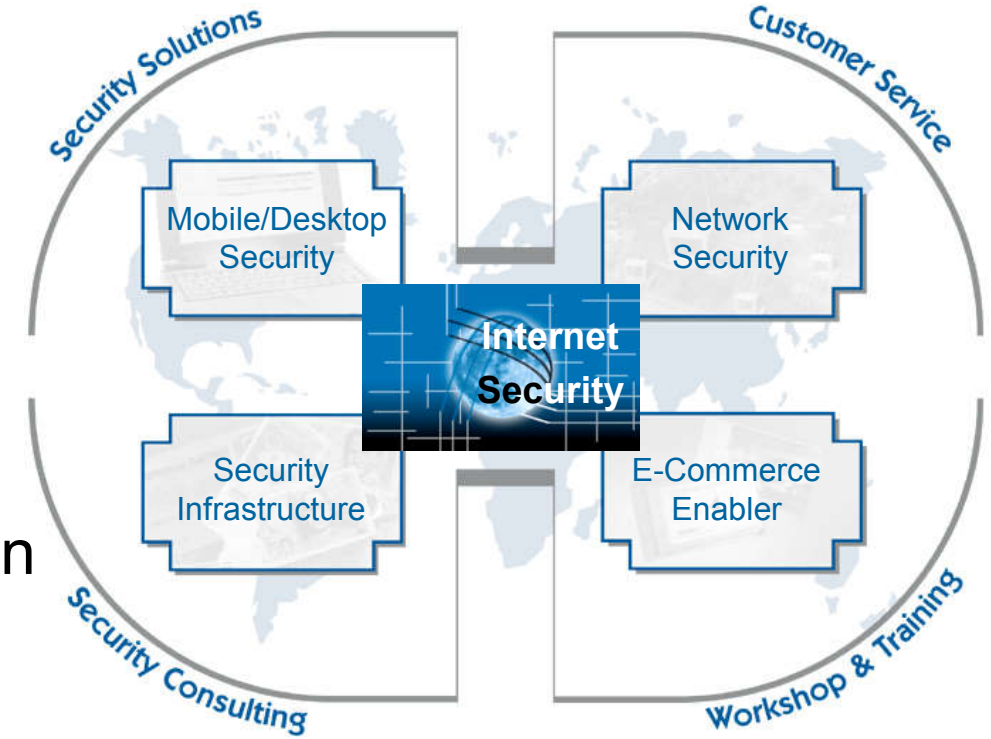
Firewalls - State of the art



Dipl.-Ing. Norbert Pohlmann
Mitglied des Vorstandes
Utimaco Safeware AG

utimaco®
safeware

Inhalt

- Sicherheitsziele von umfassenden Firewall-Systemen
- Bedrohungspotentiale
- Firewall-Sicherheitsdienste und deren Wirkung
- Konzeptionelle Möglichkeiten und Grenzen von zentralen Firewall-Systemen
- Ergänzende Sicherheitsmechanismen:
  - VPN
  - Intrusion Detection
  - Anti-Malware / Viren Scanner
  - Personal Firewall
- Die Wirkung von umfassenden Firewall-Systemen
- Marktübersicht und Einordnung von Firewall-Produkten

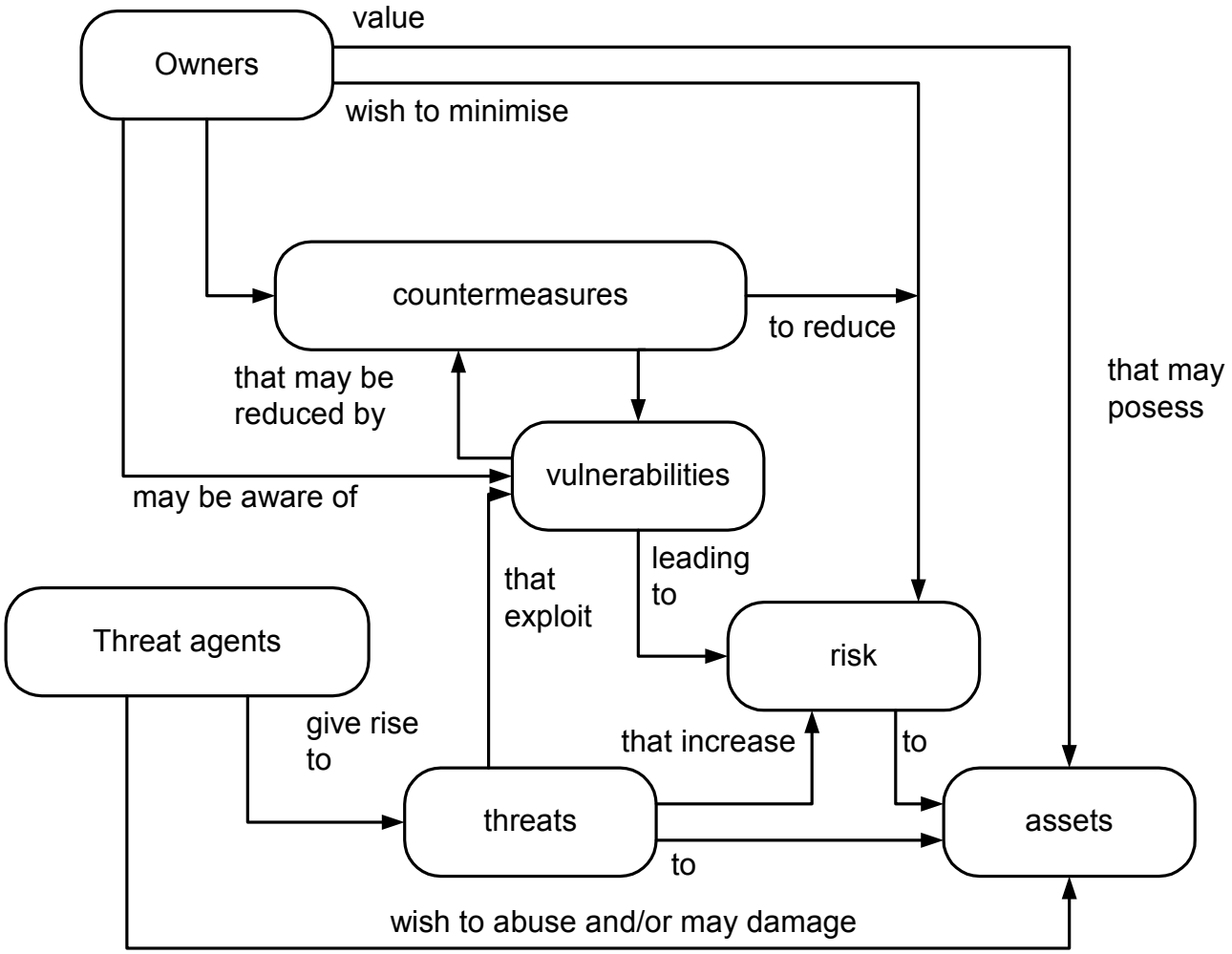
© Utimaco Safeware AG 09.07.2016

Sicherheitsziele bei der Umsetzung eines umfassenden Firewall-Systems

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

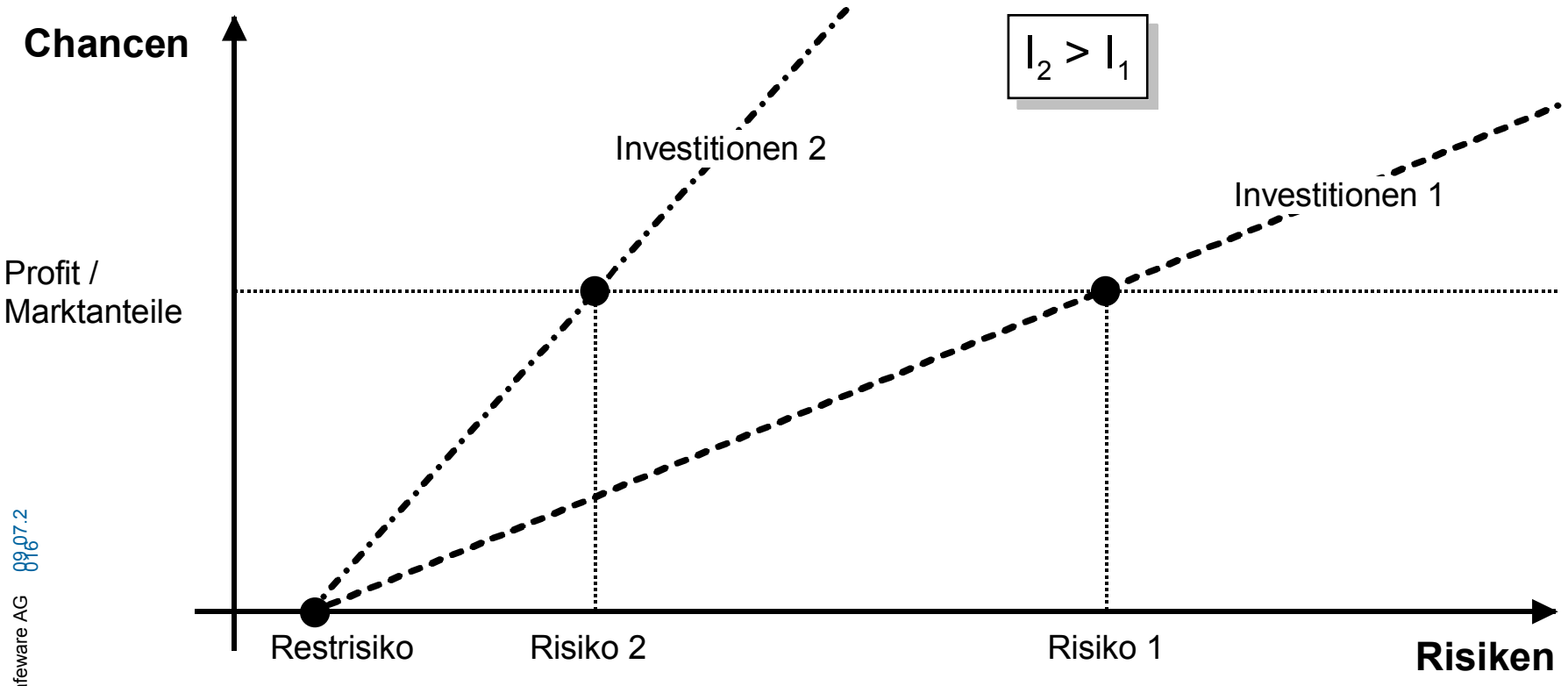
© Utimaco Safeware AG

IT-Sicherheit als Wirkungs- und Handlungszusammenhang



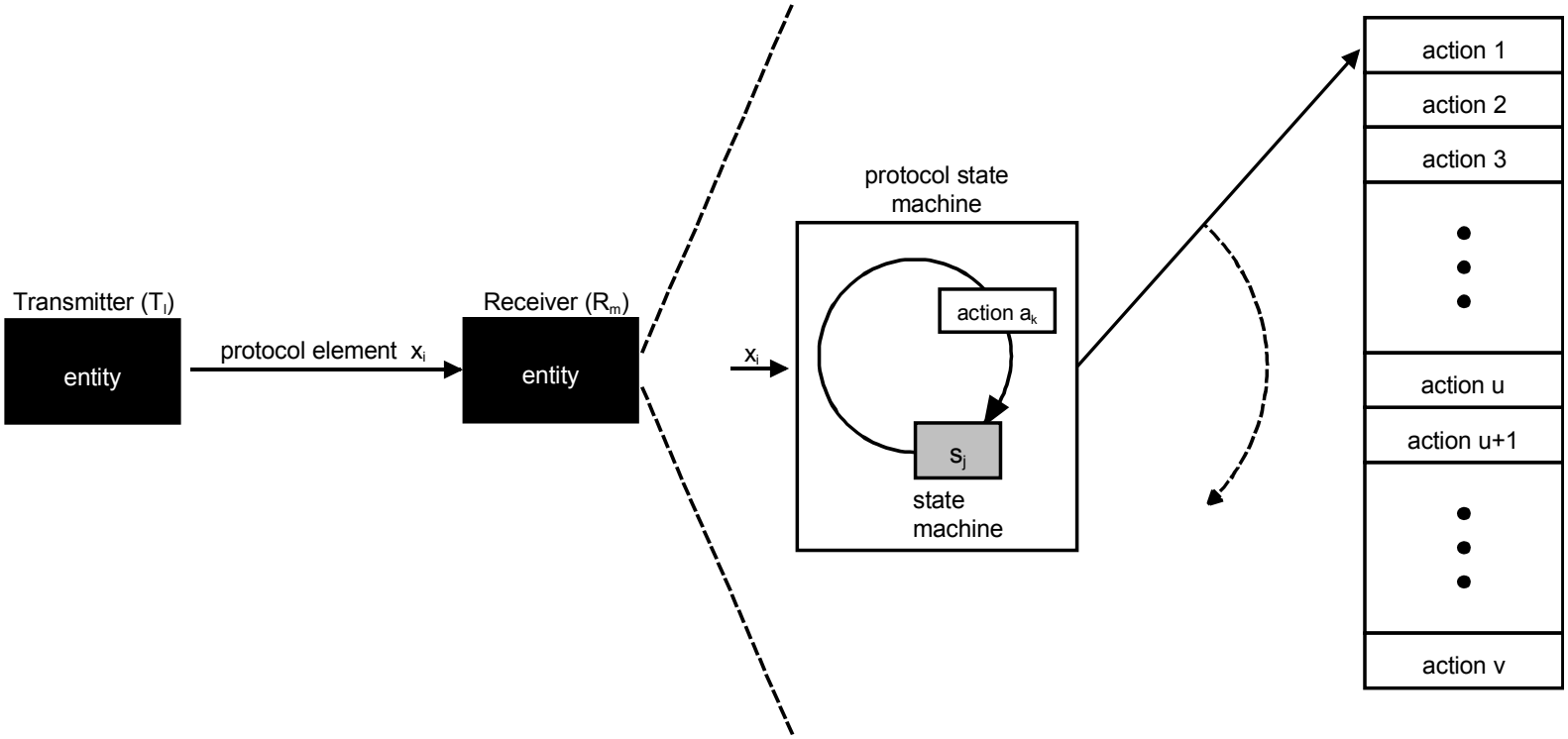
© Utimaco Safeware AG 09.07.2016

Reduzierung von Risiken



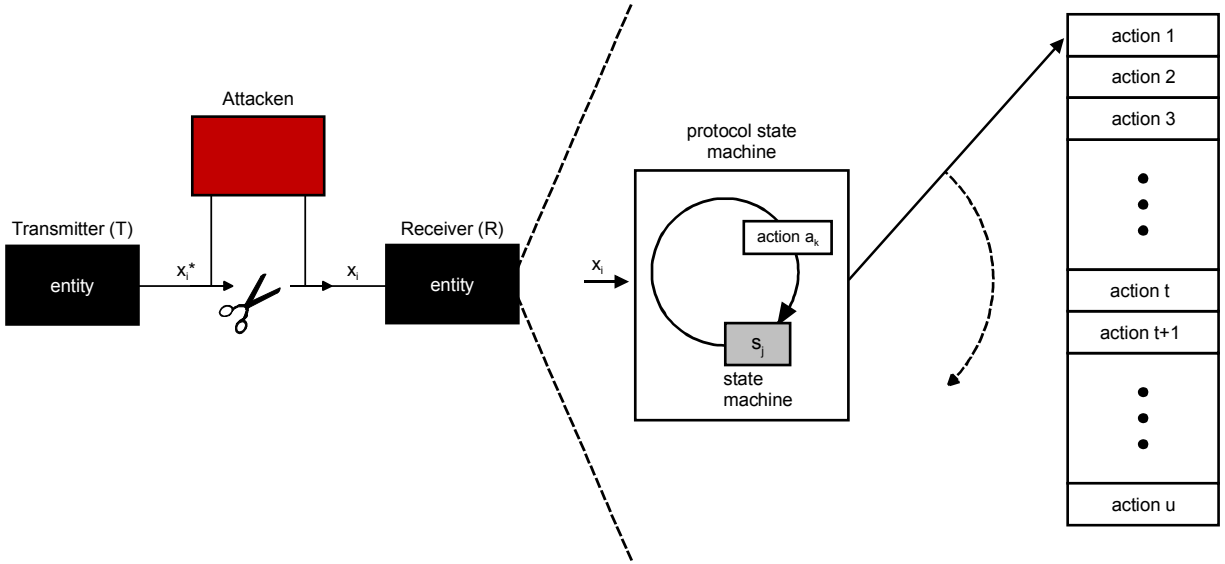
© Utimaco Safeware AG 09.07.2016

Vereinfachtes logisches Kommunikationsmodell



© Utimaco Safeware AG

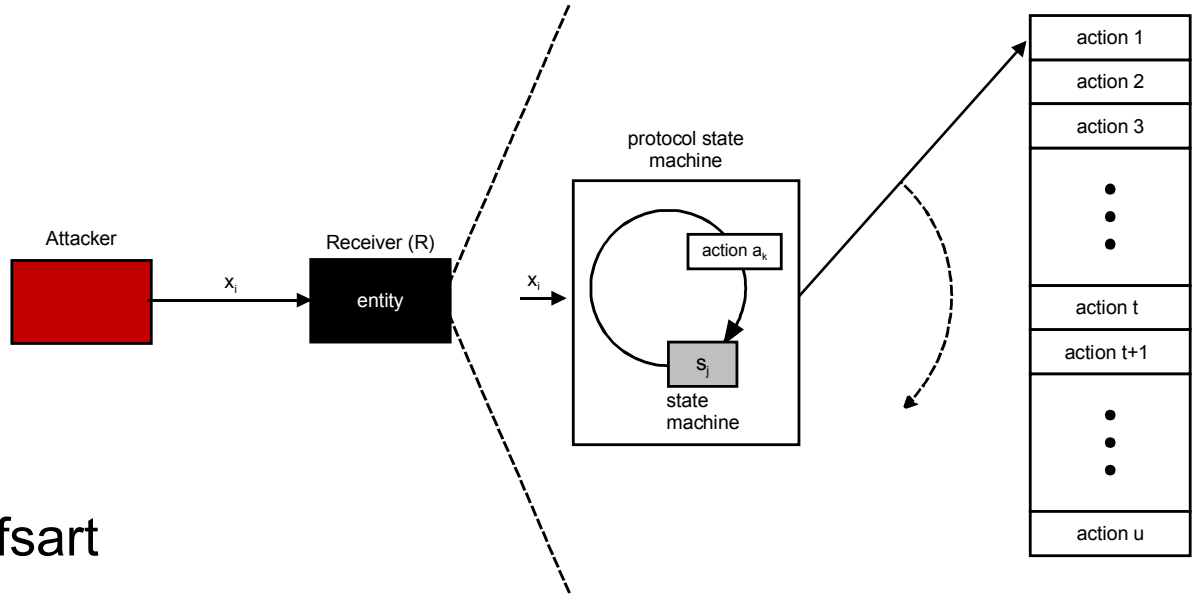
Bedrohungen
-> Angriffe durch Dritte



- 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, ...)

© Utimaco Safeware AG

Bedrohungen
-> Angriffe von Kommunikationspartnern

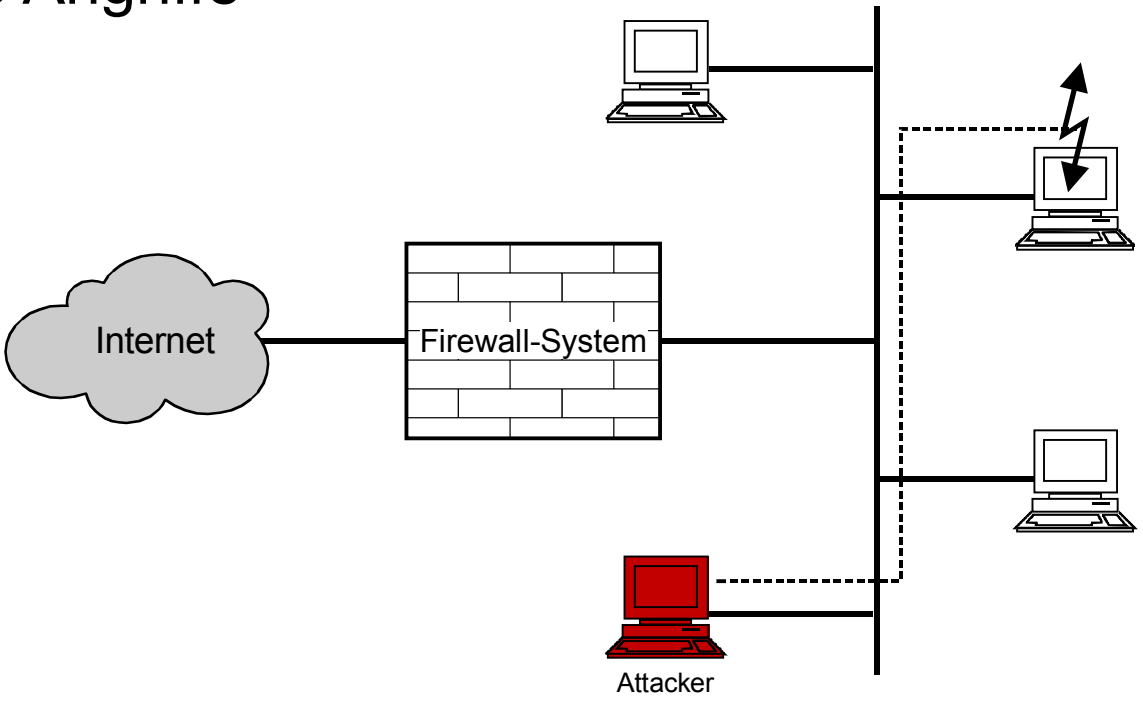


- Angriffsart
  - Unberechtigter Aufbau und Nutzung einer Kommunikationsverbindung
  - Unberechtigte Nutzung von Kommunikationsprotokollen und -diensten
  - Vortäuschen einer falschen Identität (Maskerade-Angriff)
  - Nutzung der Kommunikationsverbindung zum Receiver für gezielte Angriffe (z.B. Java-Applets,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

© Utimaco Safeware AG

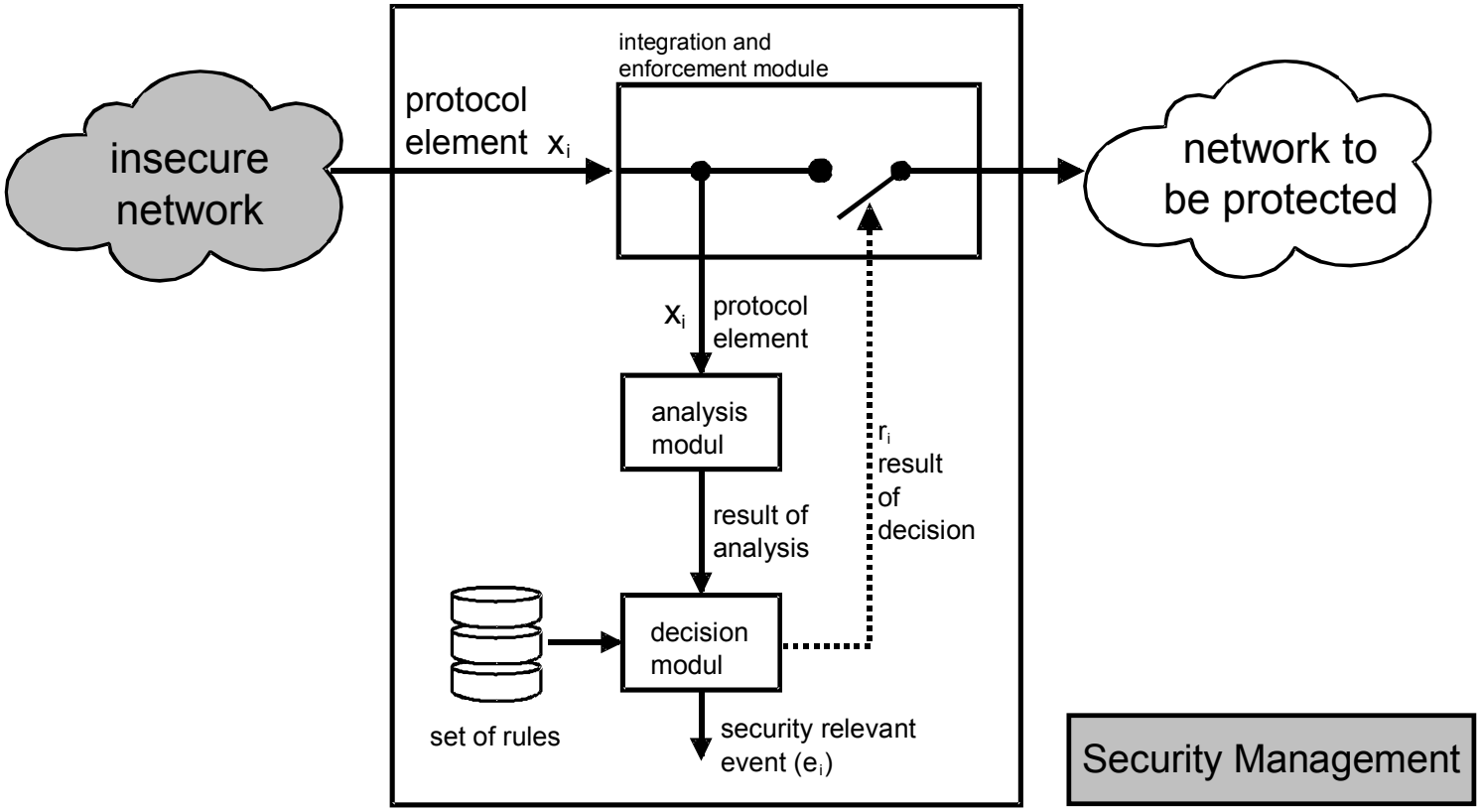
Bedrohung
-> Vorbereitung eines Angriffs

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



© Utimaco Safeware AG

Definition eines Firewall-Elements

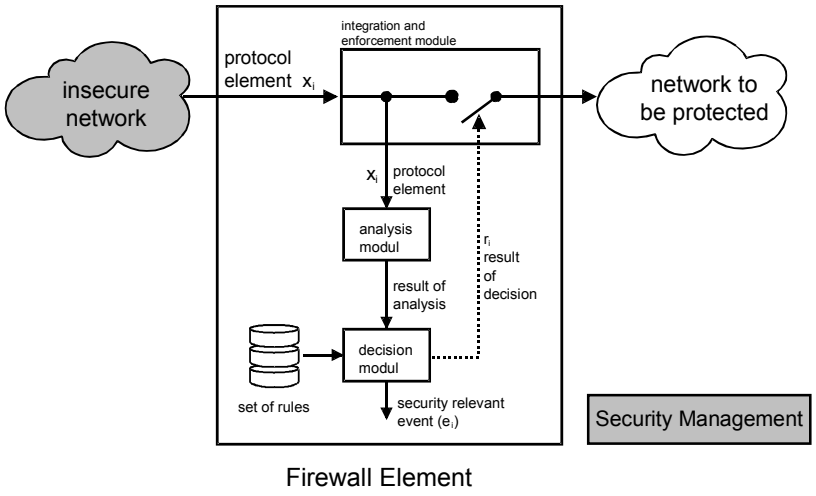


Firewall Element

© Utimaco Safeware AG 09.07.2016

Bedrohungen
-> Angriffe auf das Firewall-System

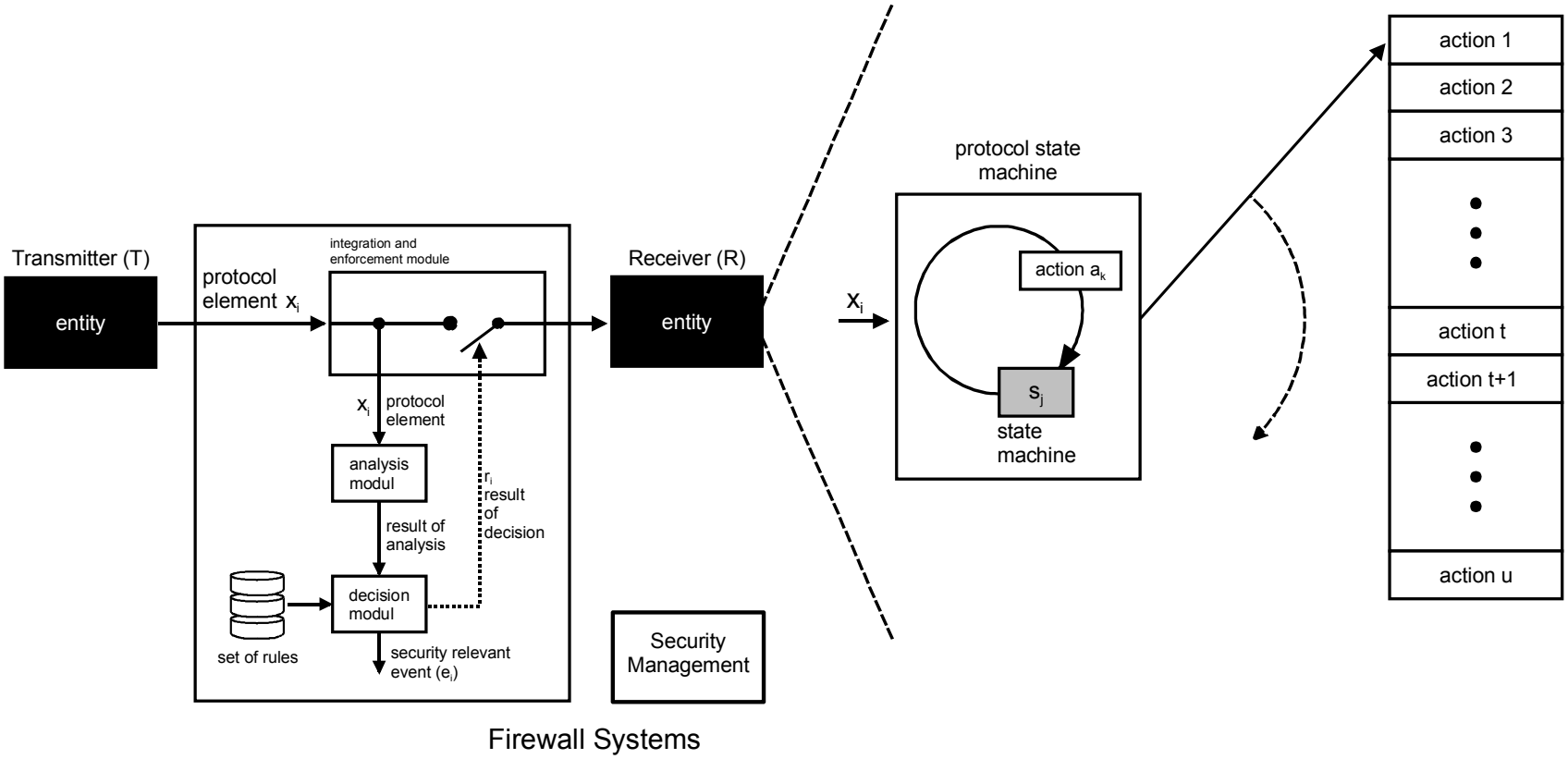
- Angriffsart
  - Manipulation des Firewall-Systems
  - Einbau einer Trap-Door
  - Nutzung einer falschen Konfiguration des Firewall-Systems
  - Nutzung von Implementierungsfehlern des Firewall-Systems



Firewall Element

© Utimaco Safeware AG 09.07.2016

Das Kommunikationsmodell mit integriertem Firewall-System



Firewall Systems

© Utimaco Safeware AG 09.07.2016

Sicherheitsdienste eines Firewall-Systems

- Zugangskontrolle auf Netzwerkebene
- Zugangskontrolle auf Benutzerebene
- Zugangskontrolle auf Datenebene
- Rechteverwaltung
- Kontrolle auf Anwendungsebene
- Entkopplung von Diensten
- Beweissicherung und Protokollauswertung
- Alarmierung
- Verbergen der internen Netzstruktur

© Utimaco Safeware AG

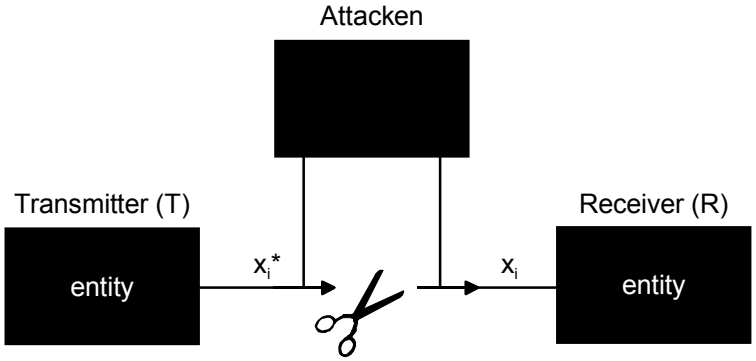
Definition der verwendeten Symbole

Symbol	Kurzbeschreibung	Definition
●	sehr große Wirkung	Der entsprechende Sicherheitsmechanismus wirkt so stark gegen den definierten Angriff, daß praktisch kein Schaden auftreten kann. Stärke des Sicherheitsmechanismus: „hoch“
◕	große Wirkung	Der entsprechende Sicherheitsmechanismus wirkt stark gegen den definierten Angriff, daß normalerweise kein Schaden auftreten kann. Stärke des Sicherheitsmechanismus: „hoch/mittel“
◑	Wirkung	Der entsprechende Sicherheitsmechanismus wirkt gegen den definierten Angriff, daß typischerweise kein Schaden auftreten kann. Stärke des Sicherheitsmechanismus: „mittel“
◔	gering Wirkung	Der entsprechende Sicherheitsmechanismus wirkt gering gegen den definierten Angriff, daß unbeabsichtigt kein Schaden auftreten kann. Stärke des Sicherheitsmechanismus: „niedrig“
○	keine Wirkung	Der entsprechende Sicherheitsmechanismus hat gegen den definierten Angriff keine Wirkung, so daß ein Schaden auftreten kann.
◆	Grundlage für die Wirkung	Der entsprechende Sicherheitsmechanismus ist eine Grundlage damit das Firewall-System überhaupt gegen Angriffe wirken kann.

© Utimaco Safeware AG 09.07.2

Die Wirkung der Sicherheitsdienste 1/3

Zugangskontrolle auf Netzwerkebene

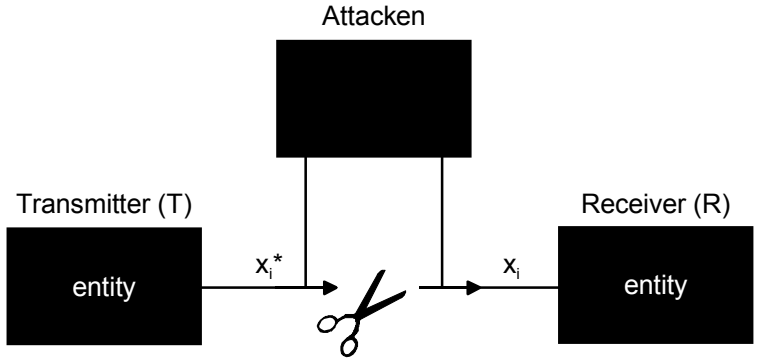
Angriffsart	Sicherheitsfunktionen	Zugangskontrolle auf Netzwerkebene	Zugangskontrolle auf Benutzerebene	Zugangskontrolle auf Datenebene	Rechteverwaltung	Kontrolle auf Anwendungsebene	Entkoppelung von Diensten	Beweissicherung u. Protokollauswertung	Alarmierung	Verbergen der internen Netzstruktur
										
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

© Utimaco Safeware AG 2007

Die Wirkung der Sicherheitsdienste 1/3

Zugangskontrolle auf Benutzerebene

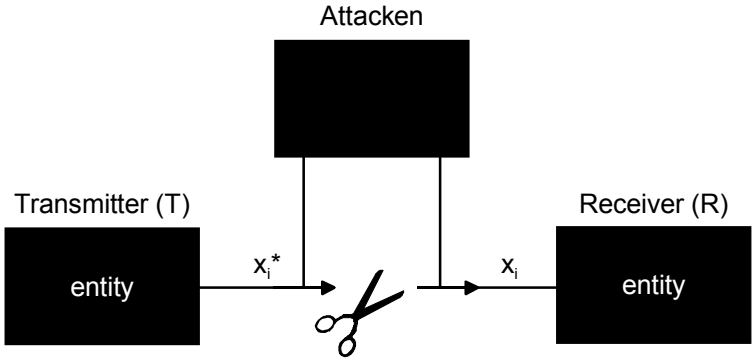
Angriffsart	Sicherheitsfunktionen	Zugangskontrolle auf Netzwerkebene	Zugangskontrolle auf Benutzerebene	Zugangskontrolle auf Datenebene	Rechteverwaltung	Kontrolle auf Anwendungsebene	Entkoppelung von Diensten	Beweissicherung u. Protokollauswertung	Alarmierung	Verbergen der internen Netzstruktur
										
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

© Utimaco Safeware AG 2007

Die Wirkung der Sicherheitsdienste 1/3

Zugangskontrolle auf Datenebene

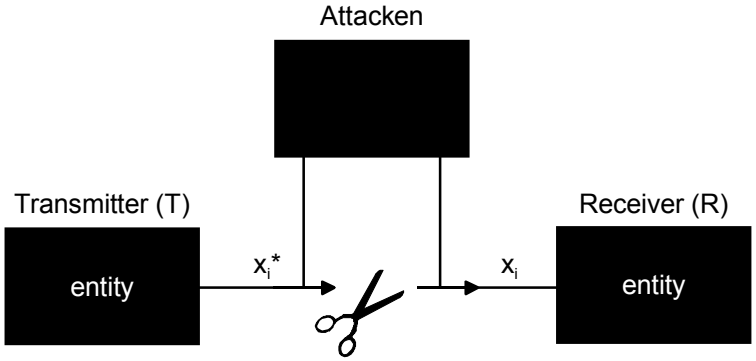
Angriffsart	Sicherheitsfunktionen	Zugangskontrolle auf Netzwerkebene	Zugangskontrolle auf Benutzerebene	Zugangskontrolle auf Datenebene	Rechteverwaltung	Kontrolle auf Anwendungsebene	Entkoppelung von Diensten	Beweissicherung u. Protokollauswertung	Alarmierung	Verbergen der internen Netzstruktur
										
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

© Utimaco Safeware AG 2007

Die Wirkung der Sicherheitsdienste 1/3

Rechteverwaltung

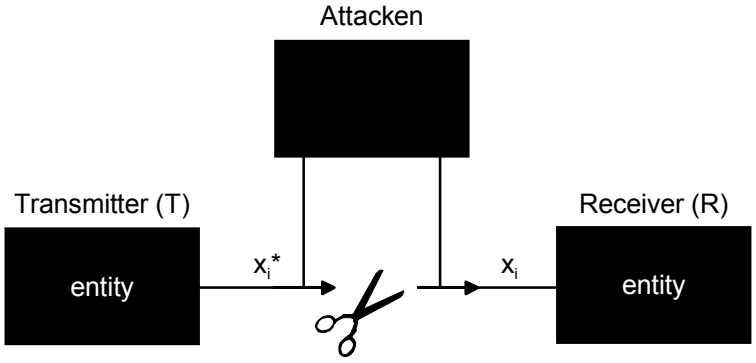
Angriffsart	Sicherheitsfunktionen	Zugangskontrolle auf Netzwerkebene	Zugangskontrolle auf Benutzerebene	Zugangskontrolle auf Datenebene	Rechteverwaltung	Kontrolle auf Anwendungsebene	Entkoppelung von Diensten	Beweissicherung u. Protokollauswertung	Alarmierung	Verbergen der internen Netzstruktur
										
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

© Utimaco Safeware AG 2007

Die Wirkung der Sicherheitsdienste 1/3

Kontrolle auf Anwendungsebene

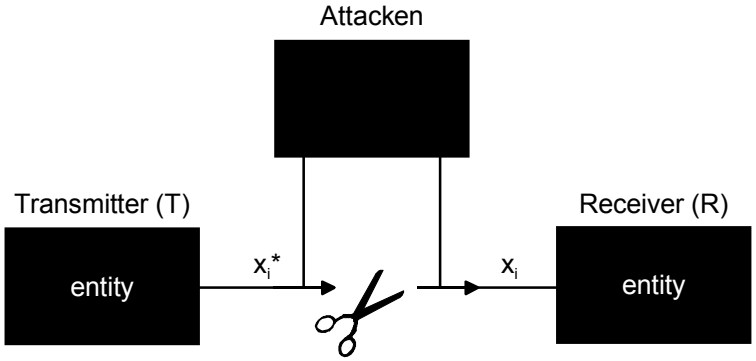
Angriffsart	Sicherheitsfunktionen	Zugangskontrolle auf Netzwerkebene	Zugangskontrolle auf Benutzerebene	Zugangskontrolle auf Datenebene	Rechteverwaltung	Kontrolle auf Anwendungsebene	Entkoppelung von Diensten	Beweissicherung u. Protokollauswertung	Alarmierung	Verbergen der internen Netzstruktur
										
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

© Utimaco Safeware AG 2007

Die Wirkung der Sicherheitsdienste 1/3

Beweissicherung u. Protokollauswertung

Angriffsart	Sicherheitsfunktionen	Zugangskontrolle auf Netzwerkebene	Zugangskontrolle auf Benutzerebene	Zugangskontrolle auf Datenebene	Rechteverwaltung	Kontrolle auf Anwendungsebene	Entkoppelung von Diensten	Beweissicherung u. Protokollauswertung	Alarmierung	Verbergen der internen Netzstruktur
										
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,	○	○	○	◑	◕	○	◔	◔	○

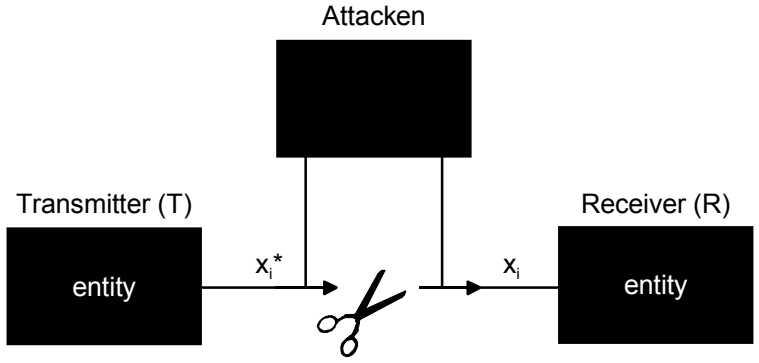
●	sehr große Wirkung	◕	große Wirkung	◑	Wirkung
◔	wenig Wirkung	○	keine Wirkung	◆	Grundlage f.d. Wirkung

© Utimaco Safeware AG 2007

Die Wirkung der Sicherheitsdienste 1/3

Alarmierung

Angriffsart	Sicherheitsfunktionen	Zugangskontrolle auf Netzwerkebene	Zugangskontrolle auf Benutzerebene	Zugangskontrolle auf Datenebene	Rechteverwaltung	Kontrolle auf Anwendungsebene	Entkoppelung von Diensten	Beweissicherung u. Protokollauswertung	Alarmierung	Verbergen der internen Netzstruktur
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,	○	○	○	◑	◕	○	◔	◔	○



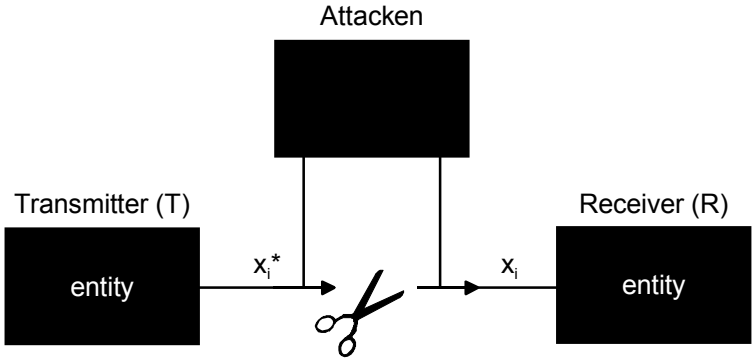
●	sehr große Wirkung	◕	große Wirkung	◑	Wirkung
◔	wenig Wirkung	○	keine Wirkung	◆	Grundlage f.d. Wirkung

© Utimaco Safeware AG 09.07.2

utimaco safeware

Die Wirkung der Sicherheitsdienste 1/3

Verbergen der internen Netzstruktur

Angriffsart	Sicherheitsfunktionen	Zugangskontrolle auf Netzwerkebene	Zugangskontrolle auf Benutzerebene	Zugangskontrolle auf Datenebene	Rechteverwaltung	Kontrolle auf Anwendungsebene	Entkoppelung von Diensten	Beweissicherung u. Protokollauswertung	Alarmierung	Verbergen der internen Netzstruktur
										
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,	○	○	○	◑	◕	○	◔	◔	○

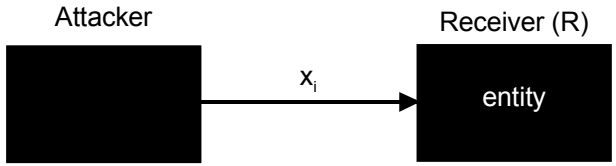
●	sehr große Wirkung	◕	große Wirkung	◑	Wirkung
◔	wenig Wirkung	○	keine Wirkung	◆	Grundlage f.d. Wirkung

© Utimaco Safeware AG 2007

Die Wirkung der Sicherheitsdienste 2/3

Zugangskontrolle auf Netzwerkebene

Angriffsart	Sicherheitsfunktionen	Zugangskontrolle auf Netzwerkebene	Zugangskontrolle auf Benutzerebene	Zugangskontrolle auf Datenebene	Rechteverwaltung	Kontrolle auf Anwendungsebene	Entkoppelung von Diensten	Beweissicherung u. Protokollauswertung	Alarmierung	Verbergen der internen Netzstruktur
Angriffe durch den Transmitter	Nutzung von Kommunikationsprotollen und -diensten	○	○	○	●	●	○	◑	◔	○
	Vortäuschen einer falschen Identität (Maskerade-Angriff)	◔	●	●	○	○	○	○	○	○
	falsche Konfiguration/Implementierungsfehler	○	○	○	○	○	◕	◑	◔	○
	Leugnen der Kommunikationsbeziehung	○	○	○	○	○	○	◕	○	○



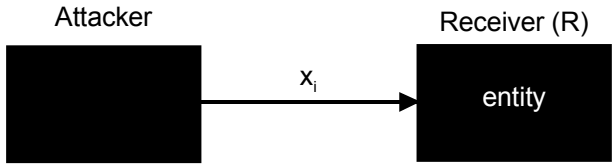
●	sehr große Wirkung	◕	große Wirkung	◑	Wirkung
◔	wenig Wirkung	○	keine Wirkung	◆	Grundlage f.d. Wirkung

© Utimaco Safeware AG 2007

Die Wirkung der Sicherheitsdienste 2/3

Zugangskontrolle auf Benutzerebene

Angriffsart	Sicherheitsfunktionen	Zugangskontrolle auf Netzwerkebene	Zugangskontrolle auf Benutzerebene	Zugangskontrolle auf Datenebene	Rechteverwaltung	Kontrolle auf Anwendungsebene	Entkoppelung von Diensten	Beweissicherung u. Protokollauswertung	Alarmierung	Verbergen der internen Netzstruktur
Angriffe durch den Transmitter	Nutzung von Kommunikationsprotollen und -diensten	○	○	○	●	●	○	◑	◔	○
	Vortäuschen einer falschen Identität (Maskerade-Angriff)	◔	●	●	○	○	○	○	○	○
	falsche Konfiguration/Implementierungsfehler	○	○	○	○	○	◕	◑	◔	○
	Leugnen der Kommunikationsbeziehung	○	○	○	○	○	○	◕	○	○



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

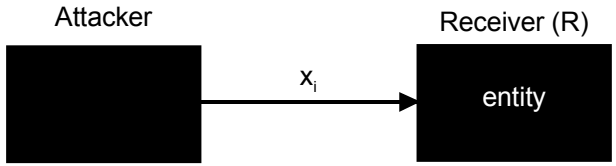
© Utimaco Safeware AG 09.07.2016

utimaco safeware

Die Wirkung der Sicherheitsdienste 2/3

Zugangskontrolle auf Datenebene

Angriffsart	Sicherheitsfunktionen	Zugangskontrolle auf Netzwerkebene	Zugangskontrolle auf Benutzerebene	Zugangskontrolle auf Datenebene	Rechteverwaltung	Kontrolle auf Anwendungsebene	Entkoppelung von Diensten	Beweissicherung u. Protokollauswertung	Alarmierung	Verbergen der internen Netzstruktur
Angriffe durch den Transmitter	Nutzung von Kommunikationsprotollen und -diensten	○	○	○	●	●	○	◑	◔	○
	Vortäuschen einer falschen Identität (Maskerade-Angriff)	◔	●	●	○	○	○	○	○	○
	falsche Konfiguration/Implementierungsfehler	○	○	○	○	○	◕	◑	◔	○
	Leugnen der Kommunikationsbeziehung	○	○	○	○	○	○	◕	○	○



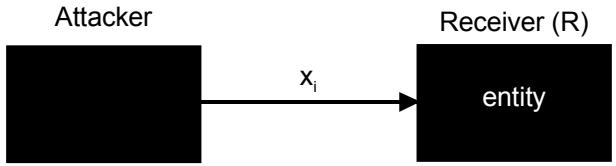
●	sehr große Wirkung	◕	große Wirkung	◑	Wirkung
◔	wenig Wirkung	○	keine Wirkung	◆	Grundlage f.d. Wirkung

© Utimaco Safeware AG 2007

Die Wirkung der Sicherheitsdienste 2/3

Rechteverwaltung

Angriffsart	Sicherheitsfunktionen	Zugangskontrolle auf Netzwerkebene	Zugangskontrolle auf Benutzerebene	Zugangskontrolle auf Datenebene	Rechteverwaltung	Kontrolle auf Anwendungsebene	Entkoppelung von Diensten	Beweissicherung u. Protokollauswertung	Alarmierung	Verbergen der internen Netzstruktur
Angriffe durch den Transmitter	Nutzung von Kommunikationsprotollen und -diensten	○	○	○	●	●	○	◑	◔	○
	Vortäuschen einer falschen Identität (Maskerade-Angriff)	◔	●	●	○	○	○	○	○	○
	falsche Konfiguration/Implementierungsfehler	○	○	○	○	○	◕	◑	◔	○
	Leugnen der Kommunikationsbeziehung	○	○	○	○	○	○	◕	○	○



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

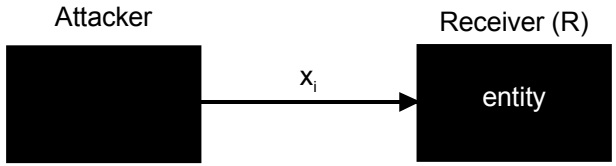
© Utimaco Safeware AG 09.07.2016

utimaco safeware

Die Wirkung der Sicherheitsdienste 2/3

Kontrolle auf Anwendungsebene

Angriffsart	Sicherheitsfunktionen	Zugangskontrolle auf Netzwerkebene	Zugangskontrolle auf Benutzerebene	Zugangskontrolle auf Datenebene	Rechteverwaltung	Kontrolle auf Anwendungsebene	Entkoppelung von Diensten	Beweissicherung u. Protokollauswertung	Alarmierung	Verbergen der internen Netzstruktur
Angriffe durch den Transmitter	Nutzung von Kommunikationsprotollen und -diensten	○	○	○	●	●	○	◑	◔	○
	Vortäuschen einer falschen Identität (Maskerade-Angriff)	◔	●	●	○	○	○	○	○	○
	falsche Konfiguration/Implementierungsfehler	○	○	○	○	○	◕	◑	◔	○
	Leugnen der Kommunikationsbeziehung	○	○	○	○	○	○	◕	○	○



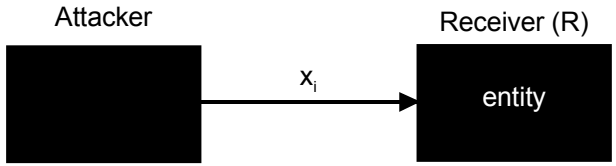
●	sehr große Wirkung	◕	große Wirkung	◑	Wirkung
◔	wenig Wirkung	○	keine Wirkung	◆	Grundlage f.d. Wirkung

© Utimaco Safeware AG

Die Wirkung der Sicherheitsdienste 2/3

Entkoppelung von Diensten

Angriffsart	Sicherheitsfunktionen	Zugangskontrolle auf Netzwerkebene	Zugangskontrolle auf Benutzerebene	Zugangskontrolle auf Datenebene	Rechteverwaltung	Kontrolle auf Anwendungsebene	Entkoppelung von Diensten	Beweissicherung u. Protokollauswertung	Alarmierung	Verbergen der internen Netzstruktur
Angriffe durch den Transmitter	Nutzung von Kommunikationsprotollen und -diensten	○	○	○	●	●	○	◑	◔	○
	Vortäuschen einer falschen Identität (Maskerade-Angriff)	◔	●	●	○	○	○	○	○	○
	falsche Konfiguration/Implementierungsfehler	○	○	○	○	○	◕	◑	◔	○
	Leugnen der Kommunikationsbeziehung	○	○	○	○	○	○	◕	○	○



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

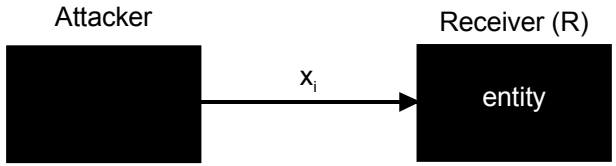
© Utimaco Safeware AG 09.07.2

utimaco safeware

Die Wirkung der Sicherheitsdienste 2/3

Beweissicherung u. Protokollauswertung

Angriffsart	Sicherheitsfunktionen	Zugangskontrolle auf Netzwerkebene	Zugangskontrolle auf Benutzerebene	Zugangskontrolle auf Datenebene	Rechteverwaltung	Kontrolle auf Anwendungsebene	Entkoppelung von Diensten	Beweissicherung u. Protokollauswertung	Alarmierung	Verbergen der internen Netzstruktur
Angriffe durch den Transmitter	Nutzung von Kommunikationsprotollen und -diensten	○	○	○	●	●	○	◑	◔	○
	Vortäuschen einer falschen Identität (Maskerade-Angriff)	◔	●	●	○	○	○	○	○	○
	falsche Konfiguration/Implementierungsfehler	○	○	○	○	○	◕	◑	◔	○
	Leugnen der Kommunikationsbeziehung	○	○	○	○	○	○	◕	○	○



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

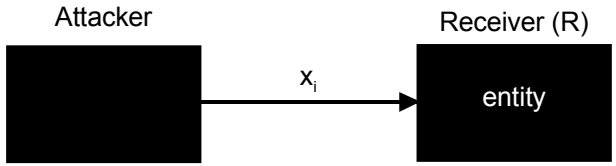
© Utimaco Safeware AG 2007

utimaco safeware

Die Wirkung der Sicherheitsdienste 2/3

Alarmierung

Angriffsart	Sicherheitsfunktionen	Zugangskontrolle auf Netzwerkebene	Zugangskontrolle auf Benutzerebene	Zugangskontrolle auf Datenebene	Rechteverwaltung	Kontrolle auf Anwendungsebene	Entkoppelung von Diensten	Beweissicherung u. Protokollauswertung	Alarmierung	Verbergen der internen Netzstruktur
Angriffe durch den Transmitter	Nutzung von Kommunikationsprotollen und -diensten	○	○	○	●	●	○	◑	◔	○
	Vortäuschen einer falschen Identität (Maskerade-Angriff)	◔	●	●	○	○	○	○	○	○
	falsche Konfiguration/Implementierungsfehler	○	○	○	○	○	◕	◑	◔	○
	Leugnen der Kommunikationsbeziehung	○	○	○	○	○	○	◕	○	○

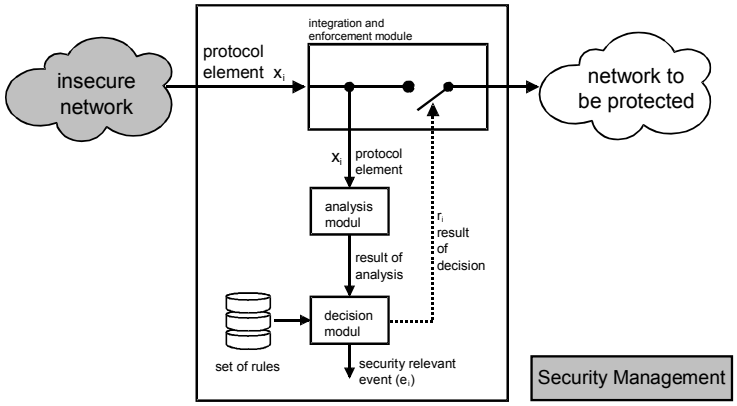


●	sehr große Wirkung	◕	große Wirkung	◑	Wirkung
◔	wenig Wirkung	○	keine Wirkung	◆	Grundlage f.d. Wirkung

© Utimaco Safeware AG 2007

Die Wirkung der Sicherheitsdienste 3/3

Beweissicherung u. Protokollauswertung

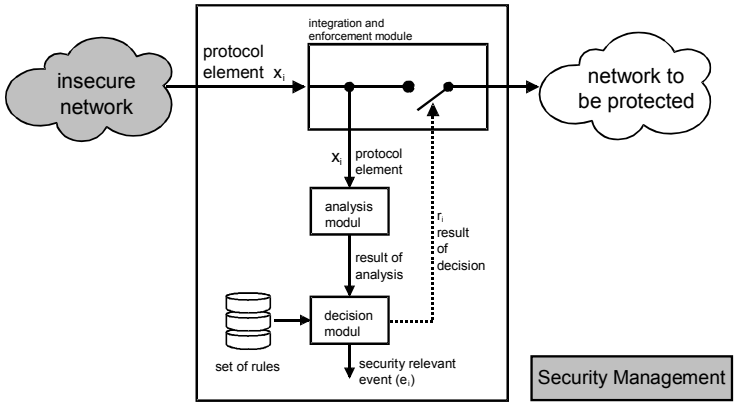
Angriffsart	Sicherheitsfunktionen	Zugangskontrolle auf Netzwerkebene	Zugangskontrolle auf Benutzerebene	Zugangskontrolle auf Datenebene	Rechteverwaltung	Kontrolle auf Anwendungsebene	Entkoppelung von Diensten	Beweissicherung u. Protokollauswertung	Alarmierung	Verbergen der internen Netzstruktur
	 Firewall Element									
Vorbereitung für Angriffe	Social Engineering	○	○	○	○	○	○	○	○	○
	Analyse mit Hilfe von Scannerprogrammen	○	○	○	○	○	○	◔	◔	●
Angriffe auf das Firewall-System	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

© Utimaco Safeware AG 09.07.2016

Die Wirkung der Sicherheitsdienste 3/3

Alarmierung

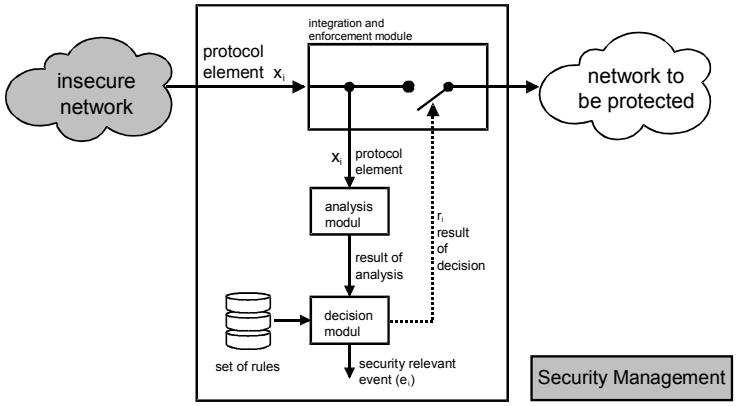
Angriffsart	Sicherheitsfunktionen	Zugangskontrolle auf Netzwerkebene	Zugangskontrolle auf Benutzerebene	Zugangskontrolle auf Datenebene	Rechteverwaltung	Kontrolle auf Anwendungsebene	Entkoppelung von Diensten	Beweissicherung u. Protokollauswertung	Alarmierung	Verbergen der internen Netzstruktur
	 Firewall Element									
Vorbereitung für Angriffe	Social Engineering	○	○	○	○	○	○	○	○	○
	Analyse mit Hilfe von Scannerprogrammen	○	○	○	○	○	○	◔	◔	●
Angriffe auf das Firewall-System	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

© Utimaco Safeware AG 2007.2

Die Wirkung der Sicherheitsdienste 3/3

Verbergen der internen Netzstruktur

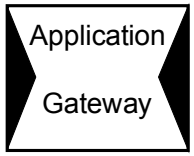
Angriffsart	Sicherheitsfunktionen	Zugangskontrolle auf Netzwerkebene	Zugangskontrolle auf Benutzerebene	Zugangskontrolle auf Datenebene	Rechteverwaltung	Kontrolle auf Anwendungsebene	Entkoppelung von Diensten	Beweissicherung u. Protokollauswertung	Alarmierung	Verbergen der internen Netzstruktur
	 Firewall Element									
Vorbereitung für Angriffe	Social Engineering	○	○	○	○	○	○	○	○	○
	Analyse mit Hilfe von Scannerprogrammen	○	○	○	○	○	○	◔	◔	●
Angriffe auf das Firewall-System	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

© Utimaco Safeware AG 09.07.2016

Firewall-Elemente und -Konzepte

- Firewall-Elemente
  - Packet Filter 

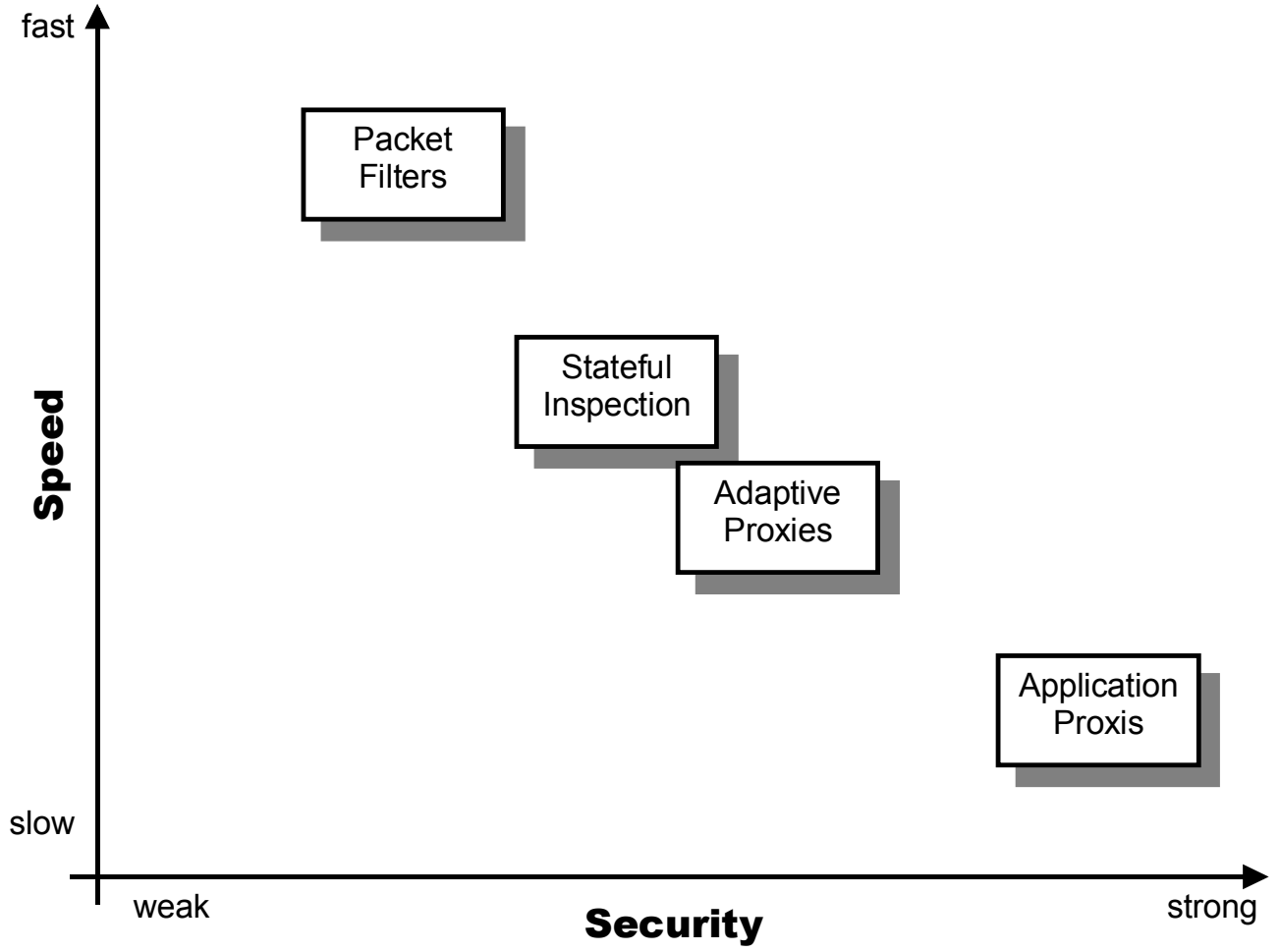
  - Zusandsorientierter Packet Filter (stateful inspection)
  - Application Gateway 

  - Adaptive Proxy

- Firewall-Konzepte
  - Ausschließlicher Einsatz von Firewall-Elementen
  - Kombination von Firewall-Elementen
    - High-level Security Firewall-System

© Utimaco Safeware AG

Firewall-Elemente im Verhältnis zu Schnelligkeit und Sicherheit

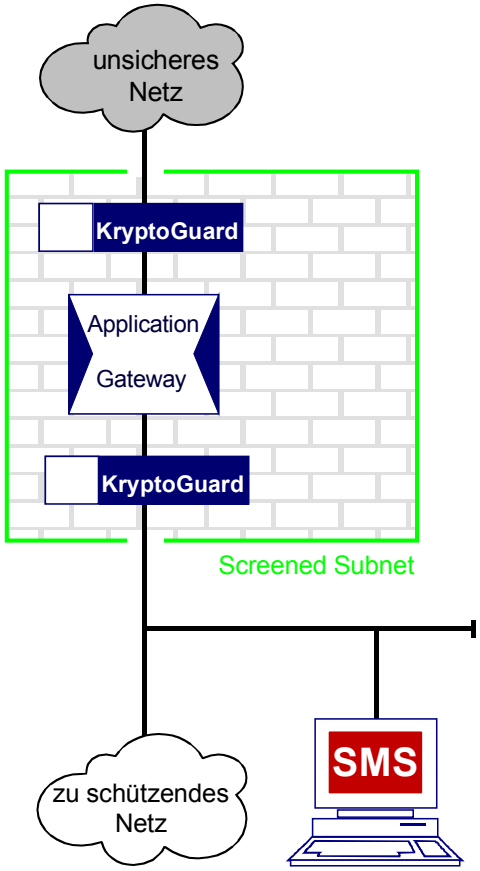


© Utimaco Safeware AG 09.07.2016

utimaco safeware

High-level Security Firewall-System

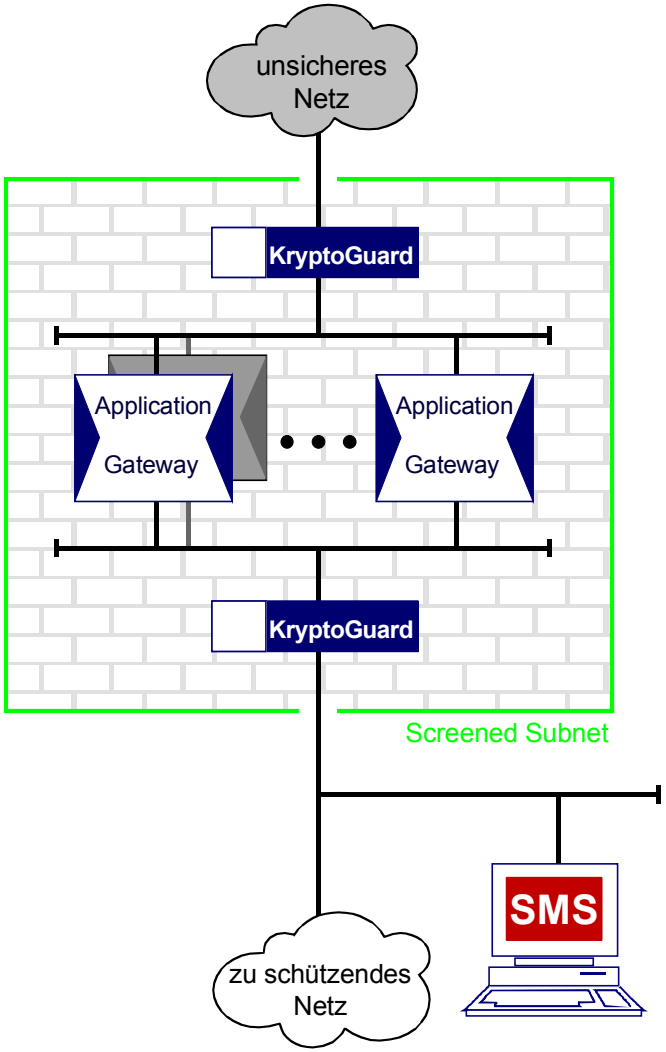
- Einfache Regeln
- Gegenseitiger Schutz
- Geschachtelte Sicherheit
- Verschiedene Betriebssysteme
- Unterschiedliche Einbindungs- und Analysemöglichkeiten
- Separates Security Management



© Utimaco Safeware AG 09.07.2

Mehrere Application Gateways parallel

- Trennung bestimmter Dienste
- Leistung steigern
- Redundanz schaffen



© Utimaco Safeware AG 09.07.2016

Konzeptionelle Möglichkeiten zentraler Firewall-Systeme

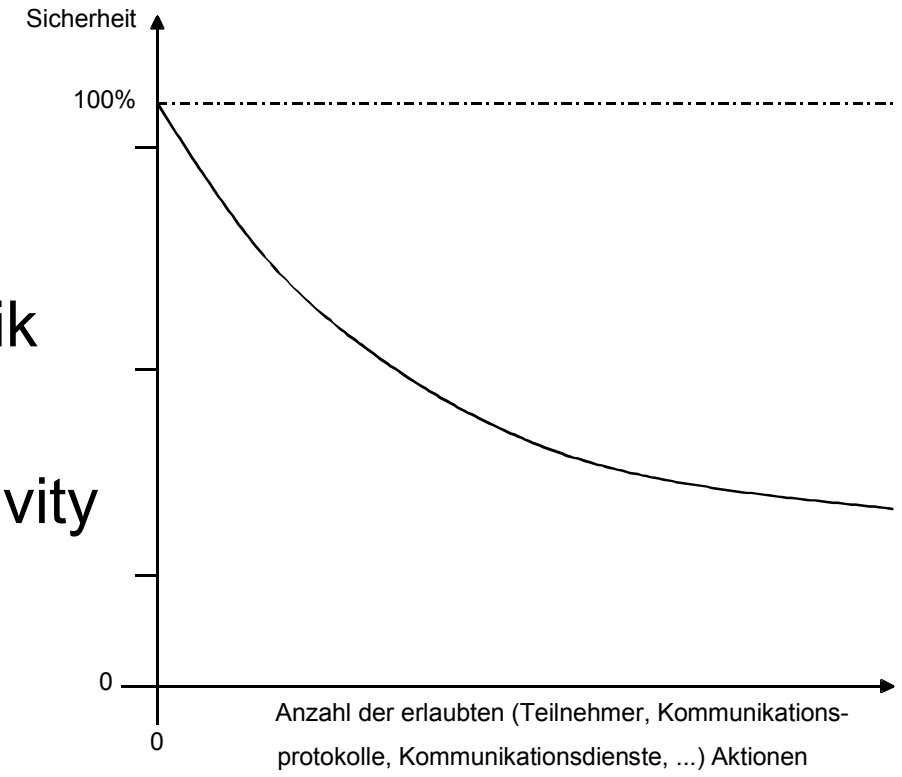
- Common Point of Trust-Konzept
  - Kosten
  - Umsetzung der Sicherheitspolitik
  - Sicherheitsinfrastruktur
  - Sicherheit durch Abschottung
  - Überprüfbarkeit
- Reduzierung des Schadensrisikos

© Utimaco Safeware AG

Konzeptionelle Grenzen eines zentralen Firewall-Systems

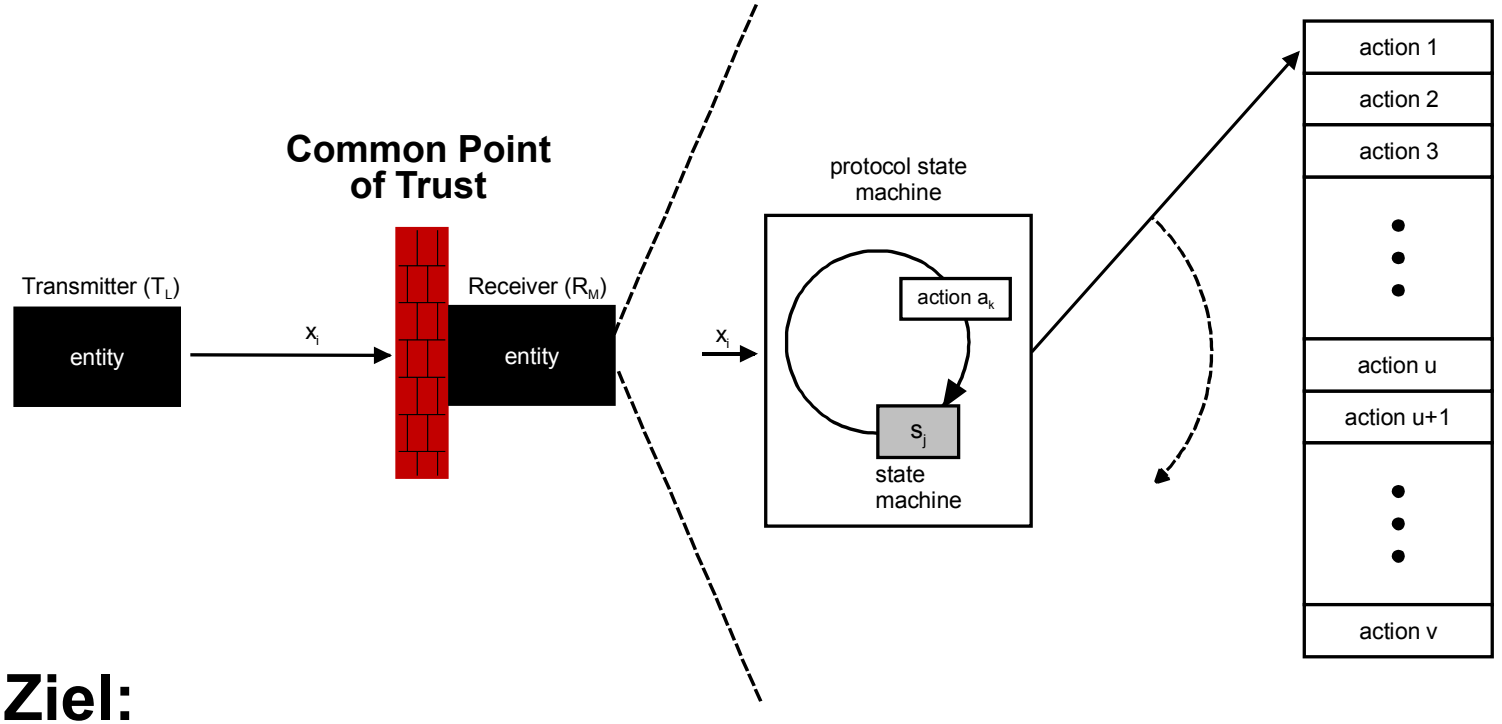
- Hintertüren (Back Door)
- Interne Angriffe
- Angriffe auf Datenebene
- Wissen und Hypothese
- Richtige Sicherheitspolitik und deren Umsetzung
- Security versus connectivity

Risiko versus Chance



© Utimaco Safeware AG 09.07.2016

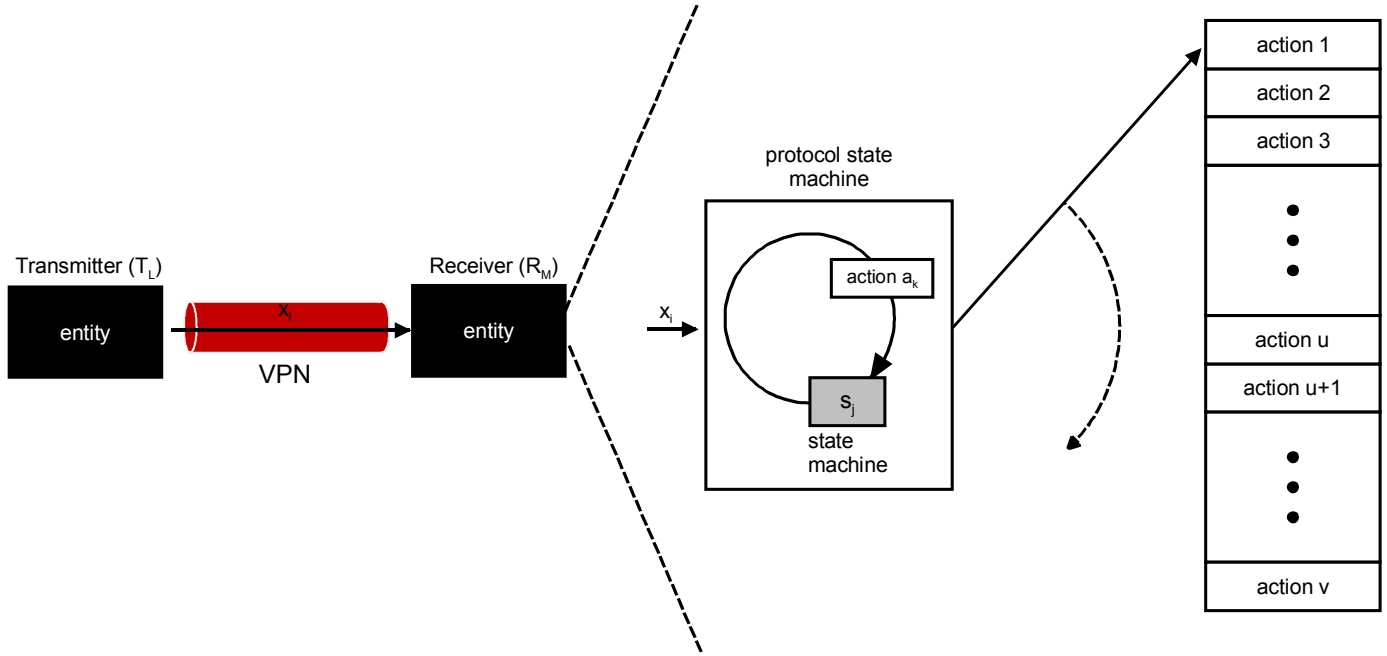
Zentrales High-level Firewall-System
-> Analogie zum Pförtner



- **Ziel:**
  - Analysiert, kontrolliert und reglementiert die Kommunikation, für alle Rechersysteme hinter dem Firewall-System, einer einheitlichen Sicherheitspolitik folgend
  - Protokolliert sicherheitsrelevante Ereignisse
  - Alarmiert bei erheblichen Verstößen

© Utimaco Safeware AG 09.07.2016

Verschlüsselung - VPNs
-> Analogie zum Sicherheitstransporter

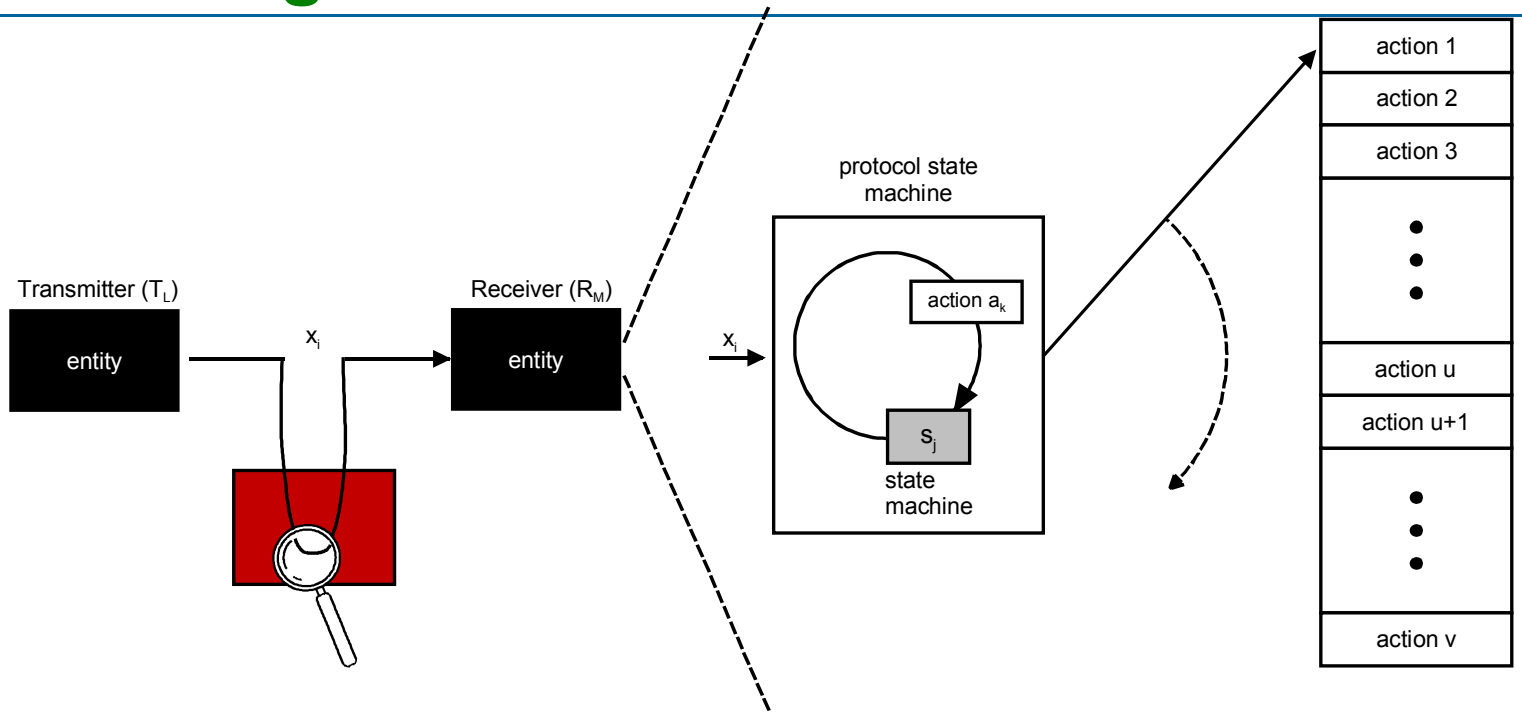


- **Ziel:**
  - **Vertraulichkeit der Protokollelemente**
  - Verhinderung von Trittbrettfahrern
  - Verhinderung einer gezielten Manipulation von Protokollelementen

© Utimaco Safeware AG 09.07.2016

Zentraler Virenscanner

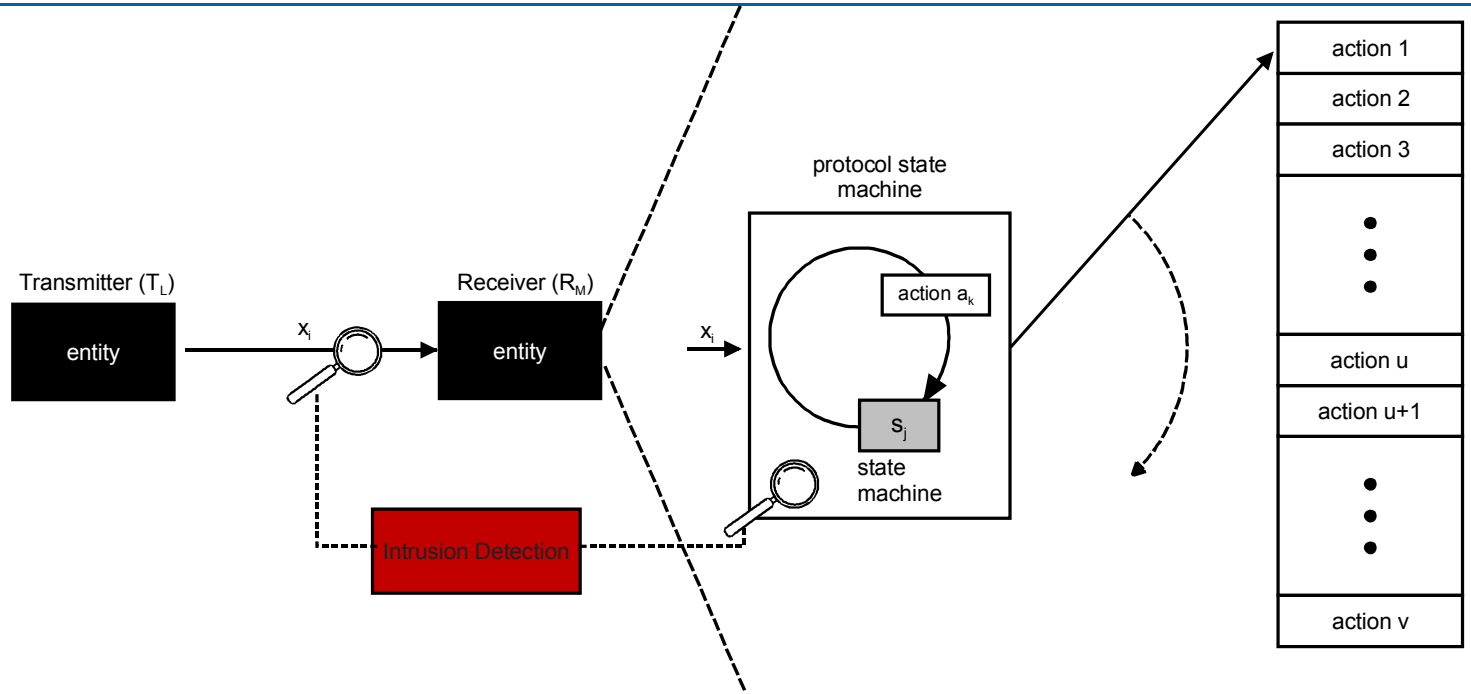
-> Analogie zur zentralen Poststelle



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

© Utimaco Safeware AG 09.07.2016

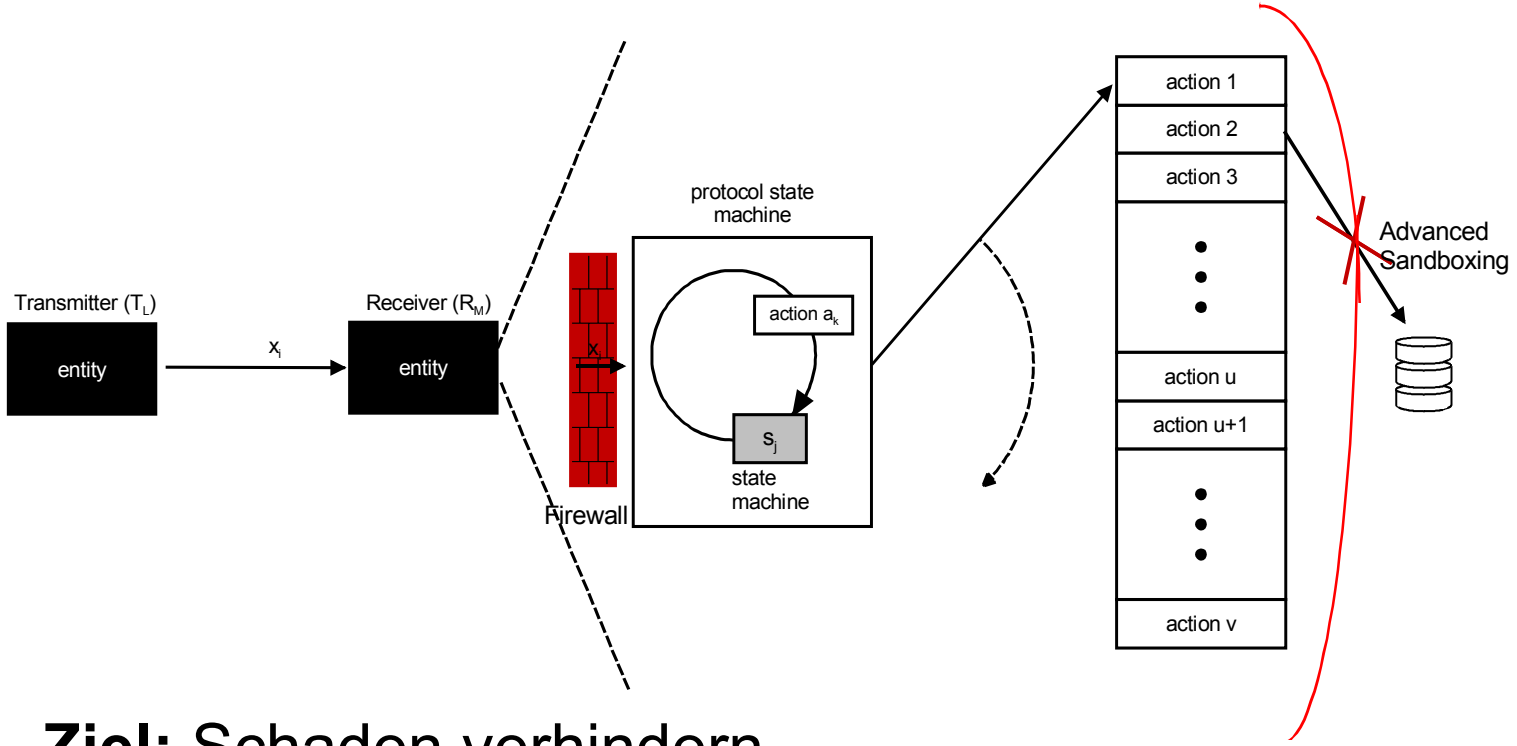
Intrusion Detection
-> Analogie zur Videoüberwachung



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

© Utimaco Safeware AG

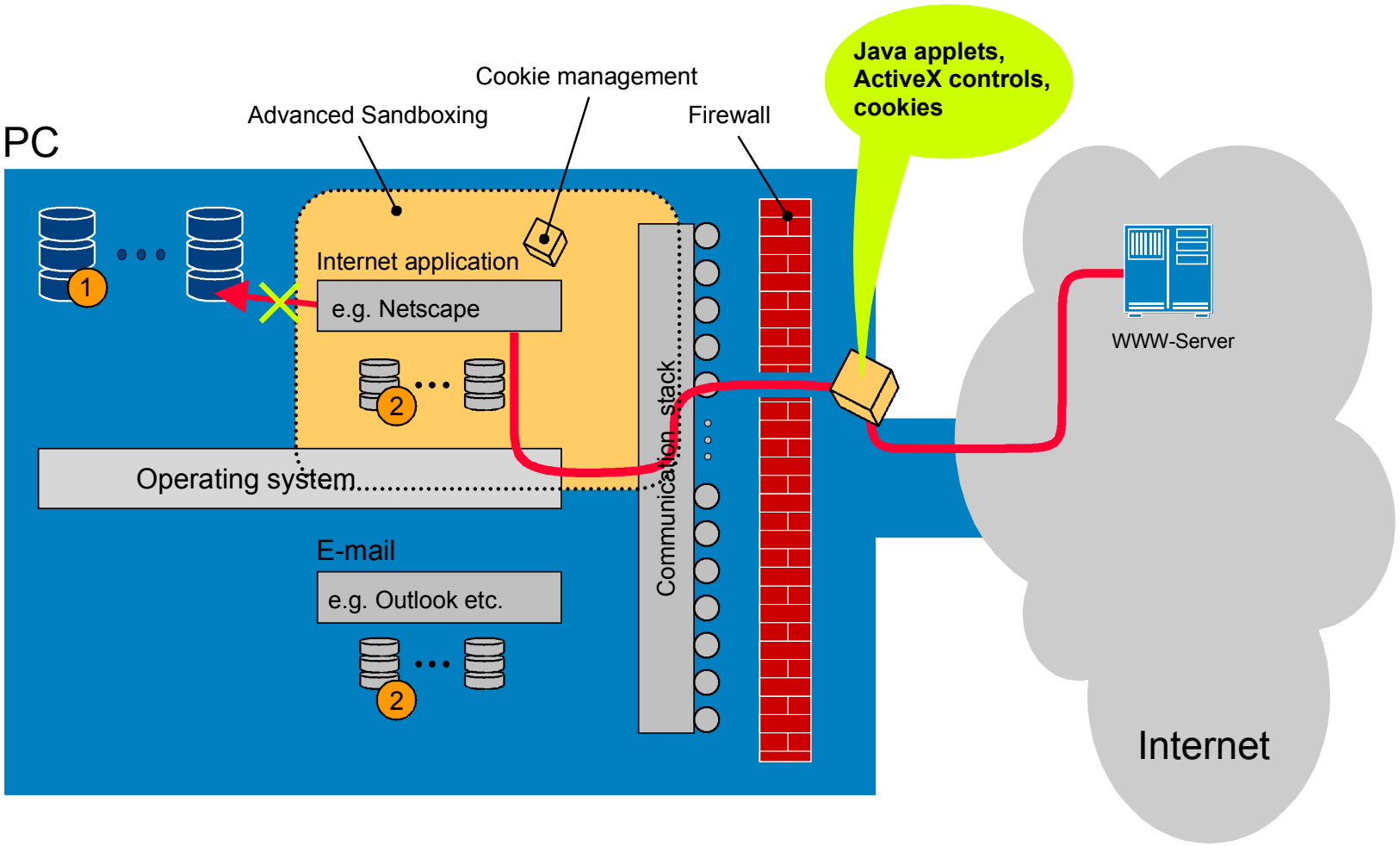
Personal Firewall



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

© Utimaco Safeware AG

Personal Firewall
Advanced Sandboxing



1 High protection necessary

2 No protection needed

© Utimaco Safeware AG 09.07.2016

Nichttechnische Sicherheitsmechanismen

- Infrastruktur
  - Zugangsgesicherter Raum
  - Unterbrechungsfreie Stromversorgung, usw.
- Organisation
  - Festlegung der Verantwortung und Zugriffsrechte
  - Kontrolle der Protokolldaten, usw.
- Personal
  - Anweisungen, Aufklärung und Sensibilisierung der Benutzer
  - Schulung zum Thema Sicherheit, usw.
- Notfall
  - Festlegung der Verfügbarkeitsanforderung
  - Schaffen und testen von Backup-Möglichkeiten, usw.

© Utimaco Safeware AG 09.07.2016

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 AG 09.07.2016

Audits, Revision

- Ziel:
  - Entdeckung von Schwachstellen und Sicherheitslücken
  - Permanente Abstimmung zwischen den Sicherheitsrichtlinien und deren praktischer Umsetzung

© Utimaco Safeware AG 09.07.2016

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

© Utimaco Safeware AG

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

© Utimaco Safeware AG 09.07.2016

Umfassendes Firewallsystem 1/3 -

Wiederholen/Verzögern von Protokollelementen

- 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.*

Angriffsart		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

© Utimaco Safeware AG 09.07.2

Umfassendes Firewallsystem 1/3 -

Einfügen/Löschen von Daten in Protokollelementen

- 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.*

Angriffsart	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

© Utimaco Safeware AG 09.07.2

Umfassendes Firewallsystem 1/3 -

Modifikation der Daten in Protokollelementen

- 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.*

Angriffsart		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

© Utimaco Safeware AG 09.07.2

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

© Utimaco Safeware AG 09.07.2

Umfassendes Firewallsystem 1/3 -

Trittbrettfahrer

Angriffsart	▪ 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.*	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

© Utimaco Safeware AG 09.07.2

Umfassendes Firewallsystem 1/3 -

Empfangen von Malware

Angriffsart	▪ 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.*	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

© Utimaco Safeware AG 2007

Umfassendes Firewallsystem 2/3 -

Aufbau und Nutzung von Kommunikationsverbindungen

Angriffsart	▪ 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.*	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

© Utimaco Safeware AG 09.07.2

Umfassendes Firewallsystem 2/3 -

Nutzung von Protokollen und Diensten

Angriffsart		High-level Security Firewall-System	Verschlüsselung	Anti-Malware-System	Intrusion Detection Systeme	Personal Firewall	nichttechnische Sicherheitsmaßnahmen	Vertrauenswürdigkeit	Audits	Sicherheitspolitik	sicherer Betrieb
	▪ Bei diesem Angriff hat ein High-level Security Firewall-System (Rechteverwaltung) 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*.										
Angriffe durch den Transmitter	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

© Utimaco Safeware AG 09.07.2

utimaco safeware

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

© Utimaco Safeware AG 09.07.2

Umfassendes Firewallsystem 2/3 -

Java, Active X, ... Angriffe

Angriffsart	▪ 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.*	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

© Utimaco Safeware AG 09.07.2

Umfassendes Firewallsystem 2/3 -

Falsche Konfiguration/Implementierungsfehler

Angriffsart	▪ 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.*	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

© Utimaco Safeware AG 2007

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

© Utimaco Safeware AG 09.07.2

utimaco safeware

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

© Utimaco Safeware AG 2007

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

© Utimaco Safeware AG 2007

Umfassendes Firewallsystem 3/3 -

Manipulation des Firewall-Systems

Angriffsart	▪ Ein high-level Security Firewall-System verhindert diesen Angriff: sicheres Designkonzept, eigene Schutzmechanismen, separates und zentrales Security Management, versch. Firewall-Elemente. ▪ Durch die Verwendung von Intrusion Detection Systemen kann dieser Angriff erkannt werden. ▪ Durch infrastrukturelle Sicherheitsmaßnahmen, wie z.B. zugangsgesicherter Raum, ist eine große Wirkung zu erzielen ▪ Durch regelmäßige Audits kann ein Schaden verhindert werden.	High-level Security Firewall-System	Verschlüsselung	Anti-Malware-System	Intrusion Detection Systeme	Personal Firewall	nichttechnische Sicherheitsmaßnahmen	Vertrauenswürdigkeit	Audits	Sicherheitspolitik	sicherer Betrieb
Vorbereitung 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

© Utimaco Safeware AG 2007

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

© Utimaco Safeware AG 2007

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 Schutzmechanismen 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.										
Vorbereitung 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

© Utimaco Safeware AG 2007

Umfassendes Firewallsystem 3/3 -

Nutzung von Implementierungsfehlern

Angriffsart	▪ Ein high-level Security Firewall-System verhindert diesen Angriff: sicheres Designkonzept,eigene Schutzmechanismen 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.	High-level Security Firewall-System	Verschlüsselung	Anti-Malware-System	Intrusion Detection Systeme	Personal Firewall	nichttechnische Sicherheitsmaßnahmen	Vertrauenswürdigkeit	Audits	Sicherheitspolitik	sicherer Betrieb
Vorbereitung 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

© Utimaco Safeware AG 2007

Umfassendes Firewallsystem 3/3 -

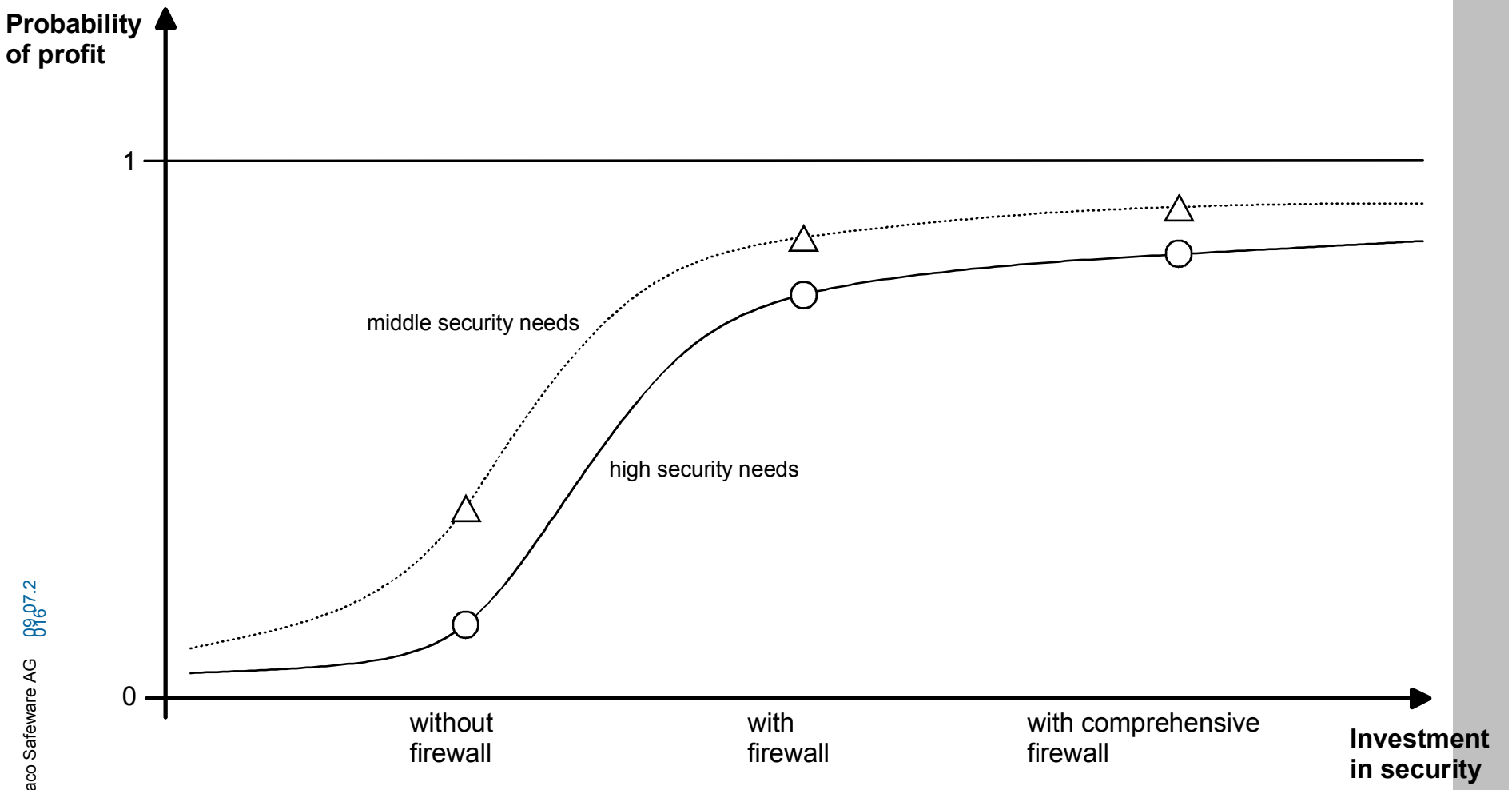
Interne Angriffe

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

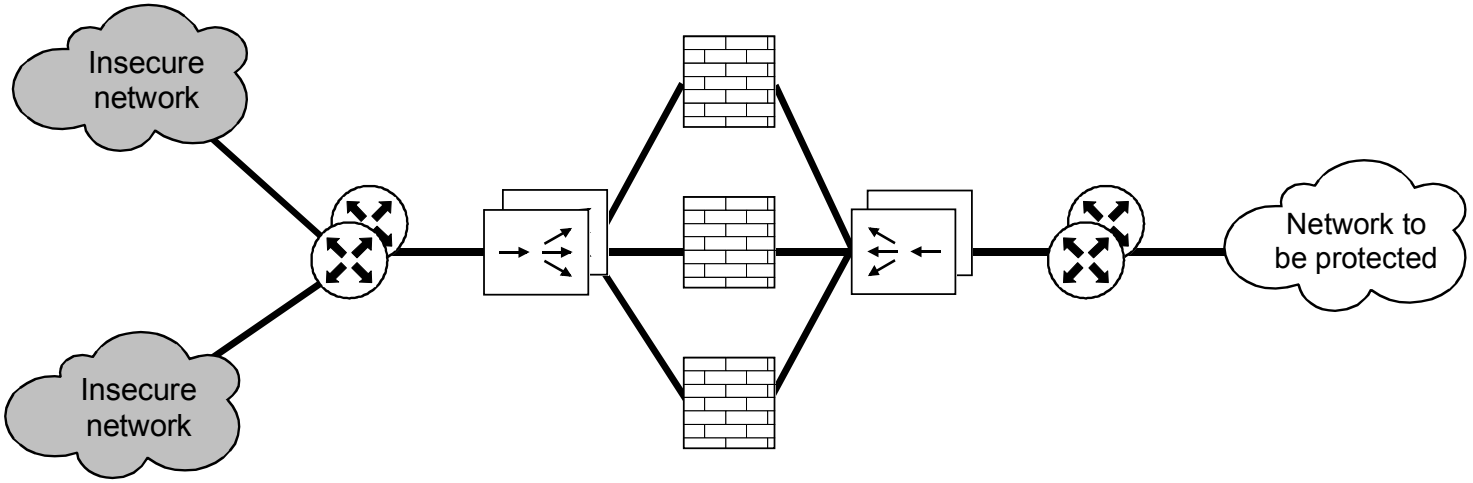
© Utimaco Safeware AG 2007

Zusammenhang zwischen Investment, Schutzbedarf und Profitwahrscheinlichkeit



© Utimaco Safeware AG 09.07.2

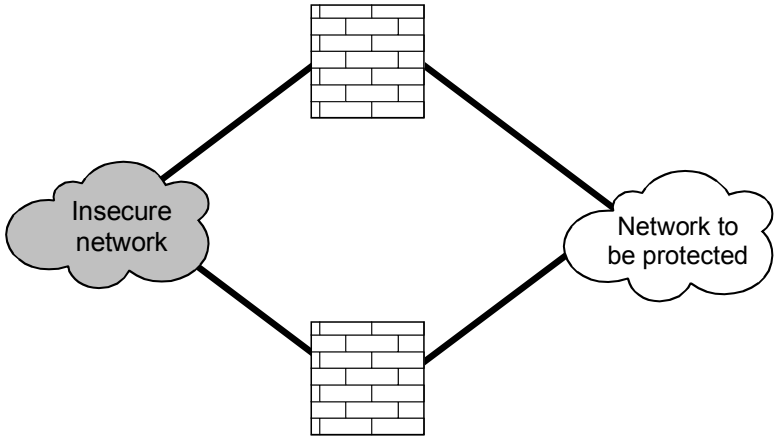
Hochverfügbarkeit (1/3)
-> Redundanz aller Komponenten (horizontal)



- Redundanz aller Komponenten
- Vorteile:
  - Nur 1 System zu administrieren
  - Einheitliche Security Policy

© Utimaco Safeware AG 09.07.2016

Hochverfügbarkeit (2/3)
-> Redundanz vertikal



- Völlig getrennte Firewall-Systeme evtl. verschiedener Hersteller
- Vorteile:
  - Auch verfügbar bei Sicherheitslücken (Security „holes“) in einem System

© Utimaco Safeware AG

Hochverfügbarkeit (3/3)
-> Generelle Aspekte

- Hohe Verfügbarkeit aller Komponenten
  - RAID für Festplatten
  - Redundante Netzteile
  - Backup&Recovery Strategie
  - Physikalisch sichere Aufstellung
  - Unterbrechungsfreie Stromversorgung
  - Organisatorische Maßnahmen
    - Admin immer erreichbar
    - Krisenplan
  - Firewall-Service (Lieferant) mit 7/24 h garantierter Reaktionszeiten

© Utimaco Safeware AG

Verbreitete Firewall-Systeme

- Check Point FireWall-1 und Cisco PIX sind die meistverkauften Firewalls (ca. 80% Marktanteil)
- Symantec/Axent Raptor FW und Network Associates Gauntlet sind die meistgenutzten Proxy-Firewalls
- WatchGuard Firebox kommt im Office-Bereich oft zum Einsatz
- Utimaco Safeware FireWall hat die stärkste Verbreitung der im deutschsprachigen Raum im Bereich der öffentlichen Verwaltung und Behörden => High-level Security Firewall-System

© Utimaco Safeware AG 09.07.2016

Utimaco Safeware AG

Safeware for your e-@ssets

www.utimaco.de

info.de@utimaco.de

© Utimaco Safeware AG 09.07.2016

utimaco® safeware