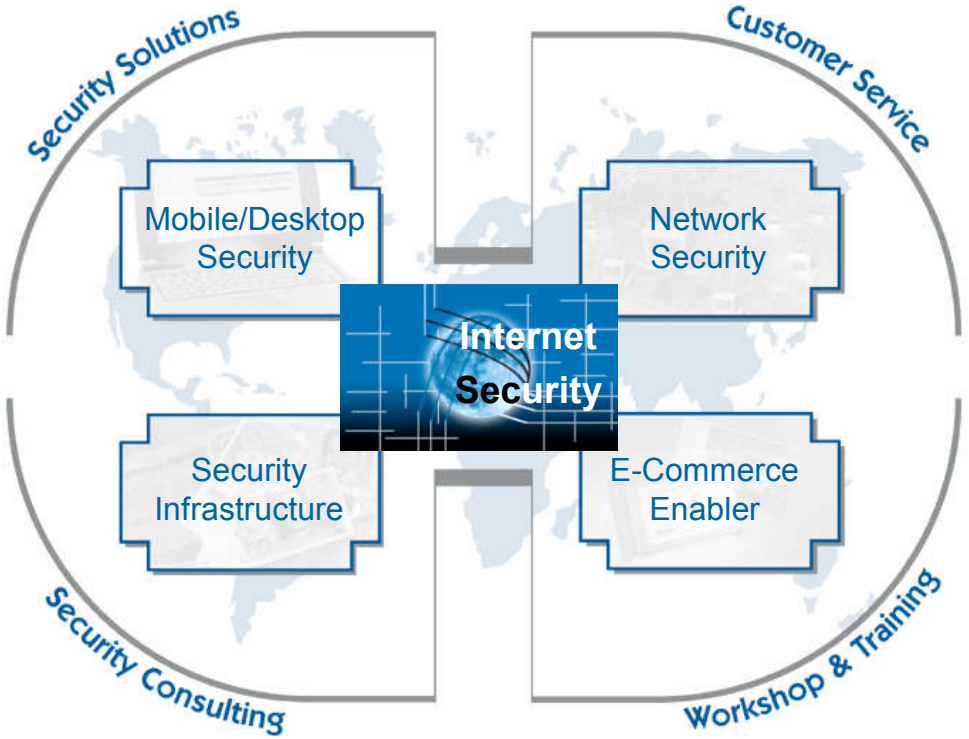
Möglichkeiten und Grenzen von Firewall-Systemen



Norbert Pohlmann

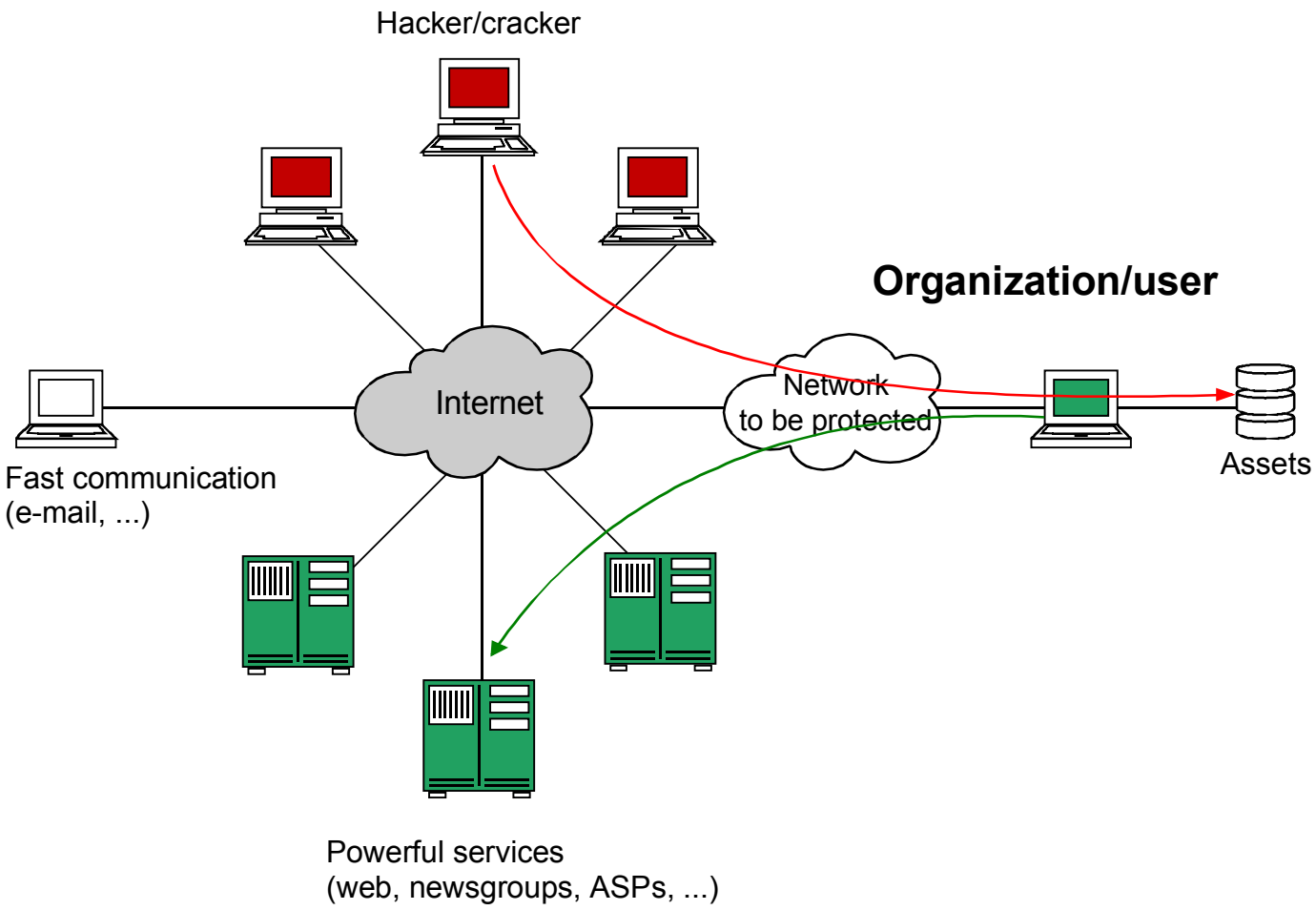
Mitglied des Vorstandes

Utimaco Safeware AG

utimaco® safeware

Chance und Risiko - Zwei Seiten einer Medaille

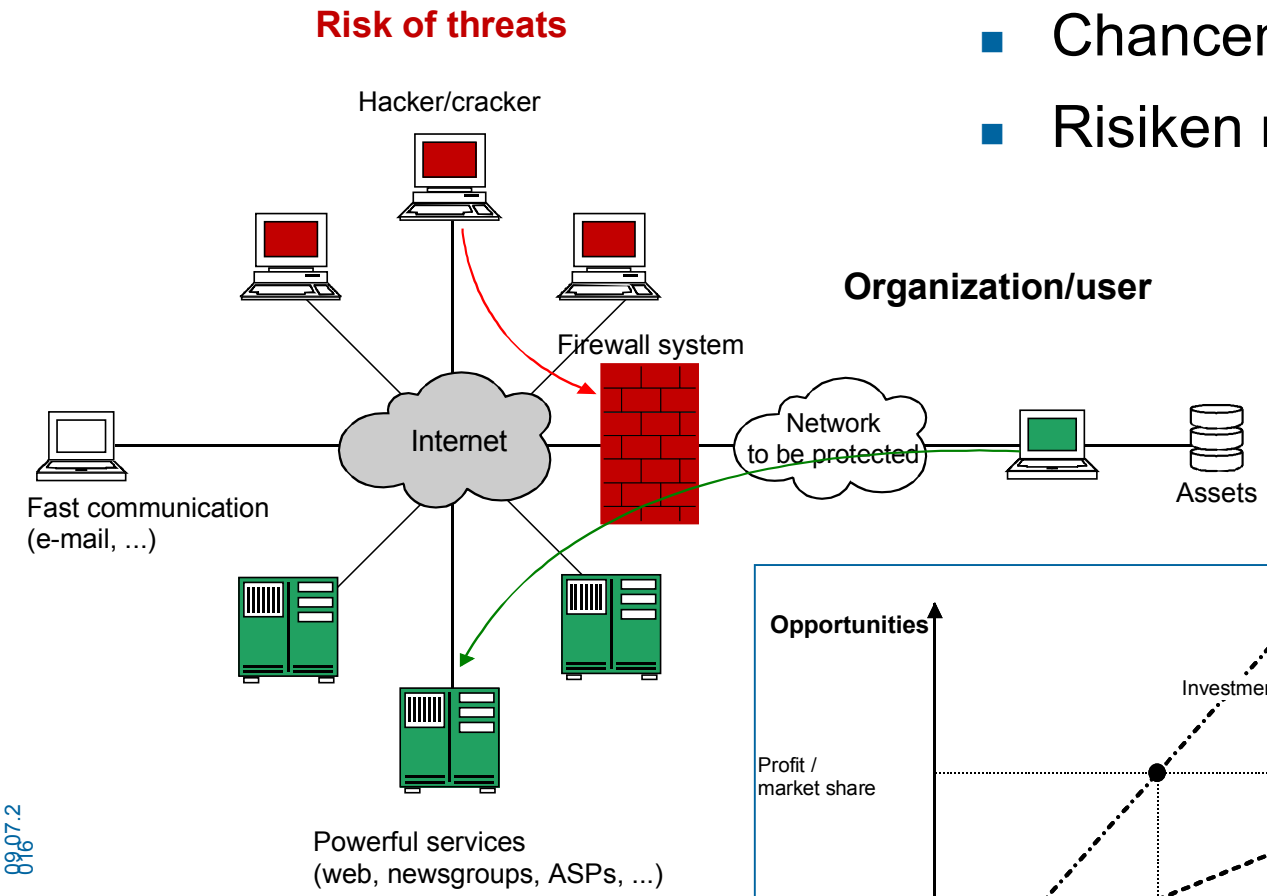
Risk of threats

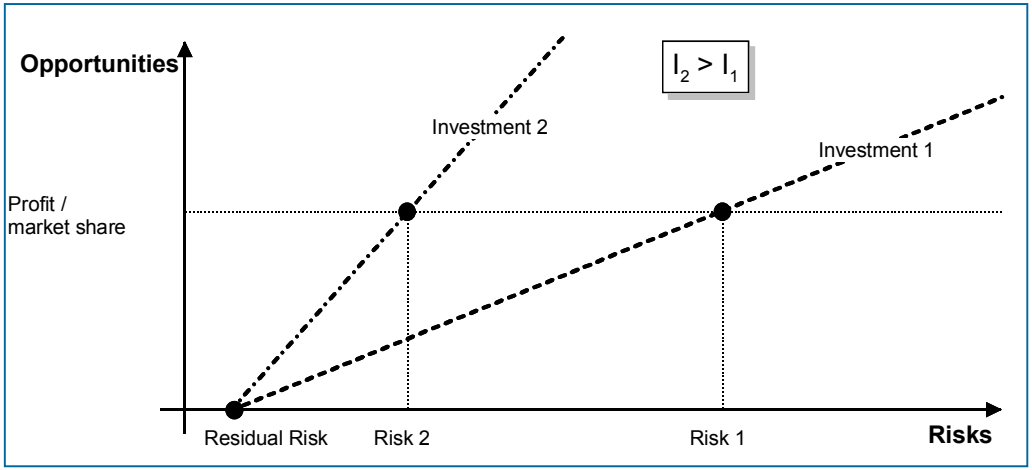


Chance of opportunities

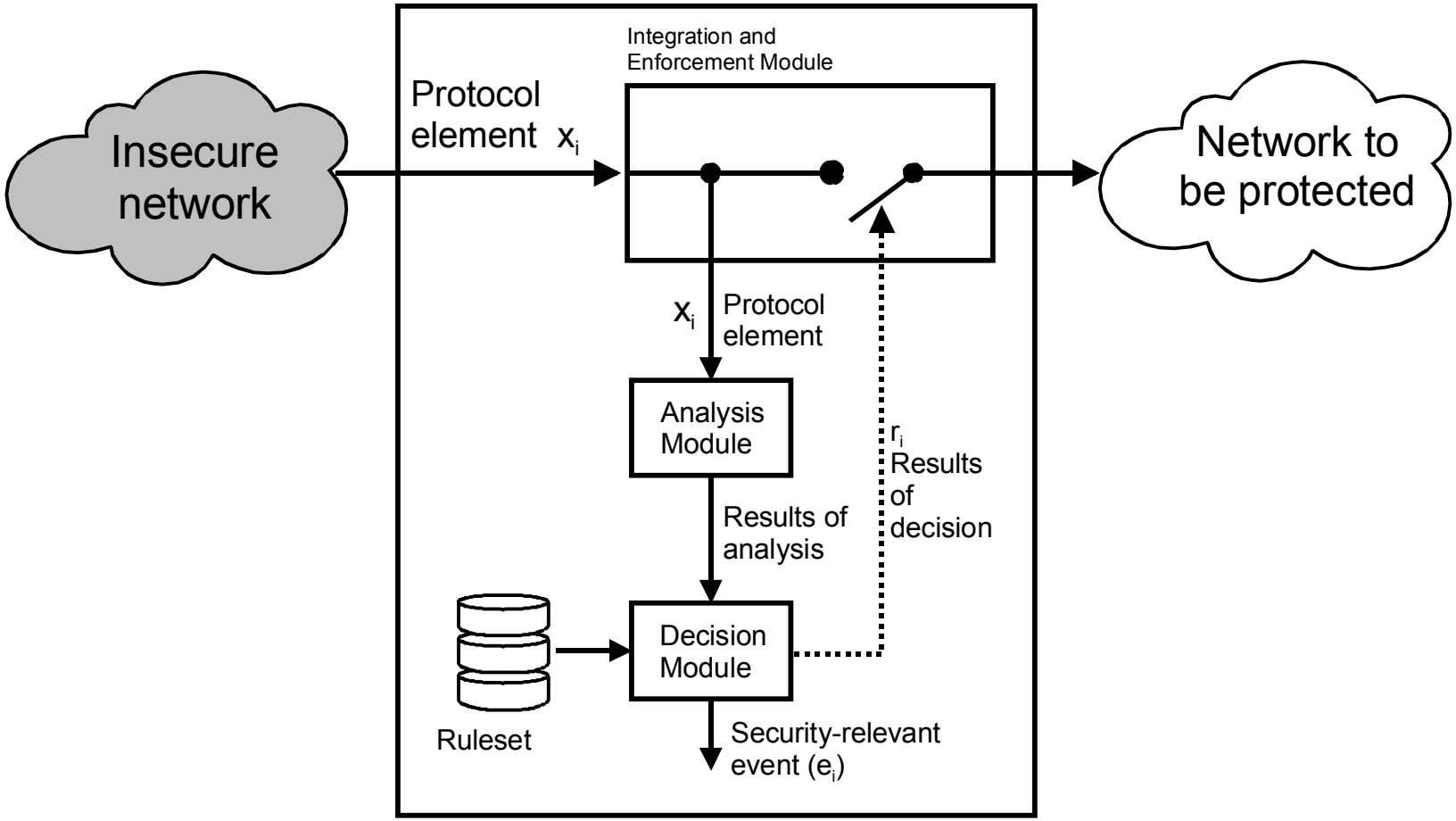
Idee eines Firewall-Systems

- Chancen nutzen
- Risiken minimieren

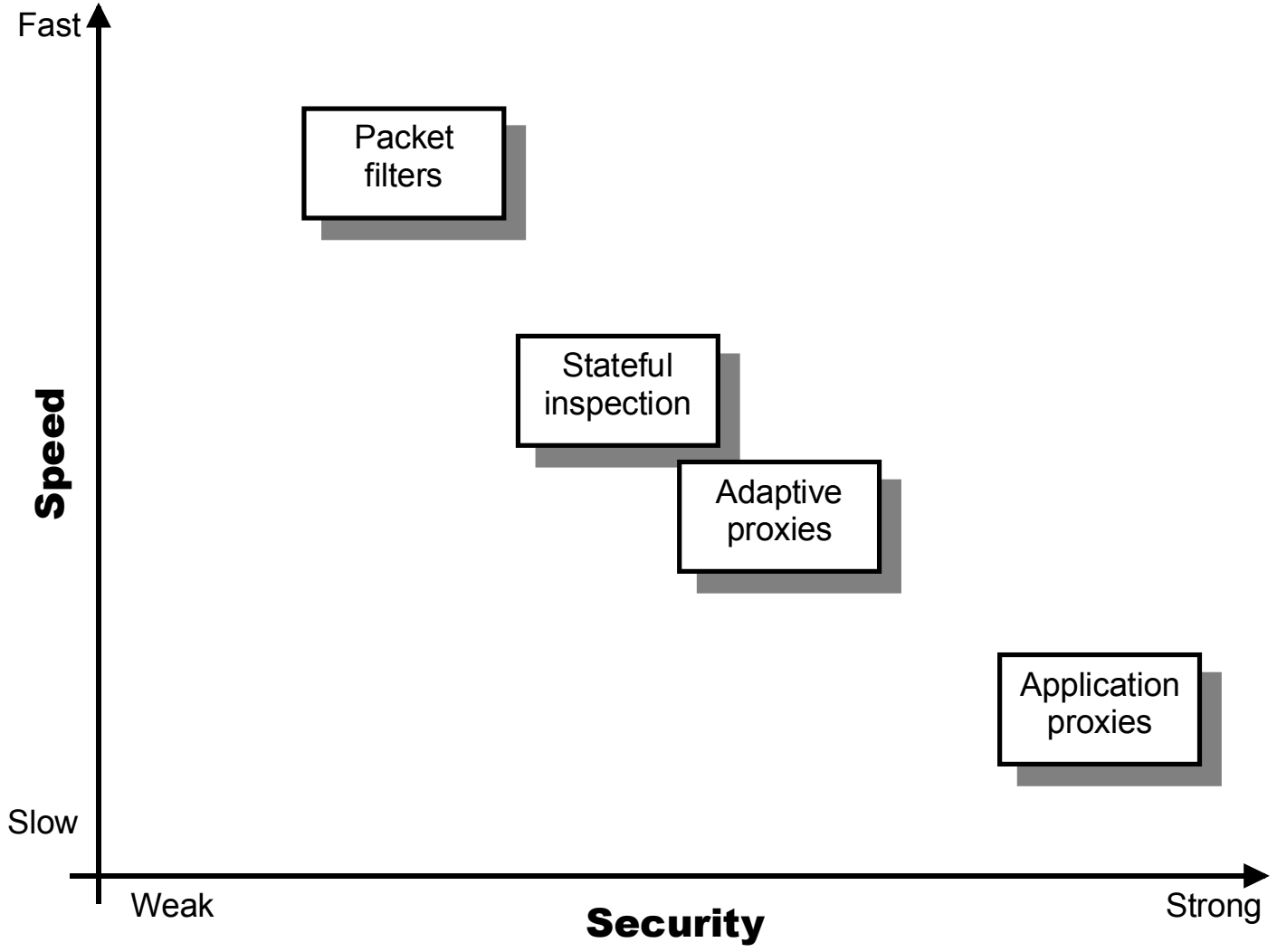




Definition eines Firewall-Elements



Firewall-Elemente im Verhältnis zu Schnelligkeit und Sicherheit

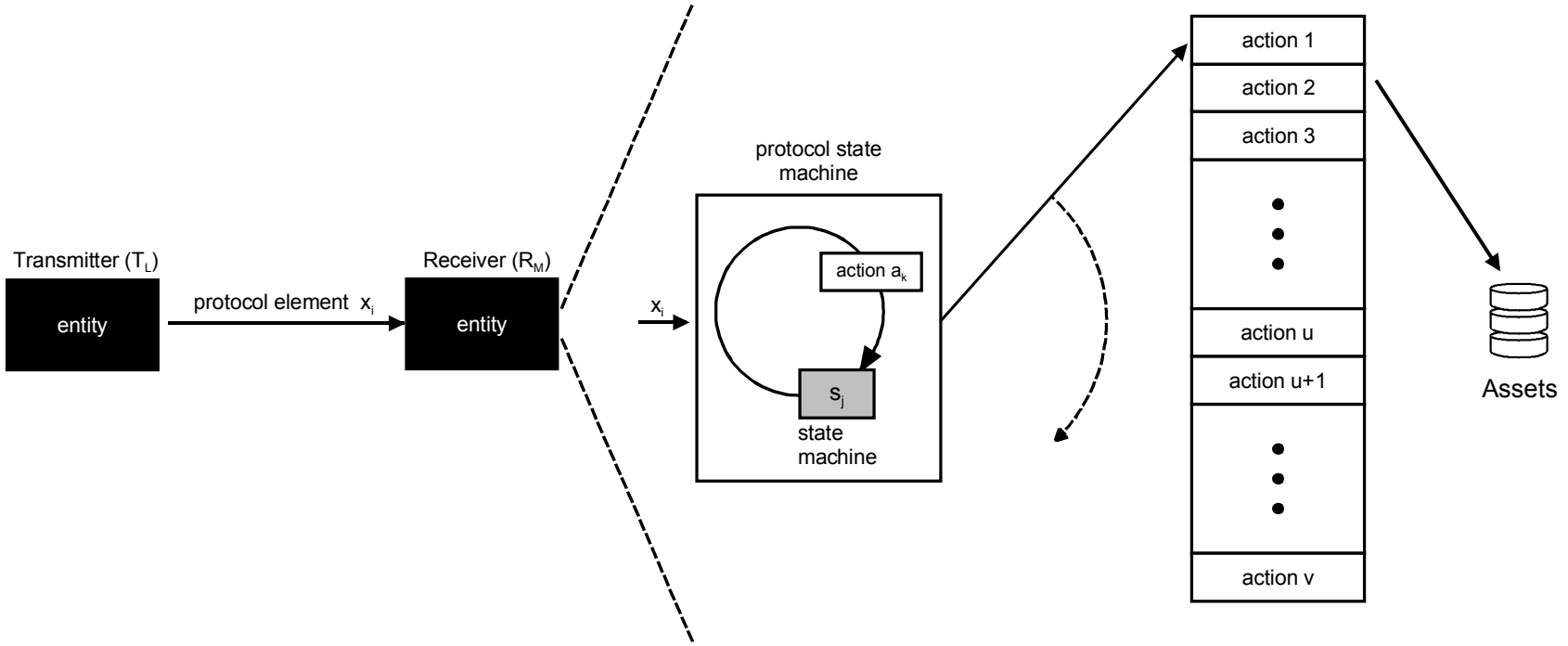


Sicherheitsziele bei der Umsetzung eines umfassenden Firewall-Systems

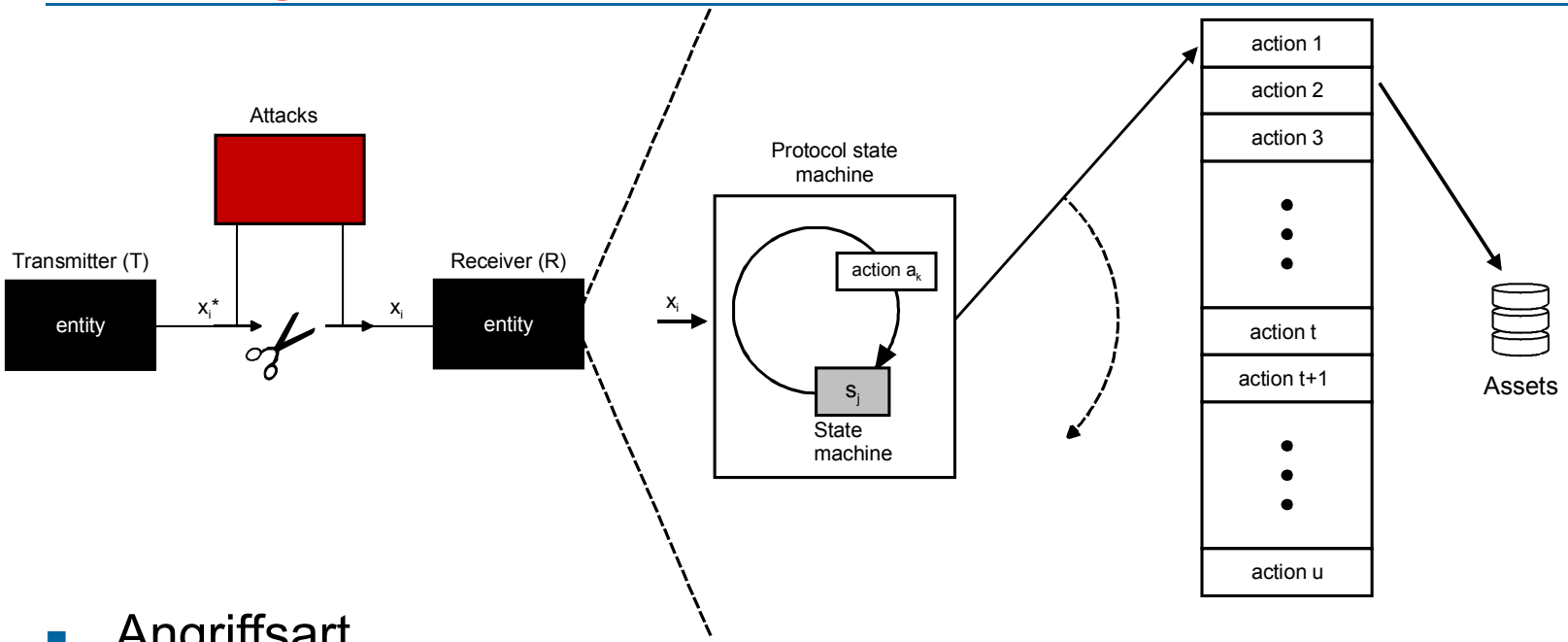
- Alle Unsicherheiten mit größtmöglicher Wahrscheinlichkeit vollständig zu eliminieren
- Möglichst vielen Unsicherheiten mit passenden Sicherheitsmechanismen entgegen zu wirken, damit die Wahrscheinlichkeit eines Schadens auf eine praktisch nicht vorkommende Größe minimiert wird
- Unsicherheiten, die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

utimaco safeware

Vereinfachtes logisches Kommunikationsmodell

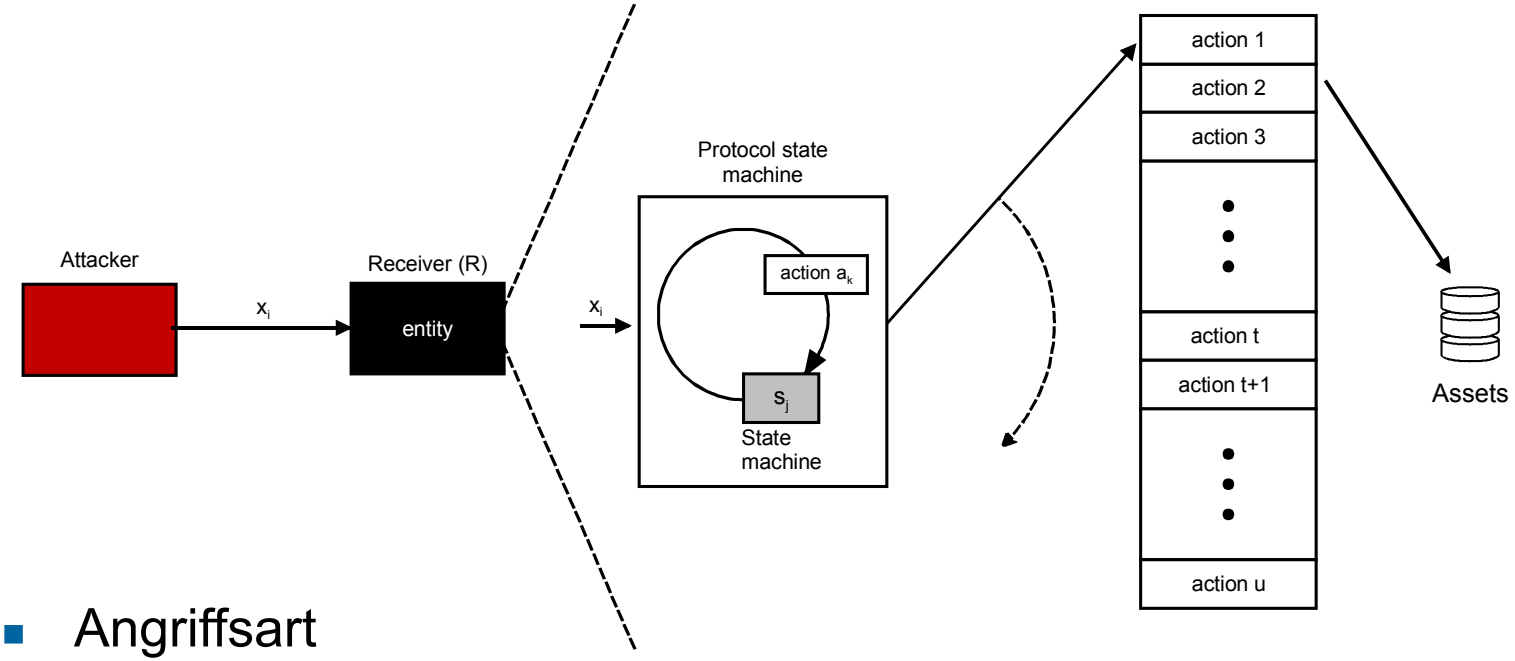


Bedrohungen
-> Angriffe durch Dritte



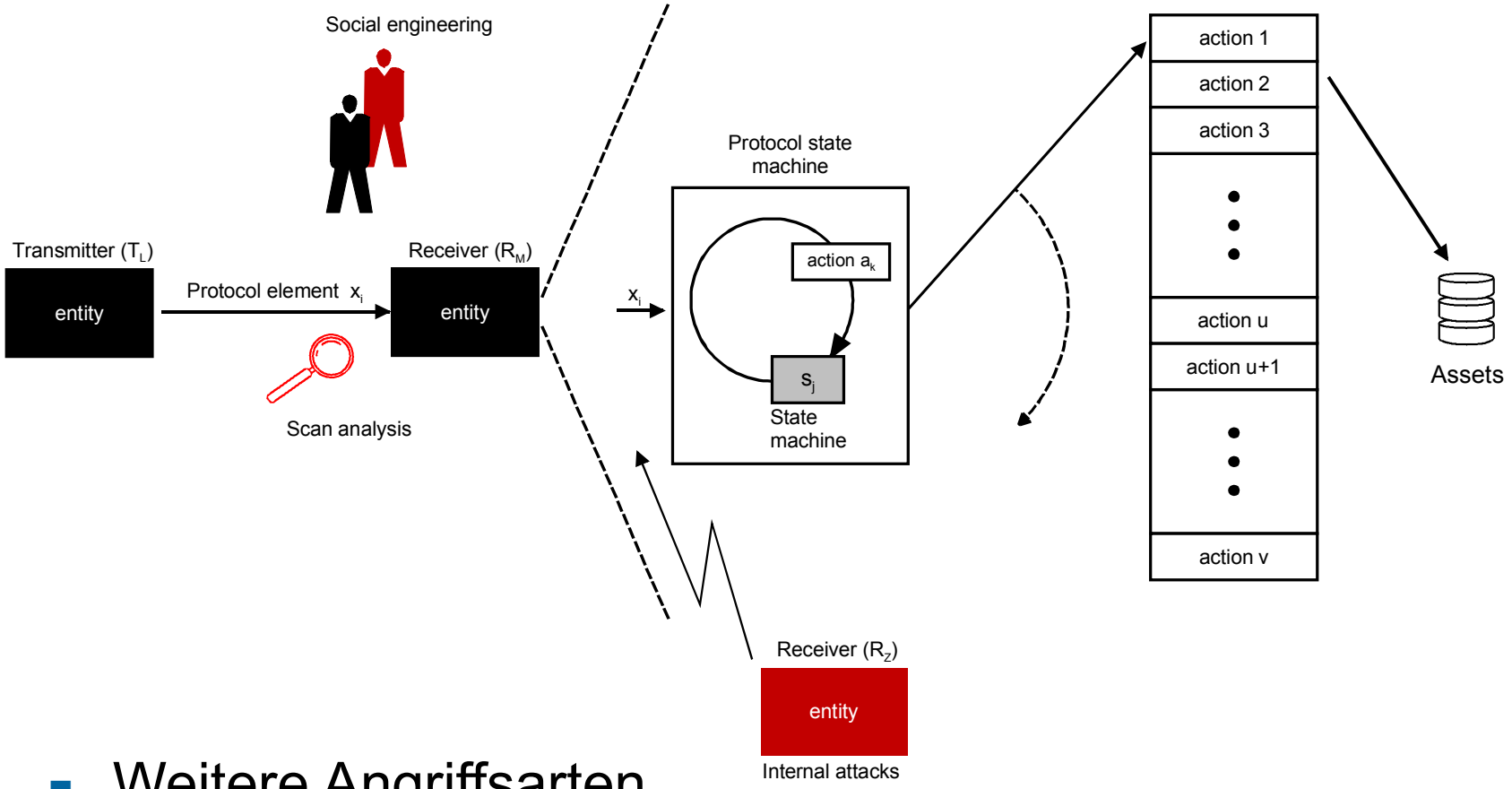
- Angriffsart
  - Wiederholen oder Verzögern der/des Protokollelemente(s)
  - Einfügen oder Löschen bestimmter Daten in den Protokollelementen
  - Modifikation der Daten in den Protokollelementen
  - Boykott des Receivers
  - Trittbrettfahrer
  - Empfangen von Malware (Viren, Würmer, Trojanische Pferde,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

Bedrohungen
-> Angriffe von Kommunikationspartnern



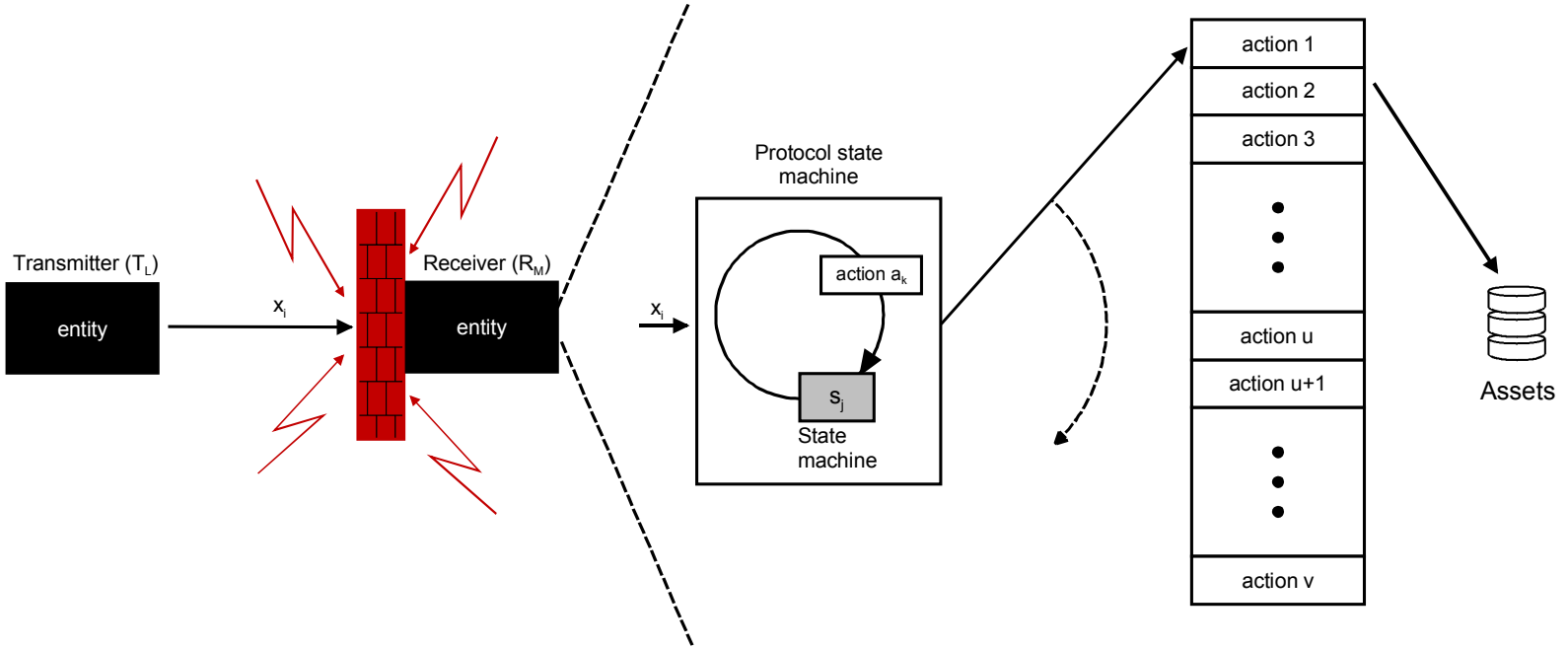
- Angriffsart
  - Unberechtigter Aufbau und Nutzung einer Kommunikationsverbindung
  - Unberechtigte Nutzung von Kommunikationsprotokollen und -diensten
  - Vortäuschen einer falschen Identität (Maskerade-Angriff)
  - Nutzung der Kommunikationsverbindung zum Receiver für gezielte Angriffe (z.B. Java-Applets,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

Bedrohung
-> Vorbereitung eines Angriffs



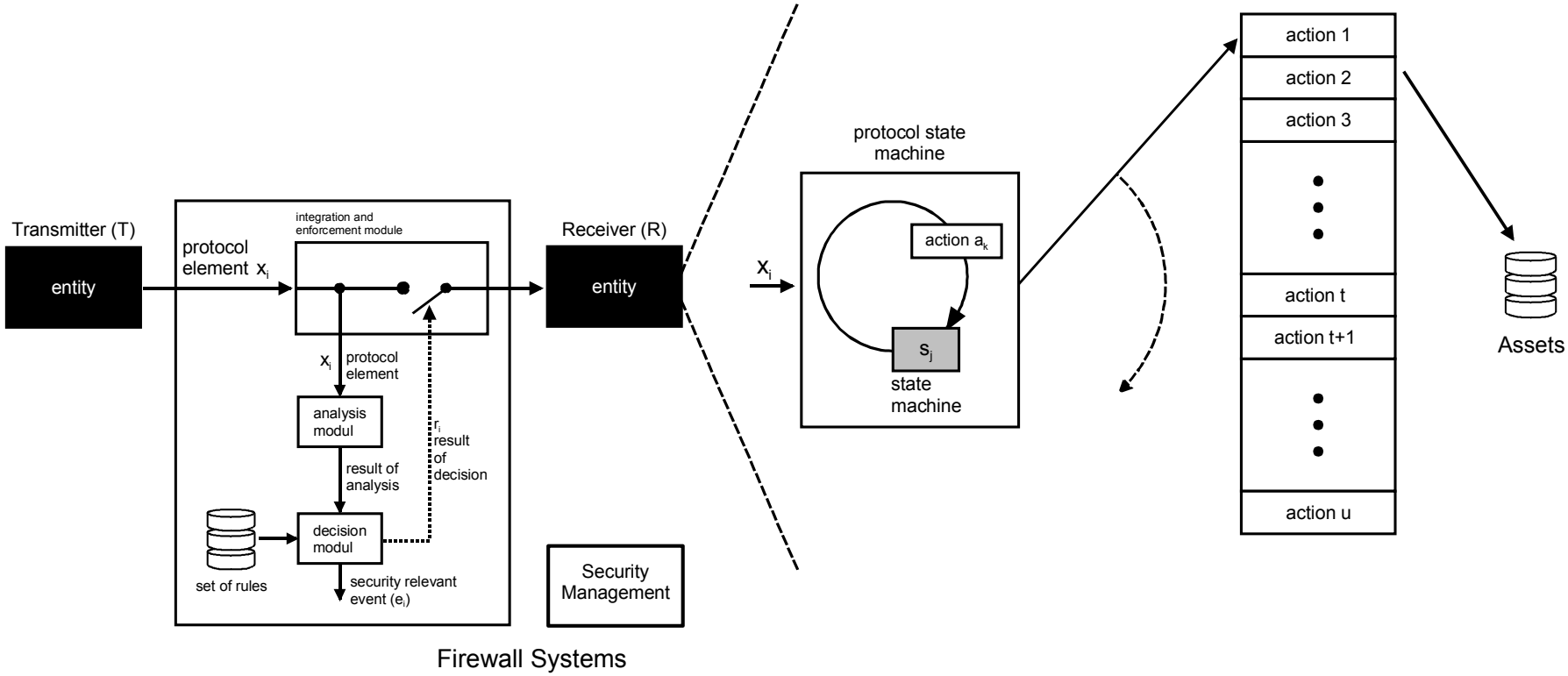
- Weitere Angriffsarten
  - Social Engineering
  - Analyse mit Hilfe von Scannerprogrammen
- Interne Angriffe

Bedrohungen
-> Angriffe auf das Firewall-System



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

Das Kommunikationsmodell mit integriertem Firewall-System



$$a_k = \textit{action-select}(\ \textit{protocol-state-machine}(x_i, s_j),\ \textit{authenticity}(x_i, t_l),\ \textit{result-of-decision}(\ \textit{analysis}(x_i), \textit{security-management}(\textbf{rules})\ ),\ \textit{functionality-of-the-firewall-system}()\ )$$

Konzeptionelle Möglichkeiten zentraler Firewall-Systeme

- Common Point of Trust-Konzept
  - Kosten
  - Umsetzung der Sicherheitspolitik
  - Sicherheitsinfrastruktur
  - Sicherheit durch Abschottung
  - Überprüfbarkeit
- Reduzierung des Schadensrisikos

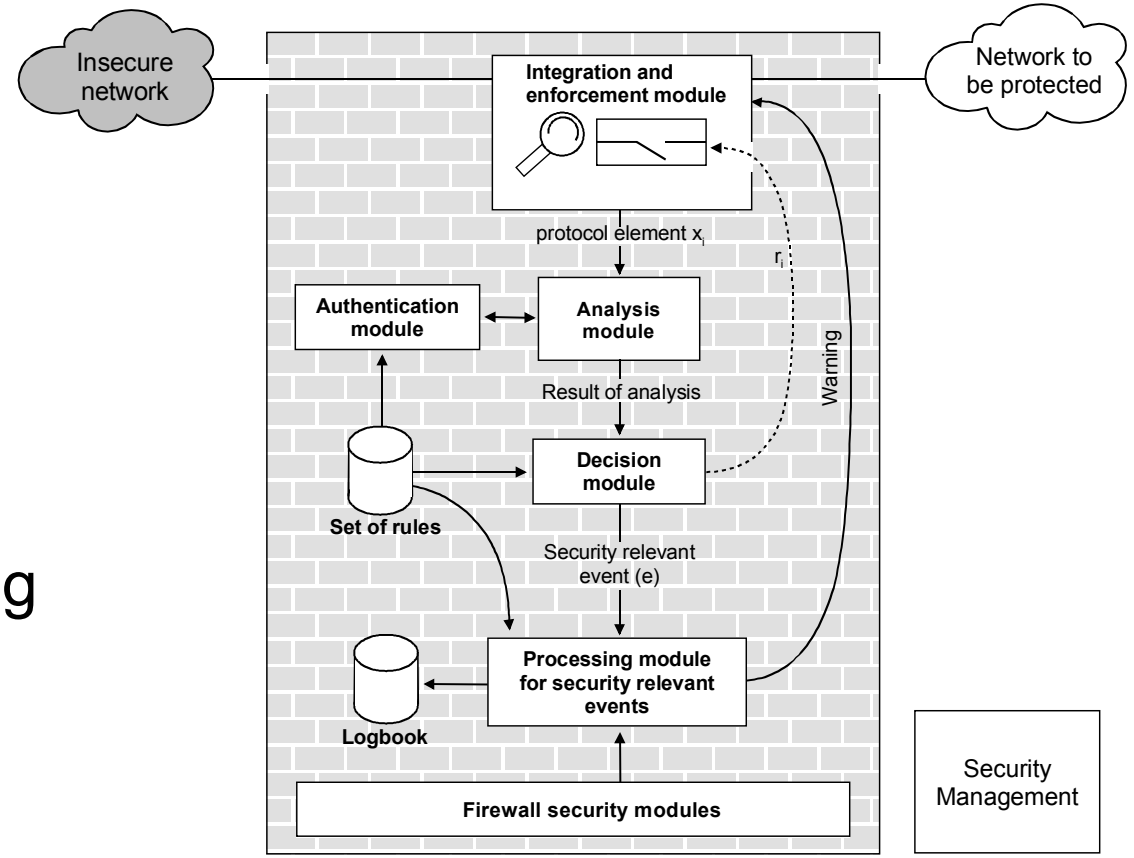
Konzeptionelle Grenzen eines zentralen Firewall-Systems

- Hintertüren (Back Door)
- Interne Angriffe
- Angriffe auf Datenebene
- Wissen und Hypothese
- Richtige Sicherheitspolitik und deren Umsetzung
- Security versus connectivity

Risiko versus Chance

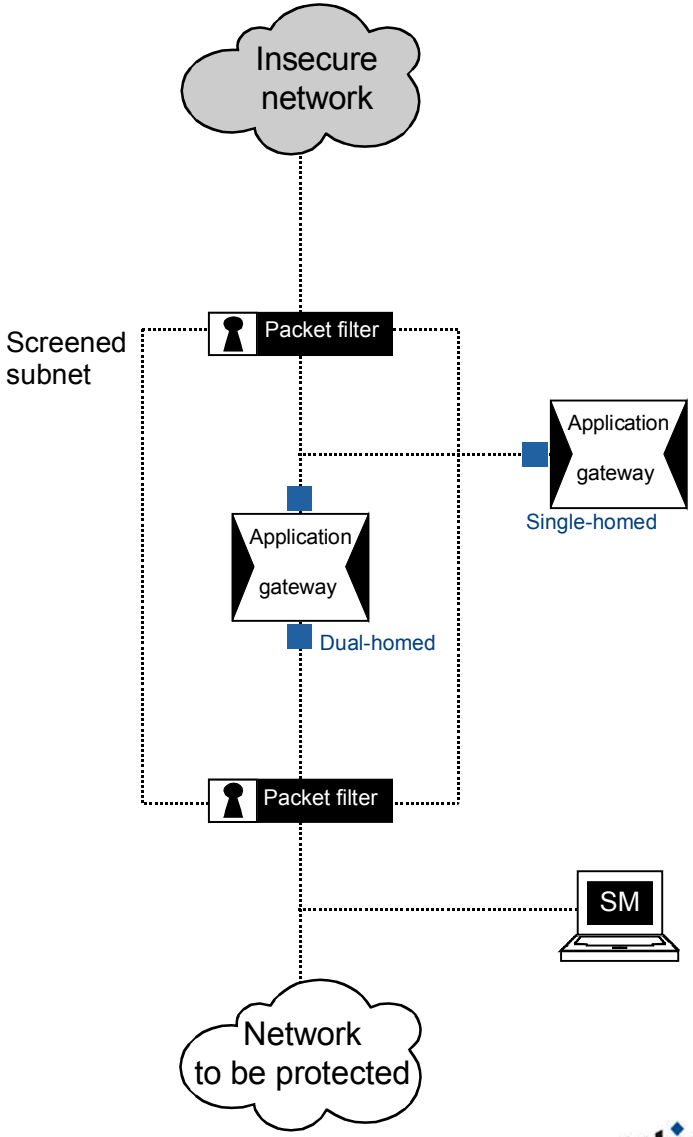
Realisierungskonzepte

- Systemaufbau
- Designkonzept
- Turn-Key Lösung

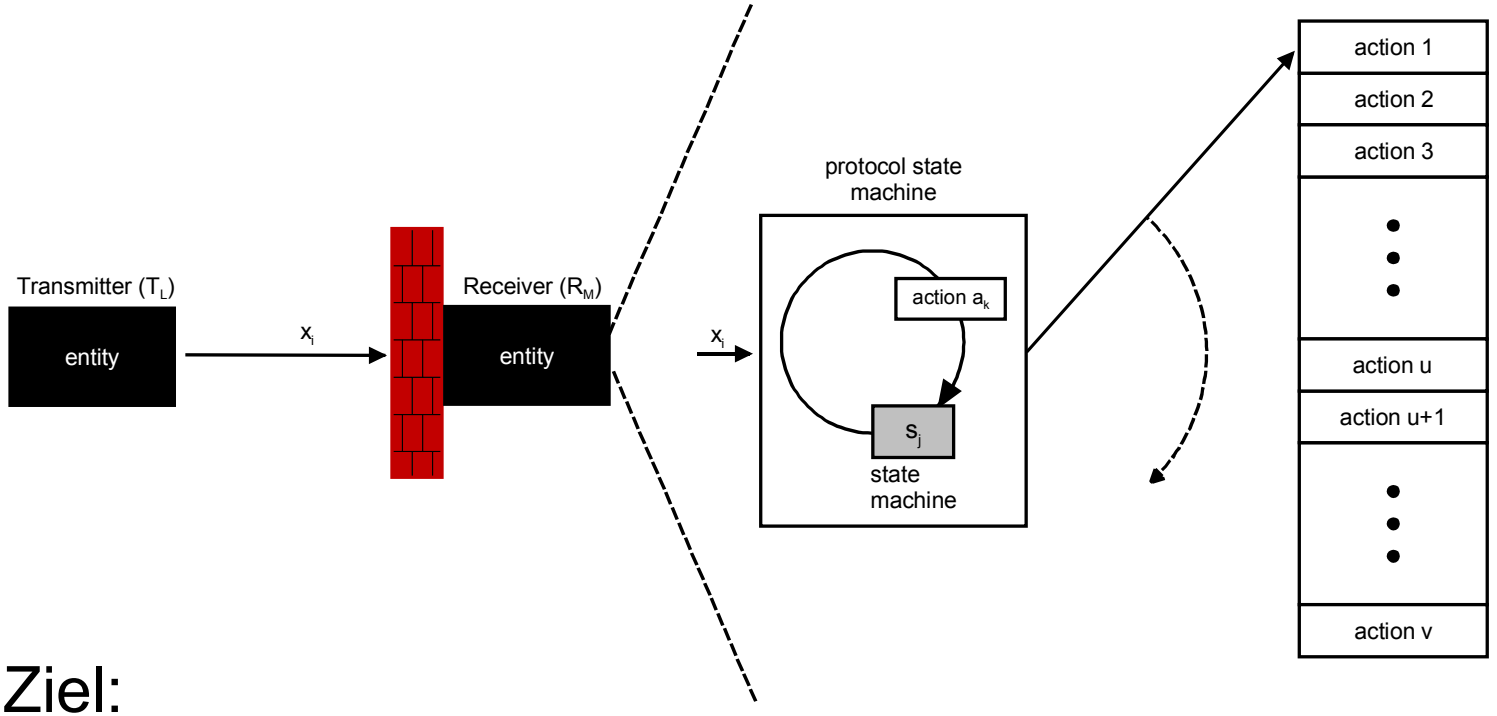


Firewall Konzepte

- Packet Filter
- Single-homed Application Gateway
- Dual-homed Application Gateway
- Packet Filter und single-homed Application Gateway
- Stateful Inspection
- Adaptive Proxy
- Packet Filter und dual-homed Application Gateway
- Screend Subnet mit Packet Filter und single-homed Application Gateway
- Screend Subnet mit Packet Filter und dual-homed Application Gateway



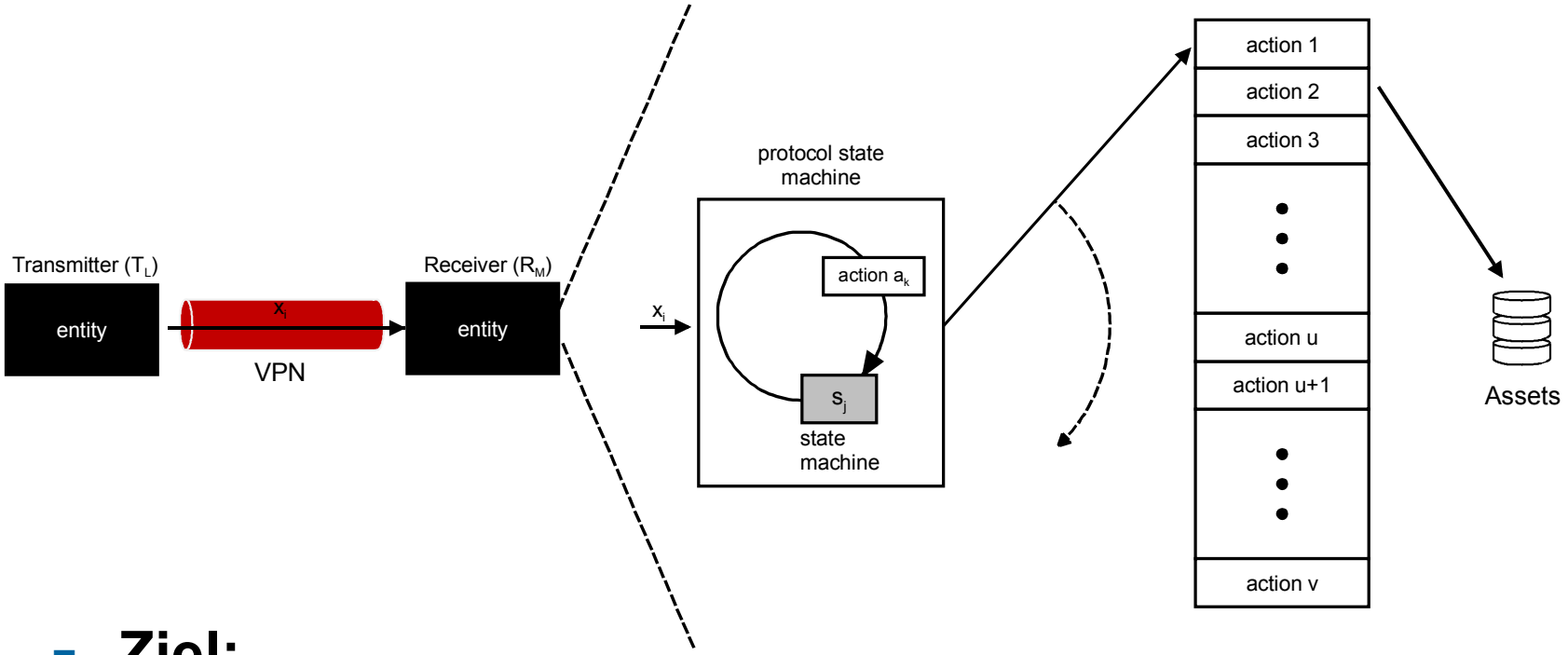
Zentrales High-level Firewall-System



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

Verschlüsselung - VPNs

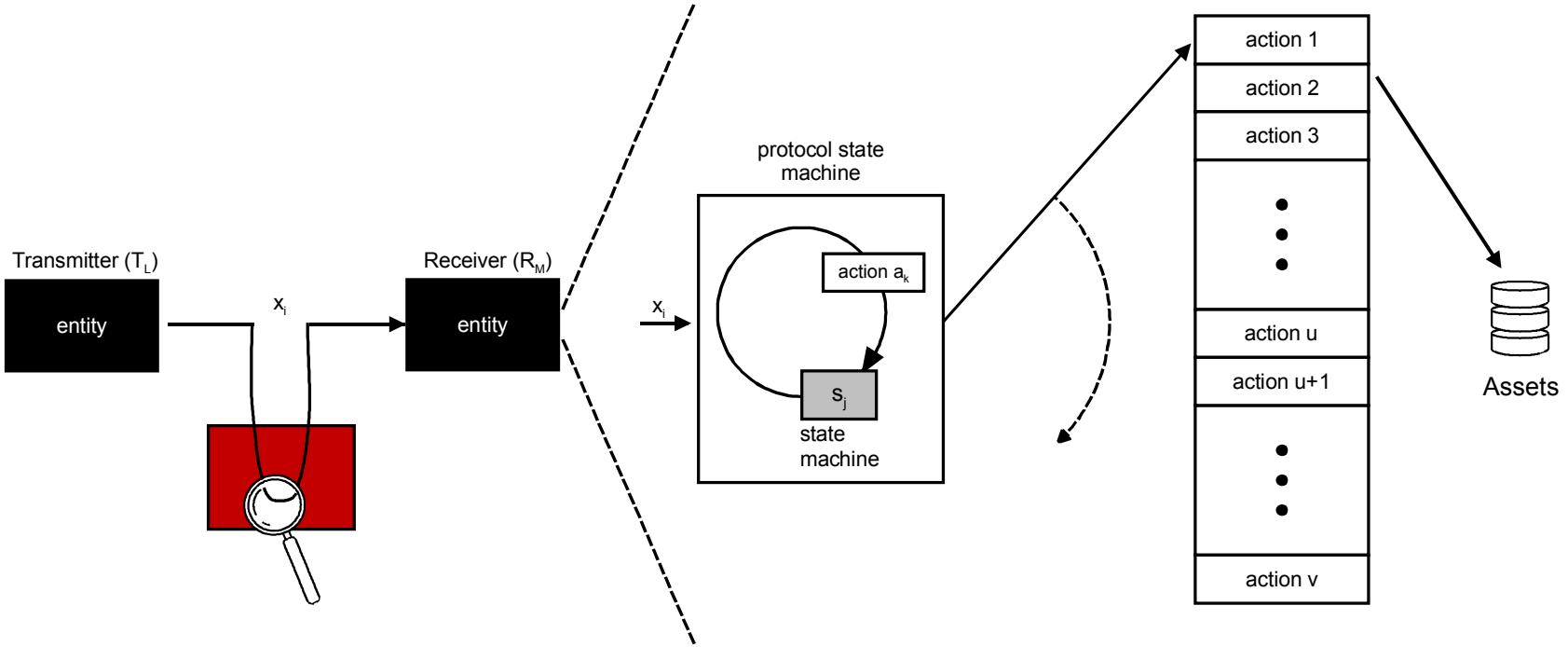
-> Analogie zum Sicherheitstransporter



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

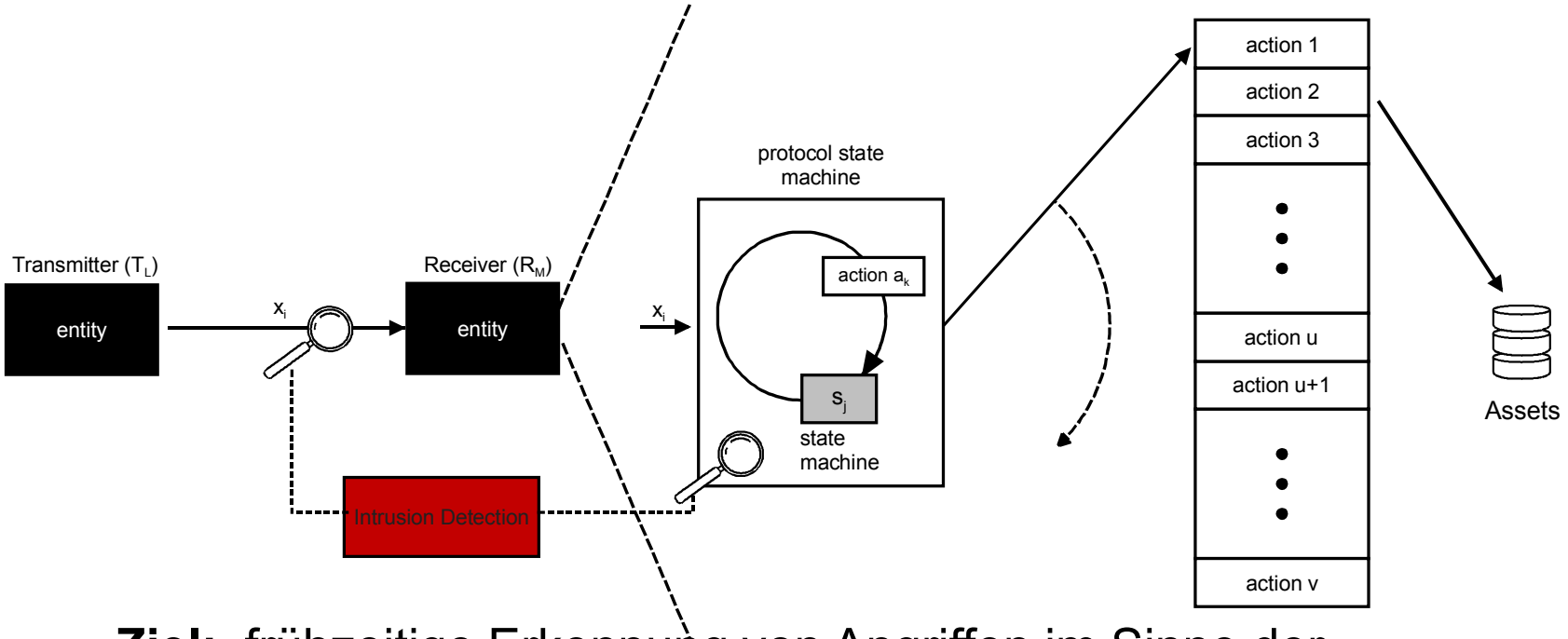
Zentraler Virenscanner

-> Analogie zur zentralen Poststelle



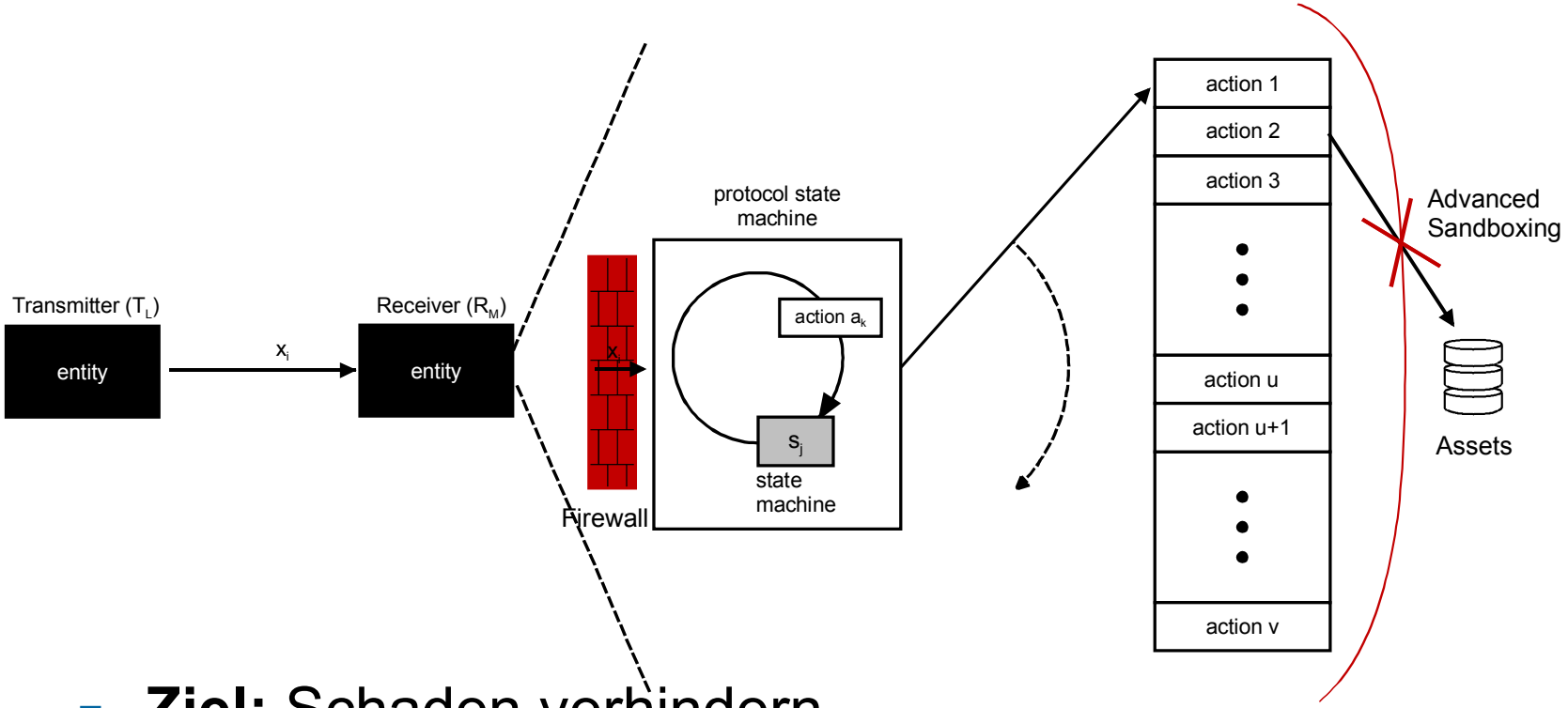
- **Ziel:**
  - Erkennen von Viren an zentraler Stelle
  - Verhindern, daß Viren in die Organisation übertragen werden
  - Protokollieren der gefundenen Viren und Alarmierung

Intrusion Detection
-> Analogie zur Videoüberwachung



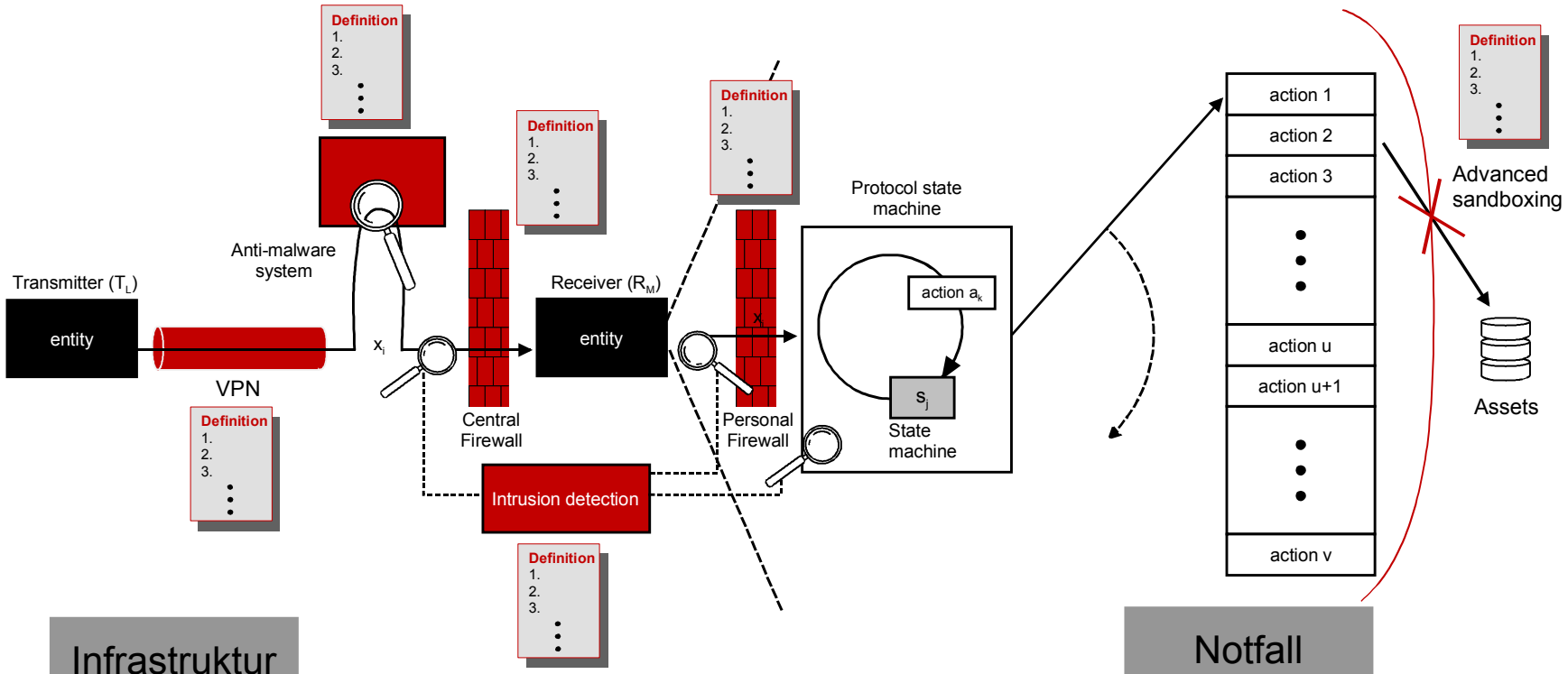
- **Ziel:** frühzeitige Erkennung von Angriffen im Sinne der Schadensverhinderung
- *Sicherheitsmechanismen*
  - Mißbrauchserkennung (Fehler-Signaturen)
  - Erkennung von Anomalien
  - Protokollierung und Berichtserstattung

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

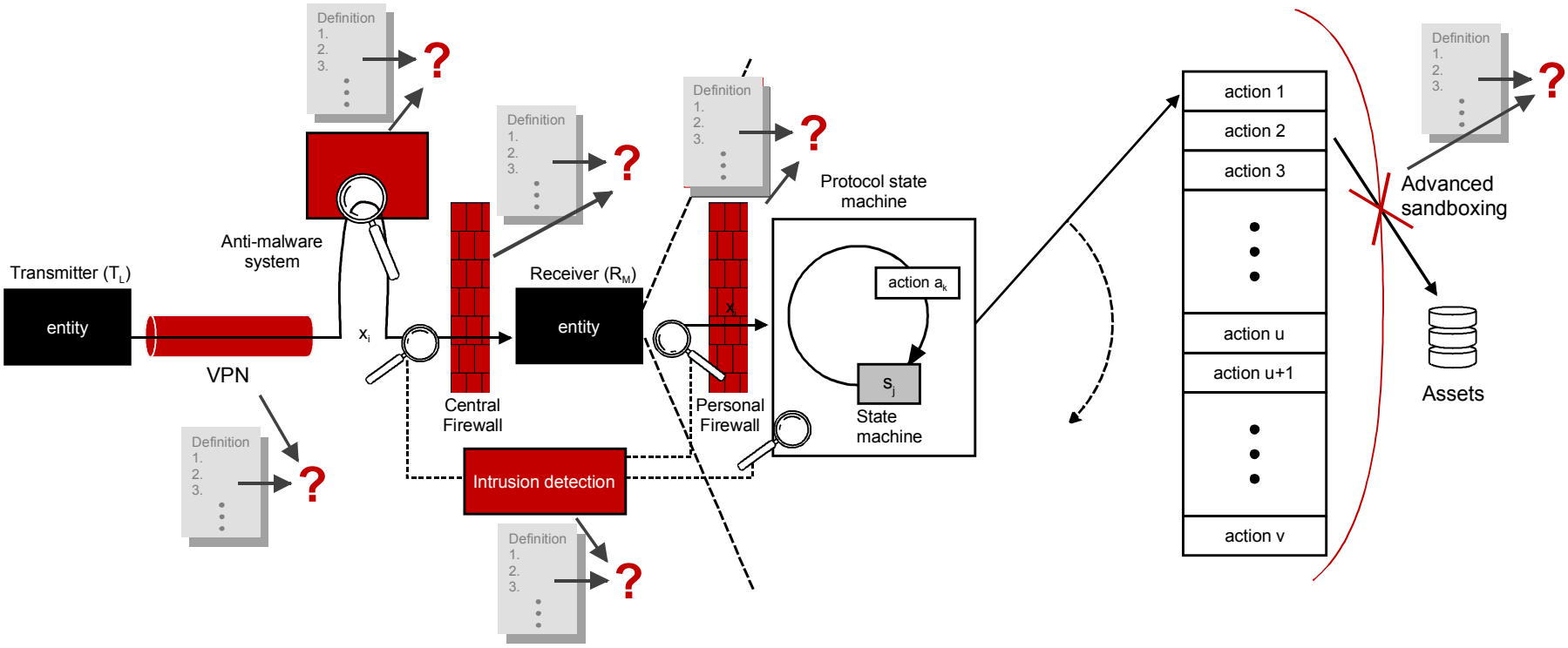
, usw.

- Festlegung der Verantwortung und Zugriffsrechte
- Kontrolled er Protokolldaten, etc.

Personal

- Anweisung, Aufklärung, Sensibilisierung der Benutzer
- Schulungen zum Thema Sicherheit, etc.

Audits



Infrastrukture ?

Organisation ?

Personal ?

Notfall ?

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

utimaco safeware

Umfassendes Firewallsystem 1/3

Angriffsart	Sicherheitsaspekte eines umfassenden Firewallsystems	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 2/3

Angriffsart	Sicherheitsaspekte eines umfassenden Firewallsystems	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	◑	○	○	○	○	◕	◆	◆	◆	◆

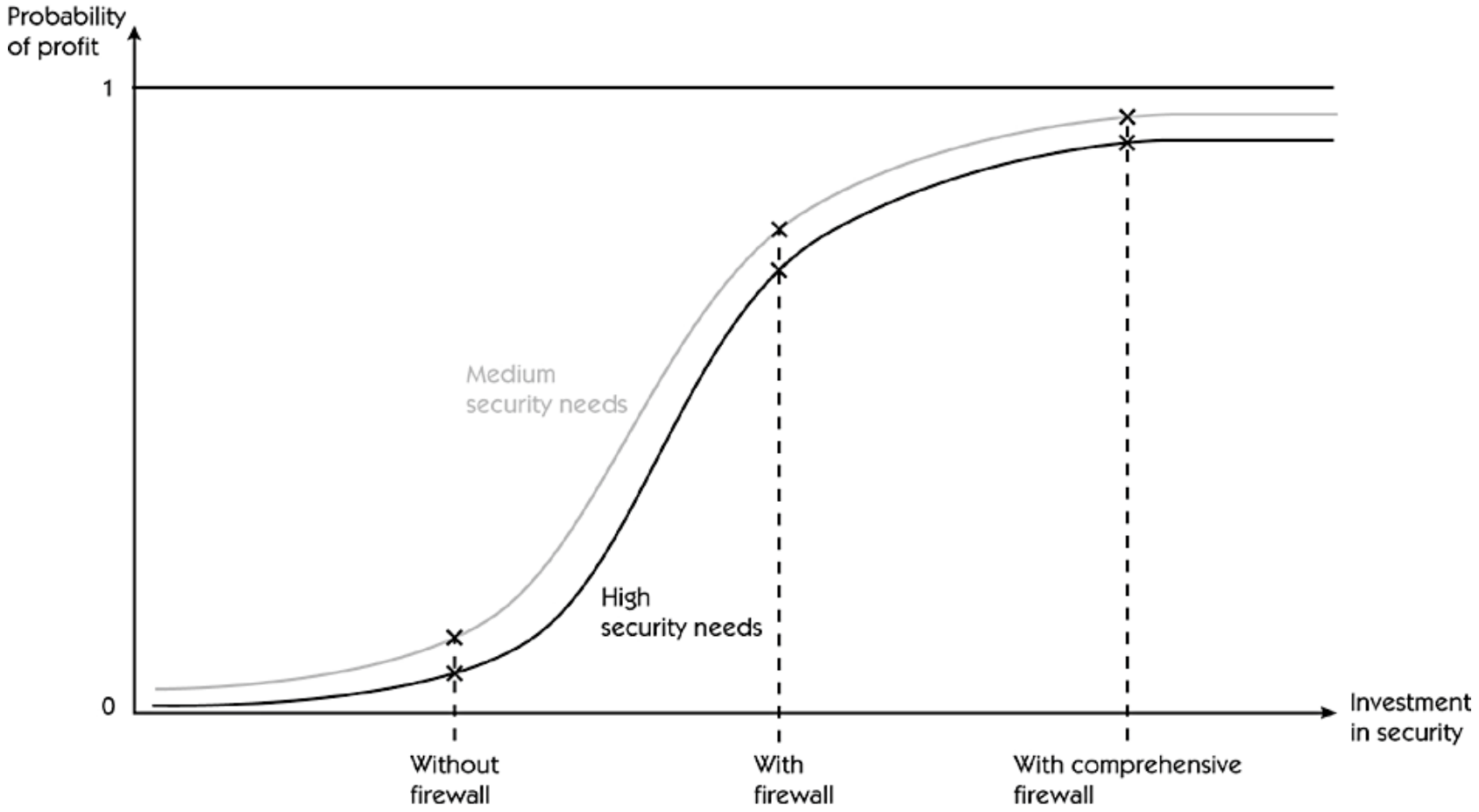
●	sehr große Wirkung	◕	große Wirkung	◑	Wirkung
◔	wenig Wirkung	○	keine Wirkung	◆	Grundlage f.d. Wirkung

Umfassendes Firewallsystem 3/3

Angriffsart	Sicherheitsaspekte eines umfassenden Firewallsystems	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

Der Zusammenhang zwischen Investiton, Schutzbedarf und Profitwahrscheinlichkeit



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

Utimaco Safeware AG

Safeware for your e-@ssets

www.utimaco.com

info.de@utimaco.de