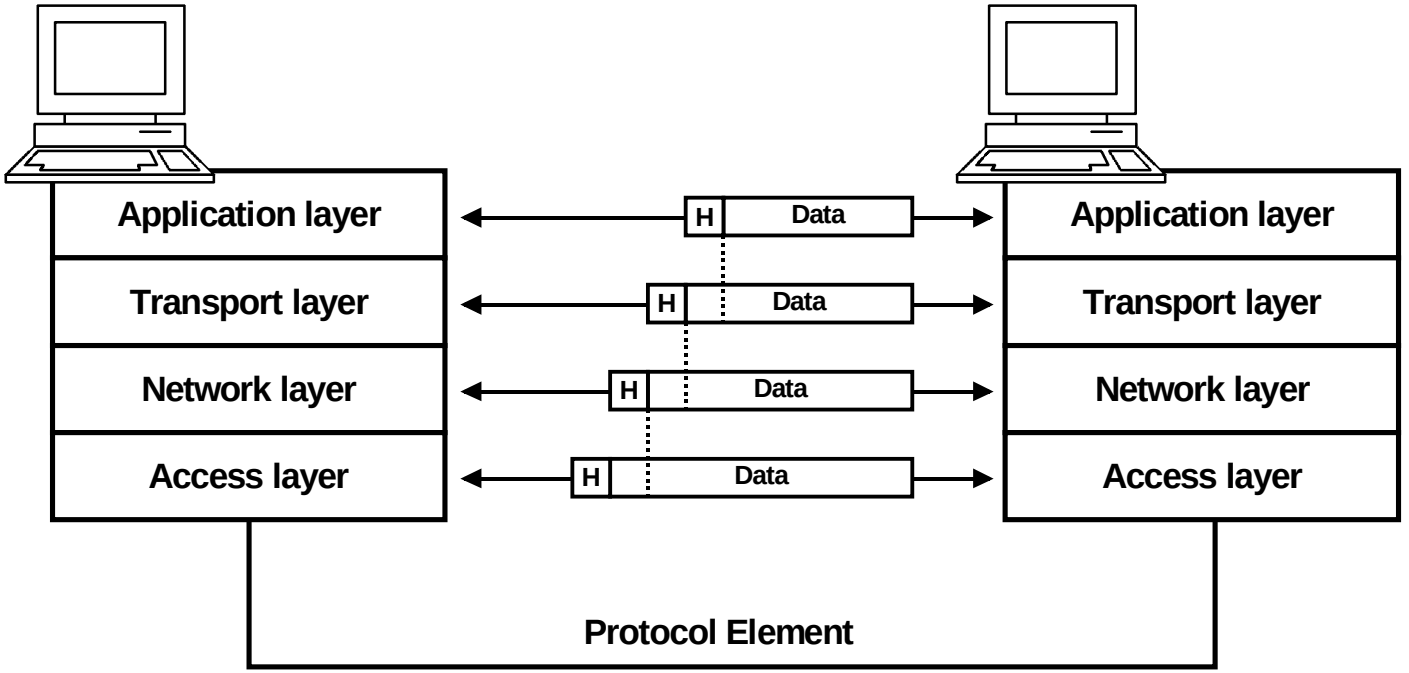
- Zugangskontrolle auf der Vermittlungsebene
- Zugangskontrolle auf Benutzerebene
- Rechteverwaltung
- Kontrolle auf der Applikationsebene
- Entkopplung von unsicheren Diensten
- Beweissicherung und Protokollauswertung
- Alarmierung
- Verbergen der internen Netzstruktur
- Vertraulichkeit der Nachrichten



Inhalt

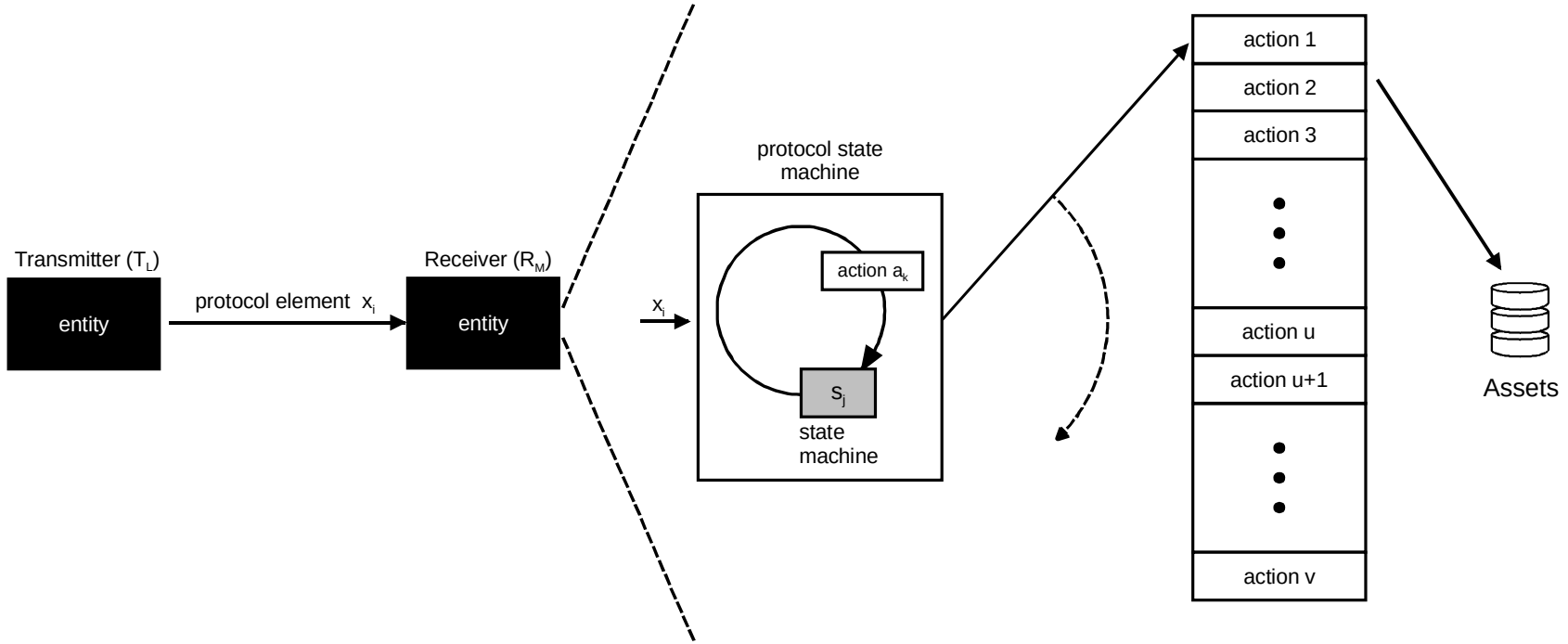
- Ziele
- **Kommunikationsmodell**
- Bedrohungen (Firewall-System)
- Definition eines Firewall-Elements
- Angriffsmethoden und prinzipielle Gegenmaßnahmen
- Zusammenfassung

TCP/IP-Protokollarchitektur



- In einer Schicht N kommunizieren (Peer) Entities miteinander
- Zwischen den Entities werden Protokollelemente (x_i) ausgetauscht
- Protokollelemente bestehen aus Headern und/oder Nutzdaten

Vereinfachtes logisches Kommunikationsmodell
→ Übersicht



- Jede Schicht hat eine eigene **„protocol state machine“**

Vereinfachtes logisches Kommunikationsmodell
→ Protokollelemente, die erlaubt sind

Summe der Protokollelemente

$$X = \{x_1, \ldots x_t, x_{t+1}, \ldots x_u, x_{u+1}, \ldots x_v, x_{v+1}, \ldots x_n\}$$

genormt und erlaubt $\{x_1, \ldots x_t\}$

- Menge der Protokollelemente aus der Norm, die für eine spezielle Aufgabe **notwendig und damit erlaubt sind** z.B.: die Kommandos »cdir« (Change Directory) and »put« (Transmit), um mit Hilfe vom FTP eine Datei vom Sender zu versenden und auf der Empfängerseite zu speichern

Vereinfachtes logisches Kommunikationsmodell
→ Protokollelemente, die nicht erlaubt sind

genormt und nicht erlaubt $\{x_{t+1}, \ldots x_u\}$

- Menge der Protokollelemente aus der Norm, die für die spezielle Aufgabe **nicht notwendig und damit nicht erlaubt sind**. z.B. bei FTP das Kommando »del« (Löschen von Dateien)

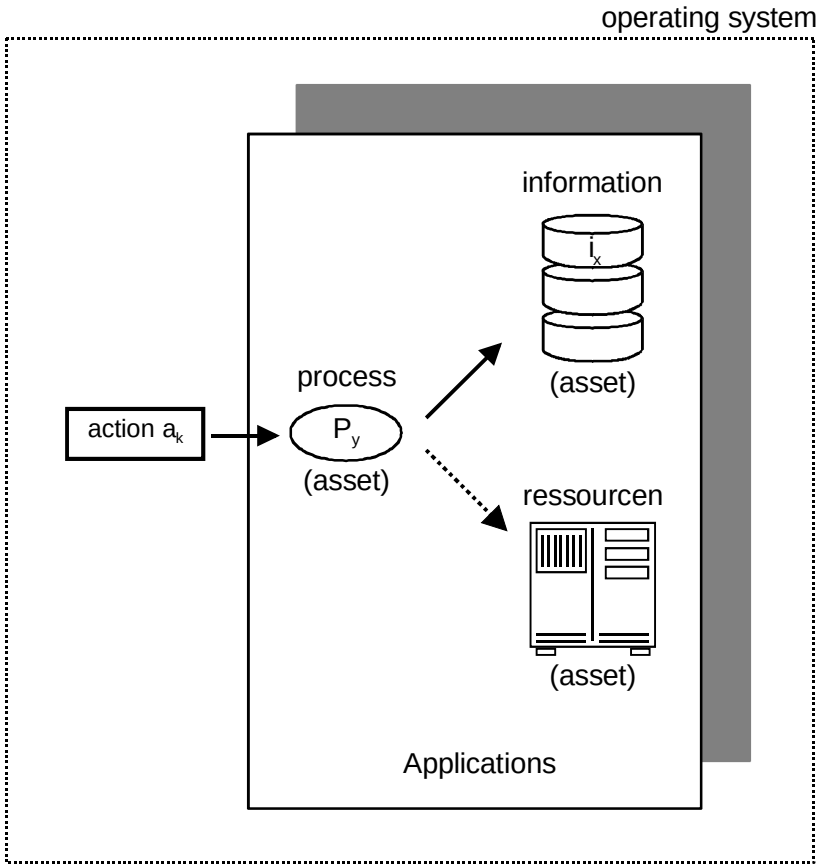
Herstellerdefiniert und nicht genormt $\{x_{u+1}, \ldots x_v\}$

- Menge der Protokollelemente, die **nicht in der Norm definiert sind**, aber zusätzliche Dienste anbieten.
  - **Fehleranalyse** (Zustand des Protokoll-Automats, Zustand des Betriebssystems, ...)
  - **Trap-Doors**, mit denen Angriffe realisiert werden und nicht definierte oder erlaubte Aktionen auf der Empfängerseite unautorisiert durchgeführt werden können.

Fehler $\{x_{v+1}, \ldots x_n\}$

- Menge der Protokollelemente, die **nicht in der Norm und nicht vom Hersteller definiert und damit nicht erlaubt sind**. Im Normalfall werden solche Protokollelemente von der Implementierung als Fehler erkannt und entsprechend behandelt.

Vereinfachtes logisches Kommunikationsmodell
→ Ablauf der Aktionen



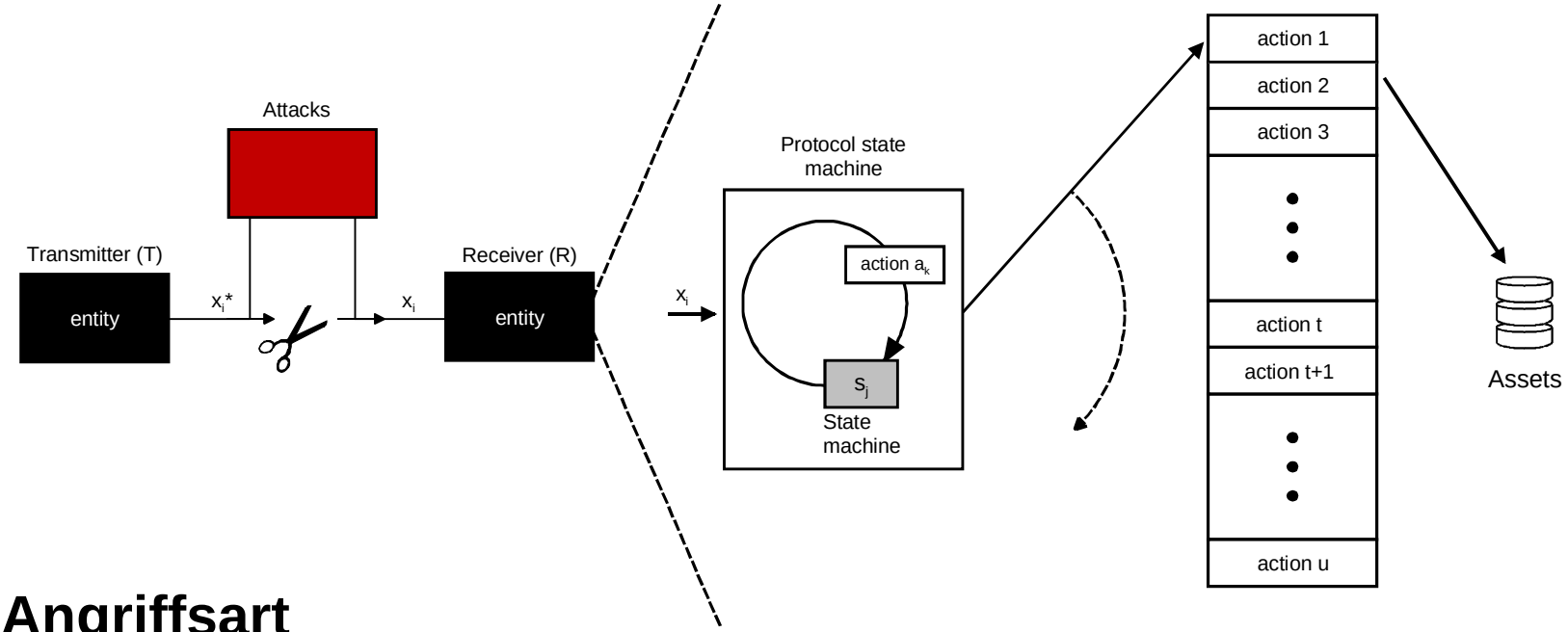
- **Informationen**
  - Entwicklungsdaten
  - Finanzdaten
  - ...
- **Ressourcen**
  - CPU-Kapazitäten
  - Drucker
  - spezielle Berechnungen (z.B. Steuer)
  - ...

- Auf welche Informationen und Ressourcen zugegriffen werden darf, wird über die **Rechteverwaltung des Betriebssystems oder der Anwendung** definiert

Inhalt

- Ziele
- Kommunikationsmodell
- **Bedrohungen (Firewall-System)**
- Definition eines Firewall-Elements
- Angriffsmethoden und prinzipielle Gegenmaßnahmen
- Zusammenfassung

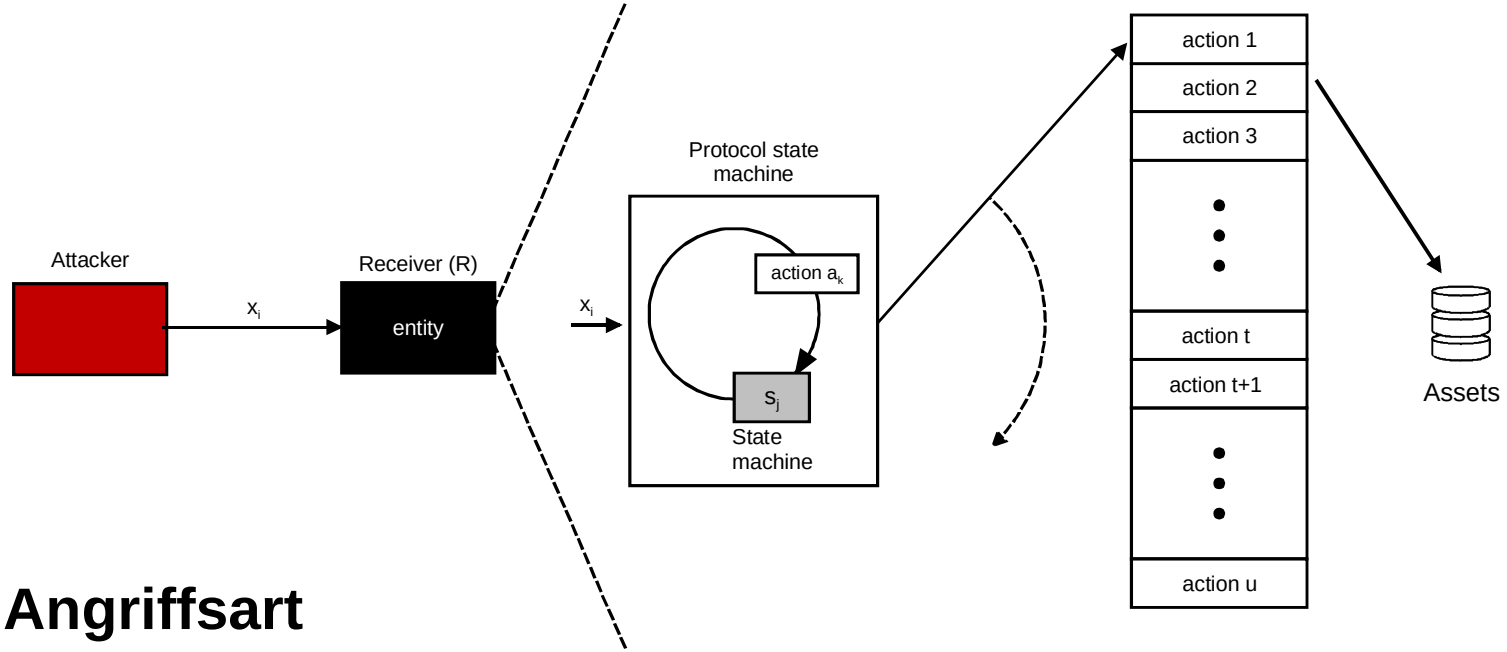
Bedrohungen (1/4)
→ Angriffe durch Dritte



- **Angriffsart**
  - Wiederholen oder Verzögern der/des Protokollelemente(s)
  - Einfügen oder Löschen bestimmter Daten in den Protokollelementen
  - Modifikation der Daten in den Protokollelementen
  - Boykott des Receivers
  - Trittbrettfahrer
  - **Empfangen von Malware (Viren, Würmer, Trojanische Pferde, ...)**

Bedrohungen (2/4)

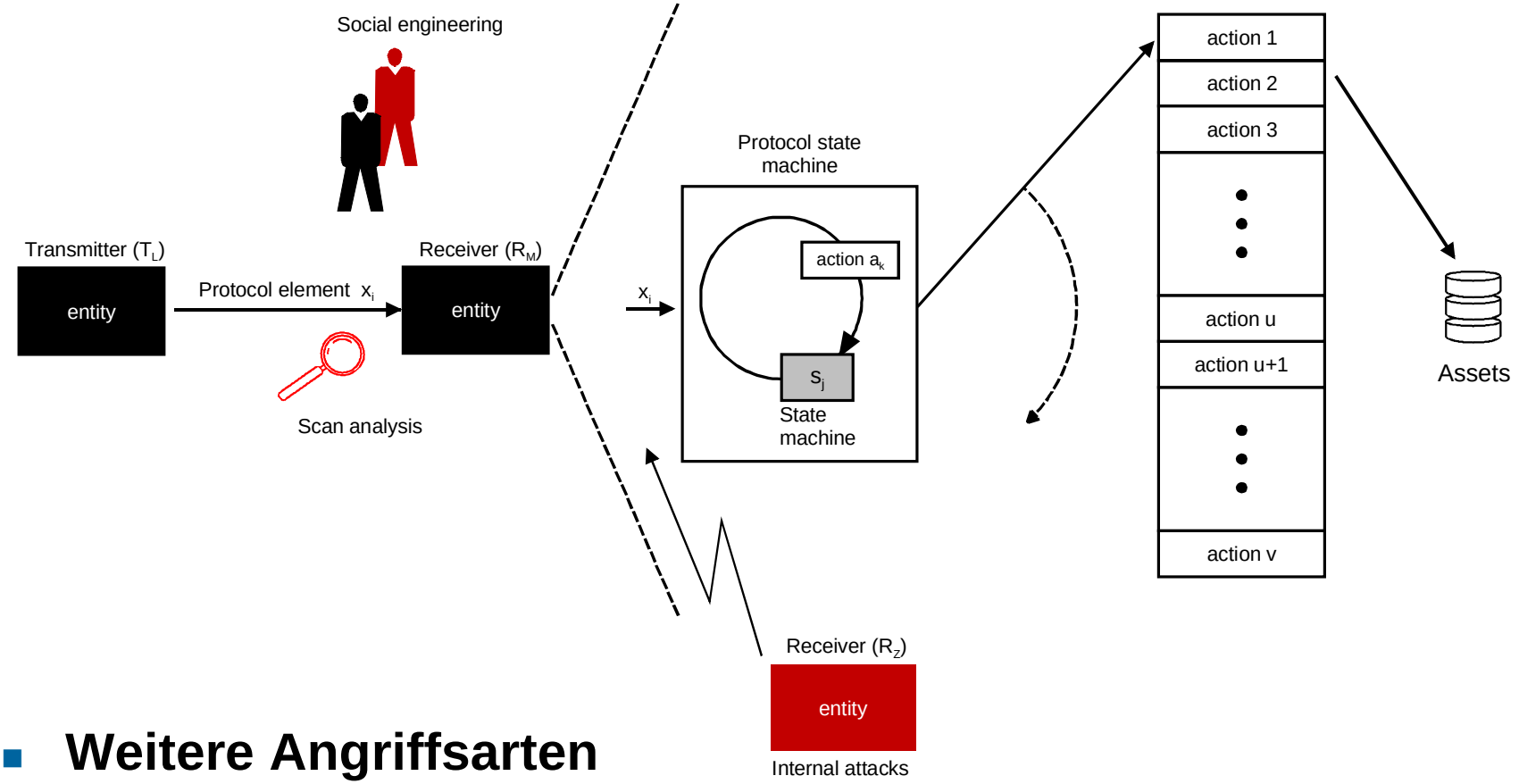
→ Angriffe von Kommunikationspartnern



- **Angriffsart**
  - Unberechtigter Aufbau und Nutzung einer Kommunikationsverbindung
  - Unberechtigte Nutzung von Kommunikationsprotokollen und -diensten
  - Vortäuschen einer falschen Identität (Maskerade-Angriff)
  - **Nutzung der Kommunikationsverbindung zum Receiver für gezielte Angriffe (z.B. Java-Applets, ActiveX-Control, Cookies, ...)**
  - Nutzung einer falschen Konfiguration
  - Nutzung von Implementierungsfehlern
  - Leugnen der Kommunikationsbeziehung

Bedrohung (3/4)

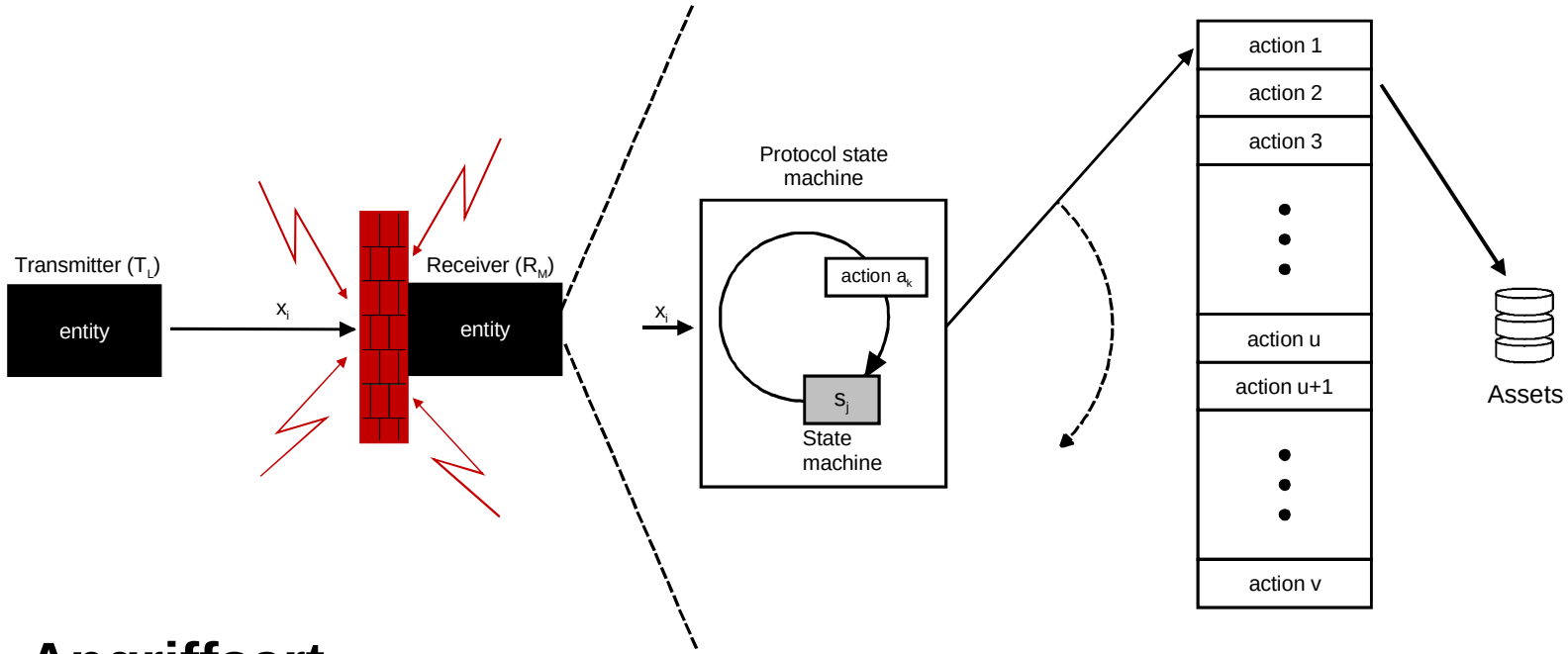
→ Vorbereitung eines Angriffs



- **Weitere Angriffsarten**
  - Social Engineering
  - Analyse mit Hilfe von Scannerprogrammen
- **Interne Angriffe**

Bedrohungen (4/4)

→ Angriffe auf das Firewall-System



- **Angriffsart**
  - Manipulation des Firewall-Systems
  - Einbau einer Trap-Door
  - Nutzung einer falschen Konfiguration des Firewall-Systems
  - Nutzung von Implementierungsfehlern des Firewall-Systems

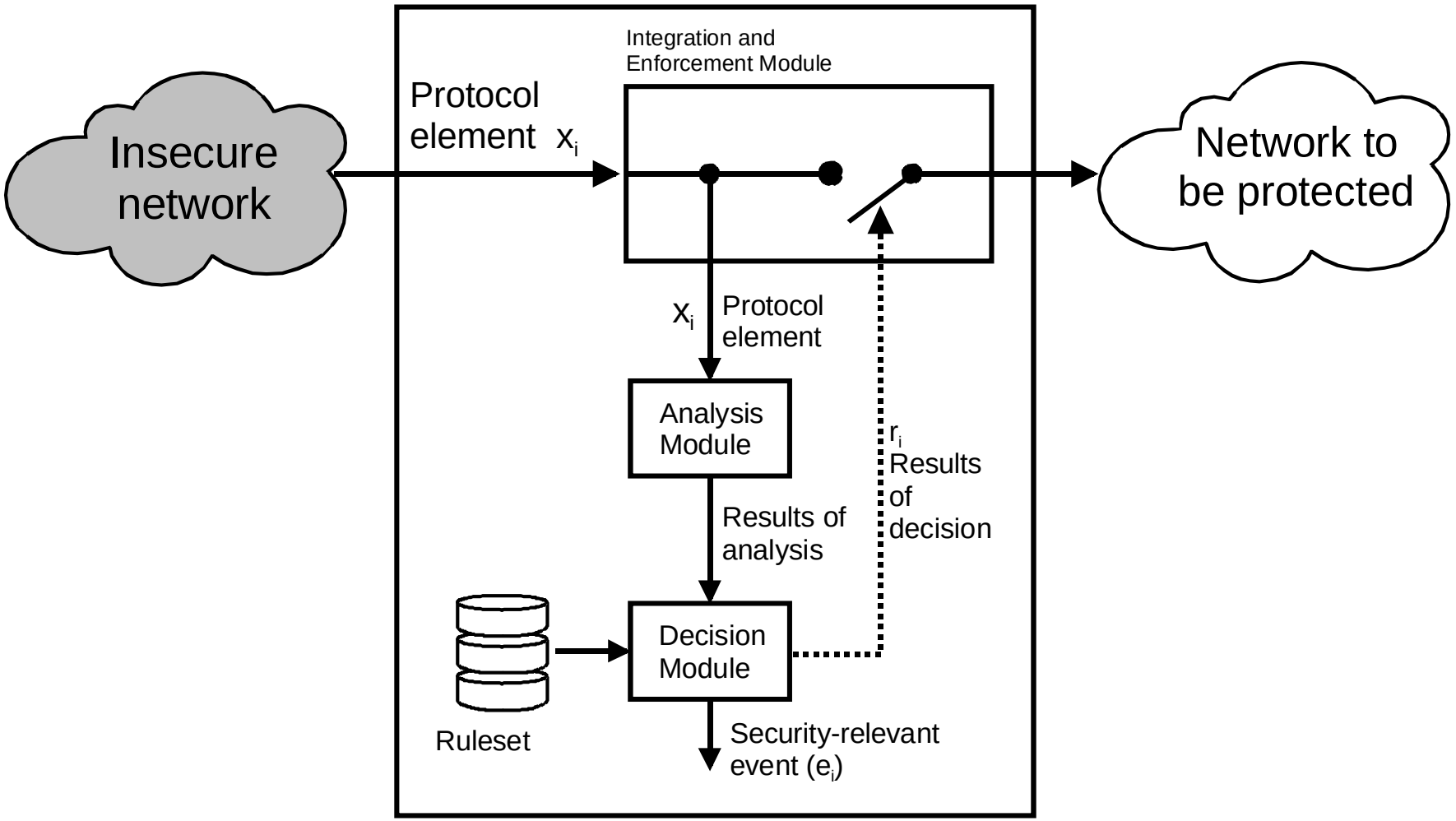
Inhalt

- Ziele
- Kommunikationsmodell
- Bedrohungen (Firewall-System)
- **Definition eines Firewall-Elements**
- Angriffsmethoden und prinzipielle Gegenmaßnahmen
- Zusammenfassung

Definition eines Firewall-Elements
→ Grundsätzliches

- Ein zentrales Firewall-System ist ein **separates Kommunikationssicherheitssystem**
- Es besteht in der Regel keine **direkte Verbindung mit den Sicherheitsfunktionen der Betriebssysteme und Anwendungen**
- Ein Firewall-System hat **keinen Einfluß** (Erweiterung, Veränderung) auf die **verwendeten Kommunikationsprotokolle und -dienste**
- Ein **Firewall-System** wird von der Organisation verwaltet, die es betreibt, und ist im Prinzip **unabhängig** von allen anderen Organisationen in dieser Verwaltung (anders als bei VPN-Systemen)

Definition eines Firewall-Elements
→ Grundsätzlicher Aufbau



Definition eines Firewall-Elements
→ Beschreibung der Komponeten (1/4)

- **Einbindungs- und Durchsetzungsmodul:**
  - Das Einbindungs- und Durchsetzungsmodul realisiert die Einbindung des aktiven Firewall-Elements in das Kommunikationssystem sowie die **Durchsetzung der im Regelwerk festgehaltenen Sicherheitspolitik**.
  - Die Einbindung in das Kommunikationssystem muss so realisiert werden, dass die Kommunikationsdaten nicht am Einbindungsmodul vorbeifließen können, ohne einer Analyse und einer Entscheidung unterzogen worden zu sein.
  - Aus diesem Grund ist die Einbindung **besonders sicherheitskritisch**.
  - In Abhängigkeit vom verwendeten Protokollelement wird das Einbindungsmodul an unterschiedlichen Stellen der Protokollarchitektur eingebunden.

Definition eines Firewall-Elements
→ Beschreibung der Komponeten (2/4)

- **Analysemodul** → *analysis*(x_i)**:**
  - Im Analysemodul werden die Kommunikationsdaten des **Protokollelements (x_i)** den Möglichkeiten des aktiven Firewall-Elements entsprechend **analysiert**.
  - Die Ergebnisse der Analyse werden an das Entscheidungsmodul weitergeleitet.
  - Im Analysemodul können mit Hilfe von Zustandsautomaten Statusinformationen (zum Beispiel Verbindungsaufbau, Transferzustand oder Verbindungsabbau) der Kommunikation festgehalten werden.

Definition eines Firewall-Elements
→ Beschreibung der Komponeten (3/4)

- **Entscheidungsmodul**
  - Im Entscheidungsmodul werden die **Analyseergebnisse** ausgewertet und **mit den im Regelwerk** festgelegten Definitionen der Sicherheitspolitik **verglichen**.
  - Hier wird anhand von Access-Listen überprüft, ob das ankommende Protokollelement (x_i) passieren darf oder nicht (r_i = result of the decision).
  - Falls ja, wird das Einbindungsmodul zum Durchlaß aktiviert.
  - Falls nein, wird das Protokollelement (x_i) nicht durchgelassen; das Ereignis (e_i) wird als sicherheitsrelevant eingestuft und entsprechend weiterverarbeitet.

Definition eines Firewall-Elements
→ Beschreibung der Komponeten (4/4)

- **Regelwerk** → *security-management* **(rules):**
  - Das Regelwerk ist die **technische Umsetzung der Sicherheitspolitik** und wird mit Hilfe eines Security Managements erstellt.
  - Im Regelwerk stehen alle Informationen (rules: Schlüssel, Access-Listen, Attribute usw.) über Benutzer, Authentikationsverfahren, Kommunikationsverbindungen, Kommunikationsprotokolle und -dienste, die notwendig sind, um eine Entscheidung für oder gegen eine Übertragung des Protokollelements (x_i) über das aktive Firewall-Element fällen zu können, und wie mit sicherheitsrelevanten Ereignissen (e_i) verfahren werden soll.

Firewall-Elemente

Ein so definiertes Firewall-Element kann ein

- Packet Filter
- Stateful Inspection
- Application Gateway
- Adaptive Proxy
- usw.

sein.

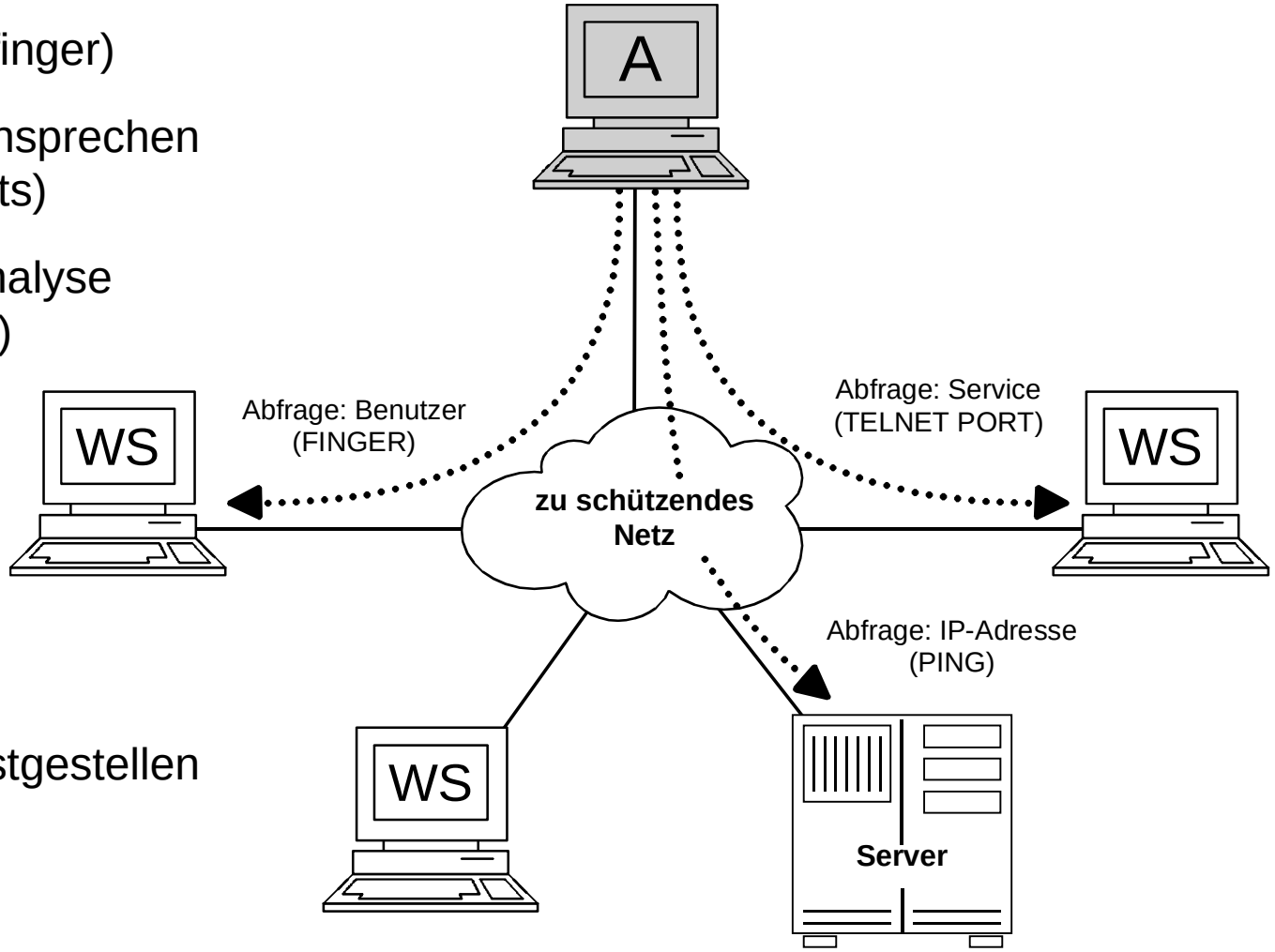
Inhalt

- Ziele
- Kommunikationsmodell
- Bedrohungen (Firewall-System)
- Definition eines Firewall-Elements
- **Angriffsmethoden und prinzipielle Gegenmaßnahmen**
- Zusammenfassung

Analyse des Netzes mit Hilfe von Scannerprogrammen

Was kann analysiert werden?

- Rechnersysteme (ping)
- Aktive Benutzer (finger)
- Aktive Dienste (Ansprechen der einzelnen Ports)
- Schwachstellenanalyse (z.B. ISS, SATAN)

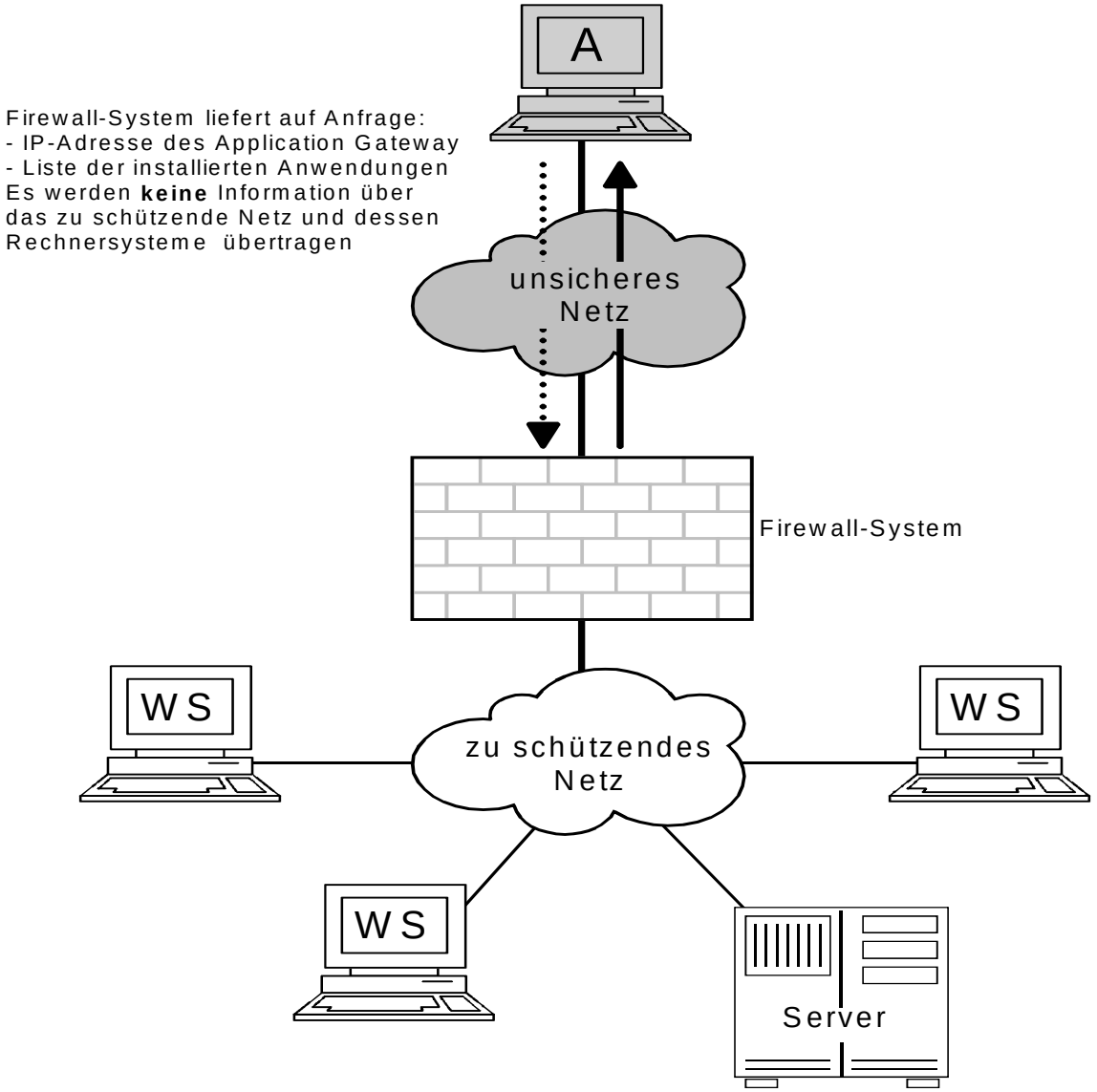


Ziel:

- Ausnutzen der festgestellen Schwachstellen

Wie kann ein Firewall-System helfen?

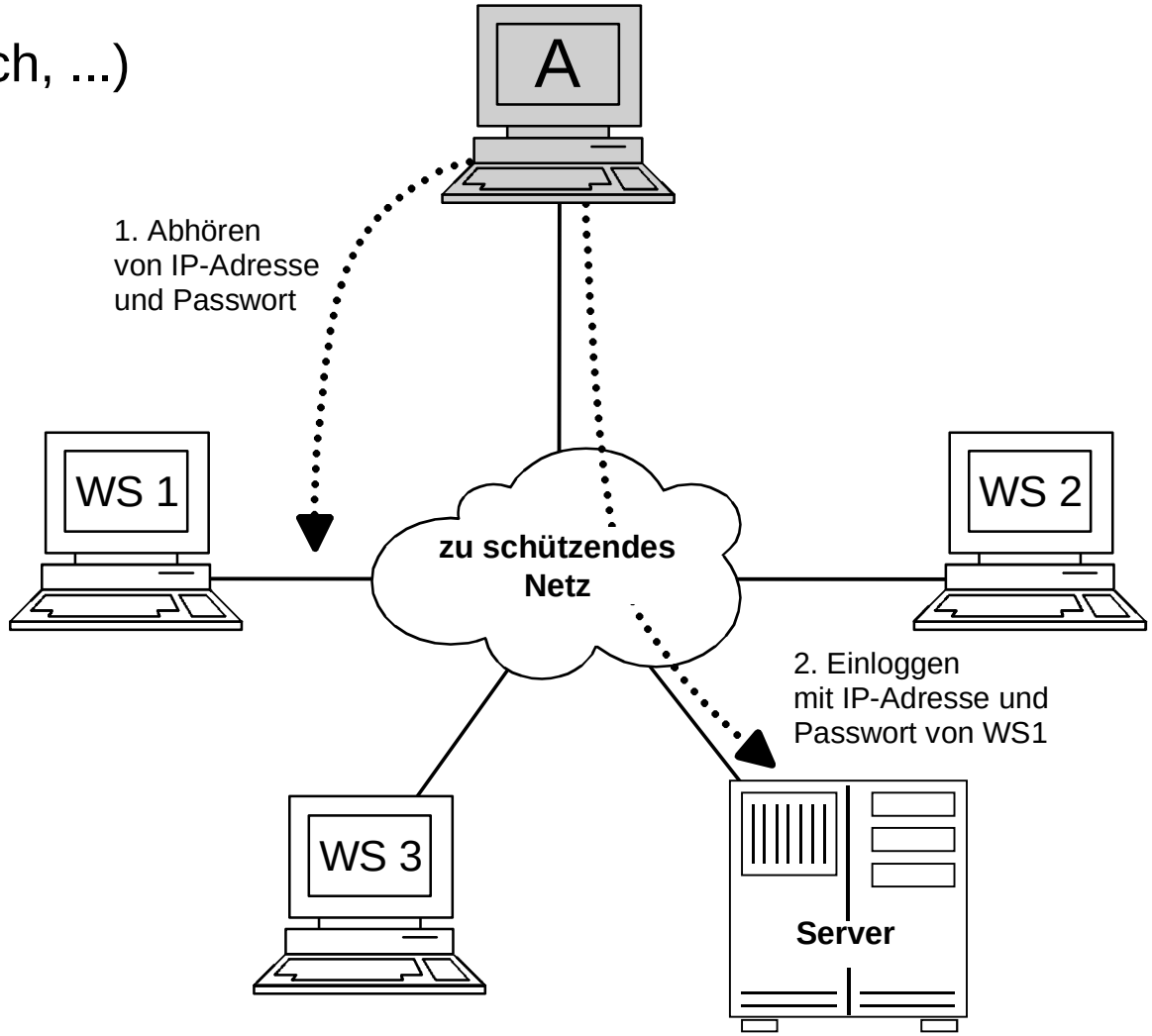
- **Verbergen der internen Netzstruktur**



Password-Snooping und IP-Maskerade

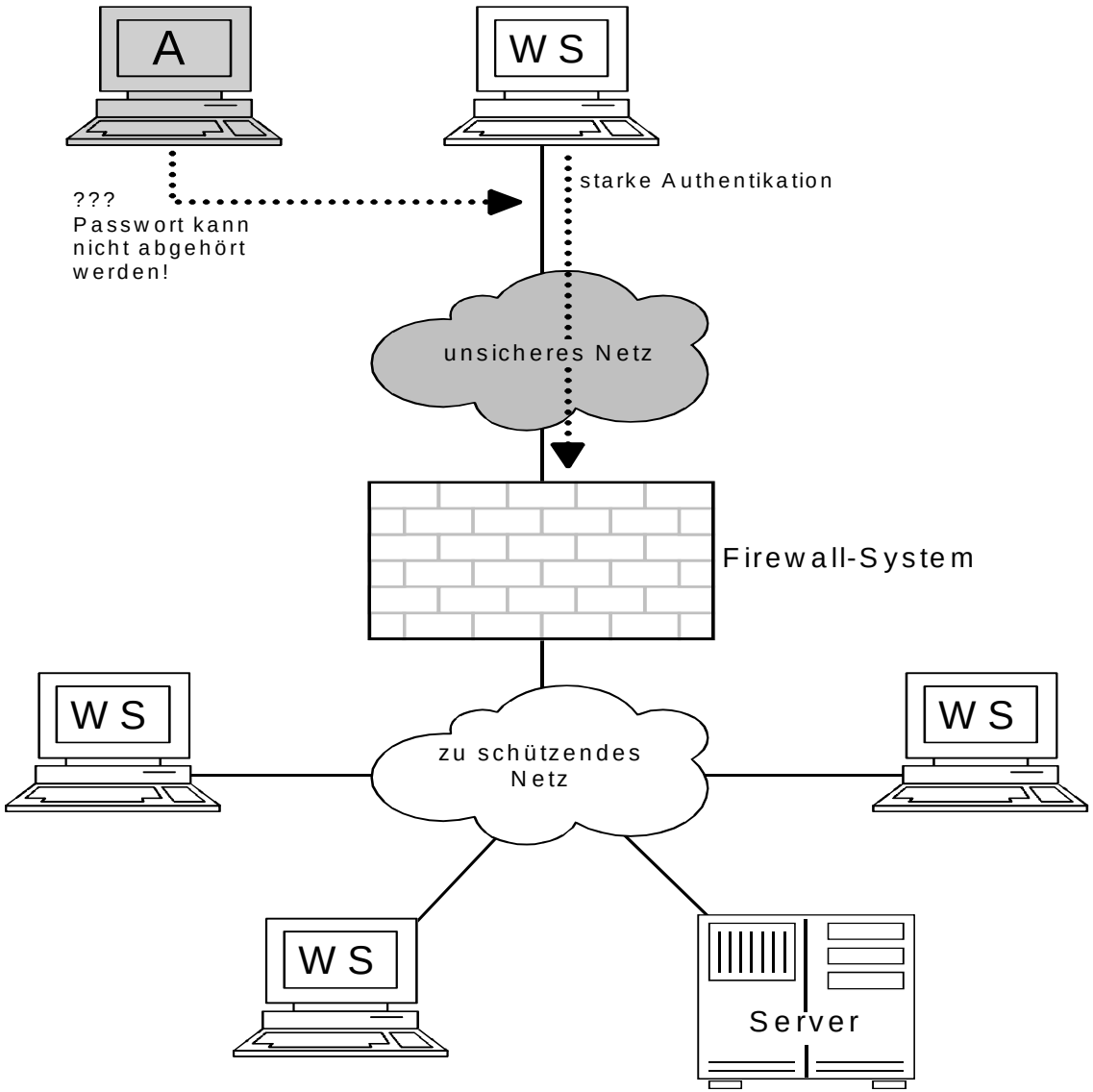
- **1. Analyse**
  (Ethereal, LAN-Watch, ...)

- **2. Nutzung**
  von IP-Adresse und Passwort



Wie kann ein Firewall-System helfen?

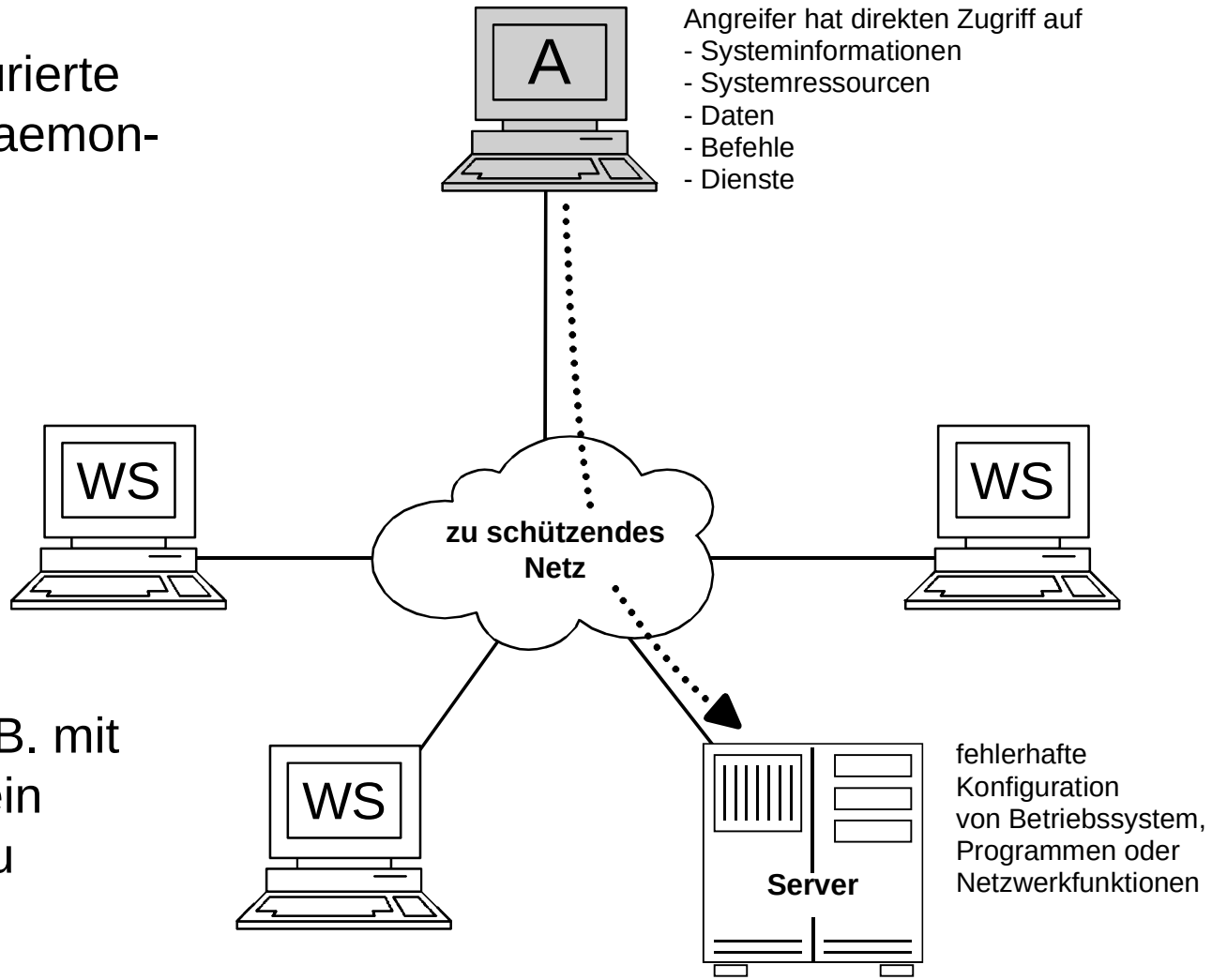
- **Starke Authentikation**



Nutzung einer falschen Konfiguration

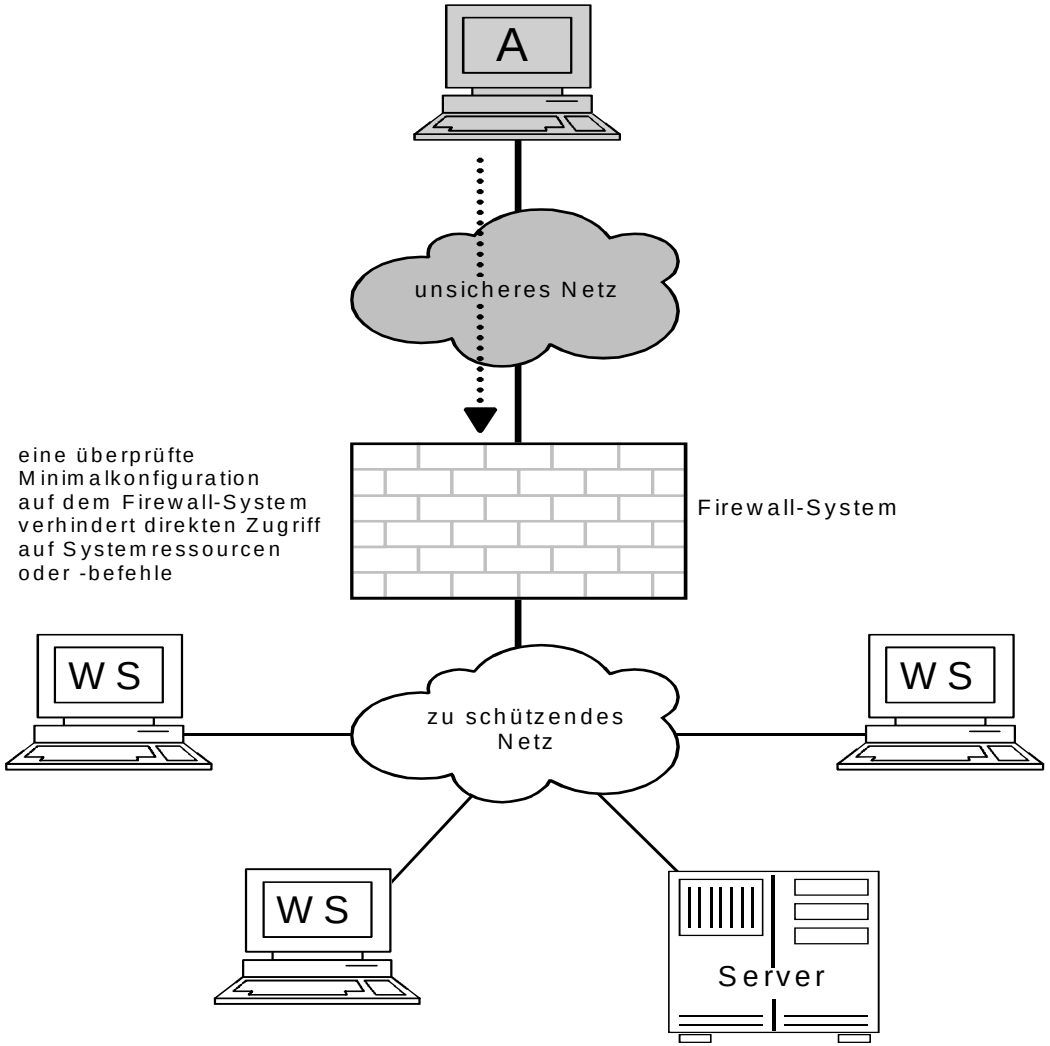
- **Problem:**
  z.B. falsch konfigurierte oder installierte Daemon-Prozesse

- **Angreifer**
  nutzt diese, um z.B. mit Root-Rechten in ein Rechnersystem zu gelangen



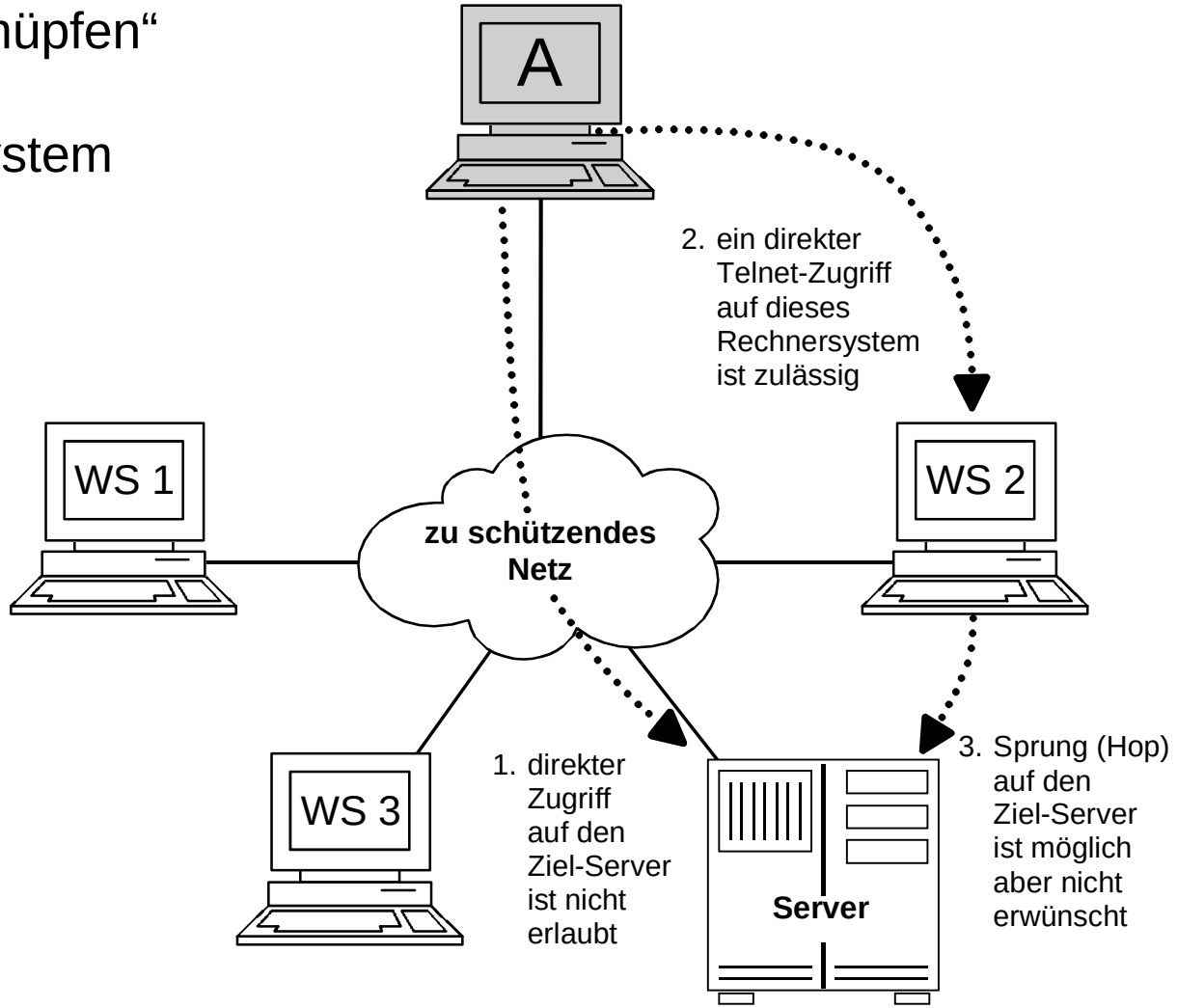
Wie kann ein Firewall-System helfen?

- Proxy-Funktionalität
- Kein direkter Zugriff auf die zu schützenden Rechnersysteme
- Sicherheit durch Entkopplung



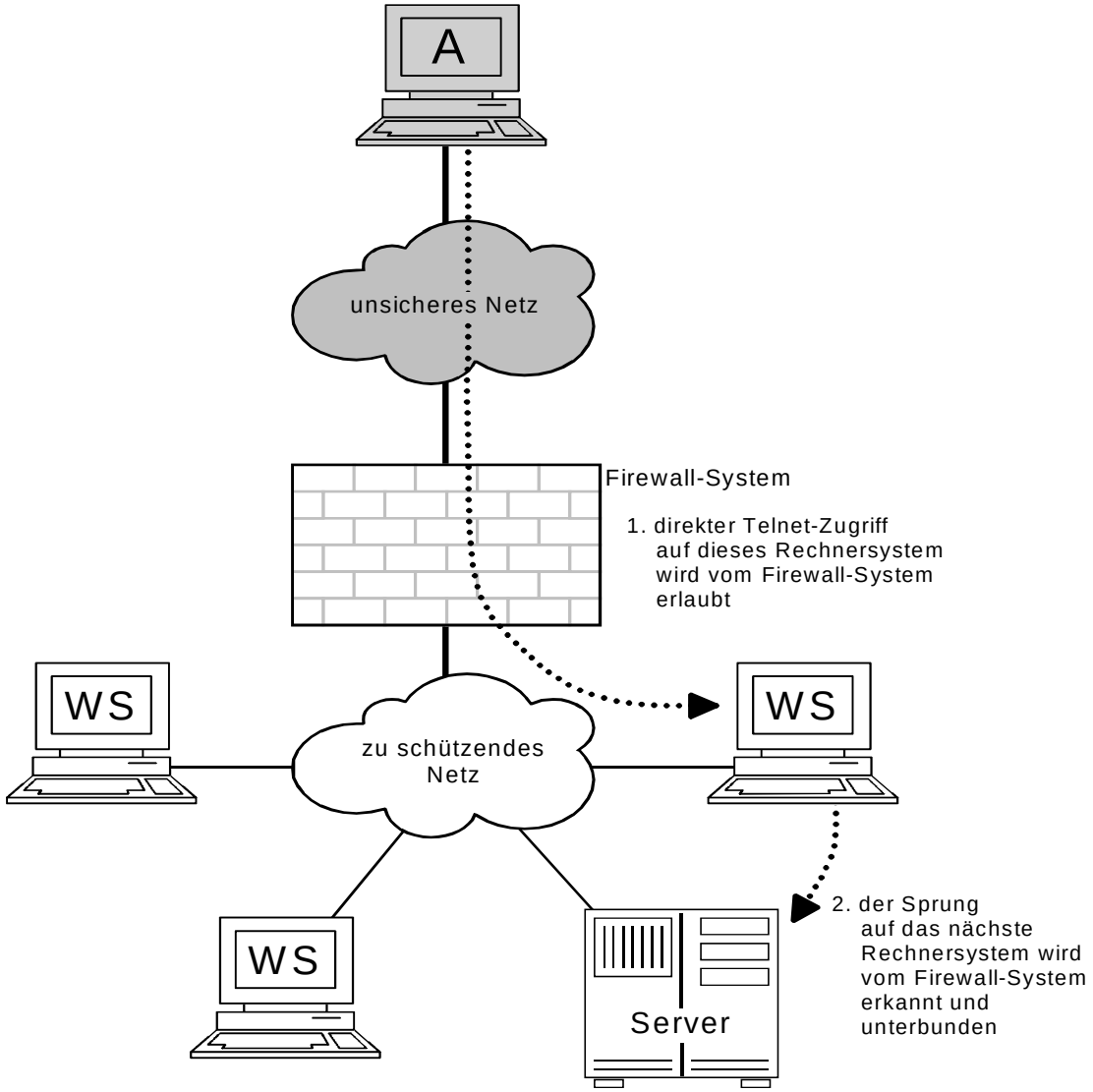
Hopping (Telnet)

- Unerlaubtes „Weiterhüpfen“ von einem remoten, erlaubten Rechnersystem auf ein weiteres nicht erlaubtes Rechnersystem



Wie kann ein Firewall-System helfen?

- **Monitoring einer Telnet-Session**



Inhalt

- Ziele
- Kommunikationsmodell
- Bedrohungen (Firewall-System)
- Definition eines Firewall-Elements
- Angriffsmethoden und prinzipielle Gegenmaßnahmen
- **Zusammenfassung**

Zusammenfassung

- Ein Firewall-System stellt Sicherheitsmechanismen zur Verfügung, die den Übergang zwischen unsicherem und sicherem Netz beherrschbar machen sollen.
- Ein Firewall-System kann aus einem oder mehrere Firewall-Elemente bestehen.

Firewall-Systeme

Ziele, Bedrohungen sowie Angriffsmethoden und prinzipielle Gegenmaßnahmen

Vielen Dank für Ihre Aufmerksamkeit

Fragen ?

norbert.pohlmann@informatik.fh-gelsenkirchen.de

Fachhochschule Gelsenkirchen