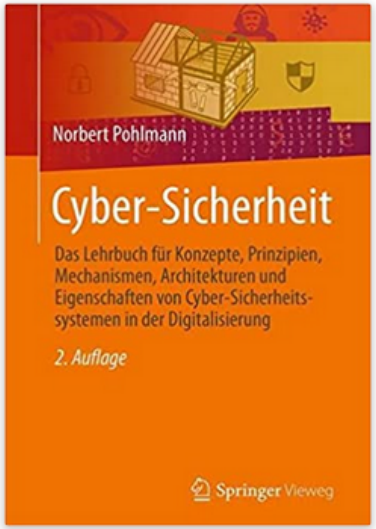
Einführung in die IT-Sicherheit

Prof. Dr. Jean-Pierre Seifert

jpseifert@sec.t-labs.tu-berlin.de

http://www.sec.t-labs.tu-berlin.de/

Literatur



Dieses Bild anzeigen

Cyber-Sicherheit: Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung Taschenbuch – 23. Mai 2022

von Norbert Pohlmann (Autor)

Alle Formate und Editionen anzeigen

Taschenbuch
32,99 € ✓prime

1 Neu ab 32,99 €

Dieses Lehrbuch gibt Ihnen einen Überblick über die Themen der IT-Sicherheit Die digitale Transformation eröffnet viele neue Möglichkeiten, den dadurch lassen sich Geschäftsmodelle und Verwaltungsprozesse radikal verändern. Aber mit fortschreitender Digitalisierung nimmt jedoch die Komplexität der IT-Systeme- und Infrastrukturen zu. Zudem werden die Methoden der professionellen Angreifer ausgefeilter und die Angriffsziele kontinuierlich lukrativer, insgesamt führt dies bei Unternehmen und der Gesellschaft zu hohen Schäden. Für eine erfolgreiche Zukunft unserer Gesellschaft ist es daher entscheidend, diesen gestiegenen Risiken entgegenzuwirken und eine sichere sowie vertrauenswürdige IT zu gestalten. Von daher ist es notwendig, dass mit den wachsenden Herausforderungen auch neue Entwicklungen und Prozessen in der Cyber-Sicherheit einhergehen. Was sich hier getan hat können Sie in der 2. Auflage des Lehrbuchs ‚Cyber-Sicherheit', von Prof. Norbert Pohlmann, nachlesen. Denn in der Überarbeitung der sehr erfolgreichen Erst-Auflage wurden die bestehenden Kapitel ergänzt und aktualisiert sowie zusätzlich für neue Themen weitere Kapitel hinzugefügt. Aber auch Lehrmaterialien, wie 19 komplette Vorlesungen und Überbungen auf den Webseiten wurden angepasst und erweitert.

Auf insgesamt 746 Seiten bietet Informatikprofessor Norbert Pohlmann grundlegendes Wissen über die Cyber-Sicherheit und geht bei innovativen Themen, wie Self Sovereign Identity oder dem Vertrauenswürdigkeits-Modell, detailliert in die Tiefe. Dabei ist dem Autor wichtig, nicht nur theoretisches Fachwissen zu vermitteln, sondern auch den Leser in die Lage zu versetzen, die Cyber-Sicherheit aus der anwendungsorientierten Perspektive zu betrachten.

Lernen Sie mithilfe dieses Lehrbuchs mehr über Mechanismen, Prinzipien, Konzepte und Eigenschaften von Cyber-Sicherheitssystemen. So sind Sie in der Lage, die Sicherheit und Vertrauenswürdigkeit von IT-Lösungen zu beurteilen.

0. Organisation

- **Lerninhalte:**

  Den Studierenden werden grundlegende Kenntnisse bezüglich der folgenden Themen vermittelt:

  - Begriffe, Definitionen, Zielsetzung und Motivation der IT-Sicherheit
  - Kryptographie: Symmetrische und asymmetrische Verschlüsselung
  - Identifikation und Authentifikation
  - Entwurf sicherer Systeme + Access Control + Principle of Least Privilege
  - Netzwerksicherheit
  - Schwachstellen in Soft- und Hardware
  - Security Testing

Firewall-Systeme

Firewall-Systeme

→ **Inhalt**

- **Ziele und Ergebnisse der Vorlesung**
- **Bedrohungen im Netz**
- **Sicherheitskonzept**
- **Kommunikationsmodell**
- **Firewall-Elemente**
- **Firewall-Konzepte**
- **Zusammenfassung**

- **Ziele und Ergebnisse der Vorlesung**
- Bedrohungen im Netz
- Sicherheitskonzept
- Kommunikationsmodell
- Firewall-Elemente
- Firewall-Konzepte
- Zusammenfassung

Ziele und Ergebnisse der Vorlesung

→ **Firewall-Systeme**

- Gutes Verständnis für die **Bedrohungen** im Netz und die entsprechenden **Sicherheitskonzepte** von Firewall-Systemen.

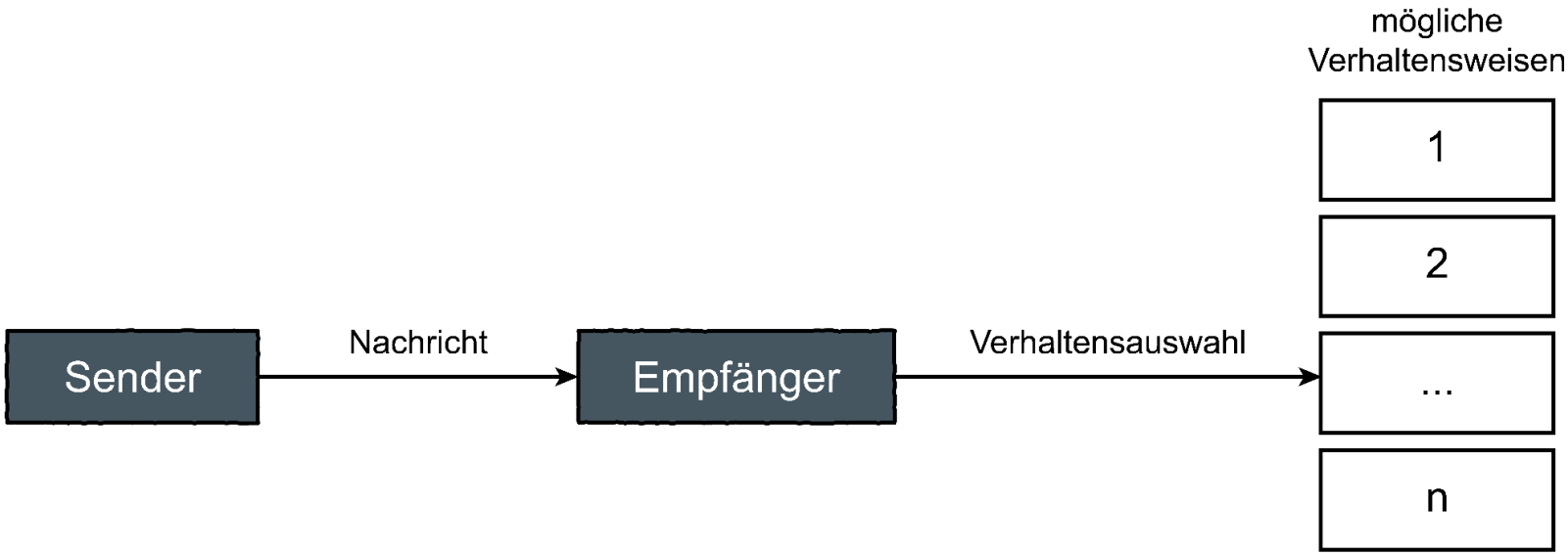
- Erlangen der Kenntnisse über das **Kommunikationsmodell** von Firewall-Systemen und die verschiedenen **Firewall-Elemente**.

→ **Inhalt**

- Ziele und Ergebnisse der Vorlesung
- **Bedrohungen im Netz**
- Sicherheitskonzept
- Kommunikationsmodell
- Firewall-Elemente
- Firewall-Konzepte
- Zusammenfassung

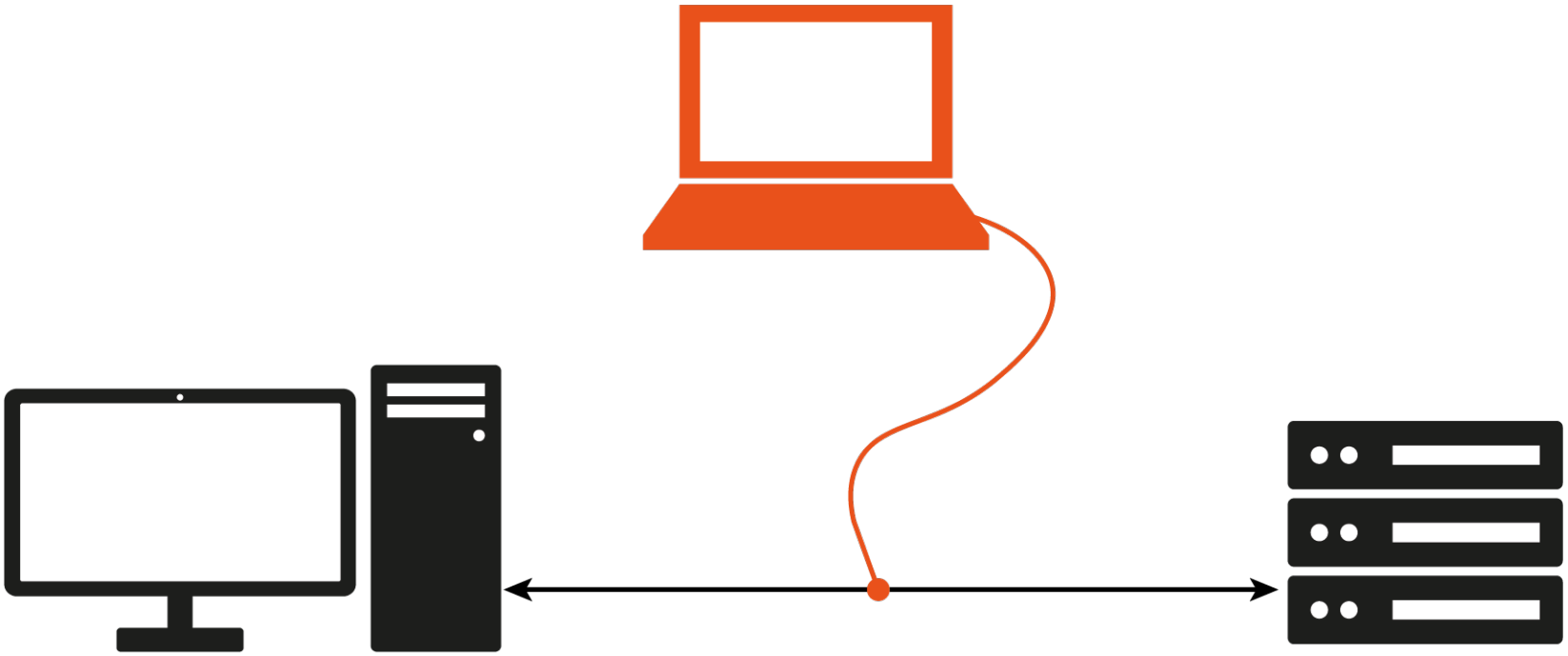
Bedrohungen im Netz

→ **Angriffsmöglichkeiten in Kommunikationssystemen**



Bedrohungen im Netz

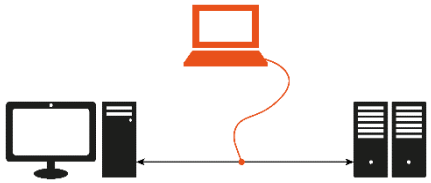
→ Passive Angriffe (1/4)



Bedrohungen im Netz

→ Passive Angriffe (2/4)

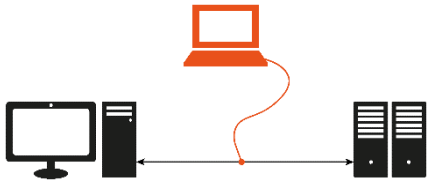
- **Abhören von Daten:**
  - Ein Abhörer gelangt unmittelbar in den Besitz der Nachricht und kann sie zu seinem Zweck verwerten.
  - Beispiele:
    - Bei einer unverschlüsselten IP-Verbindung zwischen einem Webserver und einem Client während der LogIn-Prozedur den Nutzernamen und das Passwort eines Nutzers abhören.
    - Das Abhören von vertraulichen Informationen, wie Entwicklungsunterlagen von neuen Produkten.
    - Das Abhören von Daten, die unter die EU-Datenschutzgrundverordnung fallen.
  - Diese Angriffe sind prinzipiell problemlos durchführbar.



Bedrohungen im Netz

→ Passive Angriffe (3/4)

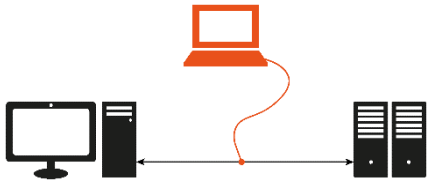
- **Abhören der Nutzer-Identitäten:**
  - Der Lauscher erfährt, welche Nutzer oder IT-Systeme untereinander eine Datenverbindung aufbauen und Daten austauschen.
  - Allein aus der Kenntnis, wer mit wem zu welchem Zeitpunkt Nachrichten ausgetauscht hat, sind oft Rückschlüsse auf den Inhalt der Nachricht oder das Verhalten der Nutzer möglich.
  - Wenn jemand z.B. auf die WWW-Seiten eines Waschmaschinenherstellers zugreift, kann vermutet werden, dass er eine Waschmaschine kaufen wird.



Bedrohungen im Netz

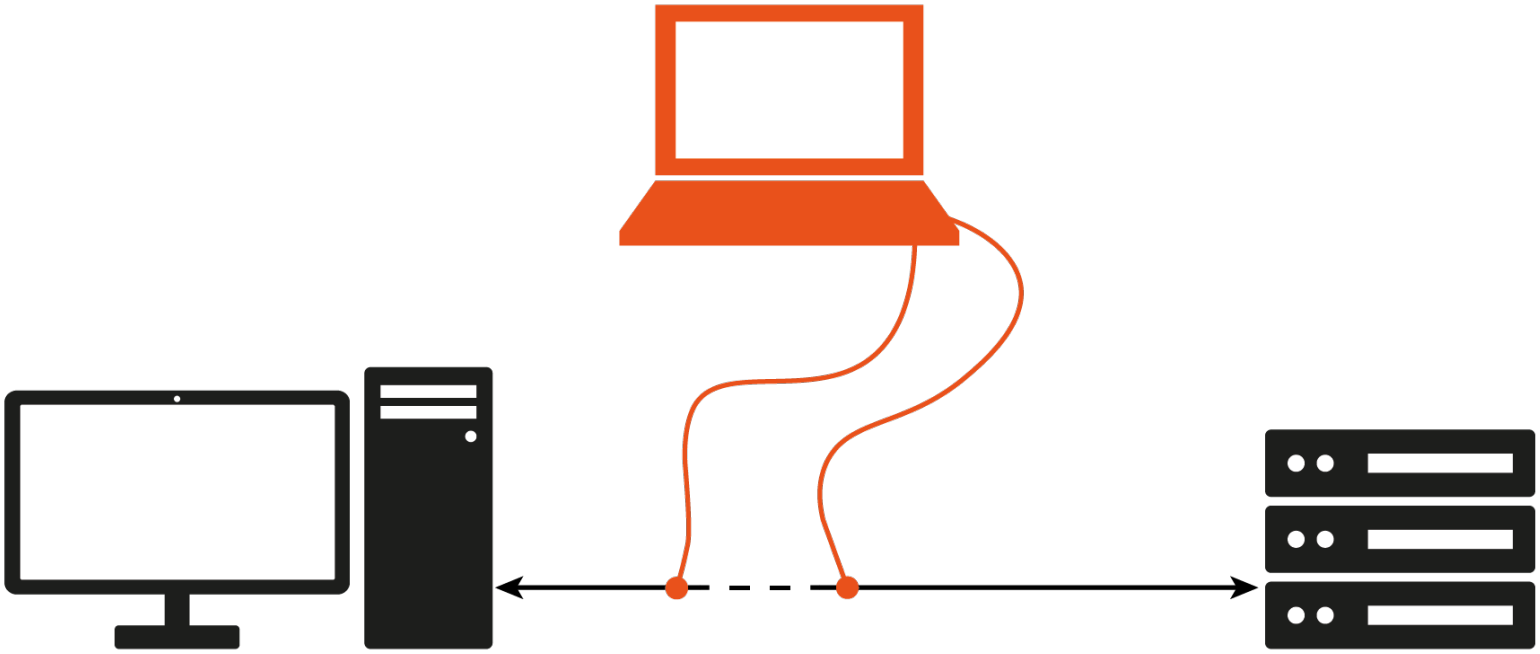
→ Passive Angriffe (4/4)

- **Verkehrsflussanalyse:**
  - Auch wenn die Daten verschlüsselt sind, ist es einem Abhörer möglich, durch eine „Verkehrsflussanalyse“ gewisse Informationen zu erhalten, wie z.B. Größenordnungen, Zeitpunkte, Häufigkeit und Richtung des Datentransfers.
  - Diese Informationen können für bestimmte spezielle Anwendungen interessant sein, z.B. für Börsen-Transaktionen oder militärische Operationen.



Bedrohungen im Netz

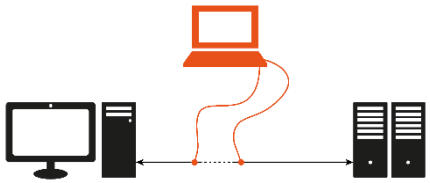
→ Aktive Angriffe (1/7)



Bedrohungen im Netz

→ Aktive Angriffe (2/7)

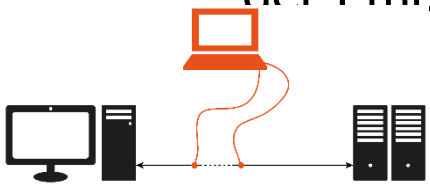
- **Wiederholen oder Verzögern von Informationen:**
  - Durch Wiederholen oder Verzögern von Informationen kann der Empfänger irritiert oder zu einer falschen Aktion veranlasst werden.
  - Beispiel:
    - Mehrfache Überweisung eines Geldbetrages.
    - Wiederholung eines abgefangenen LogIns.



Bedrohungen im Netz

→ Aktive Angriffe (3/7)

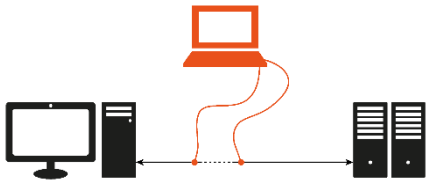
- **Einfügen und Löschen bestimmter Daten:**
  - Um ein IT-System zu manipulieren, fügt ein Angreifer bestimmte Nachrichten oder Daten innerhalb der Nachrichten ein oder löscht sie.
  - Ein Empfänger kann durch Unterdrückung oder zusätzlichen Empfang entscheidender Informationen zu einem falschen Verhalten veranlasst werden.
  - Beispiel: In der E-Mail
    - „Kaufen Sie keinesfalls neue Aktien" wird das Wort „keinesfalls" während der Übertragung gelöscht, sodass der Empfänger die Instruktion „Kaufen Sie neue Aktien"



Bedrohungen im Netz

→ Aktive Angriffe (4/7)

- **Modifikation von Daten:**
  - Modifikation von Daten bedeutet, dass die Veränderung der Daten von den Kommunikationspartnern nicht erkannt wird.
  - Durch Ändern der Daten während der Datenübertragung ist es dem Angreifer möglich, falsche Aktionen zu veranlassen.
  - Beispiel: Die Veränderung einer Kontonummer bei einer Geldüberweisung führt dazu, dass ein anderer als der intendierte Empfänger das Geld bekommt.

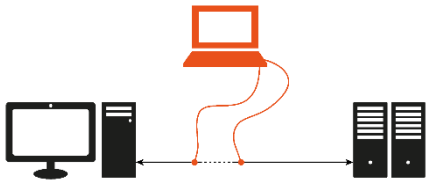


Bedrohungen im Netz

→ Aktive Angriffe (5/7)

- **Boykott des Kommunikationssystems (Denial of Service):**
  - Wenn der Umfang von eingefügten oder unterdrückten Daten zu groß wird oder realzeitorientierte Daten zu lange verzögert werden, kann hierdurch das gesamte Kommunikationssystem boykottiert werden.
  - Beispiel: Durch permanenten Verbindungsaufbau zu einem bestimmten Server kann dieser blockiert und isoliert werden.

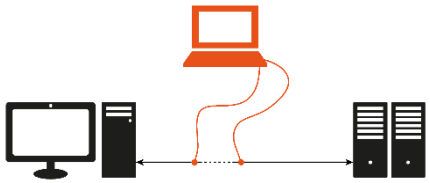
- **Vortäuschung einer falschen Identität (Maskerade-Angriff):**
  - Wenn sich ein Nutzer für einen anderen ausgibt, kann er sich Informationen erschleichen, die für diesen anderen Nutzer bestimmt waren, oder Aktionen auslösen, die nur der andere Nutzer veranlassen darf.
  - Beispiel: Ein Nutzer verschafft sich unerlaubt Zugang zu einer Datenbank.



Bedrohungen im Netz

→ Aktive Angriffe (6/7)

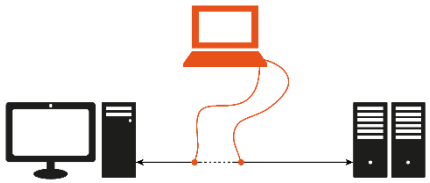
- **Leugnen einer Kommunikationsbeziehung:**
  - Der steigende Einsatz von Datenkommunikation zur Abwicklung vertraglich relevanter Vorgänge erfordert, dass sowohl der Sender einer Nachricht nicht leugnen kann, der Sender zu sein, als auch der Empfänger nicht abstreiten kann, die Nachricht erhalten zu haben.
  - Beispiele: Bestellung von Waren über das Internet bei einem Händler oder Abschluss von Verträgen über das Internet.



Bedrohungen im Netz

→ Aktive Angriffe (7/7)

- **Trittbrettfahrer (Man in the middle):**
  - So genannte Trittbrettfahrer hängen sich z.B. an einen Knoten (Router oder IT-System) im Internet und verfolgen einen Verbindungsaufbau mit.
  - Die Verbindung wird dann nach der Authentifikation des Nutzers für eigene Zwecke genutzt.
  - Mit dieser Methode können IT-Systeme, auf die eigentlich kein Zugriff möglich ist, manipuliert und Authentifikationsprozesse (auch kryptographische Methoden) unterlaufen werden.



Firewall-Systeme

→ **Inhalt**

- Ziele und Ergebnisse der Vorlesung
- Bedrohungen im Netz
- **Sicherheitskonzept**
- Kommunikationsmodell
- Firewall-Elemente
- Firewall-Konzepte
- Zusammenfassung

Sicherheitskonzept

→ Elektronische Brandschutzmauer

- Ein Firewall-System ist dafür zuständig, einen bestimmten IT-Bereich meist in der eigenen Organisation abzuschotten, damit Schäden, die außerhalb von diesem IT-Bereich auftreten, nicht auf die andere Seite übergreifen.

- Auf Kommunikationsnetze bezogen bedeutet dies, dass das Firewall-System das zu schützende Netz gegen Gefahren aus dem unsicheren Netz abschottet.

- Es wird nur ein einziger besonders sicherer Übergang zwischen den beiden Teilnetzen realisiert.

Sicherheitskonzept

→ Elektronischer Pförtner (1/3)

- Ein Firewall-System ist das elektronische Äquivalent zu einem Pförtner.

- Der Pförtner prüft:
  - Welche Besucher in ein Gebäude hinein dürfen – zum Beispiel solche, die zu Fuß kommen und eventuell noch eine Aktentasche mitbringen.
  - Aber nicht solche, die mit dem LKW, Auto oder Fahrrad ins Gebäude der Organisation hineinfahren wollen.
  - Welche Gegenstände in das Gebäude mit hinein- und hinausgenommen werden.
  - Wer in diesem Gebäude wen und wann besucht hat.

Sicherheitskonzept

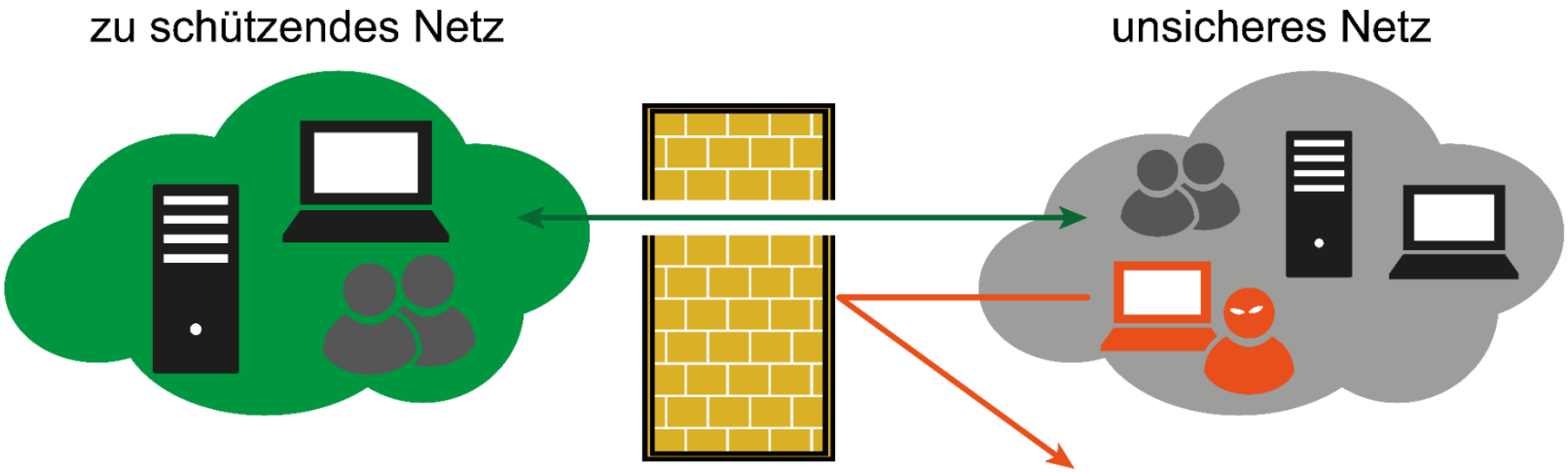
→ Elektronischer Pförtner (2/3)

- Das Firewall-System überprüft:
  - Wer aus dem unsicheren Netz auf das zu schützende Netz der Organisation zugreifen darf.
  - Welche Protokolle und Dienste zugegriffen werden.
  - Mit welchen IT-Systemen kommuniziert werden darf.

- Zusätzlich werden alle Ereignisse, die über das Firewall-System umgesetzt werden, protokolliert.

Sicherheitskonzept

→ Elektronischer Pförtner (3/3)



Sicherheitskonzept

→ Aufgaben von Firewall-Systemen (1/5)

- **Zugangskontrolle auf der Netzwerkebene**
  - Es wird überprüft, welche IT-Systeme über das Firewall-System miteinander kommunizieren dürfen.
- **Zugangskontrolle auf Nutzerebene**
  - Das Firewall-System überprüft, welche Nutzer und IT-Systeme über das Firewall-System eine Kommunikation aufbauen dürfen.
  - Dazu wird die Echtheit (Authentizität) des Nutzers und IT-Systeme festgestellt.
- **Zugangskontrolle auf Datenebene**
  - Das Firewall-System überprüft, welche Daten eines definierten Nutzers und IT-Systems über das Firewall-System übertragen werden dürfen.

Sicherheitskonzept

→ Aufgaben von Firewall-Systemen (2/5)

- **Rechteverwaltung**
  - Im Rahmen der Rechteverwaltung wird festgelegt, mit welchen Protokollen und Diensten und zu welchen Zeiten über das Firewall-System eine Kommunikation stattfinden darf.

- **Kontrolle auf der Anwendungsebene**
  - Es wird überprüft, ob Kommandos genutzt oder Dateiinhalte übertragen werden, die nicht zur Anwendung der definierten Aufgabenstellung gehören, generell unerwünscht sind (wie Spam) oder Schaden auf einem IT-System verursachen könnten (wie Malware).

- **Entkopplung von Diensten**
  - Dienste werden entkoppelt, damit Implementierungsfehler, Schwachstellen und Konzeptionsfehler der Dienste nicht die Möglichkeit für Angriffe bieten.

Sicherheitskonzept

→ Aufgaben von Firewall-Systemen (3/5)

- **Beweissicherung und Protokollauswertung**
  - Verbindungsdaten und sicherheitsrelevante Ereignisse werden protokolliert und können für die Beweissicherung von Handlungen der Nutzer und für die Erkennung von Sicherheitsverletzungen ausgewertet werden.

- **Alarmierung**
  - Besonders sicherheitsrelevante Ereignisse werden an ein Security Management gesendet, damit bei Sicherheitsverletzungen schnell reagiert werden kann.

Sicherheitskonzept

→ Aufgaben von Firewall-Systemen (4/5)

- **Verbergen der internen Netzstruktur**
  - Ziel ist es, die Struktur des zu schützenden Netzes gegenüber dem unsicheren Netz zu verbergen.
  - Es soll aus dem unsicheren Netz möglichst nicht sichtbar sein, ob im zu schützenden Netz 10, 100, 1.000 oder 10.000 IT-Systeme vorhanden sind oder wie dieses strukturiert sind.

- **Vertraulichkeit der Nachrichten, wenn zusätzlich eine VPN-Funktion genutzt wird**
  - Nachrichten können nicht im Klartext gelesen werden.
  - Dadurch ist die Vertraulichkeit der Daten bei einer Übertragung über unsichere Netze gewährleistet.

→ Aufgaben von Firewall-Systemen (5/5)

- Weitere, mögliche Ziele eines Firewall-Systems:
  - Das Firewall-System selbst muss gegen Angriffe resistent sein.
  - Accounting (IP- und Nutzerorientiert)
  - Network Address Translation
  - Intrusion Detection
  - Network/Traffic Monitoring
  - SMTP White- oder Blacklisting

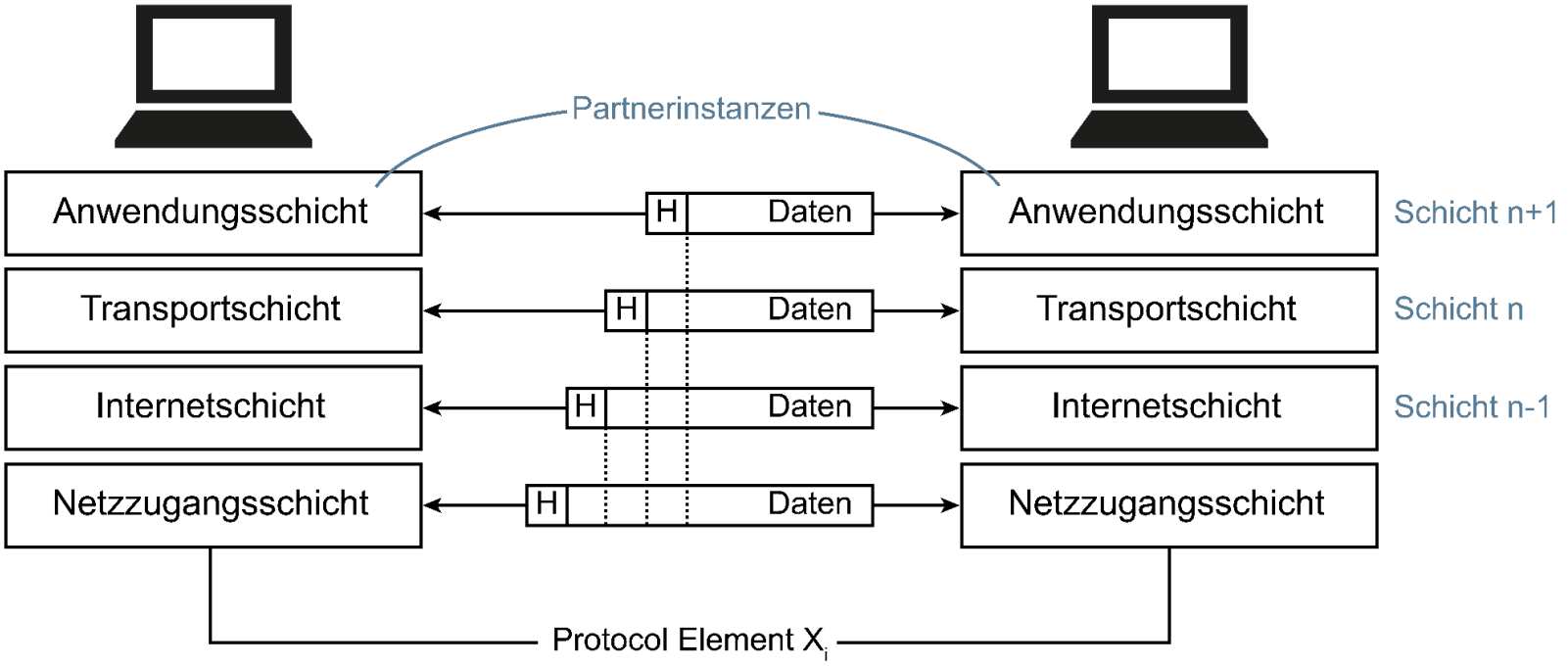
Firewall-Systeme

→ **Inhalt**

- Ziele und Ergebnisse der Vorlesung
- Bedrohungen im Netz
- Sicherheitskonzept
- **Kommunikationsmodell**
- Firewall-Elemente
- Firewall-Konzepte
- Zusammenfassung

Kommunikationsmodell

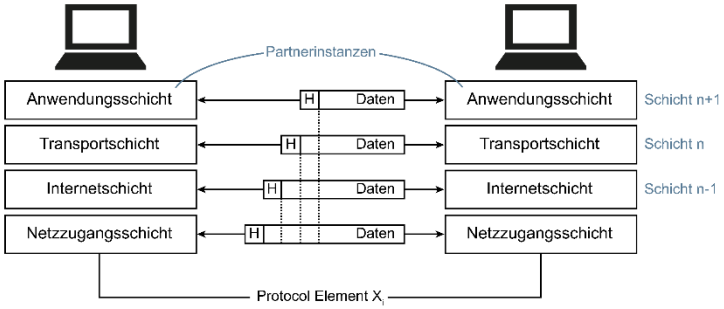
→ TCP/IP-Protokollarchitektur (1/3)



Kommunikationsmodell

→ TCP/IP-Protokollarchitektur (2/3)

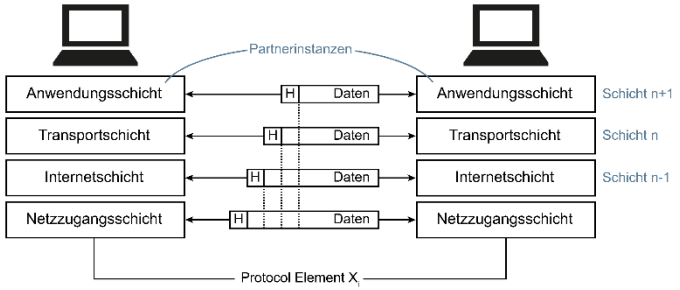
- In einer Schicht N **kommunizieren Partnerinstanzen** miteinander.
- Zwischen den Partnerinstanzen werden **Protokollelemente (x_i)** ausgetauscht.
- Protokollelemente bestehen aus **Headern** (H) und/oder **Daten** (Daten).
- **Header** (H) enthalten **Steuerinformationen** wie Adressen, laufende Nummern, Zähler, Informationen über den Übertragungsweg, Hinweise auf die Verwendung der Daten.
- Die Header-Informationen (H) können feste Größen, aber auch Variablen sein.
- Jede Schicht hat eigene Header (H), die auch leer sein können.



Kommunikationsmodell

→ TCP/IP-Protokollarchitektur (3/3)

- Die Daten werden von der übergeordneten Schicht zur nächst tieferen Schicht weitergereicht.
- Jede Kommunikationsschicht fügt den Daten eigene Kontrollinformationen hinzu, bis sie über das Netz gesendet werden.
- Der Empfänger reicht diese Daten dann Schicht für Schicht nach oben weiter, wobei jede Schicht nur die für sie relevanten Daten auswertet und diese aus dem Datenpaket entfernt.
- In welcher Reihenfolge und zu welchem Zwecke die Protokollelemente ausgetauscht werden, wird im Kommunikationsprotokoll festgelegt.
- Die Implementierung des Kommunikationsprotokolls auf den IT-Systemen und Netzwerkelementen (z.B. Router) ist Sache des Herstellers und nicht festgelegt.



Kommunikationsmodell

→ Schichten (1/3)

- **Netzzugangsschicht:**
  - Die Netzzugangsschicht ermöglicht es einem IT-System, Daten zu einem anderen IT-System über ein Medium (Kupfer- u. Glasfaser-Leitung, Luft, …) zu übertragen.
  - Protokolle auf der Netzzugangsschicht sind z.B. FDDI, Ethernet, WLAN.
  - Die Netzzugangsschicht umfasst die zwei unteren Schichten des OSI-Modells und beinhaltet die Kapselung von IP-Paketen in Netzrahmen (Frames und die Zuordnung von IP-Adressen zu physikalischen Netzadressen, z.B. MAC-Adressen) aber auch Zugriffssteuerung auf das Medium, die Fehlererkennung / Behandlung auf der Netzzugangsschicht.

Kommunikationsmodell

→ Schichten (2/3)

- **Netzwerkschicht:**
  - Die Netzwerkschicht definiert den Aufbau von IP-Paketen und bestimmt, auf welchem Weg die Daten durch das Internet übertragen werden (Routing).

- **Transportschicht:**
  - Die Transportschicht stellt eine Verbindung zwischen zwei Endpunkten oder IT-Systemen über das Netzwerk her.
  - Die wichtigsten Protokolle sind TCP und UDP.

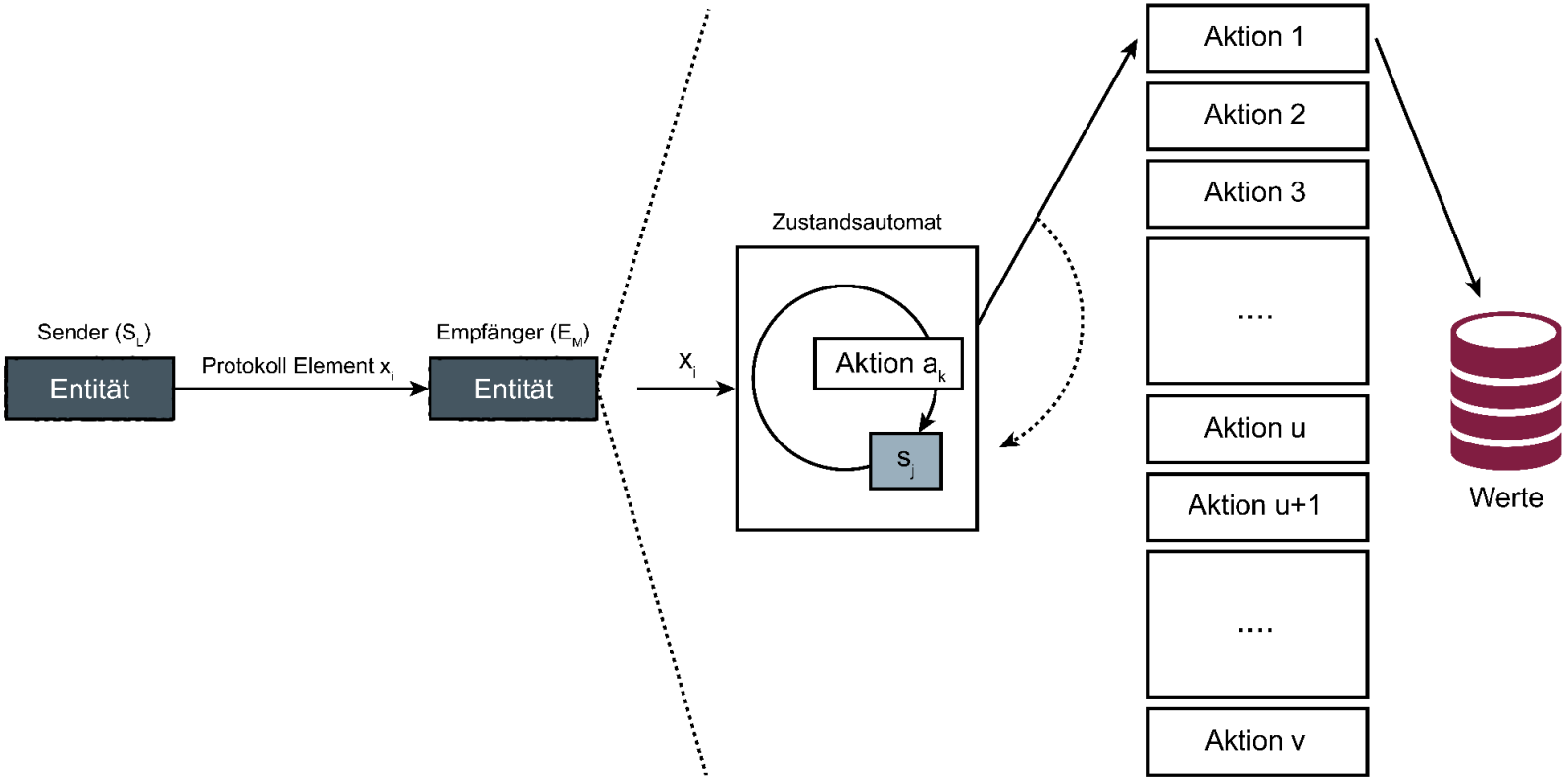
Kommunikationsmodell

→ Schichten (3/3)

- **Anwendungsschicht:**
  - Die Anwendungsschicht beinhaltet sämtliche Programme und Dienste, die über die Netzwerkverbindung durchgeführt werden sollen.
  - Dazu gehören vor allem Anwendungsprotokolle wie HTTP (World Wide Web, SMTP (E-Mail-Funktionen), FTP (File Transfer Protocol), usw.

Kommunikationsmodell

→ **Vereinfachtes logisches Kommunikationsmodell mit Aktionen**



Kommunikationsmodell

→ Definition der Transmitter (1/2)

- Es gibt eine endliche Menge von Transmittern, die wie folgt definiert werden:

$$\text{Transmitter (T)} = \{t_1, \ldots, t_l\}$$

- Erlaubte Transmitter sind solche Transmitter, die Aktionen beim Receiver veranlassen dürfen.
  - Erlaubte Transmitter stellen ein kalkulierbares Risiko bezüglich der Verwundbarkeit der Werte da.

$$\text{Erlaubte Transmitter } \{t_1, \ldots, t_g\}:$$

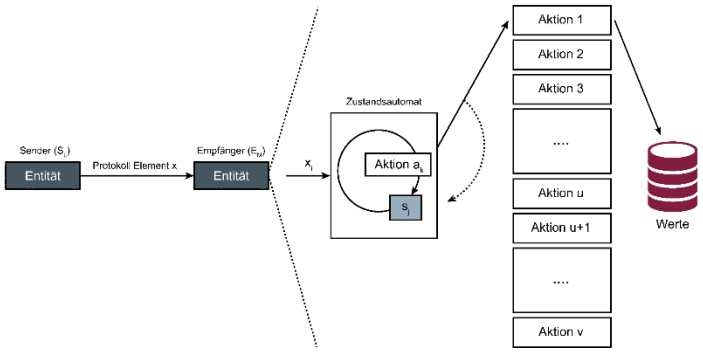
Kommunikationsmodell

→ Definition der Transmitter (2/2)

- Nicht erlaubte Transmitter sind solche Transmitter, die keine Aktionen beim Receiver veranlassen dürfen.
  - Nicht erlaubte Transmitter (Angreifer, Fremde, Unbefugte, …) stellen ein sehr hohes Risiko bezüglich der Verwundbarkeit der Werte da.

Nicht erlaubte Transmitter $\{t_{g+1}, \ldots t_l\}$:

- Welche Transmitter erlaubt sind und welche nicht, wird durch die Sicherheitspolitik festgelegt.



Kommunikationsmodell

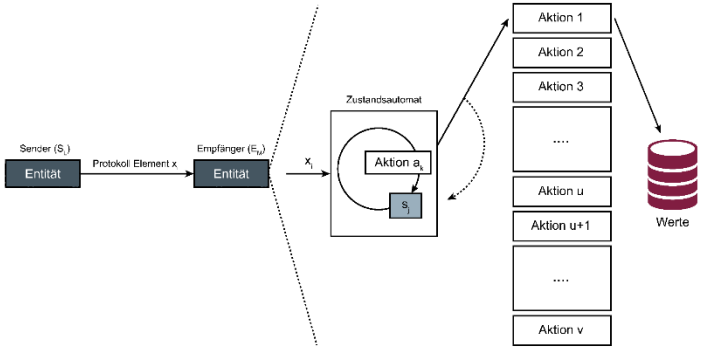
→ Definition der Receiver (1/2)

- Es gibt eine endliche Menge von Receivern, die wie folgt definiert werden.

$$\text{Receiver (R)} = \{r_1, \ldots, r_m\}$$

- Erlaubte Receiver sind solche Receiver, bei denen erlaubte Transmitter erlaubte Aktionen veranlassen dürfen.
  - Erlaubte Receiver stellen ein kalkulierbares Risiko bezüglich der Verwundbarkeit der Werte dar.

$$\text{Erlaubte Receiver } \{r_1, \ldots, r_h\}$$

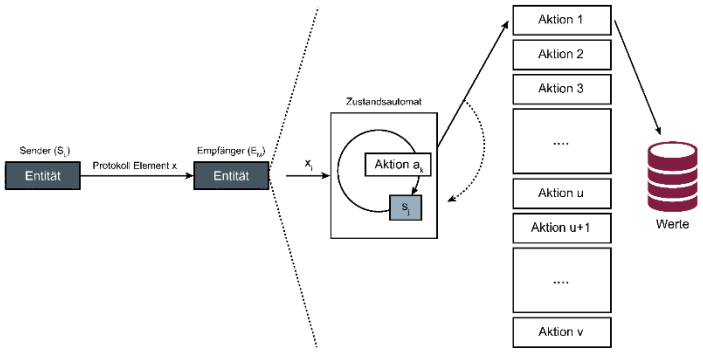


Kommunikationsmodell

→ Definition der Receiver (2/2)

- Bei nicht erlaubten Receivern (Unbefugte) dürfen keine Aktionen veranlasst werden.
  - Welche Receiver erlaubt sind und welche nicht, wird durch die Sicherheitspolitik festgelegt.

Nicht erlaubte Receiver $\{r_{h+1}, \ldots r_m\}$



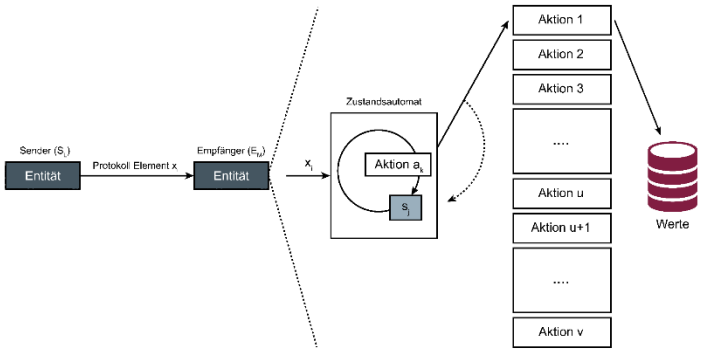
Kommunikationsmodell

→ Definition der Protokollelemente (1/5)

- Die Protokollelemente, die zwischen Sender und Empfänger ausgetauscht werden, können wie folgt klassifiziert:

Summe aller Protokollelemente: $\Sigma = 2^n$

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



Kommunikationsmodell

→ Definition der Protokollelemente (2/5)

$\{x_1, \ldots x_u\}$	Menge der Protokollelemente, die in der Norm definiert sind (ISO, RFC, ...).		
genormt	$\{x_1, \ldots x_t\}$ genormt und erlaubt	Menge der Protokollelemente aus der Norm, die für eine spezielle Aufgabe notwendig und damit erlaubt sind z.B. die Kommandos „cdir“ (Change Directory) und „put“ (Transmit), um mithilfe vom FTP eine Datei vom Sender zu versenden und auf der Empfängerseite zu speichern	erlaubt
	$\{x_{t+1}, \ldots x_u\}$ genormt und nicht erlaubt	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)	nicht erlaubt

$t <= u$

$u <= n$ (ist $u = n$, dann $v = n$, dann gibt es keine undefinierten Protokollelemente)

$v <= n$ (ist $v = n$, dann gibt es keine undefinierten Protokollelemente)

Kommunikationsmodell

→ Definition der Protokollelemente (3/5)

<table>
<tr><td rowspan="4">{x_{u+1}, … x_n }

nicht
genormt</td><td colspan="2">Menge der Protokollelemente, die nicht in der Norm definiert sind, und für die eigentliche Aufgabe nicht notwendig und damit in der Regel nicht erlaubt sind.</td><td></td></tr>
<tr><td>{x_{u+1}, … x_v }

Hersteller-
definiert</td><td>Menge der Protokollelemente, die nicht in der Norm definiert sind, aber zusätzliche Dienste anbieten. Hersteller haben bei ihrer Implementierung der Kommunikationsprotokolle oder -dienste weitere, eigene Protokollelemente definiert, um z.B. folgende Aufgaben durchführen zu können:
Fehleranalyse (Zustand des Protokoll-Automats, Zustand des Betriebssystems, ...). Diese zusätzlichen Dienste werden von den Herstellern angeboten, um aus der Ferne eine Fehleranalyse oder sonstige Servicearbeiten durchführen zu können.
Trap-Doors, mit denen Angriffe realisiert werden und nicht definierte oder erlaubte Aktionen auf der Empfängerseite unautorisiert durchgeführt werden können. Diese Protokollelemente sind in der Regel nicht erlaubt.</td><td>nicht
erlaubt</td></tr>
<tr><td>{x_{v+1}, … x_n }

nicht
definiert</td><td>Menge der Protokollelemente, die nicht in der Norm und nicht vom Hersteller definiert und damit nicht erlaubt ist. Im Normalfall werden solche Protokollelemente von der Implementierung als Fehler erkannt und entsprechend behandelt. Es werden aber immer wieder Implementierungen bekannt, die beim Empfang von nicht definierten Protokoll-elementen eine fehlerhafte Aktion durchführen, die für einen Angriff verwendet werden kann.</td><td>nicht
erlaubt</td></tr>
<tr><td colspan="3">t <= u
u <= n (ist u = n, dann v = n, dann gibt es keine undefinierten Protokollelemente)
v <= n (ist v = n, dann gibt es keine undefinierten Protokollelemente)</td></tr>
</table>

Kommunikationsmodell

→ Definition der Protokollelemente (4/5)

- Welche Protokollelemente erlaubt sind und welche nicht, wird durch die Sicherheitspolitik festgelegt.

- Bei der Betrachtung der Sicherheit von Protokollelementen $\{x_1, ..., x_n\}$ müssen weitere Aspekte berücksichtigt werden:
  - Nicht alle Felder in den Protokollelementen sind sicherheitsrelevant in Bezug auf die Möglichkeiten eines Firewall-Systems (z.B. Laufzähler, Zufallszahlen, ...).
  - Aus diesem Grund reduziert sich die praktische Anzahl der Protokollelemente, die betrachtet werden müssen, sehr stark.
  - Bestimmte Protokollelemente sind in Abhängigkeit vom Zustand des Kommunikationsprotokolls erlaubt oder nicht erlaubt.
  - Aus diesem Grund muss die obige Tabelle immer in Abhängigkeit vom Zustand des Kommunikationsprotokolls betrachtet werden.

Kommunikationsmodell

→ Definition der Protokollelemente (5/5)

- Die Möglichkeit, über verdeckte Kanäle Informationen zu übertragen, wird in diesem Modell nicht betrachtet.
- Erlaubte Protokollelemente $\{x_1, ..., x_t\}$ dürfen nur zwischen erlaubten Transmittern $\{t_1, ... t_g\}$ und Receivern $\{r_1, ..., r_h\}$ zu erlaubten Zeiten ausgetauscht werden.

Kommunikationsmodell

→ Definition der Aktionen (1/2)

- Die Aktionen auf der Empfängerseite sind wie folgt definiert:

$$\text{Aktion (A)} = \{a_1, \ldots, a_f\}$$

- Eine Aktion, die aus einer definierten Anzahl von Teilaktionen besteht, ist z.B. das Schreiben einer Datei auf die Festplatte des Empfängers mithilfe von FTP. Teilaktionen sind z.B. das Selektieren der Subdirectory, das Empfangen von Teildatenmengen, das Abspeichern der Daten, usw. Aufteilung der Aktionen.

- Erlaubte Aktionen sind solche Aktionen, die für die erlaubten Anwendungen, bzw. Aufgabenstellung notwendig sind.
  - Erlaubte Anwendungen auf definierten „Assets" stellen ein kalkulierbares Risiko bezüglich der Verwundbarkeit der Werte da.
  - In den Bereich der erlaubten Aktionen fallen auch die Fehlerbehandlungen bzgl. der nicht definierten Zustände und Ereignisse.

$$\text{Erlaubte Aktionen } \{a_1, \ldots, a_t\}$$

Kommunikationsmodell

→ Definition der Aktionen (2/2)

- Nicht erlaubte Aktionen sind solche Aktionen, die zwar die Implementierung eines Kommunikationsprotokolls oder -dienstes auf der Empfängerseite ermöglichen, aber für die eigentliche Aufgabenstellung nicht notwendig und deshalb nicht erlaubt sind, damit das Risiko eines beabsichtigten oder auch unbeabsichtigten Schadens minimiert wird.
  - Welche Aktionen erlaubt sind und welche nicht, wird durch die Sicherheitspolitik festgelegt.

Nicht erlaubte Aktionen $\{a_{t+1}, ..., a_f\}$

- Erlaubte Aktionen $\{a_{t+1}, ..., a_f\}$ dürfen nur durch erlaubte Protokollelemente $\{x_1, ..., x_t\}$ ausgelöst werden, die zwischen erlaubten Transmittern $\{t_1, ..., t_g\}$ und Receivern $\{r_1, ..., r_h\}$ zu erlaubten Zeiten ausgetauscht werden.

Kommunikationsmodell

→ Kommunikationsabläufe

- Der Transmitter sendet dem Receiver Protokollelemente (x_i) über das Netz.

- Der Receiver interpretiert die empfangenen Protokollelemente als externe Ereignisse und startet mit diesen und weiteren Informationen seine „protocol-state-machine".

  a_k = protocol-state-machine (x_i^*, s_j)

  a_k = Teil-Aktion in einer Schicht, die in Abhängigkeit vom empfangenen Protokollelement x_i und vom aktuellen Zustand s_j ausgeführt wird

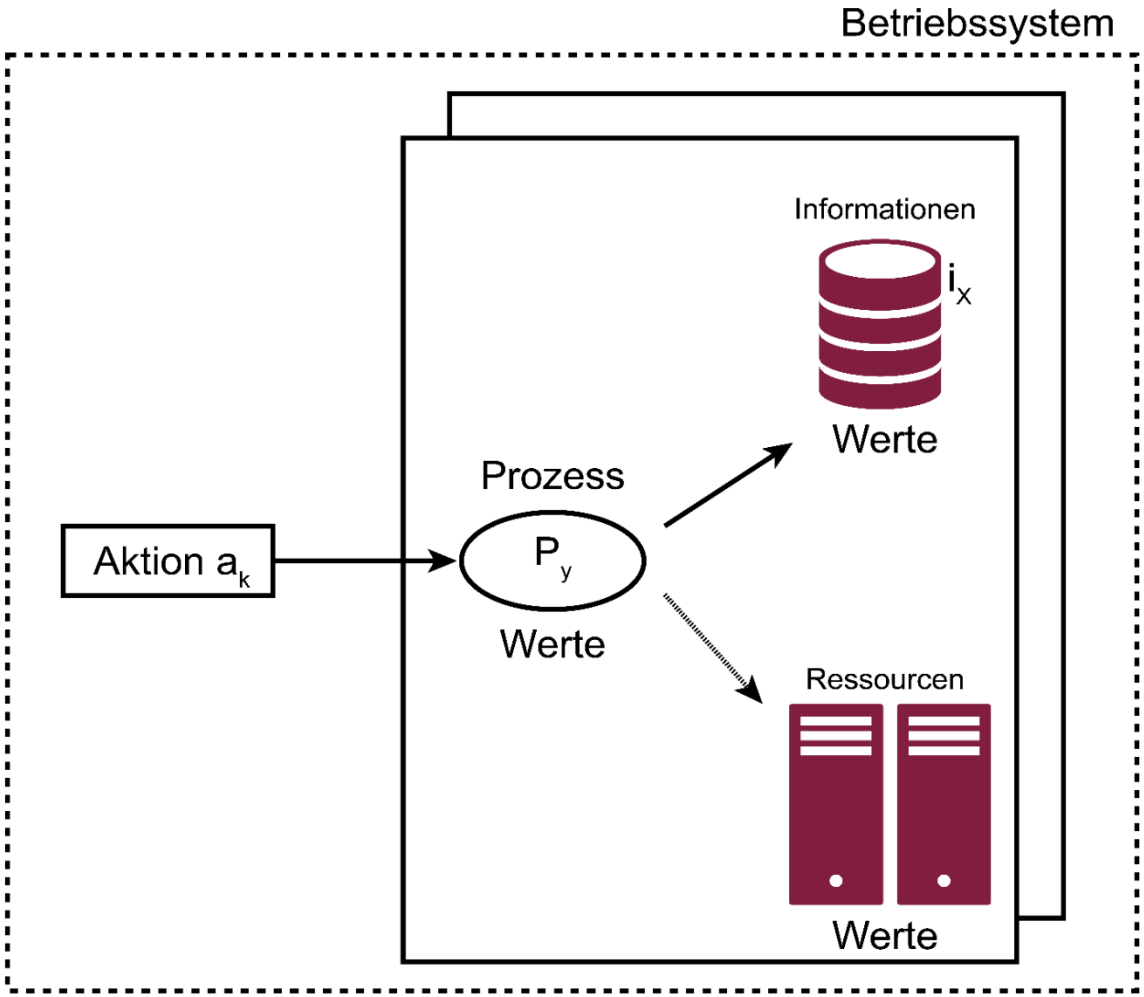
  x_i = Protokollelement

  s_j = aktueller Zustand

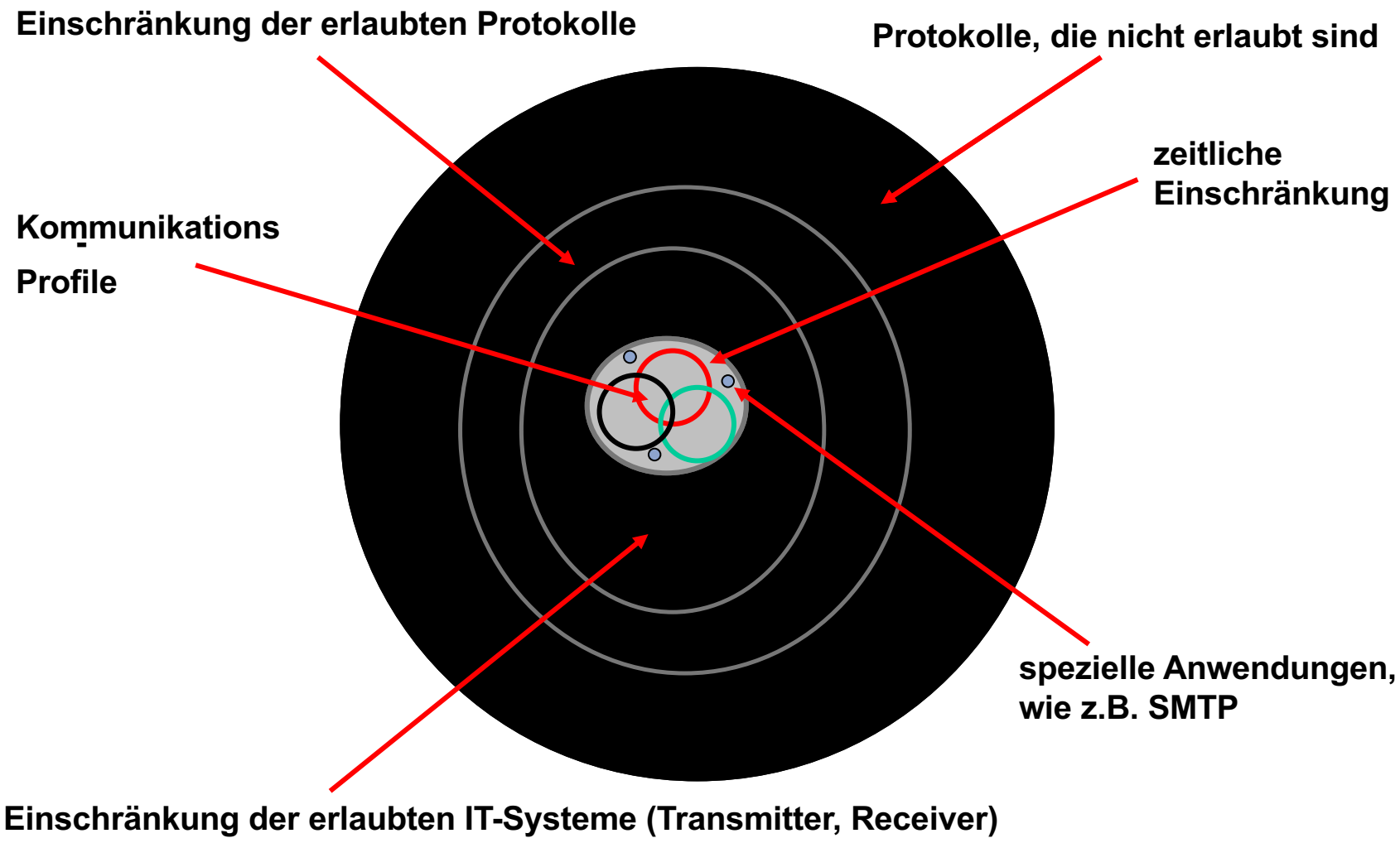
- Das Protokoll wird als State-Machine betrachtet, in der sich der Zustand s_j in Abhängigkeit von den empfangenen Protokollelementen und von weiteren Ereignissen (Timerabläufen, Statusmeldungen, ...) verändern kann.

Kommunikationsmodell

→ Ablauf der Aktionen beim Receiver



Kommunikationsmodell
→ Reduzierung des Schadensrisikos



Firewall-Systeme

→ **Inhalt**

- Ziele und Ergebnisse der Vorlesung
- Bedrohungen im Netz
- Sicherheitskonzept
- Kommunikationsmodell
- **Firewall-Elemente**
- Firewall-Konzepte
- Zusammenfassung

Firewall-Elemente

→ **Grundsätzliche Aspekte eines Firewall-Elementes (1/2)**

- Ein Firewall-Element ist ein separates Kommunikationssicherheitssystem.

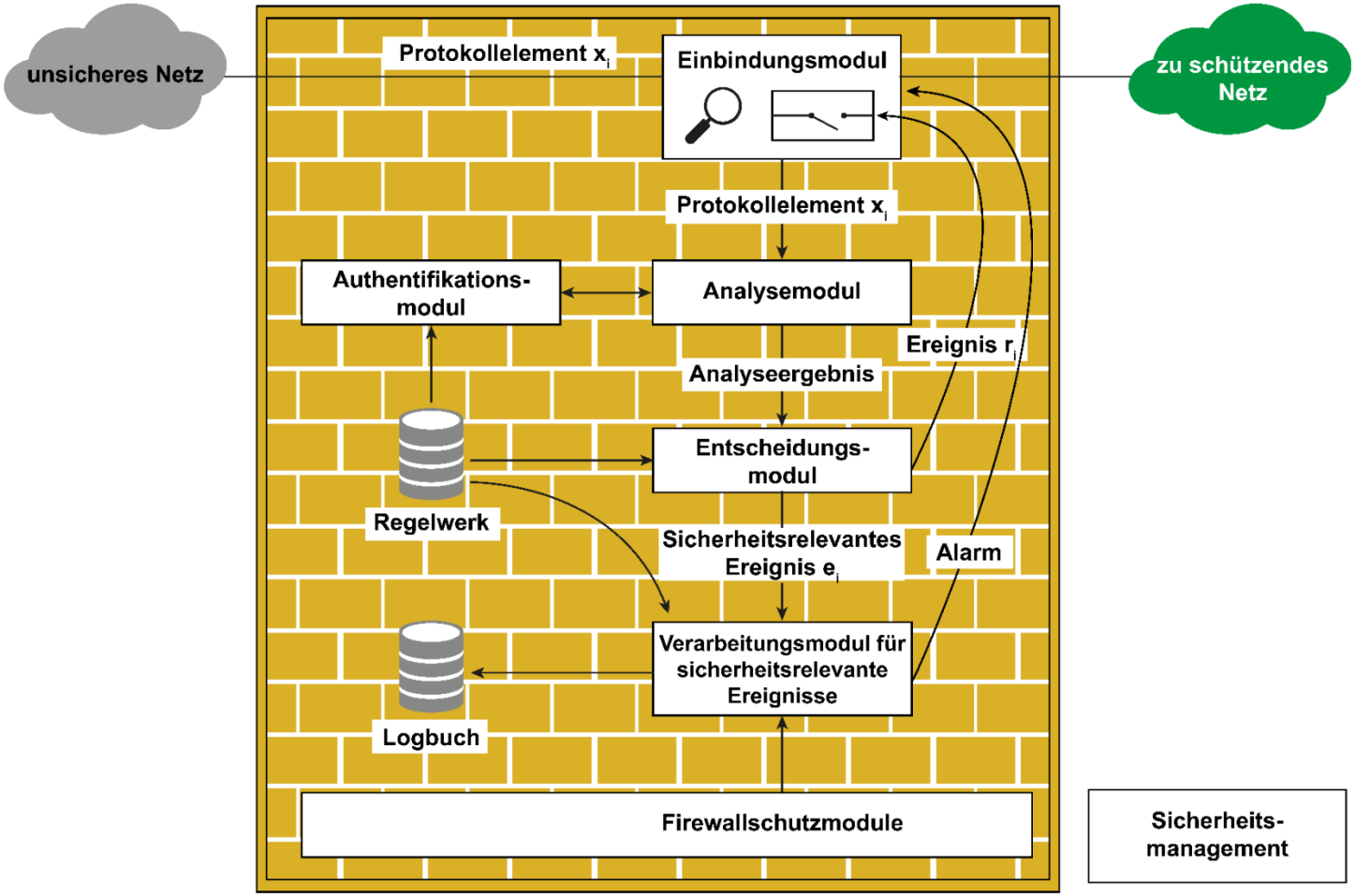
- Es besteht in der Regel keine direkte Verbindung mit den Sicherheitsfunktionen der Betriebssysteme und der IT-Systeme (Receiver, Transmitter).

- Ein Firewall-Element hat keinen Einfluss (Erweiterung, Veränderung) auf die verwendeten Kommunikationsprotokolle und -dienste.

- Ein Firewall-Element wird von der Organisation verwaltet, die es betreibt, und ist im Prinzip unabhängig von allen anderen Organisationen in dieser Verwaltung.

Firewall-Elemente

→ Grundsätzliche Aspekte eines Firewall-Elementes (2/2)



Firewall-Elemente

→ Einbindungs- und Durchsetzungsmodul

- **Funktion: enforcement (r_i)**

- 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.

- In Abhängigkeit des verwendeten Firewall-Elementes (Packet Filter, Stateful Inspection, Application Gateway mit Proxies, usw.) wird das Einbindungsmodul an unterschiedlichen Stellen der Protokollarchitektur eingebunden.

Firewall-Elemente

→ Analysemodul (1/2)

- **Funktion: analysis (x_i)**

- Im Analysemodul werden die Kommunikationsdaten des Protokollelementes (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 (z.B. Verbindungsaufbau, Transferzustand oder Verbindungsabbau) der Kommunikation festgehalten werden.

- Vor allem die Tiefe der Analyse, d.h., wie weit und umfangreich analysiert wird, ist sicherheitskritisch und stellt ein besonderes Qualitätsmerkmal eines aktiven Firewall-Elements dar.

Firewall-Elemente

→ Analysemodul (2/2)

- Die unterschiedlichen prinzipiellen aktiven Firewall-Elemente (Packet Filter und Application Gateway) analysieren auf unterschiedlichen Kommunikationsebenen.

Firewall-Elemente

→ Entscheidungsmodul

- **Funktion: result-of-decision (analysis (), security-management ())**

- 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.

Firewall-Elemente

→ Regelwerk

- **Funktion: security-management (rules):**

- Das Regelwerk ist die technische Umsetzung der Sicherheitspolitik und wird mit Hilfe eines Security Management erstellt.

- Im Regelwerk stehen alle Informationen (rules: Schlüssel, Access-Listen, Attribute usw.) über Nutzer, Authentifikationsverfahren, Kommunikationsverbindungen etc., die notwendig sind, um eine Entscheidung für oder gegen eine Übertragung des Protokollelementes (x_i) über das aktive Firewall-Element fällen zu können, und wie mit sicherheitsrelevanten Ereignissen (e_i) verfahren werden soll.

Firewall-Elemente

→ **Verarbeitungsmodul für sicherheitsrelevante Ereignisse**

- **Funktion: event (e_i)**

- In diesem Verarbeitungsmodul werden alle sicherheitsrelevanten Ereignisse (e_i) verarbeitet, die im aktiven Firewall-Element erzeugt werden.

- In Abhängigkeit des Regelwerks wird ein sicherheitsrelevantes Ereignis mit den dazugehörigen Protokolldaten je nach Einstellung in eine Log-Datei geschrieben oder über den Alarmmechanismus als spontane Meldung an ein Security-Management weitergeleitet.

Firewall-Elemente

→ Authentisierungsmodul

- **Funktion: authentication (t_i)**

- Das Authentisierungsmodul sorgt für die Identifikation und Authentisierung der Instanzen (Prozesse in den IT-Systemen, Nutzer etc.), die über das aktive Firewall-Element kommunizieren möchten.

- Hier können unterschiedliche Authentisierungsverfahren verwendet werden.

Firewall-Elemente

→ Firewall-Schutzmodul (1/2)

- **Funktion: safeguard ()**

- Das aktive Firewall-Element muss nicht nur Sicherheitsdienste erbringen, sondern auch selbst gegen Angriffe resistent sein.

- Im Firewall-Schutzmodul verbergen sich aktive Sicherheitsfunktionen, die für den sicheren Betrieb des aktiven Firewall-Elements selbst sorgen.

Dazu gehören z.B. die folgenden Sicherheitsmechanismen:

- **Integritätstest:**
  - Dieser Sicherheitsmechanismus gewährleistet, dass Veränderungen der Software (Betriebssystem, Firewall, Sicherheitsmechanismen etc.), des Regelwerks und des Logfiles erkannt werden.
  - Dies wird z.B. durch eine regelmäßige und/oder spontane Checksummenüberprüfung der Software und der Daten realisiert.

Firewall-Elemente

→ Firewall-Schutzmodul (2/2)

- **Authentisierungsmechanismus**:
  - Dieser Sicherheitsmechanismus sorgt dafür, dass nur vom (dazu berechtigten) Security Management das Regelwerk beeinflusst und die Protokolldaten aus dem Logfile ausgelesen werden können.

- **Betriebssicherungsmechanismen**:
  - Hier werden Sicherheitsmechanismen zusammengefasst, die für den sicheren Betrieb der aktiven Firewall-Elemente sorgen.
  - Zu diesen Sicherheitsmechanismen gehören z.B. die Überprüfung des Überlaufs von Logbüchern und Speichermedien (z.B. Festplatte) und die Überprüfung, ob sich die Software in einem definierten Zustand (Automatenzustand) befindet, usw.

Firewall-Elemente

→ Logfile

- **Funktion: logfile (e_i)**

- Im Logfile stehen alle Protokolldaten der sicherheitsrelevanten Ereignisse, die während des Betriebs eines aktiven Firewall-Elements aufgetreten sind und dem Regelwerk entsprechend registriert werden sollen.

Firewall-Elemente

→ Security Management

- **Funktion: security-management (rules)**

- Mithilfe des Security Managements können die Regeln für die aktiven Firewall-Elemente festgelegt und die Protokolldaten der sicherheitsrelevanten Ereignisse aus den Logbüchern analysiert werden.

Firewall-Elemente

→ Designkonzept aktiver Firewall-Elemente (1/4)

- **Minimale Software**
  - Zusätzlich zu den Sicherheitsdienstleistungen, die ein aktives Firewall-Element erbringen soll, muss das Firewall-Element selbst gegen Angriffe resistent sein.
  - Daher ist es besonders wichtig, nur fehlerfreie Software einzusetzen.
  - Das Firewall-Element muss klar strukturiert und nachvollziehbar aufgebaut und realisiert werden.
  - Da jedes Programm aber potenziell Sicherheitslücken enthalten kann, sollten nur die für die Erbringung der Firewall-Funktionalität unbedingt notwendigen Programme auf dem aktiven Firewall-Element eingesetzt werden (keine Routerfunktionalität, keine weiteren Anwendungen, ...).
  - Es ist auch möglich, mit Hilfe einer virtuellen Umgebung eine Separierung und starke Isolierung umzusetzen.

Firewall-Elemente

→ Designkonzept aktiver Firewall-Elemente (2/4)

- **Sichere Einbindung in das Kommunikationssystem (Netzwerk-Software, Betriebssystem usw.)**
  - Die Sicherheit eines aktiven Firewall-Elementes hängt in entscheidendem Maße davon ab, wie gut die Sicherheitsmechanismen in das Kommunikationssystem eingebunden werden.
  - Es muss sichergestellt werden, dass es nicht möglich ist, die Firewall-Sicherheitsfunktionen über das Betriebssystem oder über die verwendete Kommunikations-Software (TCP/IP-Software, Netzzugangs-Treiber, etc.) zu umgehen.
  - Beispiele: Bei Verwendung von IP-Forwarding (Kernel-Funktionalität) kann die Kommunikation am Firewall-Element vorbeigeleitet werden, ohne dass die Sicherheitsmechanismen wirken können.

Firewall-Elemente

→ Designkonzept aktiver Firewall-Elemente (3/4)

- **Getrenntes Security Management**
  - Die Forderung, auf den aktiven Firewall-Elementen nur minimale Software zu installieren, bedingt, dass das Security Management von den eigentlichen Sicherheitsfunktionen des aktiven Firewall-Elementes getrennt realisiert werden muss, damit ein Höchstmaß an Sicherheit auf dem aktiven Firewall-Element gewährleistet werden kann.
  - Die getrennte Realisierung des Security Management kann auf einem separaten IT-System realisiert werden.

Firewall-Elemente

→ Designkonzept aktiver Firewall-Elemente (4/4)

- **Einfache, zuverlässige und berechtigte Bedienung des Security Managements**
  - Für das Security Management ist eine einfache und zuverlässige Bedienung erforderlich, damit die Regeln ohne Fehler eingegeben werden können.
  - Außerdem ist eine Überprüfung der Widerspruchsfreiheit der Regeln erforderlich, damit nicht versehentlich sicherheitskritische Eingaben gemacht werden.
  - Ebenso muss sichergestellt werden, dass nur vom berechtigten Administrator mithilfe des Security Management auf die aktiven Firewall-Elemente zugegriffen werden kann, damit das Security Management nicht von Angreifern genutzt werden kann, um eine Kommunikation über das aktive Firewall-Element zuzulassen.

Firewall-Elemente

→ Packet Filter (1/6)

- Das aktive Firewall-Element Packet Filter analysiert und kontrolliert die ein- und ausgehenden Pakete auf der Netzzugangs-, der Netzwerk- und der Transportebene.
- Dazu werden die Pakete (z.B. Ethernet), die auf dem physikalischen Kabel übertragen werden, aufgenommen und analysiert.
- Durch den Packet Filter werden die Netze physikalisch entkoppelt.
- Ein Packet Filter verhält sich wie eine einfache Bridge.
- Packet Filter sind nicht nur auf TCP/IP-Protokolle beschränkt.

Firewall-Elemente

→ Packet Filter (2/6)

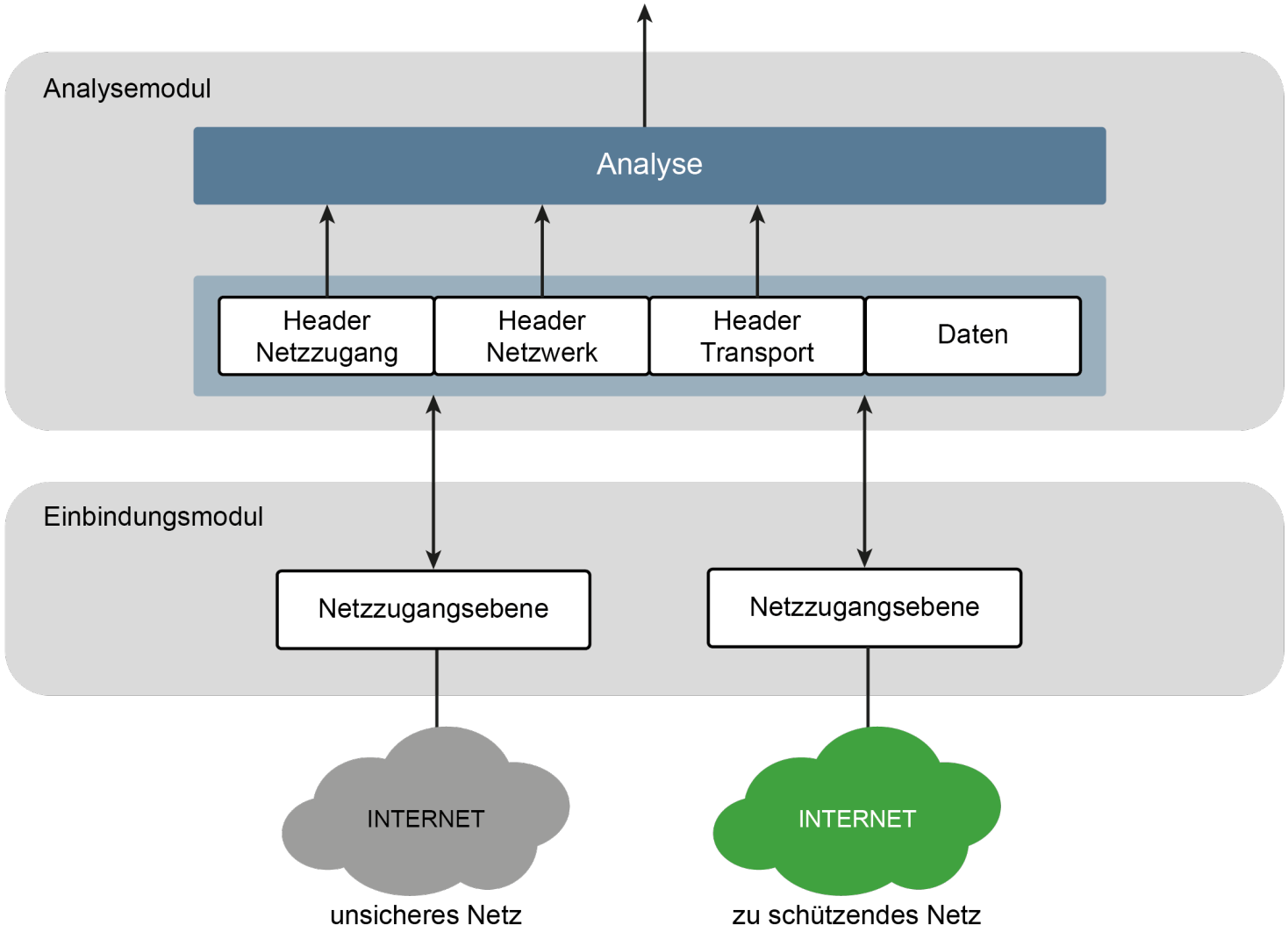
- Ein Packet Filter interpretiert den Inhalt der Pakete und verifiziert, ob die Daten in den entsprechenden Headers der Kommunikationsebenen den definierten Regeln entsprechen.

- Die Regeln werden so definiert, dass nur die notwendige Kommunikation erlaubt ist und bekannte sicherheitskritische Einstellungen vermieden werden, z.B. die IP-Fragmentierung.

- Die Packet Filter werden transparent in die Leitung eingefügt.

Firewall-Elemente

→ Packet Filter (3/6)



Firewall-Elemente

→ Packet Filter (4/6)

- Es wird überprüft, von welcher Seite das Paket empfangen wird (Information aus dem Einbindungsmodul).
- Auf der Netzzugangsebene werden die Quell- und Ziel-Adresse und der verwendete Protokolltyp kontrolliert.
- Auf Netzwerkebene wird je nach Protokoll überprüft:
  - IP-Protokoll: die Ziel- und die Quell-Adresse und das verwendete Schicht-4-Protokoll, aber auch das Optionsfeld und die Flags
  - Das Optionsfeld wird in der Regel nicht durchgelassen
  - Mit Hilfe der Flags kann eine Fragmentierung unterbunden werden
    - ICMP: die ICMP-Kommandos
    - IPX-Protokoll: Network/Node
    - OSI-Protokoll: die OSI-Netzwerkadresse

Firewall-Elemente

→ Packet Filter (5/6)

- Auf Transportebene findet
  - bei UDP/TCP eine Überprüfung der Portnummern (Quell- und Ziel-Port) statt (hierüber werden alle Dienste wie HTTP, FTP, Telnet, definiert);
  - bei TCP findet zusätzlich eine Überprüfung der Richtung des Verbindungsaufbaus mit Hilfe der Code Bits statt.

- Zusätzlich kann überprüft werden, ob der Zugriff über den Packet Filter in einem definierten Zeitraum durchgeführt wird (z.B. montags bis freitags von 7 Uhr bis 19 Uhr, samstags von 7 bis 13 Uhr, sonntags nicht).

Firewall-Elemente

→ Packet Filter (6/6)

- Die entsprechenden Prüfinformationen werden dem Regelwerk (Accessliste, Rechteliste) entnommen und mit den Analyse-Ergebnissen verglichen.

- Bei Verstoß gegen die Regeln wird dies als sicherheitsrelevantes Ereignis entsprechend protokolliert, und falls diese Option, eingerichtet ist wird eine spontane Meldung mit den Protokolldaten des sicherheitsrelevanten Ereignisses an das Security Management gesendet, damit schnell reagiert werden kann.

Firewall-Elemente

→ Anwendungsgebiete von Packet Filtern (1/3)

- Ein Firewall-System, das nur auf Packet Filtern aufbaut, wird sicherlich nicht für die Kopplung eines zu schützenden Netzes an das Internet eingesetzt werden können, da der Schutzbedarf der meisten zu schützenden Netze für die Kontrollmöglichkeiten eines Packet Filter zu hoch ist.

- Packet Filter werden zum Aufbau von High-level-Security-Firewall-Systemen und für die kontrollierte Kommunikation im Intranet verwendet.

- Für diese Anwendungen sind besonders Packet Filter, die gleichzeitig verschlüsseln, eine wirkungsvolle Sicherheitskomponente, mit der Internet- und Intranet-Anwendungen sicher und beherrschbar realisiert werden können.

Firewall-Elemente

→ **Anwendungsgebiete von Packet Filtern (2/3)**

- **Möglichkeiten, Vorteile und besondere Aspekte von Packet Filtern:**
  - transparent, d.h. unsichtbar für den Nutzer und die IT-Systeme und ohne ihre aktive Einwirkung tätig
  - einfach erweiterungsfähig für neue Protokolle
  - flexibel für neue Dienste
  - für andere Protokollfamilien verwendbar (IPX, OSI, DECNET, SNA, ...)
  - hohe Performance durch optimale Mechanismen (Betriebssystem, Treiber, usw.)
  - leicht realisierbar, da geringere Komplexität

Firewall-Elemente

→ Anwendungsgebiete von Packet Filtern (3/3)

- **Nachteile und Grenzen von Packet Filtern:**
  - Daten, die oberhalb der Transportebene liegen, werden in der Regel nicht analysiert. Daher kann erfolgreich ein Port-Hopping-Angriff umgesetzt werden.
  - Für die Anwendungen (HTTP, FTP, SMTP, ...) besteht keine Sicherheit, z.B. können bei der Freischaltung von SMTP (Port 25) Angriffe über Sendmail auf den IT-Systemen des zu schützenden Netzes durchgeführt werden.
  - Falsch konfigurierte Programme auf IT-Systemen im zu schützenden Netz können bei erlaubten Kommunikationsverbindungen von außen genutzt werden.
  - Typische Packet Filter können die Struktur des zu schützenden Netzes nicht verbergen.
  - Protokolldaten werden nur bis zur Transportebene zur Verfügung gestellt.

Firewall-Elemente

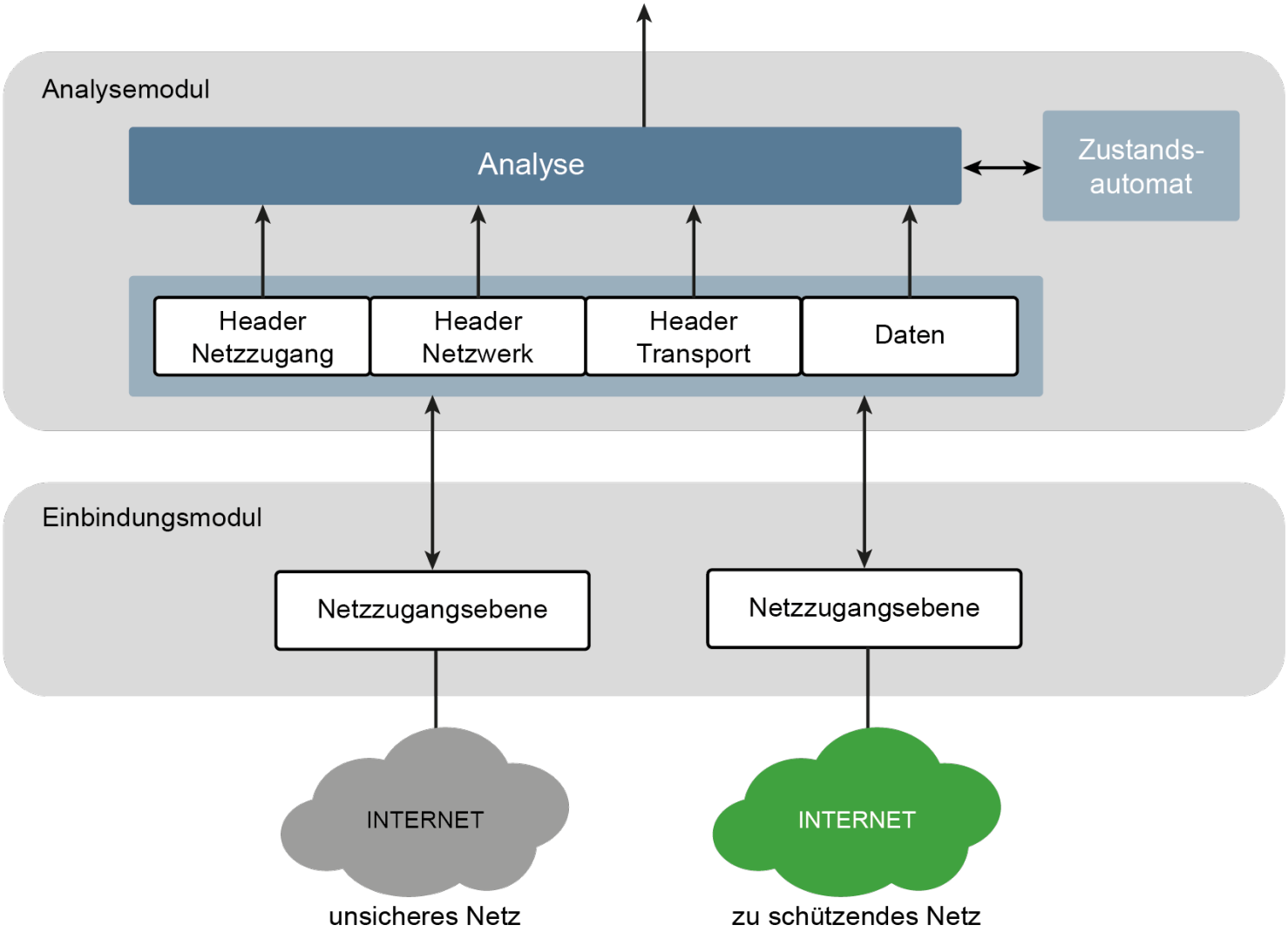
→ Zustandsorientierte Packet Filter (1/7)

- Der Leistungsumfang von Packet Filtern kann erweitert werden, indem die Analyse und Interpretation der Pakete auch auf höheren Kommunikationsebenen durchgeführt wird.

- In diesem Fall werden die Pakete auch auf der Anwendungsebene interpretiert und Statusinformationen für jede aktuelle Verbindung auf den unterschiedlichen Kommunikationsebenen bewertet und festgehalten.

Firewall-Elemente

→ Zustandsorientierte Packet Filter (2/7)



Firewall-Elemente

→ Zustandsorientierte Packet Filter (3/7)

- Die Statusinformationen können in Form von Zuständen mit den entsprechenden Informationen festgehalten werden.
- Zustände sind zum Beispiel Verbindungsaufbau, Transferzustand oder Verbindungsabbau für die jeweilige Kommunikationsebene.
- In jedem Zustand kann dann eine andere Interpretation der Kommunikationsdaten erfolgen.
- Mit dieser erweiterten Funktionalität werden sie oft als Stateful Inspection Firewall angeboten.
- Diese zustandsorientierten Packet Filter haben die Vorteile von Packet-Filtern, können aber zusätzlich die Anwendungen kontrollieren.

→ Zustandsorientierte Packet Filter (4/7)

- Das gleichzeitige Festhalten und Interpretieren der Kommunikationsdaten auf den verschiedenen Kommunikationsebenen ist sehr komplex.
- Aus diesem Grund haben zustandsorientierte Packet Filter in der Regel eine geringere Tiefe der Analyse oder sind besonders fehleranfällig.
- Kommunikationsprotokolle sind aus Gründen der Komplexität extra in Schichten unterteilt.
- Jede Schicht ist für eine Kernfunktionalität der Kommunikation verantwortlich.
- Darunterliegende Schichten müssen sich mit diesen Komplexitäten nicht beschäftigen, sondern können sich vielmehr auf dessen Funktionalitäten verlassen.

→ Zustandsorientierte Packet Filter (5/7)

- Aus diesem Grund ist eine Zusammenführung der Schichten im Rahmen einer Analyse bereits konzeptionell mit großen Hürden behaftet und führt in der praktischen Umsetzung zu Fehlern.

- Prinzipiell ist es auch nicht möglich, die komplexe Software von zustandsorientierten Packet Filtern soweit auszutesten, dass in nachweislich keinem Betriebszustand Fehler auftreten können.

- Aus diesem Grund muss auch in Zukunft immer wieder damit gerechnet werden, dass die komplexen Programme potenzielle Sicherheitsrisiken aufweisen, die für Angriffe verwendet werden können.

→ Zustandsorientierte Packet Filter (6/7)

- **Möglichkeiten, Vorteile und besondere Aspekte von zustandsorientierten Packet Filtern:**
  - wenn keine Authentifikation notwendig ist: transparent, d.h. unsichtbar für den Nutzer und die IT-Systeme und ohne ihre aktive Einwirkung tätig
  - einfach erweiterungsfähig für neue Protokolle
  - flexibel für neue Dienste
  - eventuell für andere Protokollfamilien verwendbar (IPX, OSI, DECNET, SNA...)

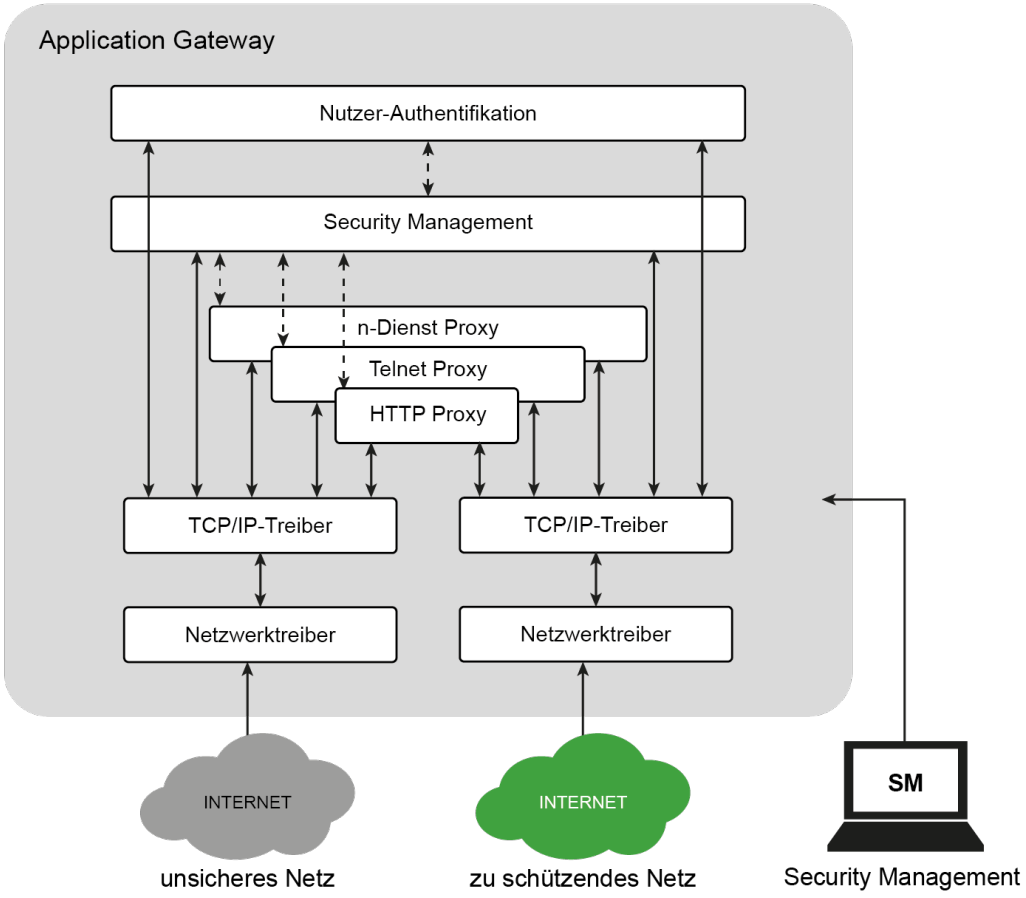
→ Zustandsorientierte Packet Filter (7/7)

- **Nachteile und Grenzen von zustandsorientierten Packet Filtern:**
  - **Komplexität** der Lösung
  - falsch konfigurierte und **fehlerbehaftete Programme** auf IT-Systemen im zu schützenden Netz können bei erlaubten Kommunikationsverbindungen von außen genutzt werden, da ein direkter Zugriff auf das IT-Systemen besteht
  - typische zustandsorientierte Packet Filter können die Struktur des zu schützenden Netzes nicht verbergen

Firewall-Elemente

→ Application Gateway/Proxy-Technik (1/6)

- Das Application Gateway zeichnet sich dadurch aus, dass es die Netze sowohl **logisch** als auch **physikalisch entkoppeln** kann.



Firewall-Elemente

→ Application Gateway/Proxy-Technik (2/6)

- Da in einigen Firewall-Konzepten das Application Gateway das einzige vom unsicheren Netz erreichbare IT-System ist, muss das Application Gateway besonders geschützt werden.

- Aus diesem Grund wird das IT-System, auf dem das Application Gateway realisiert ist, auch als Bastion bezeichnet.

- Das Application Gateway – als Dual-homed Gateway realisiert – arbeitet mit zwei Netzwerk-Anschlüssen.

- Dual-homed bedeutet, dass das Application Gateway die vollständige Kontrolle über die Pakete hat, die zwischen dem unsicheren und dem zu schützenden Netzwerk übertragen werden sollen.

Firewall-Elemente

→ Application Gateway/Proxy-Technik (3/6)

- **Allgemeine Arbeitsweise des Application Gateway**
  - Ein Nutzer, der über das Application Gateway kommunizieren möchte, muss sich zuerst identifizieren und authentisieren.
  - Application Gateways bieten in der Regel unterschiedliche Authentifikationsverfahren an.
  - Aus diesem Grund baut der Nutzer zuerst eine Verbindung mit dem Application Gateway auf.
  - Der direkte Kommunikationspartner ist nicht sein Ziel-IT-System, sondern das Application Gateway, beziehungsweise der entsprechende Proxy für die Anwendung.
  - Nach der Identifikation und Authentifikation arbeitet das Application Gateway aber transparent, sodass der Nutzer den Eindruck hat, direkt auf dem Ziel-IT-System zu arbeiten.

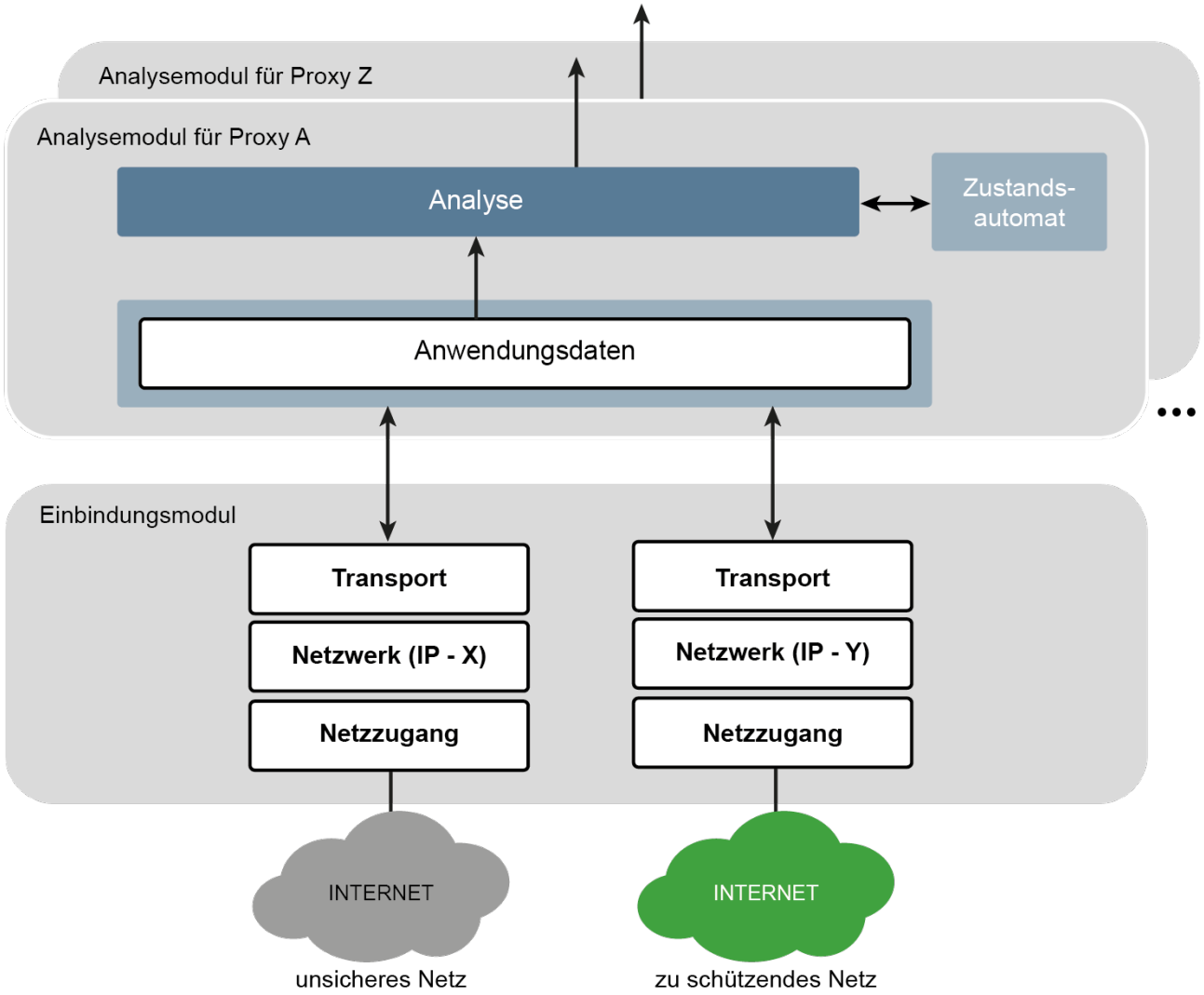
Firewall-Elemente

→ Application Gateway/Proxy-Technik (4/6)

- **Grundsätzlicher Ansatz**
  - Über die Netzzugangs- und TCP/IP-Treiber empfängt das Application Gateway die Pakete an den entsprechenden Ports.
  - Soll nur ein Dienst über einen entsprechenden Port möglich sein, muss auf dem Application Gateway eine Software zur Verfügung gestellt werden, die das entsprechende Paket von der einen Netzwerkseite zur anderen Netzwerkseite des Application Gateway überträgt und umgekehrt.
  - Eine solche Software, die die Paketübertragung nur für einen speziellen Dienst (HTTP, FTP, Telnet, usw.) im Application Gateway durchführt, wird als Proxy bezeichnet.
  - Der Name Proxy – Stellvertreter – wird verwendet, weil es aus Sicht des zugreifenden Nutzers so aussieht, als würde er mit dem eigentlichen Server-Prozess des Dienstes auf dem Ziel-IT-System kommunizieren.

Firewall-Elemente

→ Application Gateway/Proxy-Technik (5/6)



Firewall-Elemente

→ Application Gateway/Proxy-Technik (6/6)

- Jeder Proxy auf dem Application Gateway kann speziell für den Dienst, für den er zuständig ist, weitere Sicherheitsdienste anbieten.

- Bedingt durch den jeweiligen speziellen Proxy und das Wissen um den Kontext eines speziellen Dienstes ergeben sich umfangreichere Sicherungs- und Protokollierungsmöglichkeiten im Application Gateway.

- Die Analyse ist auf dieser Kommunikationsebene besonders intensiv möglich, da der Kontext der Anwendungsdaten für den jeweiligen Dienst klar definiert ist.

- Der Vorteil ist, dass kleine überschaubare Module verwendet werden können, da eine Analyse innerhalb einer Schicht erfolgt.
  - Dadurch wird die Fehleranfälligkeit durch Implementationsfehler reduziert.

Firewall-Elemente

→ **Sicherheitskonzept eines Application Gateway (1/3)**

- Für jeden Dienst, der über das Application Gateway möglich sein soll, muss ein spezieller Proxy zur Verfügung gestellt werden.

- Sollen bestimmte Dienste generell nicht möglich sein, dann darf für diese Dienste kein Proxy auf dem Application Gateway vorhanden sein, aber auch keine weitere Software, die den Dienst ermöglichen könnte!

- Aus diesem Grund ist so wenig Software wie möglich auf dem Application Gateway zu installieren, damit nicht zufällig – oder absichtlich durch einen Angreifer von außen provoziert – eine andere Software die Aufgabe eines Proxys (Paketübertragung im Application Gateway) für einen Dienst übernimmt, der nicht erlaubt sein soll.

Firewall-Elemente

→ **Sicherheitskonzept eines Application Gateway (2/3)**

- Das Security Management, das dem Nutzer die Arbeit so leicht wie möglich gestalten soll und deshalb mit einer mächtigen Software (X-Terminal, Datenbank, ...) ausgestattet ist, darf aus Sicherheitsgründen nicht auf dasselbe IT-System.

- Application Gateways sollen aus Sicherheitsgründen keine Routing-Funktionalität haben, damit nicht an den Proxies vorbeigeroutet werden kann.

- Da das Application Gateway bei der Kommunikation jeweils zum IT-System des unsicheren Netzes und zu dem des zu schützenden Netzes eine Kommunikationsverbindung hat, bietet das Application Gateway eine „Network Address Translation".

- Dazu hat das Application Gateway eine IP-Adresse im unsicheren Netz (z.B. eine offizielle Internet IP-Adresse 194.173.3.1) und eine IP-Adresse im zu schützenden Netz (z.B. eine für diesen Zweck reservierte IP-Adresse 192.168.1.60).

Firewall-Elemente

→ **Sicherheitskonzept eines Application Gateway (3/3)**

- Bei der Kommunikation mit den IT-Systemen des unsicheren Netzes verwendet das Application Gateway die IP-Adressen des unsicheren Netzes, und bei der Kommunikation mit den IT-Systemen des zu schützenden Netzes verwendet das Application Gateway die IP-Adressen des zu schützenden Netzes.

Firewall-Elemente

→ Proxies (1/2)

- Bei der Realisierung von Proxies wird zwischen Application Level und Circuit Level Proxies unterschieden.
- Application Level Proxies sind für bestimmte Dienste/Anwendungen implementiert.
- Das heißt, sie kennen die Kommandos der Anwendungsprotokolle und können diese analysieren und kontrollieren.
- Application-Level Proxies arbeiten mit der gängigen, unveränderten Client-Software für FTP, Telnet oder Browser zusammen.

Firewall-Elemente

→ Proxies (2/2)

- Einige Proxies funktionieren nach dem Store-and-Forward-Prinzip (SMTP), andere interaktiv und nutzerorientiert (Telnet, FTP, HTTP, ...).

- Da bei Application Gateways ein Routing auf der Netzwerkebene aus Sicherheitsgründen nicht möglich sein darf, könnten für Dienste, für die kein Application Level Proxy zur Verfügung steht, so genannte Circuit Level Proxies zur Verfügung gestellt werden, wenn eine Kommunikation über das Application Gateway realisiert werden soll.

- Circuit Level Proxies sind eine Art generische Proxies, die für eine Mehrzahl von Diensten mit verschiedenen Protokollen verwendet werden können.

- Diese Circuit Level Proxies, die auch als generische Proxies, Port-Relays oder Plug-Gateways bezeichnet werden, können in der Regel für TCP und UDP-Anwendungen verwendet werden.

Firewall-Elemente

→ Anwendungsgebiete von Application Gateways (1/4)

- Immer dann, wenn es notwendig ist, Schutzmaßnahmen für die Anwendungen zur Verfügung zu stellen, ist ein Application Gateway ein ideales aktives Firewall-Element.

- Die Möglichkeit der Protokollierung auf der Anwendungsebene kann ebenfalls ein besonderer Grund sein, das Application Gateway in einem Firewall-Konzept zu berücksichtigen.

- Für die Ankopplung an das Internet ist auf jeden Fall ein Application Gateway in der Firewall-Konstellation zu berücksichtigen, wenn die IT-Systeme im zu schützenden Netz einen hohen Schutzbedarf haben.

- Außerdem können Organisationseinheiten, die sich abschotten wollen, hiermit einen besonderen Schutz erzielen.

Firewall-Elemente

→ **Anwendungsgebiete von Application Gateways (2/4)**

- **Vorteile und besondere Aspekte eines Application Gateway**
  - sicheres Design-Konzept, da kleine, gut überprüfbare Module (Proxies)
  - Konzentration auf das Wesentliche
  - Alle Pakete müssen über Proxies übertragen werden, das bedeutet höhere Sicherheit.
  - Der Kommunikationspartner der IT-Systeme, die über das Application Gateway kommunizieren, ist der Proxy; dadurch kann eine echte Entkopplung der Dienste erreicht werden.
  - Verbindungsdaten und Applikationsdaten können protokolliert werden, wodurch die Handlungen der Nutzer, die über das Application Gateway kommunizieren, festgehalten werden können.
  - Verbergen der internen Netzstruktur.

Firewall-Elemente

→ **Anwendungsgebiete von Application Gateways (3/4)**

- Sicherheitsfunktionen für die Anwendungen werden zur Verfügung gestellt (Kommando-, Datei- und Daten-Filter usw.)
- Eine Network Address Translation findet statt.

- **Nachteile und Grenzen eines Application Gateway**
  - geringe Flexibilität, da für jeden neuen Dienst ein neuer Proxy zur Verfügung gestellt werden muss
  - Die Kosten für ein Application Gateway sind in der Regel höher.
  - andere Vorgehensweise bei der Kommunikation über das Application Gateway (ist nicht transparent)
  - Bei verschlüsselten Kommunikationskanälen zwischen Server und Client muss das Application Gateway eigene Zertifikate zu der Serveranwendung erzeugen und mit einer eigenen CA signieren.

Firewall-Elemente

→ **Anwendungsgebiete von Application Gateways (4/4)**

- Das entsprechende Root-Zertifikat der CA muss von den Clients im zu schützenden Netz installiert und akzeptiert werden.
- Hiermit wird das Prinzip von End-to-End-Verschlüsselung und PKIs ausgehebelt.
- Daraus könnte eine Reduzierung derCyber-Sicherheit resultieren.

Firewall-Elemente

→ Next-Generation Firewall (1/6)

- Bei einer Next-Generation Firewall können die Analyse-Module unterschiedliche Anwendungsdaten in einem Datenstrom unabhängig von der Portnummer erkennen und entsprechend filtern.
  - Zum Beispiel über das Universalprotokoll HTTP werden fast alle Arten von Informationen transportiert.

- Aus diesem Grund ist es für den Administrator einer Firewall nur schwer kontrollierbar, welche Dienste die Mitarbeiter nutzen dürfen und welche nicht.
  - Mit einer herkömmlichen Firewall ist es beispielsweise nicht möglich den Remotezugriff der Team-Viewer Software zu blockieren ohne gleichzeitig den gesamten Webseitenzugriff zu blockieren, da Team-Viewer HTTP (Port 80) verwendet.

Firewall-Elemente

→ Next-Generation Firewall (2/6)

- Bisherige Firewalls erlauben es nicht, solche Dienste explizit zu erkennen und ggf. zu blockieren.

- Ein weiterer Nachteil der herkömmlichen Firewall-Variante ist, dass viele Anwendungen die freigegebenen Standard-Ports durch sogenanntes Port Hopping ausnutzen, um so eine mühelose Kommunikation zu erlangen.

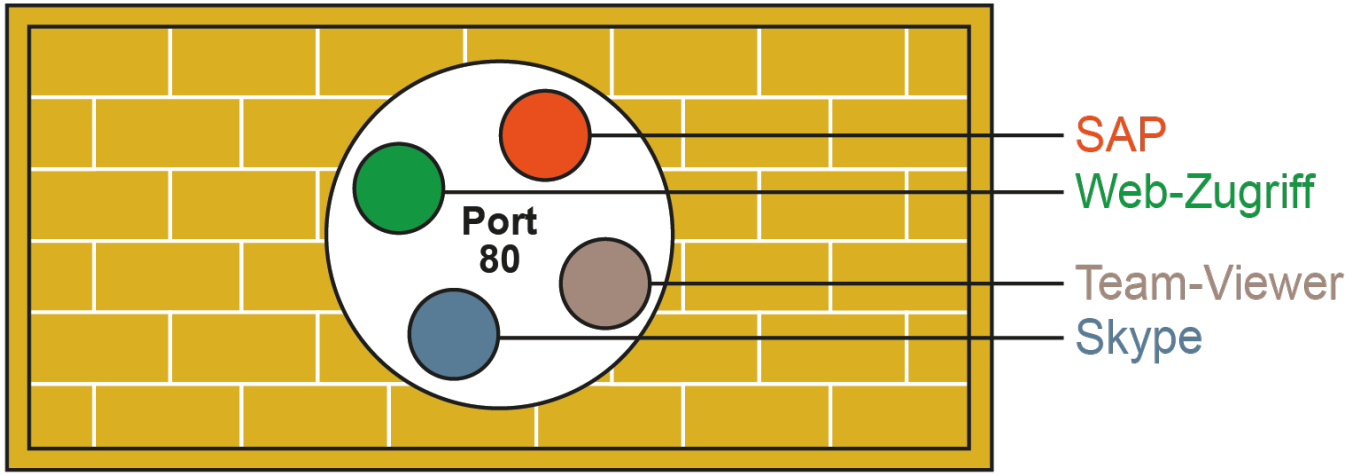
- Port-Hopping ist eine Technik, die von vielen Programmen für eine erfolgreiche Kommunikation durch Firewalls genutzt wird.

- Im Fall eines geblockten Ports wechselt die Software auf einen Standard-Port (z.B. Port 80) und kommuniziert über diesen Weg typischerweise ungehindert weiter.

Firewall-Elemente

→ Next-Generation Firewall (3/6)

- **Identifizieren von Anwendungen**
  - Die Anwendungserkennung stellt die wesentliche Funktion einer Next-Generation Firewall dar und ermöglicht einem Administrator eine erhöhte Kontrolle über den Datenstrom.
  - Sie erkennt zum einen, welche Anwendung den Datenstrom erzeugt und zum anderen, welche Funktionen einer Anwendung genutzt werden.



Firewall-Elemente

→ Next-Generation Firewall (4/6)

- Somit kann ein Administrator z.B. das Telefonieren über Skype erlauben, den Datentransfer über die selbige Software jedoch blockieren.

- Die Erkennung der Anwendungen verläuft unabhängig vom Port oder Protokoll mittels Analyse durch Erkennungsmuster.

- Vergleichbar mit Anti-Malware-Lösung besitzt eine Next-Generation Firewall eine Datenbank mit Signaturen zu den Anwendungen und deren Funktionen bzw. Subanwendungen.

- Häufig bleiben die Protokolle, die von Anwendungen genutzt werden, viele Jahre unverändert, womit eine Signatur zur Erkennung der Anwendung ausreicht.

Firewall-Elemente

→ Next-Generation Firewall (5/6)

- Auf der andern Seite werden Webanwendungen häufig angepasst.
- Damit die Next-Generation Firewall auch hier die Webanwendungen richtig analysieren kann, sind regelmäßige Aktualisierungen der Signaturen seitens der Next-Generation Firewall Hersteller nötig.
- Laut einiger Herstellerangaben identifizieren die Next-Generation Firewalls bis zu 1.000 Anwendungen und bis zu 100.000 Subanwendungen, mit denen einzelne Funktionen der Anwendungen gesteuert werden können.
- Ein weiteres wesentliches Merkmal einer Next-Generation Firewall ist auch, dass sie Datenströme zu Nutzern zuordnen kann.
  - Dazu wird eine Kombination von Nutzern und IP-Adressen ermittelt.

Firewall-Elemente

→ Next-Generation Firewall (6/6)

- Der Vorteil der Nutzererkennung ergibt sich dadurch, dass den Nutzern Rollen und Gruppenzugehörigkeiten zugeordnet werden können.
- Damit ist genau erkennbar, welcher Nutzer welche Kommunikation aufbaut und welche Anwendungen dabei verwendet wird.
- So lässt sich zum Beispiel die Verwendung von sozialen Netzwerken, wie Facebook oder Xing auf die Personalverwaltung begrenzen, da diese die für die Personalbeschaffung benötigt.
- Anderen Abteilungen könnte der Zugriff an dieser Stelle verwehrt werden.

→ **Inhalt**

- Ziele und Ergebnisse der Vorlesung
- Bedrohungen im Netz
- Sicherheitskonzept
- Kommunikationsmodell
- Firewall-Elemente
- **Firewall-Konzepte**
- Zusammenfassung

Firewall-Konzepte

→ Einleitung

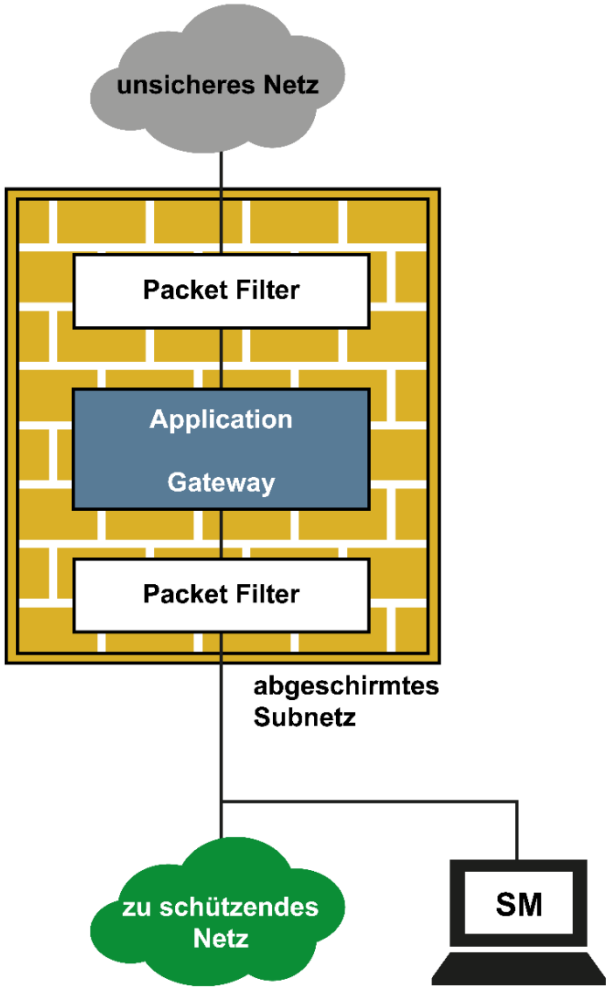
- Bei aktiven Firewall-Elementen handelt es sich um Sicherheitskomponenten, die ausschließlich für die Erbringung von Sicherheitsdiensten verantwortlich sind.

- Die vorgestellten Firewall-Elemente unterscheiden sich nach dem Maß an Sicherheit, das sie erbringen können, und nach den Einsatzfällen, für die sie sich eignen.

- Die verschiedenen Firewall-Elemente können als Firewall-System eigenständig Sicherheit zum Schutz zwischen Netzen erbringen oder mit einer geschickten Kombination der einzelnen Firewall-Elemente ein höheres Maß an Sicherheit erzielen.

Firewall-Konzepte

→ High-level-Security-Firewall-System



Firewall-Konzepte

→ **Bewertung des High-level-Security-Firewall-System (1/6)**

- Die Kommunikation zwischen IT-Systemen im zu schützenden Netz und IT-Systemen aus dem unsicheren Netz wird durch die Packet Filter und das dual-homed Application Gateway kontrolliert.
  - Dieses Konzept lässt keine Möglichkeit zu, das dual-homed Application Gateway zu umgehen.

- Das Maß an Sicherheit, das dieses Firewall-Konzept bietet, addiert sich aus der Sicherheitsleistung des Packet Filter und der Sicherheit des dual-homed Application Gateway, sodass eine besonders hohe Gesamtsicherheit erreicht wird.

→ **Bewertung des High-level-Security-Firewall-System (2/6)**

- **Einfache Regeln:**
  - Die Anordnung der Elemente ermöglicht eine einfache Definition der Regeln für die einzelnen aktiven Firewall-Elemente.
  - Aus der Sicht des Packet Filter kommuniziert immer nur der Application Gateway mit den IT-Systemen des entsprechenden Netzes.

- **Gegenseitiger Schutz:**
  - Die Packet Filter sorgen dafür, dass nicht jeder auf das dual-homed Application Gateway zugreifen darf, und schützen damit das dual-homed Application Gateway selbst.

Firewall-Konzepte

→ **Bewertung des High-level-Security-Firewall-System (3/6)**

- **Geschachtelte Sicherheit:**
  - Wer auf ein zu schützendes Netz zugreifen will, muss verschiedene Barrieren überwinden:
    - zuerst einen Packet Filter,
    - dann ein dual-homed Application Gateway
    - und zum Schluss wieder einen Packet Filter.
- **Verschiedene Betriebssysteme:**
  - Ein LINUX-Betriebssystem für das dual-homed Application Gateway.
  - Ein Real-Time-Betriebssystem für die Packet Filter.
  - Eventuell auftretende Betriebssystemfehler oder Lücken wirken sich dadurch nur jeweils auf ein aktives Firewall-Element aus.

Firewall-Konzepte

→ **Bewertung des High-level-Security-Firewall-System (4/6)**

- **Unterschiedliche Einbindungs- und Analysemöglichkeiten:**
  - Außerdem arbeiten die verschiedenen aktiven Firewall-Elemente mit unterschiedlichen Strategien (Sicherheitsansätzen).
  - Die Packet Filter interpretieren die übertragenen Pakete von unten nach oben auf der Netzzugangs-, der Netzwerk- und der Transportebene.
  - Das dual-homed Application Gateway interpretiert die Kommunikation auf der Anwendungsebene.
  - Auch hier können sich mögliche Schwächen der Einbindungs- und Analysemöglichkeiten nur jeweils auf ein aktives Firewall-Element auswirken.

Firewall-Konzepte

→ **Bewertung des High-level-Security-Firewall-System (5/6)**

- **Separates Security Management:**
  - Das separate Security Management stellt viele eigene Sicherheitsmechanismen wie Zugangskontrolle, Rechteverwaltung, Verschlüsselung und Protokollierung zur Verfügung und sorgt auf diese Weise ebenfalls für High-level Security.

- **Mehr als die Summe der Einzelteile!**
  - Alle diese Sicherheitsmechanismen zusammen garantieren ein höheres Maß an Sicherheit als jeder Sicherheitsmechanismus für sich alleine.
  - So wie bei einem Auto der Sicherheitsgurt, der Airbag, der Seitenaufprallschutz und die Knautschzone zusammen ein Höchstmaß an Sicherheit bieten.

Firewall-Konzepte

→ **Bewertung des High-level-Security-Firewall-System (6/6)**

- **Einsatzfall**
  - Der Einsatz eines High-level-Security-Firewall-Systems empfiehlt sich immer dann, wenn ein zu schützendes Netz an ein unsicheres Netz angekoppelt wird, das ein geringes oder nicht einschätzbares Schutzniveau hat und außerhalb des eigenen Verantwortungsbereiches liegt.
  - Dies ist bei der Ankopplung an das Internet der Fall.

Firewall-Konzepte

→ Common Point of Trust

- Ein Firewall-System stellt den „Common Point of Trust" für den Übergang zwischen unterschiedlichen Netzen dar.
- Das heißt, der einzige Weg zwischen den Netzen führt kontrolliert über das Firewall-System.
- Firewall-Systeme werden verwendet, um sich an unsichere Netze wie z.B. das Internet anzukoppeln.
- Firewall-Systeme werden aber auch eingesetzt, um das eigene Netz zu strukturieren und hier Sicherheitsdomänen mit unterschiedlichem Schutzbedarf zu schaffen.

Firewall-Konzepte

→ **Vorteile des "Common Point of Trust"-Konzepts (1/4)**

- **Kosten**
  - Die Realisierung von Cyber-Schutzmaßnahmen in einem zentralen Firewall-System ist wesentlich effizienter als die Realisierung von Cyber-Schutzmaßnahmen auf jedem einzelnen IT-System, das im zu schützenden Netz steht.

- **Umsetzung der Sicherheitsleitlinie**
  - Mithilfe eines zentralen Firewall-Systems kann die Sicherheitsleitlinie einer Organisation auf einfache Weise zentral durchgesetzt werden.
  - Zum Beispiel werden die Dienste und Protokolle, die über ein Firewall-System möglich sein sollen, an einer zentralen Stelle für alle Nutzer definiert und überprüft.

→ **Vorteile des "Common Point of Trust"-Konzepts (2/4)**

- **Möglichkeiten**
  - Eine kryptographische (starke) Authentisierung von Nutzern und IT-Systemen ist auf einem Firewall-System zu realisieren und nicht auf jedem einzelnen IT-System im zu schützenden Netz, damit die Nutzer sicher identifiziert und authentisiert werden können.
  - Für heterogene IT-Systemlandschaften gibt es zzt. keine Konzepte und Realisierungen, wie kryptographische Authentisierung auf den unterschiedlichen Betriebssystemen (LINUX, Microsoft Windows, iOS, Android, ...) praktisch realisiert werden kann.
  - Hier können Kosten eingespart werden.

Firewall-Konzepte

→ **Vorteile des "Common Point of Trust"-Konzepts (3/4)**

- **Sicherheit durch Abschottung**
  - Durch die reduzierte Funktionalität, die ein Firewall-System anbietet, existieren weniger Angriffspunkte für Angreifer aus dem unsicheren Netz.
  - Der Aufwand für Schutzmaßnahmen konzentriert sich auf das Firewall-System.
  - Dadurch wird erreicht, dass die IT-Systeme des zu schützenden Netzes nicht mehr von einem IT-System aus dem unsicheren Netz (z.B. Internet) angegriffen werden können, sondern IT-Systeme von außerhalb durch das Firewall-System abgeblockt werden.
  - IT-Systeme können nicht mehr zum Ziel von Angreifern aus dem unsicheren Netz werden, wenn sie falsch installiert oder konfiguriert sind.
  - Alle Schutzmaßnahmen sind in dem Firewall-System konzentriert realisiert.

Firewall-Konzepte

→ **Vorteile des "Common Point of Trust"-Konzepts (4/4)**

- **Überprüfbarkeit**
  - Durch den klaren Übergang (Common Point of Trust) zwischen zwei Netzen ist eine einfache und vollständige Protokollierungsmöglichkeit vorhanden, da die gesamte Kommunikation über das Firewall-System läuft.

Firewall-Konzepte

→ Konzeptionelle Grenzen (1/7)

- Die Firewall-Systeme, die die Sicherheitsdienste für die Kommunikation im Internet und Intranet bereitstellen, sind sehr komplexe technische Sicherheitsmaßnahmen.

- Dennoch können auch aufwendige Firewall-Systeme keine hundertprozentige Sicherheit gewährleisten.

- **Hintertüren**
  - Ein Firewall-System schützt genau die Kommunikationsverbindungen, die darüber erfolgen.
  - Gibt es Kommunikationsübergänge am Firewall-System vorbei (backdoors), hat das Firewall-System keine Sicherheitswirkung mehr.
  - Dafür sind entsprechende personelle und organisatorische Sicherheitsmaßnahmen nötig.

→ Konzeptionelle Grenzen (2/7)

- **Interne Angriffe**
  - Ein Firewall-System bietet Cyber-Sicherheitsdienste zur Abschottung gegen das unsichere Netz oder zur Kontrolle der Kommunikation zwischen dem unsicheren Netz und dem zu schützenden Netz.
  - Das Firewall-System selbst bietet nur einen sehr geringen Schutz vor internen Angriffen.
  - Um internen Angriffen entgegenzuwirken, müssen weitere, ergänzende Sicherheitsmechanismen (z.B. Intrusion Detection Systeme) eingeführt werden.

→ Konzeptionelle Grenzen (3/7)

- **Wissen und Hypothese**
  - Mit einem Firewall-System können durch theoretisches Wissen und praktische Erfahrungen Fehlerursachen verhindert werden.
  - Gerade bei innovativen Anwendungen und Technologien, wie dem Internet wird mit einer Vielzahl von Hypothesen gearbeitet.
  - Daher gibt es einen Bereich des Neuen, Unbekannten und auch Unerwünschten und Unvorhersehbaren, was mit Hilfe eines Firewall-Systems nicht beherrscht werden kann.
  - Diesem kann nur mit weiteren, modular ergänzten Sicherheitsmechanismen entgegenwirkt werden.

→ Konzeptionelle Grenzen (4/7)

- **Richtige Sicherheitspolitik und richtige Umsetzung der Sicherheitspolitik**
  - Ein Firewall-System kann nur die Sicherheitsdienste erbringen, die eingerichtet sind.
  - Deshalb ist es von besonderer Bedeutung, dass eine Sicherheitspolitik erarbeitet wird, die darstellt, welche Ressourcen (IT-Systeme, Kommunikationseinrichtungen, Daten usw.) im zu schützenden Netz einen hohen Schutzbedarf haben und wie sie geschützt werden sollen.
  - Außerdem muss definiert werden, auf welche Weise die Sicherheitsmechanismen für die Aufrechterhaltung des sicheren Betriebs eines Firewall-Systems periodisch überprüft werden.

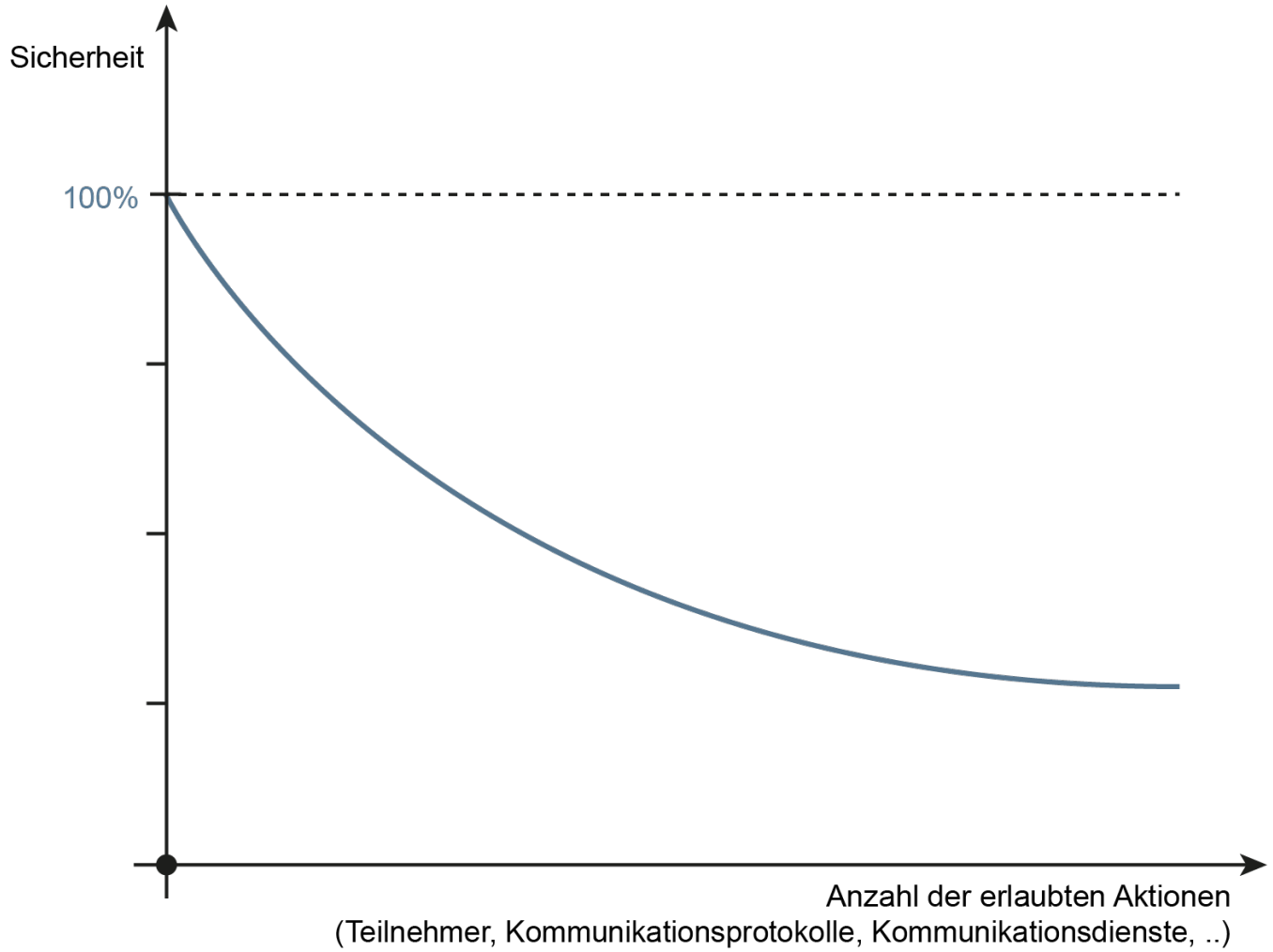
Firewall-Konzepte

→ Konzeptionelle Grenzen (5/7)

- **security versus connectivity ⇔ Risiko versus Chance**
  - Je kleiner die Menge erlaubter Aktionen ist, umso geringer ist das Risiko, dass ein Schaden auftreten kann.
  - Jeder Teilnehmer, jedes IT-System, das über ein Firewall-System kommunizieren darf, stellt ein zusätzliches Risiko dar.
  - So stellen z.B. auch die erlaubten Kommunikationspartner ein Risiko dar, falls sie unberechtigte Kommunikationsverbindungen nutzen.
  - Aus diesem Grund ist zu beachten:
    - so wenig wie möglich/nötig über das Firewall-System zulassen, damit ein Höchstmaß an Cyber-Sicherheit erreicht werden kann.

Firewall-Konzepte

→ Konzeptionelle Grenzen (6/7)



→ Konzeptionelle Grenzen (7/7)

- **Vertrauenswürdigkeit des Kommunikationspartners und der empfangenden Daten**
  - Für die Entscheidungen, die ein Firewall-System durchführt, ist die Vertrauenswürdigkeit des Kommunikationspartners und der empfangenen Daten notwendig.
  - Da diese Eigenschaften nicht durch Sicherheitsmechanismen des Firewall-Systems vollständig erbracht werden können, müssen hier weitere, ergänzende Sicherheitsmechanismen wie z.B. Verschlüsselung (VPN) oder digitale Signatur eingesetzt oder schon vorhandene im Firewall-System aktiviert werden.

Firewall-Konzepte

→ **Das richtige Konzept für jeden Anwendungsfall (1/2)**

- Um eine einschätzbare Aussage über Firewall-Systeme treffen zu können, ist die Sicherheitseinstufung von Firewall-Konzepten sehr hilfreich.

- Dabei werden Einsatzfälle definiert, die nach den Kriterien Vertrauenswürdigkeit des Netzes und des Kommunikationspartners und Angriffspotential in Abhängigkeit des Einsatzfalles betrachtet.
  - Das unsichere Netz ist **innerhalb** der eigenen Organisation.
  - Das unsichere Netz ist **außerhalb** der eigenen Organisation.

- Die wichtigste Motivation für den Einsatz eines Firewall-Systems ist also die Reduzierung des Risikos der Verwundbarkeit, wenn ein Schutzbedarf der eigenen Werte besteht.

Firewall-Konzepte

→ **Das richtige Konzept für jeden Anwendungsfall (2/2)**

- Wenn das zu schützende Netz keinen Schutzbedarf hat, muss auch kein Firewall-System eingesetzt werden.

- Wenn aber ein Schutzbedarf vorliegt, dann muss der Einsatzfall entsprechend berücksichtigt werden und ein angemessenes Firewall-Konzept ist auszuwählen.

Firewall-Konzepte

→ Einsatzfälle von Firewall-Systemen

	Einsatzfall	
Kriterien	das unsichere Netz ist innerhalb der eigenen Organisation	das unsichere Netz ist außerhalb der eigenen Organisation
Vertrauenswürdigkeit des Netzes	sehr hoch • liegt in der eigenen Verantwortung • wird regelmäßig überprüft	von speziellen, **schwer ermessbaren** Faktoren abhängig • liegt nicht in der eigenen Verantwortung • es muss mit allen Risiken gerechnet werden
Vertrauenswürdigkeit des Kommunikationspartners	sehr hoch • die Kommunikationsteilnehmer gehören zur gleichen Organisation und arbeiten unter der gleichen Sicherheitspolitik	es wird hier angenommen, dass diese **sehr gering** ist
Angriffspotential	sehr gering • die Kommunikationsteilnehmer gehören zur gleichen Organisation und arbeiten unter der gleichen Sicherheitspolitik	**sehr hoch** • die Teilnehmer des Netzes haben einen sehr unterschiedlichen Schutzbedarf (Hacker neben professionellen Anwendungen) • z.B. Internet

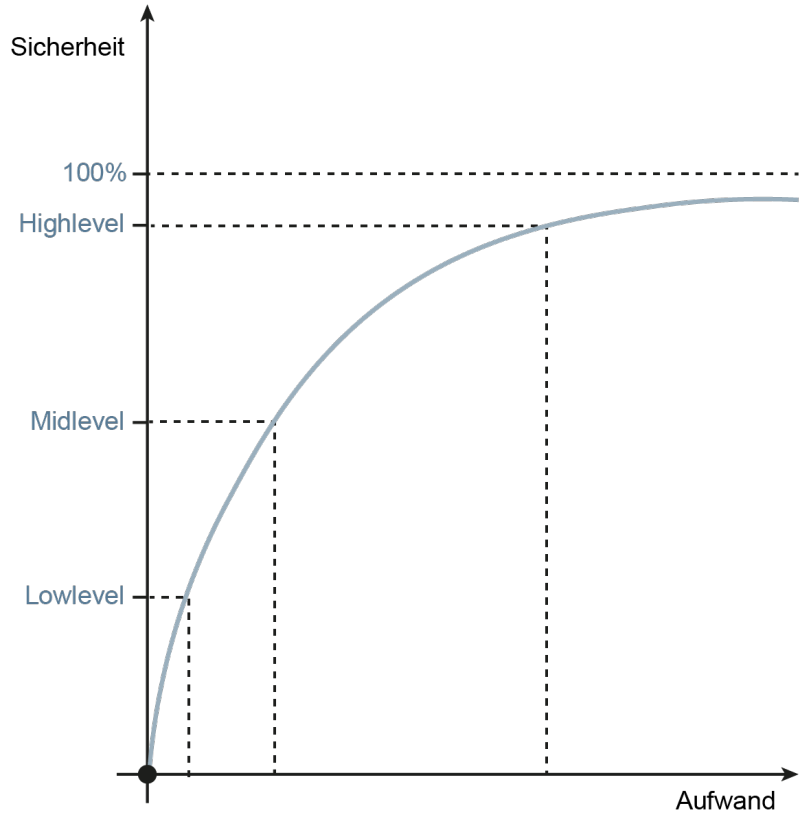
Firewall-Konzepte

→ Entscheidungsmatrix für das Firewall-Konzept

Schutz-bedarf	Risiken	Einsatzfall	Firewall-Konzept
niedrig	• geringfügiger Verstoß gegen Gesetze • beschränkte negative Außenwirkung • finanzieller Schaden < 25.000 EUR	innerhalb der Organisation:	Packet Filter
		außerhalb der Organisation:	Dual homed Applikation Gateway
hoch	• erheblicher Verstoß gegen Gesetze • breite negative Außenwirkung • finanzieller Schaden < 5 Mio. EUR	innerhalb der Organisation:	Packet Filter + Single-homed Applikation Gateway *oder* Stateful Inspection *oder* Adaptiv Proxy
		außerhalb der Organisation:	Packet Filter + dual homed Applikation Gateway
Sehr hoch	• fundamentaler Verstoß gegen Gesetze • existenzgefährdend negative Außenwirkung • finanzieller Schaden > 5 Mio. EUR	innerhalb der Organisation:	Screened Subnet mit Packet Filter + Single-homed Applikation Gateway
		außerhalb der Organisation:	Screened Subnet mit Packet Filter + dual homed Applikation Gateway ⇨ High-Level Firewall-System

→ Sicherheit in der Praxis

- Praxisgerechte Sicherheit von Firewall-Systemen ist gegeben, wenn das Firewall-System mit den nachfolgenden Eigenschaften nicht überwunden werden kann:
  - mit den verfügbaren Ressourcen
  - durch die bekannten Angriffe
  - mit vertretbarem Aufwand



Firewall-Konzepte

→ **Kommunikationsmodell mit integriertem Firewall-Element (1/8)**

- Das Firewall-System soll den Receiver $\{r_1, ..., r_m\}$ vor Angriffen auf seine Werte aus dem unsicheren Netz schützen.

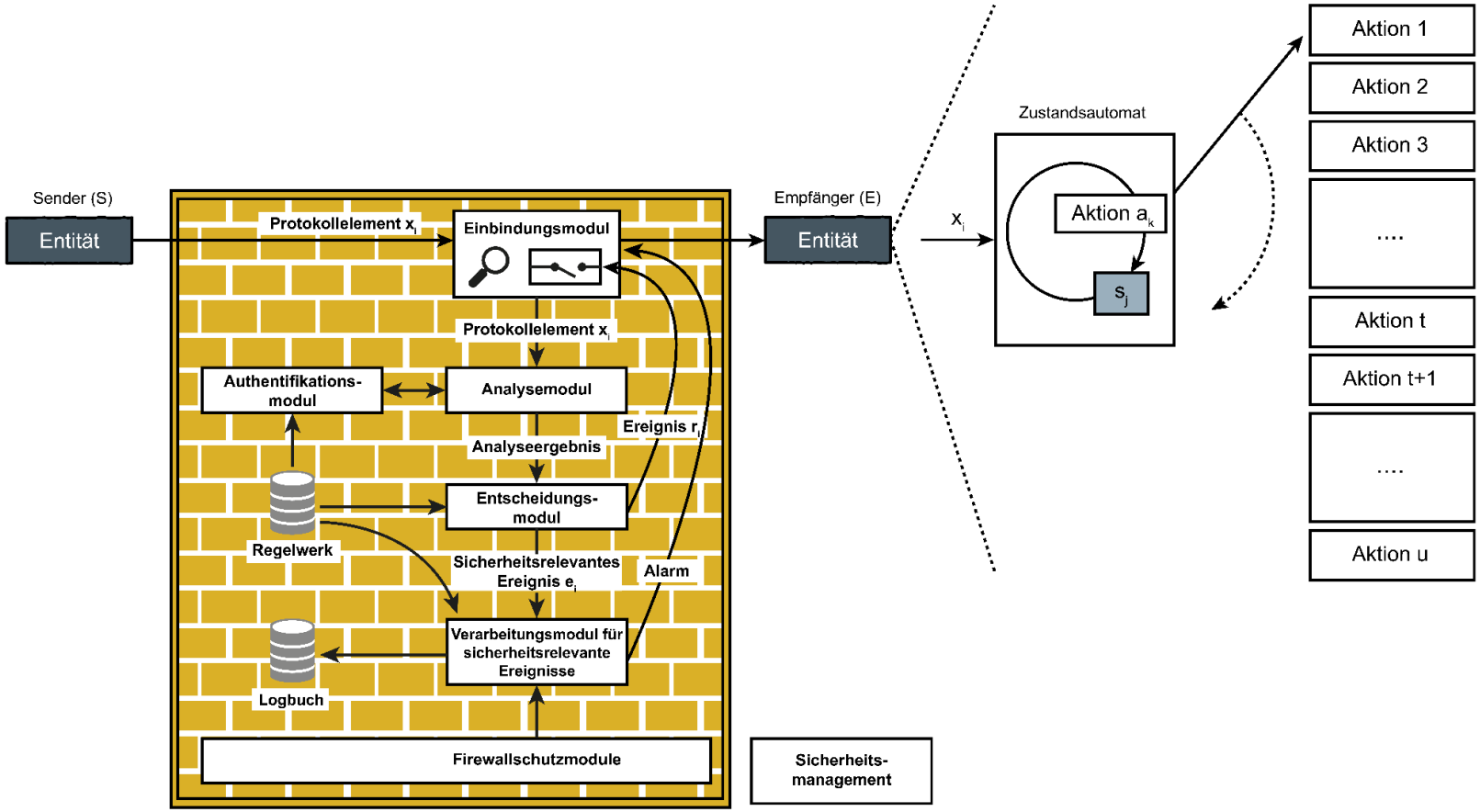
- Es wird davon ausgegangen, dass mit Hilfe eines Security-Managements die Rechte in das Firewall-Element, in Übereinstimmung mit der vorher festgelegten Sicherheitspolitik, eingetragen worden sind, die es ermöglichen sollen, die erlaubten Protokollelemente $\{x_1, ..., x_t\}$ über das Firewall-Element übertragen zu können.

- Bei einer fehlerfreien Implementierung des Firewall-Element und der Kommunikationsprotokolle und -dienste auf der Empfängerseite, werden auch nur erlaubte Aktionen $\{a_1, ..., a_t\}$ beim Receiver $\{r_1, ..., r_h\}$ ausgeführt.

- Es müssen beliebig viele Transmitter und Receiver berücksichtigt werden.

Firewall-Konzepte

→ **Kommunikationsmodell mit integriertem Firewall-Element (2/8)**



Firewall-Konzepte

→ **Kommunikationsmodell mit integriertem Firewall-Element (3/8)**

❒ Definition der Funktionen für die Auswahl der Aktion auf der Empfängerseite für „r_n“:

ak = action-select (protocol-state-machine (xi*, sj), authenticity (xi),
result-of-decision (analysis (xi*), security-management (rules)), functionality-of-the-firewall-element ( ))

a_k	Teil-Aktion in einer Schicht, die in Abhängigkeit des empfangenen Protokollelementes x_i und des aktuellen Zustandes s_j ausgeführt wird
x_i	Protokollelement, welches vom Sender zum Empfänger gesendet wird
x_i^*	Protokollelement, welches auf der Empfangsseite ankommt
s_j	aktueller Zustand (actual state)
rules	technische Umsetzung der Sicherheitspolitik (Access-Listen, ...)

- Hinweis:
  - Neben „r_n“ sind in der Regel weitere Empfänger $\{r_1, ..., r_g\}$ zu berücksichtigen.

Firewall-Konzepte

→ **Kommunikationsmodell mit integriertem Firewall-Element (4/8)**

- **Fehlerquellen durch Angriffe aus dem Netz:**
  - Funktion: *authenticity* (x_i)
  - Für den richtigen Kommunikationsablauf ist wichtig, dass sowohl der Transmitter(t_i) authentisch/echt ist als auch das Protokollelement x_i^* authentisch/echt und unversehrt übertragen worden ist.
  - Einflussfaktoren:
    - Vertrauenswürdigkeit des Netzes
    - Vertrauenswürdigkeit des Kommunikationsteilnehmers
  - oder/und
    - Gewährleistung der Authentifikation des Kommunikationspartners
    - Gewährleistung der Authentifikation des Ursprungs der Daten

Firewall-Konzepte

→ **Kommunikationsmodell mit integriertem Firewall-Element (5/8)**

- **Fehlerquellen der Kommunikationslösung beim Receiver:**
  - Funktion: protocol-state-machine (x_i^*, s_j)
  - Verantwortung des Anwenders
    - Einflussfaktor: **Konfiguration beim Empfänger**
      - Die Konfiguration des Kommunikationsprotokolls oder -dienstes haben Fehler, die zur Folge haben, dass trotz erlaubte Protokollelemente (x_i) eine nicht erlaubte Aktion auf der Empfängerseite durchgeführt wird.
  - Verantwortung des Herstellers
    - Einflussfaktor: **Implementierung beim Empfänger**
      - Die Implementierung des Kommunikationsprotokolls oder -dienstes hat Fehler, die zur Folge haben, dass trotz erlaubte Protokollelemente (x_i) eine nicht erlaubte Aktion auf der Empfängerseite durchgeführt wird.

Firewall-Konzepte

→ **Kommunikationsmodell mit integriertem Firewall-Element (6/8)**

- **Fehlerquellen des Firewall-Elements**
  - Verantwortung des Anwenders / **Funktion:** security-management(rules)
    - Einflussfaktor: Sicherheitspolitik
    - Es wird mehr erlaubt, als für die eigentliche Aufgabenstellung der einzelnen Nutzer erforderlich ist.
    - Die unbeabsichtigte falsche Eingabe der Regeln führt zu einem Fehlverhalten des Firewall-Elements.
    - Die beabsichtigte falsche Eingabe der Regeln verfolgt das Ziel, das Firewall-Element zu umgehen.
    - Die Einschränkung der Protokollelemente kann, z.B. durch Unwissenheit oder nicht richtige Vorgabe, unzureichend sein.
    - Neue Angriffsmethoden, die dem Verantwortlichen des Firewall-Elements nicht bekannt sind, könne daher auch nicht durch eine explizite Einschränkung verhindert werden.

Firewall-Konzepte

→ **Kommunikationsmodell mit integriertem Firewall-Element (7/8)**

- Verantwortung des Herstellers / **Funktion:** *analysis* (x_i)
  - Einflussfaktor: Tiefe der Analyse
    - Die Analyse der Protokollelemente kann nicht detailliert genug Aussagen treffen, und damit nur eingeschränkt Aktionen verhindern.
    - Sie kann in der Feststellung der Entscheidungskriterien und in deren Verdichtung zur Entscheidung Durchlass oder Sperren zu sehr begrenzt sein.
    - Bei der Analyse der Protokollelemente können wichtige und/oder neue Entscheidungskriterien unberücksichtigt bleiben.
    - Bei der Synthese der Kriterien zu Entscheidungen können Entscheidungsregeln nicht ausgereift oder nicht umfassend umgesetzt sein.
    - Dieser Punkt geht einher mit der Komplexität der möglichen Einschränkungen.

Firewall-Konzepte

→ **Kommunikationsmodell mit integriertem Firewall-Element (8/8)**

- **Funktion:** result-of-decision (analysis(x_i), rules)
  - Einflussfaktor: Vertrauenswürdige Implementierung:

- **Unzureichende Qualität der Realisierung des Firewall-Elementes:**
  - Die Qualität der Realisierung eines Firewall-Elements ist derart, dass in bestimmten Situationen ein Fehlverhalten auftritt.
  - folgende Komponenten müssen betrachtet werden
    - Betriebssystem, auf dem die Firewall-Applikation läuft
    - Firewall-Applikation
    - Security Management
    - Hardware der Firewall-Elemente und des Security-Management
    - Authentifikationskomponenten der Kommunikationspartner

Firewall-Konzepte

→ Sicherheitsdienste eines Firewall-Elements (1/4)

Sicherheitsdienst	Überprüfung / Festlegung / Maßnahme	Was wird geprüft?	Einfluss auf Sicherheit und Vertrauenswürdigkeit
Zugangskontrolle auf Netzwerkebene	Welche IT-Systeme (Transmitter, Receiver) dürfen über das Firewall-Element miteinander kommunizieren?	• IP-Adressen der beteiligten IT-Systeme • Zeit, zu der eine Aktion zulässig ist	• Vertrauenswürdige Implementierung • Vertrauenswürdigkeit des Netzes • Vertrauenswürdigkeit des Kommunikationspartners • Sicherheitspolitik
Zugangskontrolle auf Nutzerebene	Welche Nutzer dürfen über das Firewall-Element eine Kommunikation aufbauen?	• Identität des Nutzers • Authentifikation des Nutzers • Zeit, zu der eine Aktion zulässig ist	• Vertrauenswürdige Implementierung • Gewährleistung der Authentifikation des Kommunikationspartners • Sicherheitspolitik
Zugangskontrolle auf Datenebene	Dürfen die Daten eines definierten Nutzers über das Firewall-Element übertragen werden?	• Identität des Absenders der Daten • Authentifikation des Absenders der Daten • Integrität der Daten • Zeit, zu der eine Aktion zulässig ist	• Vertrauenswürdige Implementierung • Gewährleistung der Authentifikation des Ursprungs der Daten • Sicherheitspolitik

→ Sicherheitsdienste eines Firewall-Elements (2/4)

Sicherheitsdienst	Überprüfung / Festlegung / Maßnahme	Was wird geprüft?	Einfluss auf Sicherheit und Vertrauenswürdigkeit
Rechteverwaltung	Festlegung, mit welchen Protokollen und Diensten und zu welchen Zeiten über das Firewall-Element eine Kommunikation stattfinden darf.	• Header-Informationen auf den verschiedenen Schichten • Zeit, zu der eine Aktion zulässig ist	• Vertrauenswürdige Implementierung • Gewährleistung der Datenunversehrtheit • Tiefe der Analyse • Sicherheitspolitik
Kontrolle auf Anwendungsebene	Überprüfung, ob Kommandos genutzt oder Dateninhalte übertragen werden, die nicht zur durch die Anwendung definierten Aufgabenstellung gehören.	• Kommandos und Dateninhalte der verschiedenen Anwendungen • Zeit, zu der eine Aktion zulässig ist	• Vertrauenswürdige Implementierung • Gewährleistung der Datenunversehrtheit • Tiefe der Analyse • Sicherheitspolitik

→ Sicherheitsdienste eines Firewall-Elements (3/4)

Sicherheitsdienst	Überprüfung / Festlegung / Maßnahme	Was wird geprüft?	Einfluss auf Sicherheit und Vertrauenswürdigkeit
Entkoppelung von Diensten	Entkoppeln verhindert, dass Implementierungsfehler, Schwachstellen und Konzeptionsfehler der Dienste Möglichkeit für Angriffe bieten.	• Kommandos • Zeit, zu der eine Aktion zulässig ist	• Vertrauenswürdige Implementierung • Konzept der Entkopplung
Beweissicherung und Protokollauswertung	Verbindungsdaten und sicherheitsrelevante Ereignisse werden protokolliert und können für die Beweissicherung von Nutzerhandlungen und für die Erkennung von Sicherheitsverletzungen ausgewertet werden.	• Aktionen und sicherheitsrelevanten Ereignisse • Zeit, zu der eine Aktion zulässig ist	• Vertrauenswürdige Implementierung • Sicherheitspolitik • Konzept der Beweissicherung und Protokollauswertung

→ Sicherheitsdienste eines Firewall-Elements (4/4)

Sicherheitsdienst	Überprüfung / Festlegung / Maßnahme	Was wird geprüft?	Einfluss auf Sicherheit und Vertrauenswürdigkeit
Alarmierung	Besonders sicherheitsrelevante Ereignisse werden an ein Security Management gesendet, damit bei Sicherheitsverletzungen schnell reagiert werden kann.	• Zeit, zu der eine Aktion zulässig ist	• Vertrauenswürdige Implementierung • Vertrauenswürdigkeit des Netzes • Sicherheitspolitik
Verbergen der internen Netzstruktur	Die Struktur des zu schützenden Netzes soll gegenüber dem unsicheren Netz verborgen werden. Es soll nicht sichtbar sein, ob im zu schützenden Netz 10, 100, 1.000 oder 10.000 IT-Systeme vorhanden sind.	• IP-Adressen	• Vertrauenswürdige Implementierung • Konzept des Verbergens der internen Netzstruktur (dual-homed Gateway)

→ **Inhalt**

- Ziele und Ergebnisse der Vorlesung
- Bedrohungen im Netz
- Sicherheitskonzept
- Kommunikationsmodell
- Firewall-Elemente
- Firewall-Konzepte
- **Zusammenfassung**

Firewall-Systeme

→ Zusammenfassung (1/2)

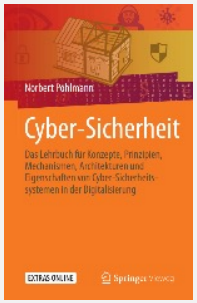
- Eine **100%tige Sicherheit** kann nicht erreicht werden:
  - Deshalb ist es zweckmäßig, die Betrachtung eines Firewall-Systems auf den Schwerpunkt der „**Unsicherheit**" zu legen.
  - Ziel muss es sein, diese **Rest-Unsicherheit zu minimieren**.
  - Denn durch die sinkende Zahl der Unsicherheiten steigt die Resistenz eines Firewall-Systems.
  - Unsicherheiten sind all diejenigen Zustände, welche zu illegalen oder unerwünschten Zuständen eines Firewall-Systems führen.
  - Auch hier muss einem bewusst sein, dass immer ein Restrisiko bestehen bleibt, das mit der Hilfe von weiteren – **modular zu ergänzenden – Sicherheitsmechanismen** wie Intrusion Detection, Antivirus-Konzepten und Verschlüsselung weiter reduziert werden muss, um so zu einer praktischen Sicherheit zu gelangen.

→ Zusammenfassung (2/2)

- Wichtig sind ebenso **periodische Audits und Revisionen** des Cyber-Sicherheitssystems sowie Überprüfungen der Sicherheitspolitik.

Anhang / Credits / Quellen

- **Cyber-Sicherheit**
  Das **Lehrbuch** für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung“, Springer Vieweg Verlag, Wiesbaden 2022
  https://norbert-pohlmann.com/cyber-sicherheit/



Vielen Dank fürs Ansehen!

- Fragen?

- Chat, Tutorium, Forum – Sie haben die Wahl!

Questions?