Umfassende Firewall-Systeme

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

Fachhochschule Gelsenkirchen

Inhalt

- **Sicherheitsziele bei der Umsetzung eines umfassenden Firewall-Systems**
- **Beschreibung der Sicherheitskomponenten und deren Ziele**
- **Bewertung der Sicherheitskomponenten**
- **Weiterentwicklung von Firewall-Systemen**

Inhalt

- **Sicherheitsziele bei der Umsetzung eines umfassenden Firewall-Systems**

- Beschreibung der Sicherheitskomponenten und deren Ziele

- Bewertung der Sicherheitskomponenten

- Weiterentwicklung von Firewall-Systemen

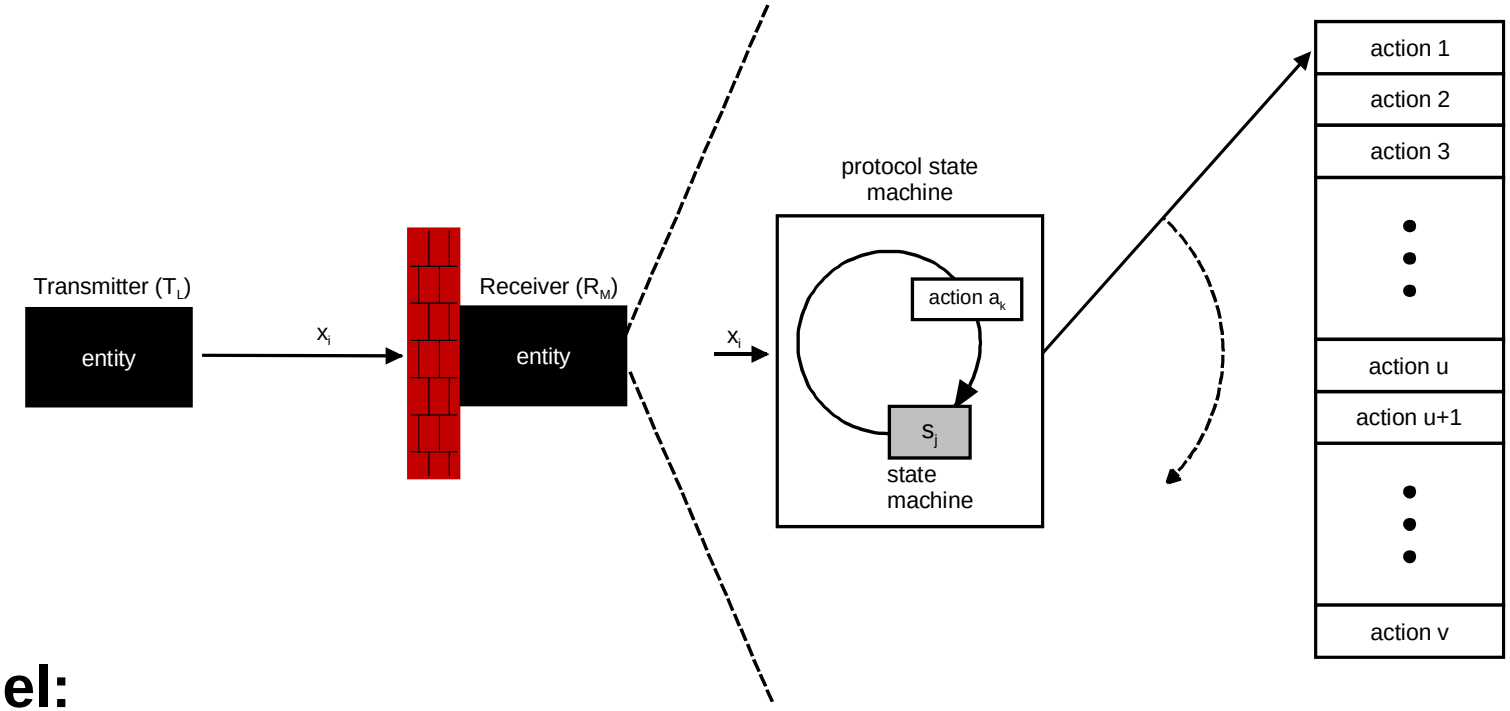
Sicherheitsziele bei der Umsetzung eines umfassenden Firewall-Systems

- **Alle Unsicherheiten mit größtmöglicher Wahrscheinlichkeit vollständig zu eliminieren**
- **Möglichst vielen Unsicherheiten mit passenden Sicherheitsmechanismen entgegen zu wirken, damit die Wahrscheinlichkeit eines Schadens auf eine praktisch nicht vorkommende Größe minimiert wird**
- **Unsicherheiten, die nicht verhindert werden können, zu erkennen, um im Angriffsfall angemessen zu reagieren**
- **Angriffe im Vorfeld zu erkennen, damit erst kein Schaden auftreten kann**

Inhalt

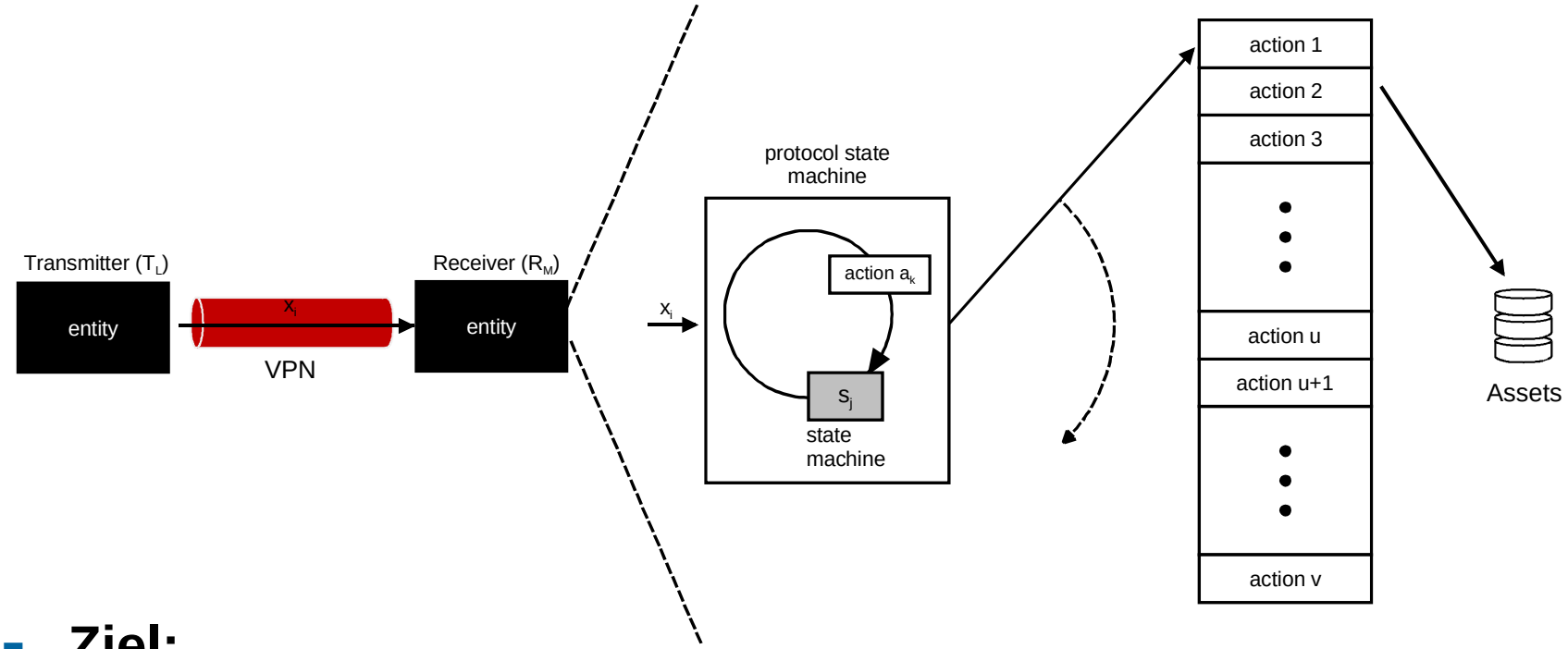
- Sicherheitsziele bei der Umsetzung eines umfassenden Firewall-Systems
- **Beschreibung der Sicherheitskomponenten und deren Ziele**
- Bewertung der Sicherheitskomponenten
- Weiterentwicklung von Firewall-Systemen

Zentrales High-level Firewall-System



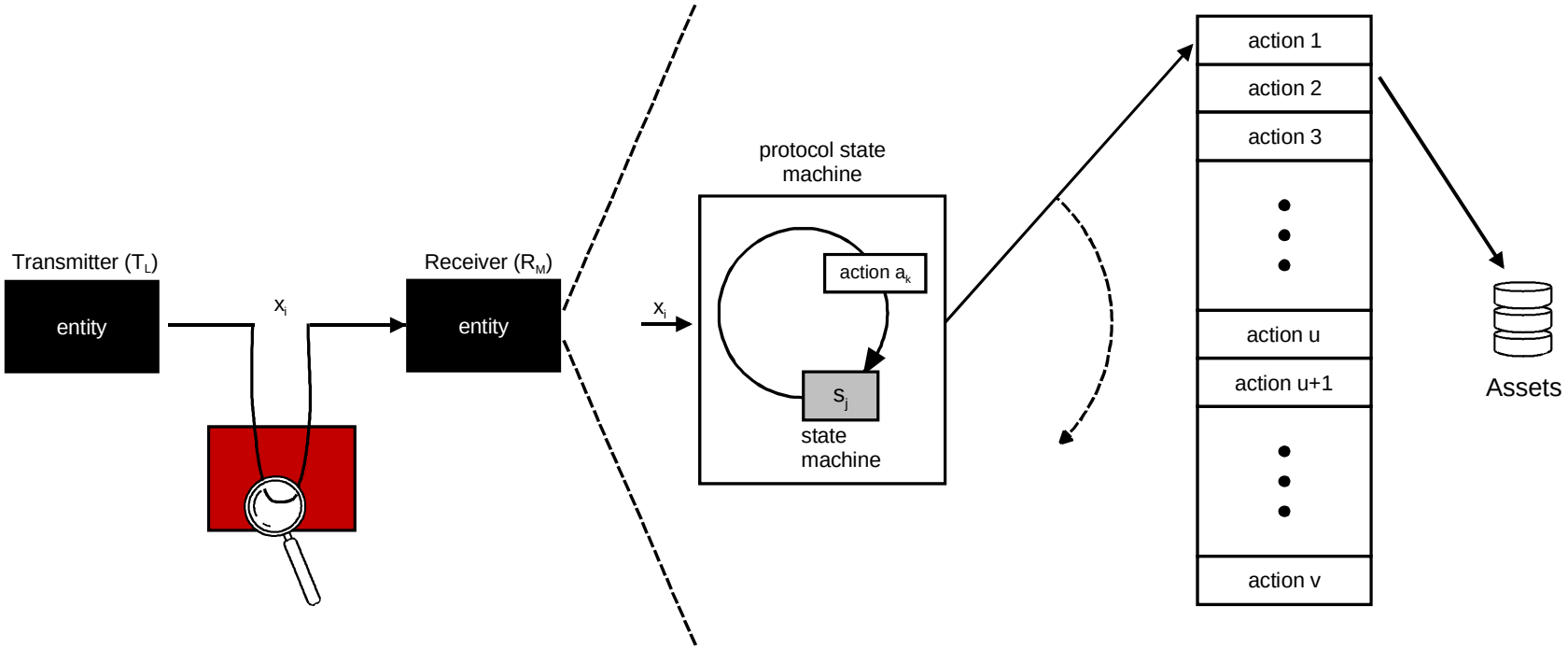
- **Ziel:**
  - analysiert, kontrolliert und reglementiert die Kommunikation entsprechend einer Sicherheitspolitik
  - protokolliert sicherheitsrelevante Ereignisse
  - alarmiert bei erheblichen Verstößen

Verschlüsselung - VPNs oder SSL (TLS)
→ Analogie zum Sicherheitstransporter



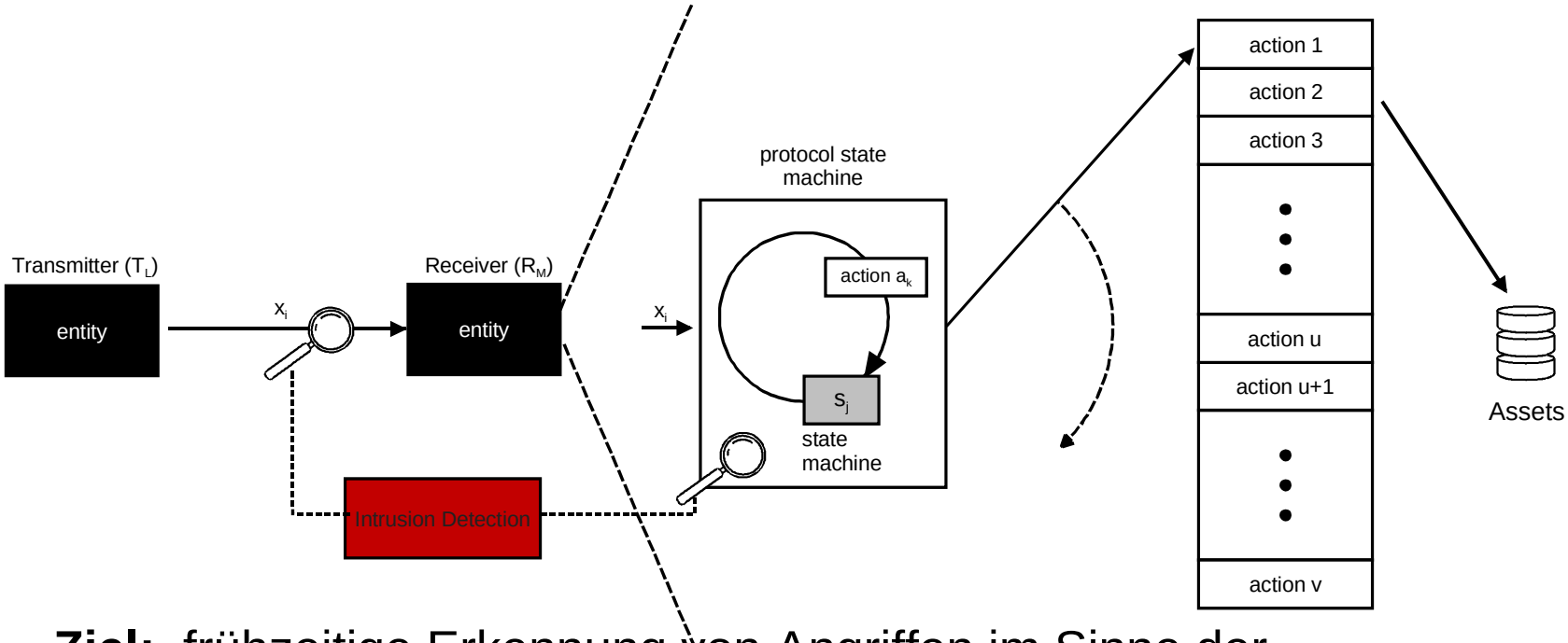
- **Ziel:**
  - **Vertraulichkeit der Protokollelemente**
  - Verhinderung von Trittbrettfahrern
  - Verhinderung einer gezielten Manipulation von Protokollelementen

Zentraler Virenscanner
→ Analogie zur zentralen Poststelle



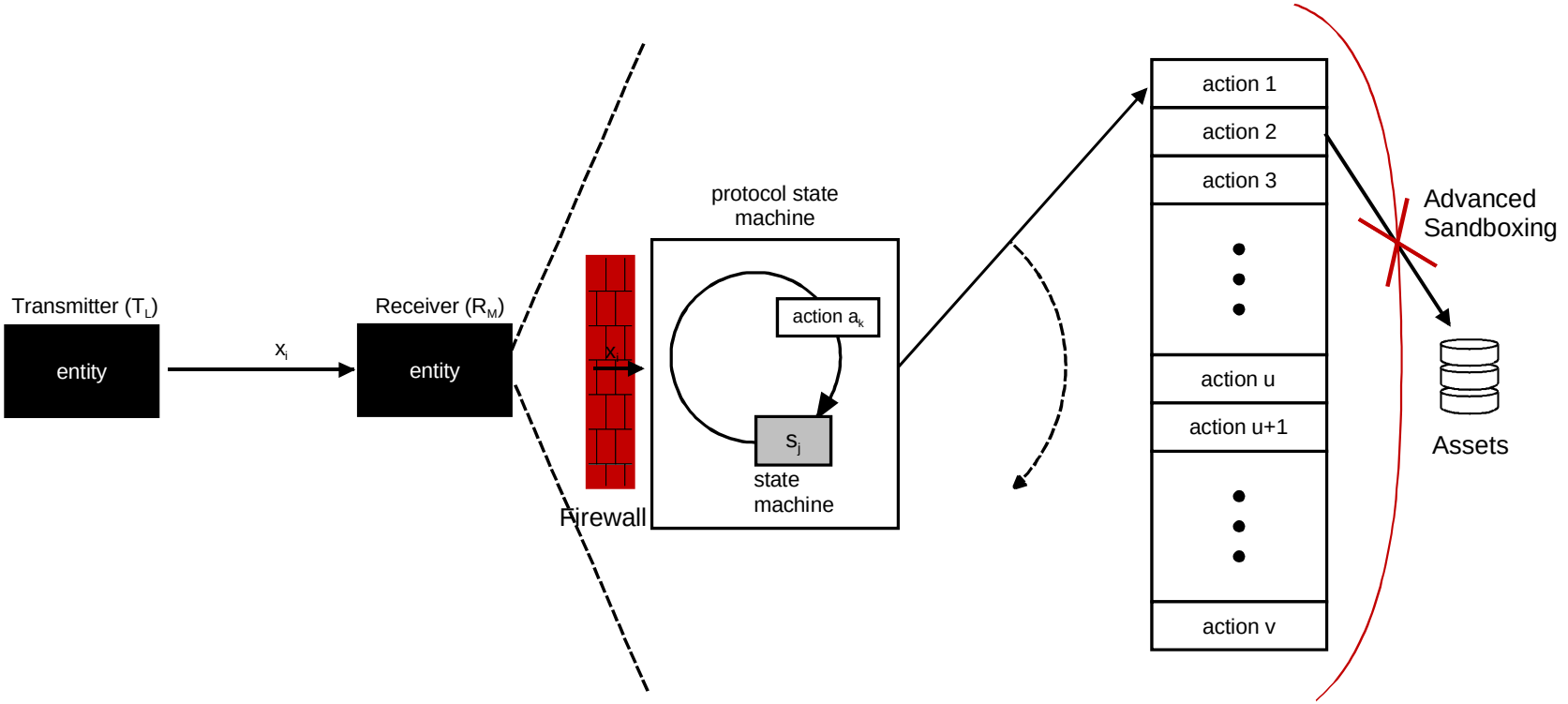
- **Ziel:**
  - Erkennen von Viren an zentraler Stelle
  - Verhindern, dass Viren in die Organisation übertragen werden
  - Protokollieren der gefundenen Viren und Alarmierung

Intrusion Detection
→ Analogie zur Videoüberwachung



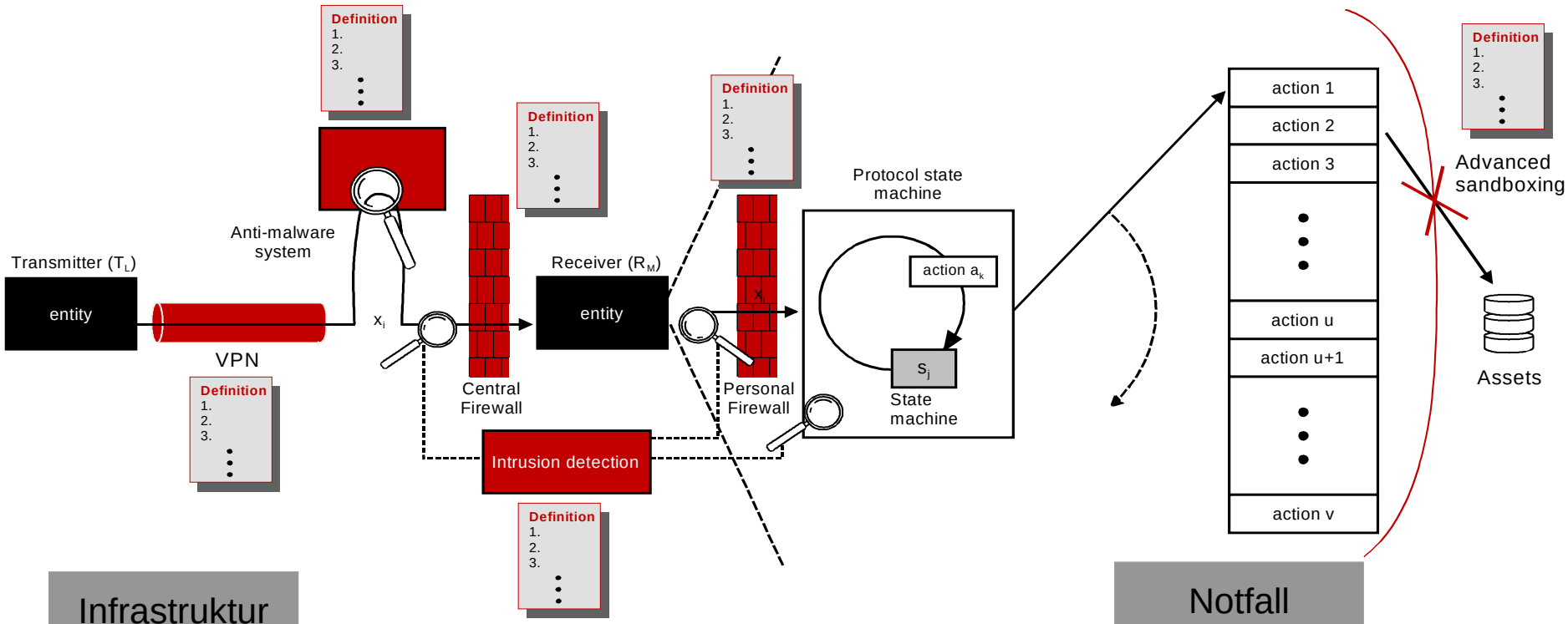
- **Ziel:** frühzeitige Erkennung von Angriffen im Sinne der Schadensverhinderung
- ***Sicherheitsmechanismen***
  - Mißbrauchserkennung (Fehler-Signaturen)
  - Erkennung von Anomalien
  - Protokollierung und Berichtserstattung

Personal Firewall



- **Ziel:** Schaden verhindern
- ***Sicherheitsmechanismen:***
  - Firewall-Funktionalitäten
  - Advanced Sandboxing

Nicht-technische Sicherheitsmaßnahmen
Sicherheitspolitik, sicherer Betrieb



Infrastruktur

Raum mit Zugangskontrolle

Unterbrechungsfreie Stromversorgung

Notfall

Definition der Verfügbarkeits-anforderungen

Entwicklung und Testen von Backup Möglichkeiten, usw.

Organisation

Festlegung der Verantwortung und Zugriffsrechte

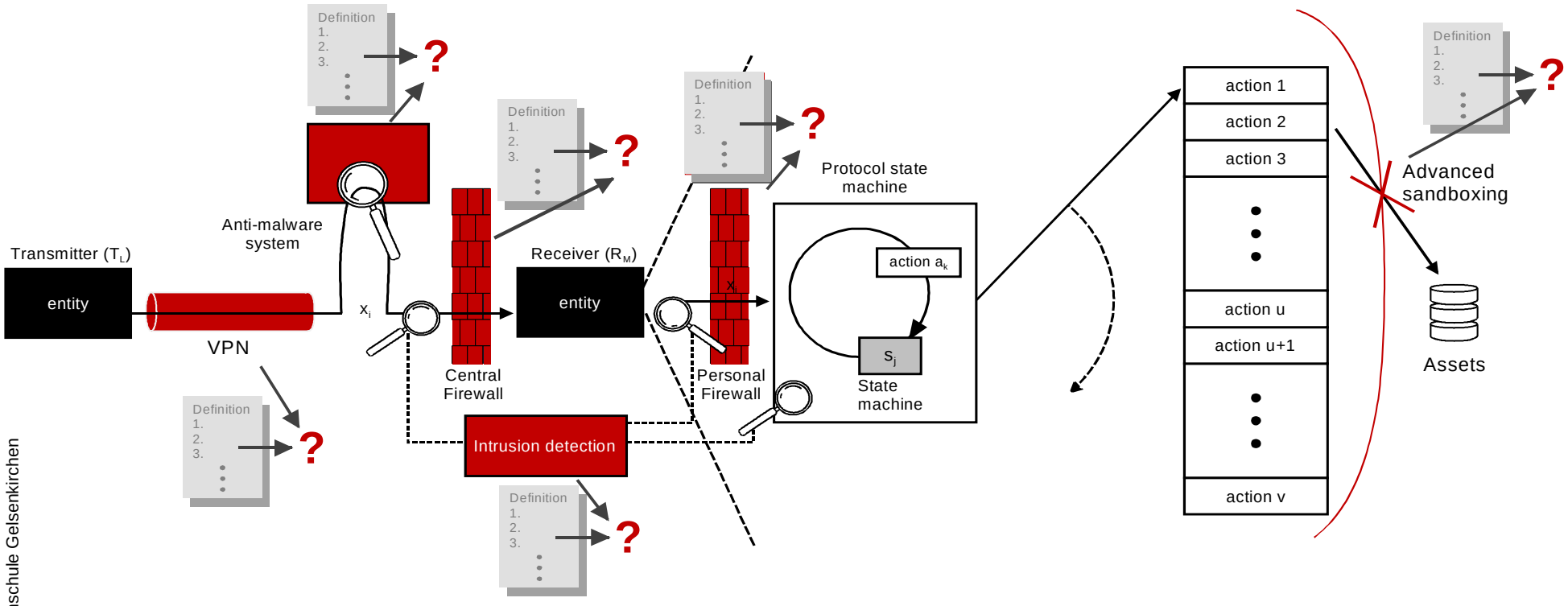
Kontrolle der Protokolldaten, etc.

Personal

Anweisung, Aufklärung, Sensibilisierung der Benutzer

Schulungen zum Thema Sicherheit, etc.

Audits



Infrastruktur ?

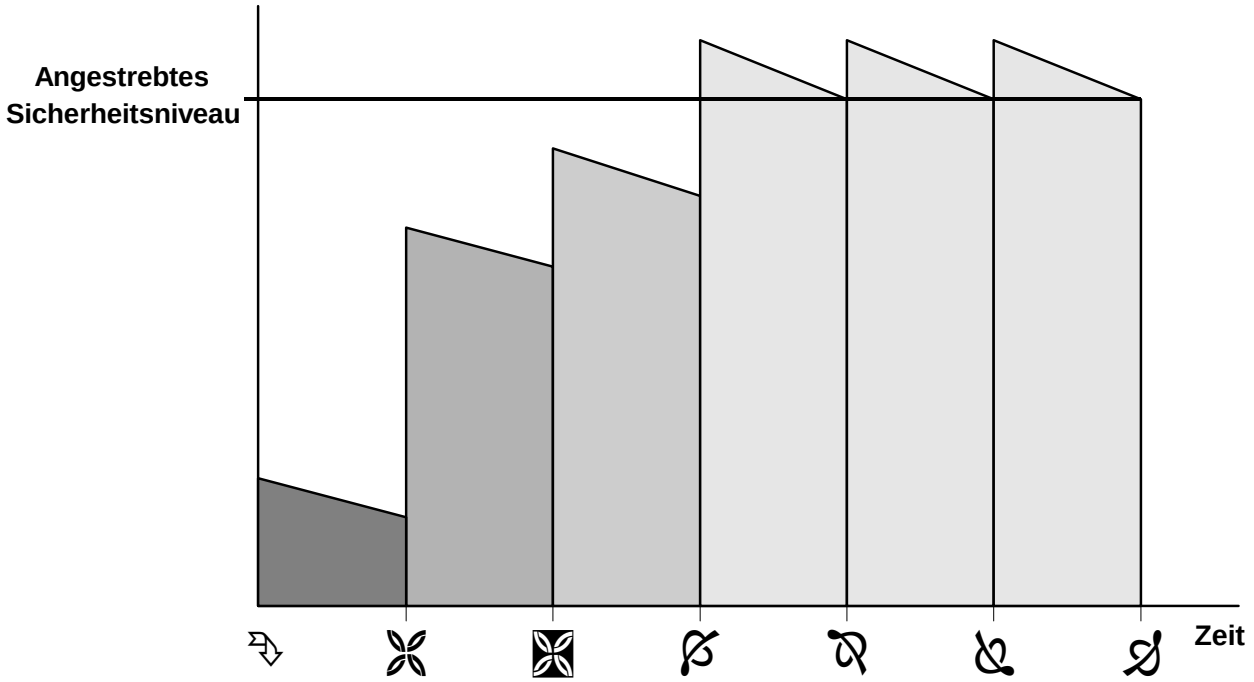
Organisation ?

Personal ?

Notfall ?

Audits, Revision

- **Ziel:**
  - Entdeckung von Schwachstellen und Sicherheitslücken
  - Permanente Abstimmung zwischen den Sicherheitsrichtlinien und deren praktischer Umsetzung
  - Erreichen eines stabilen Sicherheitsniveaus



Vertrauenswürdigkeit

- **Wirksamkeit**
  - Wirkung der Firewall-Sicherheitsmechanismen gegen die tatsächlichen Bedrohungen
  - Stärke der Sicherheitsmechanismen (zugrundeliegende Algorithmen, Prinzipien und Eigenschaften, z.B. niedrig, mittel und hoch)
- **Korrektheit**
  - Beurteilung der „richtigen“ Implementierung
  - Bewertung des Vertrauens in die Implementierung (Trap Door)

Evaluierung und Zertifizierung

Sicherheitspolitik

- **Aspekte, die definiert sein müssen:**
  - Festlegung des Sicherheitsziels einer Organisation
  - Definition der zu schützenden Ressourcen
  - Definition der zu schützenden Werte (Daten)
  - Einschätzung des Schutzbedarfs und des Angriffspotentials
  - Festlegung der Dienste und Anwendungen, die erlaubt werden sollen
  - Festlegung der Benutzer, die über das Firewall-System kommunizieren sollen, und deren Kommunikationsprofil

Sicherer Betrieb

- **Voraussetzungen für den sicheren Betrieb:**
  - Einbindung des Firewall-Systems in das IT-Konzept der Organisation
  - Der Firewall Betrieb muß auf eine umfassende Sicherheitspolitik aufgebaut sein
  - Korrekte Installation
  - Korrekte Administration

Inhalt

- Sicherheitsziele bei der Umsetzung eines umfassenden Firewall-Systems
- Beschreibung der Sicherheitskomponenten und deren Ziele
- Bewertung der Sicherheitskomponenten
- **Weiterentwicklung von Firewall-Systemen**

Umfassendes Firewallsystem 1/3 -

→ Wiederholen/Verzögern von Protokollelementen

Angriffsart		High-level Security Firewall-System	Verschlüsselung	Anti-Malware-System	Intrusion Detection Systeme	Personal Firewall	nichttechnische Sicherheitsmaßnahmen	Vertrauenswürdigkeit	Audits	Sicherheitspolitik	sicherer Betrieb
	▪ Die Nutzung von high-level Security Firewall-Systemen (Rechteverwaltung) und Verschlüsselung helfen hier eine große Wirkung zu erzielen. ▪ Die Personal Firewall bietet hier einen Grundschutz für die Rechnersysteme. ▪ *Vertrauenswürdigkeit, Audits, Sicherheitspolitik und sicherer Betrieb sind die Basis.*										
Angriffe durch einen Dritten	Wiederholen o. Verzögern von Protokollelementen	◕	◕	○	○	◔	○	◆	◆	◆	◆
	Einfügen o. Löschen von Daten in den Protokollelementen	◕	●	○	○	◔	○	◆	◆	◆	◆
	Modifikation der Daten in den Protokollelementen	◕	●	○	○	○	○	◆	◆	◆	◆
	Boykott des Receivers	◕	○	○	◑	◔	◕	◆	◆	◆	◆
	Trittbrettfahrer	◑	●	○	○	◔	○	◆	◆	◆	◆
	Empfangen von Malware (Viren, Würmer, Trojanische Pferde,…)	◕	○	◕	○	●	◕	◆	◆	◆	◆

→ Die Verschlüsselung erhöht die Schutzwirkung bei Angriffen durch Dritte deutlich !

●	sehr große Wirkung	◕	große Wirkung	◑	Wirkung
◔	wenig Wirkung	○	keine Wirkung	◆	Grundlage f.d. Wirkung

Umfassendes Firewallsystem 1/3 -

→ Einfügen/Löschen von Daten in Protokollelementen

Angriffsart	▪ Die Nutzung von high-level Security Firewall-Systemen (Rechteverwaltung) hat eine große Wirkung auf diesen Angriff. ▪ Die Verschlüsselung hat eine sehr große Wirkung auf diesen Angriff. ▪ Die Personal Firewall bietet einen Grundschutz für die Rechnersysteme. ▪ *Vertrauenswürdigkeit, Audits, Sicherheitspolitik und sicherer Betrieb sind die Basis.*	High-level Security Firewall-System	Verschlüsselung	Anti-Malware-System	Intrusion Detection Systeme	Personal Firewall	nichttechnische Sicherheitsmaßnahmen	Vertrauenswürdigkeit	Audits	Sicherheitspolitik	sicherer Betrieb
Angriffe durch einen Dritten	Wiederholen o. Verzögern von Protokollelementen	◕	◕	○	○	◔	○	◆	◆	◆	◆
	Einfügen o. Löschen von Daten in den Protokollelementen	◕	●	○	○	◔	○	◆	◆	◆	◆
	Modifikation der Daten in den Protokollelementen	◕	●	○	○	○	○	◆	◆	◆	◆
	Boykott des Receivers	◕	○	○	◑	◔	◕	◆	◆	◆	◆
	Trittbrettfahrer	◑	●	○	○	◔	○	◆	◆	◆	◆
	Empfangen von Malware (Viren, Würmer, Trojanische Pferde,…)	◕	○	◕	○	●	◕	◆	◆	◆	◆

→ Die Verschlüsselung erhöht die Schutzwirkung bei Angriffen durch Dritte deutlich !

●	sehr große Wirkung	◕	große Wirkung	◑	Wirkung
◔	wenig Wirkung	○	keine Wirkung	◆	Grundlage f.d. Wirkung

Umfassendes Firewallsystem 1/3 -

→ Modifikation der Daten in Protokollelementen

Angriffsart		High-level Security Firewall-System	Verschlüsselung	Anti-Malware-System	Intrusion Detection Systeme	Personal Firewall	nichttechnische Sicherheitsmaßnahmen	Vertrauenswürdigkeit	Audits	Sicherheitspolitik	sicherer Betrieb
	▪ Die Nutzung von high-level Security Firewall-Systemen (Rechteverwaltung) hat eine große Wirkung auf diesen Angriff. ▪ Die Verschlüsselung hat eine sehr große Wirkung auf diesen Angriff. ▪ *Vertrauenswürdigkeit, Audits, Sicherheitspolitik und sicherer Betrieb sind die Basis.*										
Angriffe durch einen Dritten	Wiederholen o. Verzögern von Protokollelementen	◕	◕	○	○	◔	○	◆	◆	◆	◆
	Einfügen o. Löschen von Daten in den Protokollelementen	◕	●	○	○	◔	○	◆	◆	◆	◆
	Modifikation der Daten in den Protokollelementen	◕	●	○	○	○	○	◆	◆	◆	◆
	Boykott des Receivers	◕	○	○	◑	◔	◕	◆	◆	◆	◆
	Trittbrettfahrer	◑	●	○	○	◔	○	◆	◆	◆	◆
	Empfangen von Malware (Viren, Würmer, Trojanische Pferde,…)	◕	○	◕	○	●	◕	◆	◆	◆	◆

→ Die Verschlüsselung erhöht die Schutzwirkung bei Angriffen durch Dritte deutlich !

●	sehr große Wirkung	◕	große Wirkung	◑	Wirkung
◔	wenig Wirkung	○	keine Wirkung	◆	Grundlage f.d. Wirkung

Umfassendes Firewallsystem 1/3 -

→ Boykott des Receivers

Angriffsart	▪ Das high-level Security Firewall-System (dual-homed AG) hat ein große Wirkung. ▪ Intrusion Detection Systeme -> Angriff wird schnell erkannt -> schnelle Reaktion (CERT,...) ▪ Die Personal Firewall bietet hier einen Grundschutz für die Rechnersysteme. ▪ DDoS-Angriffe zeigen, dass hier eine weltweite Zusammenarbeit sinnvoll ist (Organisation). ▪ *Vertrauenswürdigkeit, Audits, Sicherheitspolitik und sicherer Betrieb sind die Basis.*	High-level Security Firewall-System	Verschlüsselung	Anti-Malware-System	Intrusion Detection Systeme	Personal Firewall	nichttechnische Sicherheitsmaßnahmen	Vertrauenswürdigkeit	Audits	Sicherheitspolitik	sicherer Betrieb
Angriffe durch einen Dritten	Wiederholen o. Verzögern von Protokollelementen	◕	◕	○	○	◔	○	◆	◆	◆	◆
	Einfügen o. Löschen von Daten in den Protokollelementen	◕	●	○	○	◔	○	◆	◆	◆	◆
	Modifikation der Daten in den Protokollelementen	◕	●	○	○	○	○	◆	◆	◆	◆
	Boykott des Receivers	◕	○	○	◑	◔	◕	◆	◆	◆	◆
	Trittbrettfahrer	◑	●	○	○	◔	○	◆	◆	◆	◆
	Empfangen von Malware (Viren, Würmer, Trojanische Pferde,...)	◕	○	◕	○	●	◕	◆	◆	◆	◆

●	sehr große Wirkung	◕	große Wirkung	◑	Wirkung
◔	wenig Wirkung	○	keine Wirkung	◆	Grundlage f.d. Wirkung

Umfassendes Firewallsystem 1/3 -

→ Trittbrettfahrer

Angriffsart		High-level Security Firewall-System	Verschlüsselung	Anti-Malware-System	Intrusion Detection Systeme	Personal Firewall	nichttechnische Sicherheitsmaßnahmen	Vertrauenswürdigkeit	Audits	Sicherheitspolitik	sicherer Betrieb
	▪ Dieser Angriff muß in Zusammenhang mit dem Angriff "Vortäuschen einer falschen Identität (Maskerade-Angriff)" betrachtet werden, wo die **starke Authentikation** eine wichtige Rolle spielt (high-level Security FireWall). ▪ Hier hilft der Sicherheitsmechanismus Verschlüsselung besonders gut. ▪ Die Personal Firewall bietet hier einen Grundschutz für die Rechnersysteme. ▪ *Vertrauenswürdigkeit, Audits, Sicherheitspolitik und sicherer Betrieb sind die Basis.*										
Angriffe durch einen Dritten	Wiederholen o. Verzögern von Protokollelementen	◕	◕	○	○	◔	○	◆	◆	◆	◆
	Einfügen o. Löschen von Daten in den Protokollelementen	◕	●	○	○	◔	○	◆	◆	◆	◆
	Modifikation der Daten in den Protokollelementen	◕	●	○	○	○	○	◆	◆	◆	◆
	Boykott des Receivers	◕	○	○	◑	◔	◕	◆	◆	◆	◆
	Trittbrettfahrer	◑	●	○	○	◔	○	◆	◆	◆	◆
	Empfangen von Malware (Viren, Würmer, Trojanische Pferde,…)	◕	○	◕	○	●	◕	◆	◆	◆	◆

→ Die Verschlüsselung erhöht die Schutzwirkung bei Angriffen durch Dritte deutlich !

●	sehr große Wirkung	◕	große Wirkung	◑	Wirkung
◔	wenig Wirkung	○	keine Wirkung	◆	Grundlage f.d. Wirkung

Umfassendes Firewallsystem 1/3 -

→ Empfangen von Malware

Angriffsart		High-level Security Firewall-System	Verschlüsselung	Anti-Malware-System	Intrusion Detection Systeme	Personal Firewall	nichttechnische Sicherheitsmaßnahmen	Vertrauenswürdigkeit	Audits	Sicherheitspolitik	sicherer Betrieb
	▪ Der zentrale Virenscanner kann für alle Rechnersysteme zentral eine große Wirkung erzielen. ▪ Durch die Personal Firewalls kann dezentral ein möglicher Schaden verhindert werden, was eine sehr große Wirkung gegen diesen Angriff darstellt. ▪ Sensibilisierung, Aufklärung und Schulung haben eine große Wirkung ▪ *Vertrauenswürdigkeit, Audits, Sicherheitspolitik und sicherer Betrieb sind die Basis.*										
Angriffe durch einen Dritten	Wiederholen o. Verzögern von Protokollelementen	◕	◕	○	○	◔	○	◆	◆	◆	◆
	Einfügen o. Löschen von Daten in den Protokollelementen	◕	●	○	○	◔	○	◆	◆	◆	◆
	Modifikation der Daten in den Protokollelementen	◕	●	○	○	○	○	◆	◆	◆	◆
	Boykott des Receivers	◕	○	○	◑	◔	◕	◆	◆	◆	◆
	Trittbrettfahrer	◑	●	○	○	◔	○	◆	◆	◆	◆
	Empfangen von Malware (Viren, Würmer, Trojanische Pferde,…)	◕	○	◕	○	●	◕	◆	◆	◆	◆

●	sehr große Wirkung	◕	große Wirkung	◑	Wirkung
◔	wenig Wirkung	○	keine Wirkung	◆	Grundlage f.d. Wirkung

Umfassendes Firewallsystem 2/3 -
→ Aufbau und Nutzung von Kommunikationsverbindungen

- Bei diesem Angriff hat ein High-level Security Firewall-Systemen eine sehr große Wirkung.
- Das Intrusion Detection System kann Unregelmäßigkeiten erkennen und somit möglicherweise im Vorfeld Schäden reduzieren.
- Die Personal Firewall bietet hier einen Grundschutz für die Rechnersysteme.
- *Vertrauenswürdigkeit, Audits, Sicherheitspolitik und sicherer Betrieb sind die Basis.*

Angriffsart		High-level Security Firewall-System	Verschlüsselung	Anti-Malware-System	Intrusion Detection Systeme	Personal Firewall	nichttechnische Sicherheitsmaßnahmen	Vertrauenswürdigkeit	Audits	Sicherheitspolitik	sicherer Betrieb
Angriffe durch den Trans-mitter	Aufbau u. Nutzung von Kommunikationsverbindungen	●	○	○	◑	◔	○	◆	◆	◆	◆
	Nutzung von Kommunikationsprotollen und –diensten	●	○	○	◑	◔	○	◆	◆	◆	◆
	Vortäuschen einer falschen Identität (Maskerade-Angriff)	●	○	○	◑	◔	○	◆	◆	◆	◆
	Java, ActiveX, ... Angriffe	◕	○	○	◑	●	◕	◆	◆	◆	◆
	falsche Konfiguration/Implementierungsfehler	●	○	○	○	◔	○	◆	◆	◆	◆
	Leugnen der Kommunikationsbeziehung	◑	○	○	○	○	◕	◆	◆	◆	◆

●	sehr große Wirkung	◕	große Wirkung	◑	Wirkung
◔	wenig Wirkung	○	keine Wirkung	◆	Grundlage f.d. Wirkung

Umfassendes Firewallsystem 2/3 -
→ Nutzung von Protokollen und Diensten

Angriffsart	▪ Bei diesem Angriff hat ein High-level Security Firewall-System (Rechtever-waltung) eine sehr große Wirkung. ▪ Das Intrusion Detection System kann Unregelmäßigkeiten erkennen und somit möglicherweise im Vorfeld Schäden reduzieren. ▪ Die Personal Firewall bietet hier einen Grundschutz für die Rechnersysteme. ▪ *Vertrauenswürdigkeit, Audits, Sicherheitspolitik und sicherer Betrieb sind die Basis*.	High-level Security Firewall-System	Verschlüsselung	Anti-Malware-System	Intrusion Detection Systeme	Personal Firewall	nichttechnische Sicherheitsmaßnahmen	Vertrauenswürdigkeit	Audits	Sicherheitspolitik	sicherer Betrieb
Angriffe durch den Trans-mitter	Aufbau u. Nutzung von Kommunikationsverbindungen	●	○	○	◑	◔	○	◆	◆	◆	◆
	Nutzung von Kommunikationsprotollen und –diensten	●	○	○	◑	◔	○	◆	◆	◆	◆
	Vortäuschen einer falschen Identität	●	○	○	◑	◔	○	◆	◆	◆	◆
	Java, ActiveX, ... Angriffe	◕	○	○	◑	●	◕	◆	◆	◆	◆
	falsche Konfiguration/Implementierungsfehler	●	○	○	○	◔	○	◆	◆	◆	◆
	Leugnen der Kommunikationsbeziehung	◑	○	○	○	○	◕	◆	◆	◆	◆

●	sehr große Wirkung	◕	große Wirkung	◑	Wirkung
◔	wenig Wirkung	○	keine Wirkung	◆	Grundlage f.d. Wirkung

Umfassendes Firewallsystem 2/3 -
→ Vortäuschen einer falschen Identität

Angriffsart		High-level Security Firewall-System	Verschlüsselung	Anti-Malware-System	Intrusion Detection Systeme	Personal Firewall	nichttechnische Sicherheitsmaßnahmen	Vertrauenswürdigkeit	Audits	Sicherheitspolitik	sicherer Betrieb
	▪ Der starke Authentikationsmechanismus hat eine sehr große Wirkung. Angriff "Trittbrettfahren" -> Verschlüsselung spielt eine wichtige Rolle. ▪ Intrusion Detection System -> erkennt Unregelmäßigkeiten -> Schäden möglicherweise im Vorfeld reduzieren. ▪ Die Personal Firewall bietet hier einen Grundschutz für die Rechnersysteme. ▪ *Vertrauenswürdigkeit, Audits, Sicherheitspolitik und sicherer Betrieb sind die Basis.*										
Angriffe durch den Trans-mitter	Aufbau u. Nutzung von Kommunikationsverbindungen	●	○	○	◑	◔	○	◆	◆	◆	◆
	Nutzung von Kommunikationsprotollen und –diensten	●	○	○	◑	◔	○	◆	◆	◆	◆
	Vortäuschen einer falschen Identität	●	○	○	◑	◔	○	◆	◆	◆	◆
	Java, ActiveX, ... Angriffe	◕	○	○	◑	●	◕	◆	◆	◆	◆
	falsche Konfiguration/Implementierungsfehler	●	○	○	○	◔	○	◆	◆	◆	◆
	Leugnen der Kommunikationsbeziehung	◑	○	○	○	○	◕	◆	◆	◆	◆

●	sehr große Wirkung	◕	große Wirkung	◑	Wirkung
◔	wenig Wirkung	○	keine Wirkung	◆	Grundlage f.d. Wirkung

Umfassendes Firewallsystem 2/3 -
→ Java, Active X, ... Angriffe

Angriffsart		High-level Security Firewall-System	Verschlüsselung	Anti-Malware-System	Intrusion Detection Systeme	Personal Firewall	nichttechnische Sicherheitsmaßnahmen	Vertrauenswürdigkeit	Audits	Sicherheitspolitik	sicherer Betrieb
	▪ Durch entsprechende Mechanismen in einen high-level Firewall-System (z.B. Applet-Filter oder Java Proxy) kann eine große Wirkung zentral erzielt werden. ▪ Die Personal Firewalls kann einen möglichen Schaden verhindern, was eine sehr große Wirkung darstellt. ▪ Intrusion Detection System -> erkennt Unregelmäßigkeiten -> Schäden möglicherweise im Vorfeld reduzieren. ▪ *Vertrauenswürdigkeit, Audits, Sicherheitspolitik und sicherer Betrieb sind die Basis.*										
Angriffe durch den Trans-mitter	Aufbau u. Nutzung von Kommunikationsverbindungen	●	○	○	◑	◔	○	◆	◆	◆	◆
	Nutzung von Kommunikationsprotollen und –diensten	●	○	○	◑	◔	○	◆	◆	◆	◆
	Vortäuschen einer falschen Identität	●	○	○	◑	◔	○	◆	◆	◆	◆
	Java, ActiveX, ... Angriffe	◕	○	○	◑	●	◕	◆	◆	◆	◆
	falsche Konfiguration/Implementierungsfehler	●	○	○	○	◔	○	◆	◆	◆	◆
	Leugnen der Kommunikationsbeziehung	◑	○	○	○	○	◕	◆	◆	◆	◆

●	sehr große Wirkung	◕	große Wirkung	◑	Wirkung
◔	wenig Wirkung	○	keine Wirkung	◆	Grundlage f.d. Wirkung

Umfassendes Firewallsystem 2/3 -
→ Falsche Konfiguration/Implementierungsfehler

- Durch die Nutzung eines High-level Security Firewall-Systems, insbesondere die Einbindung mehrere unterschiedlicher Firewall-Elemente (PF, AG, ...), kann eine sehr große Wirkung erzielt werden.
- Die Personal Firewall bietet hier einen Grundschutz für die Rechnersysteme.
- *Vertrauenswürdigkeit, Audits, Sicherheitspolitik und sicherer Betrieb sind die Basis*.

Angriffsart	High-level Security Firewall-System	Verschlüsselung	Anti-Malware-System	Intrusion Detection Systeme	Personal Firewall	nichttechnische Sicherheitsmaßnahmen	Vertrauenswürdigkeit	Audits	Sicherheitspolitik	sicherer Betrieb
Angriffe durch den Trans-mitter										
Aufbau u. Nutzung von Kommunikationsverbindungen	●	○	○	◑	◔	○	◆	◆	◆	◆
Nutzung von Kommunikationsprotollen und –diensten	●	○	○	◑	◔	○	◆	◆	◆	◆
Vortäuschen einer falschen Identität	●	○	○	◑	◔	○	◆	◆	◆	◆
Java, ActiveX, ... Angriffe	◕	○	○	◑	●	◕	◆	◆	◆	◆
falsche Konfiguration/Implementierungsfehler	●	○	○	○	◔	○	◆	◆	◆	◆
Leugnen der Kommunikationsbeziehung	◑	○	○	○	○	◕	◆	◆	◆	◆

●	sehr große Wirkung	◕	große Wirkung	◑	Wirkung
◔	wenig Wirkung	○	keine Wirkung	◆	Grundlage f.d. Wirkung

Umfassendes Firewallsystem 2/3

→ Leugnen der Kommunikationsbeziehung

- Hier spielt die Protokollierung eine wichtige Rolle. Für die Kommunikation mit bekannten Kommunikationspartnern kann hier eine Wirkung erzielt werden.
- Im Bereich externer Services kann die Beweissicherung durch Protokollierung sogar in den Servicevertrag aufgenommen werden.
- *Vertrauenswürdigkeit, Audits, Sicherheitspolitik und sicherer Betrieb sind die Basis.*

Angriffsart		High-level Security Firewall-System	Verschlüsselung	Anti-Malware-System	Intrusion Detection Systeme	Personal Firewall	nichttechnische Sicherheitsmaßnahmen	Vertrauenswürdigkeit	Audits	Sicherheitspolitik	sicherer Betrieb
Angriffe durch den Trans-mitter	Aufbau u. Nutzung von Kommunikationsverbindungen	●	○	○	◑	◔	○	◆	◆	◆	◆
	Nutzung von Kommunikationsprotollen und –diensten	●	○	○	◑	◔	○	◆	◆	◆	◆
	Vortäuschen einer falschen Identität	●	○	○	◑	◔	○	◆	◆	◆	◆
	Java, ActiveX, ... Angriffe	◕	○	○	◑	●	◕	◆	◆	◆	◆
	falsche Konfiguration/Implementierungsfehler	●	○	○	○	◔	○	◆	◆	◆	◆
	Leugnen der Kommunikationsbeziehung	◑	○	○	○	○	◕	◆	◆	◆	◆

●	sehr große Wirkung	◕	große Wirkung	◑	Wirkung
◔	wenig Wirkung	○	keine Wirkung	◆	Grundlage f.d. Wirkung

Umfassendes Firewallsystem 3/3 -
→ Social Engineering

- Bei diesem Angriff haben die nichttechnischen Sicherheits-mechanismen wie Aufklärung und Schulung eine sehr hohe Wirkung.
- *Audits, Sicherheitspolitik und sicherer Betrieb sind die Basis.*

Angriffsart		High-level Security Firewall-System	Verschlüsselung	Anti-Malware-System	Intrusion Detection Systeme	Personal Firewall	nichttechnische Sicherheitsmaßnahmen	Vertrauenswürdigkeit	Audits	Sicherheitspolitik	sicherer Betrieb
Vorbe-reitung für Angriffe	Social Engieering	○	○	○	○	○	●	○	◆	◆	◆
	Analyse mit Hilfe von Scannerprogrammen	●	○	○	◑	○	○	◆	◆	◆	◆
	Manipulation des Firew all-Systems	●	○	○	◑	○	◕	◆	●	◆	◆
	Einbau einer Trap-Door	○	○	○	◔	○	○	●	○	○	○
	Nutzung einer falschen Konfiguration des Firew all-Systems	●	○	○	◑	○	◕	○	●	◆	◆
	Nutzung von Implementierungsfehlers des Firew all-Systems	●	○	○	◑	○	◕	◆	●	◆	◆
	interne Angriffe	○	○	○	◕	●	◕	○	◔	◆	◆

●	sehr große Wirkung	◕	große Wirkung	◑	Wirkung
◔	wenig Wirkung	○	keine Wirkung	◆	Grundlage f.d. Wirkung

Umfassendes Firewallsystem 3/3 -
→ Analyse mit Hilfe von Scannerprogrammen

Angriffsart		High-level Security Firewall-System	Verschlüsselung	Anti-Malware-System	Intrusion Detection Systeme	Personal Firewall	nichttechnische Sicherheitsmaßnahmen	Vertrauenswürdigkeit	Audits	Sicherheitspolitik	sicherer Betrieb
	▪ Dieser Angriff kann durch die Nutzung eines High-level Security Firewall-Systems (besonders dual-homed Application-Gateways) verhindert werden. ▪ Durch die Verwendung von Intrusion Detection Systemen kann dieser Angriff erkannt und entsprechende Gegenmaßnahmen eingeleitet werden. ▪ *Vertrauenswürdigkeit, Audits, Sicherheitspolitik und sicherer Betrieb sind die Basis*.										
Vorbe-reitung für Angriffe	Social Engieering	○	○	○	○	○	●	○	◆	◆	◆
	Analyse mit Hilfe von Scannerprogrammen	●	○	○	◑	○	○	◆	◆	◆	◆
	Manipulation des Firew all-Systems	●	○	○	◑	○	◕	◆	●	◆	◆
	Einbau einer Trap-Door	○	○	○	◔	○	○	●	○	○	○
	Nutzung einer falschen Konfiguration des Firew all-Systems	●	○	○	◑	○	◕	○	●	◆	◆
	Nutzung von Implementierungsfehlers des Firew all-Systems	●	○	○	◑	○	◕	◆	●	◆	◆
	interne Angriffe	○	○	○	◕	●	◕	○	◔	◆	◆

●	sehr große Wirkung	◕	große Wirkung	◑	Wirkung
◔	wenig Wirkung	○	keine Wirkung	◆	Grundlage f.d. Wirkung

Umfassendes Firewallsystem 3/3 -
→ Manipulation des Firewall-Systems

Angriffsart		High-level Security Firewall-System	Verschlüsselung	Anti-Malware-System	Intrusion Detection Systeme	Personal Firewall	nichttechnische Sicherheitsmaßnahmen	Vertrauenswürdigkeit	Audits	Sicherheitspolitik	sicherer Betrieb
	▪ Ein high-level Security Firewall-System verhindert diesen Angriff: sicheres Designkonzept, eigene Schutzmecha-nismen, separates und zentrales Security Management, versch. Firewall-Elemente. ▪ Durch die Verwendung von Intrusion Detection Systemen kann dieser Angriff erkannt werden. ▪ Durch infrastrukturelle Sicherheitsmaß-nahmen, wie z.B. zugangsgesicherter Raum, ist eine große Wirkung zu erzielen ▪ Durch regelmäßige Audits kann ein Schaden verhindert werden.										
Vorbe-reitung für Angriffe	Social Engieering	○	○	○	○	○	●	○	◆	◆	◆
	Analyse mit Hilfe von Scannerprogrammen	●	○	○	◑	○	○	◆	◆	◆	◆
	Manipulation des Firew all-Systems	●	○	○	◑	○	◕	◆	●	◆	◆
	Einbau einer Trap-Door	○	○	○	◔	○	○	●	○	○	○
	Nutzung einer falschen Konfiguration des Firew all-Systems	●	○	○	◑	○	◕	○	●	◆	◆
	Nutzung von Implementierungsfehlers des Firew all-Systems	●	○	○	◑	○	◕	◆	●	◆	◆
	interne Angriffe	○	○	○	◕	●	◕	○	◔	◆	◆

●	sehr große Wirkung	◕	große Wirkung	◑	Wirkung
◔	wenig Wirkung	○	keine Wirkung	◆	Grundlage f.d. Wirkung

Umfassendes Firewallsystem 3/3 -
→ Einbau einer Trap - Door

Angriffsart		High-level Security Firewall-System	Verschlüsselung	Anti-Malware-System	Intrusion Detection Systeme	Personal Firewall	nichttechnische Sicherheitsmaßnahmen	Vertrauenswürdigkeit	Audits	Sicherheitspolitik	sicherer Betrieb
	▪ Durch die Verwendung von Intrusion Detection Systeme kann dieser Angriff möglicherweise entdeckt werden. ▪ Diesem Angriff kann nur mit Hilfe einer ausreichenden Evaluierung und Zertifizierung sicher entgegengewirkt werden.										
Vorbe-reitung für Angriffe	Social Engieering	○	○	○	○	○	●	○	◆	◆	◆
	Analyse mit Hilfe von Scannerprogrammen	●	○	○	◑	○	○	◆	◆	◆	◆
	Manipulation des Firew all-Systems	●	○	○	◑	○	◕	◆	●	◆	◆
	Einbau einer Trap-Door	○	○	○	◔	○	○	●	○	○	○
	Nutzung einer falschen Konfiguration des Firew all-Systems	●	○	○	◑	○	◕	○	●	◆	◆
	Nutzung von Implementierungsfehlers des Firew all-Systems	●	○	○	◑	○	◕	◆	●	◆	◆
	interne Angriffe	○	○	○	◕	●	◕	○	◔	◆	◆

●	sehr große Wirkung	◕	große Wirkung	◑	Wirkung
◔	wenig Wirkung	○	keine Wirkung	◆	Grundlage f.d. Wirkung

Umfassendes Firewallsystem 3/3 -
→ Nutzung einer falschen Konfiguration

Angriffsart		High-level Security Firewall-System	Verschlüsselung	Anti-Malware-System	Intrusion Detection Systeme	Personal Firewall	nichttechnische Sicherheitsmaßnahmen	Vertrauenswürdigkeit	Audits	Sicherheitspolitik	sicherer Betrieb
	▪ Ein High-level Security Firewall-System verhindert diesen Angriff: sicheres Designkonzept,eigene Schutzmecha-nismen separates und zentrales Security Management, versch. Firewall-Elemente ▪ Durch die Verwendung von Intrusion Detection Systeme kann dieser Angriff möglicherweise entdeckt werden. ▪ Durch klar geregelte Verantwortung kann hier eine große Wirkung erzielt werden ▪ Durch regelmäßige Audits kann dieser Angriff verhindert werden.										
Vorbe-reitung für Angriffe	Social Engieering	○	○	○	○	○	●	○	◆	◆	◆
	Analyse mit Hilfe von Scannerprogrammen	●	○	○	◑	○	○	◆	◆	◆	◆
	Manipulation des Firew all-Systems	●	○	○	◑	○	◕	◆	●	◆	◆
	Einbau einer Trap-Door	○	○	○	◔	○	○	●	○	○	○
	Nutzung einer falschen Konfiguration des Firew all-Systems	●	○	○	◑	○	◕	○	●	◆	◆
	Nutzung von Implementierungsfehlers des Firew all-Systems	●	○	○	◑	○	◕	◆	●	◆	◆
	interne Angriffe	○	○	○	◕	●	◕	○	◔	◆	◆

●	sehr große Wirkung	◕	große Wirkung	◑	Wirkung
◔	wenig Wirkung	○	keine Wirkung	◆	Grundlage f.d. Wirkung

Umfassendes Firewallsystem 3/3 -
→ Nutzung von Implementierungsfehlern

Angriffsart		High-level Security Firewall-System	Verschlüsselung	Anti-Malware-System	Intrusion Detection Systeme	Personal Firewall	nichttechnische Sicherheitsmaßnahmen	Vertrauenswürdigkeit	Audits	Sicherheitspolitik	sicherer Betrieb
	▪ Ein high-level Security Firewall-System verhindert diesen Angriff: sicheres Designkonzept,eigene Schutzmecha-nismen separates und zentrales Security Management, versch. Firewall-Elemente ▪ Durch die Verwendung von Intrusion Detection Systeme kann dieser Angriff möglicherweise entdeckt werden. ▪ Durch klar geregelte Verantwortung kann hier eine große Wirkung erzielt werden ▪ Durch regelmäßige Audits kann dieser Angriff verhindert werden.										
Vorbe-reitung für Angriffe	Social Engieering	○	○	○	○	○	●	○	◆	◆	◆
	Analyse mit Hilfe von Scannerprogrammen	●	○	○	◑	○	○	◆	◆	◆	◆
	Manipulation des Firew all-Systems	●	○	○	◑	○	◕	◆	●	◆	◆
	Einbau einer Trap-Door	○	○	○	◔	○	○	●	○	○	○
	Nutzung einer falschen Konfiguration des Firew all-Systems	●	○	○	◑	○	◕	○	●	◆	◆
	Nutzung von Implementierungsfehlern des Firew all-Systems	●	○	○	◑	○	◕	◆	●	◆	◆
	interne Angriffe	○	○	○	◕	●	◕	○	◔	◆	◆

●	sehr große Wirkung	◕	große Wirkung	◑	Wirkung
◔	wenig Wirkung	○	keine Wirkung	◆	Grundlage f.d. Wirkung

Umfassendes Firewallsystem 3/3 -
→ Interne Angriffe

Angriffsart	▪ Mit Hilfe von Intrusion Detection Systemen kann eine große Wirkung (Früherkennung) bevor ein Schaden aufgetreten ist, erzielt werden. ▪ Dieser Angriff kann mit einer sehr großen Wirkung mit Hilfe von Personal Firewall entgegengewirkt werden. ▪ Sensibilisierung, Aufklärung und Schulung haben eine große Wirkung ▪ Durch Audits können interne Angriffe erkannt/nachgewiesen werden	High-level Security Firewall-System	Verschlüsselung	Anti-Malware-System	Intrusion Detection Systeme	Personal Firewall	nichttechnische Sicherheitsmaßnahmen	Vertrauenswürdigkeit	Audits	Sicherheitspolitik	sicherer Betrieb
Vorbe-reitung für Angriffe	Social Engieering	○	○	○	○	○	●	○	◆	◆	◆
	Analyse mit Hilfe von Scannerprogrammen	●	○	○	◑	○	○	◆	◆	◆	◆
	Manipulation des Firew all-Systems	●	○	○	◑	○	◕	◆	●	◆	◆
	Einbau einer Trap-Door	○	○	○	◔	○	○	●	○	○	○
	Nutzung einer falschen Konfiguration des Firew all-Systems	●	○	○	◑	○	◕	○	●	◆	◆
	Nutzung von Implementierungsfehlern des Firew all-Systems	●	○	○	◑	○	◕	◆	●	◆	◆
	interne Angriffe	○	○	○	◕	●	◕	○	◔	◆	◆

●	sehr große Wirkung	◕	große Wirkung	◑	Wirkung
◔	wenig Wirkung	○	keine Wirkung	◆	Grundlage f.d. Wirkung

Inhalt

- Sicherheitsziele bei der Umsetzung eines umfassenden Firewall-Systems
- Beschreibung der Sicherheitskomponenten und deren Ziele
- Bewertung der Sicherheitskomponenten
- **Weiterentwicklung von Firewall-Systemen**

Weiterentwicklung von umfassenden Firewall-Systemen

- Integratives, zentrales Sicherheitsmanagement aller Sicherheitsmechanismen
- Immer höhere Geschwindigkeit bei immer höherem Schutzbedarf
- Zunehmende Innovationen
- Universelle Authentisierung
- Einheitliche Darstellung der Angriffe und Sicherheitsdienste/-mechanismen
- Intrusion Detection Systems

Umfassende Firewall-Systeme

Vielen Dank für Ihre Aufmerksamkeit

Fragen ?

norbert.pohlmann@informatik.fh-gelsenkirchen.de

Fachhochschule Gelsenkirchen