Die Grenzen digitaler Schutzmauern: kalkuliertes Restrisiko

Autor: **Dipl.-Ing. Norbert Pohlmann**
Mitglied des Vorstandes
Utimaco Safeware AG
☎ 0241-963-1426
🖷 0241-963-1390
E-Mail: norbert.pohlmann@utimaco.de

Inhaltsverzeichnis

1 Einleitung

Um dem internationalen Wettbewerb standzuhalten, müssen sich Organisationen an öffentliche Kommunikationssysteme wie das Internet ankoppeln. Die Organisationen haben dabei meist einen hohen bis sehr hohen Bedarf dafür, ihre Rechnersysteme und Informationen gegen den Verlust von Vertraulichkeit, Integrität und Verfügbarkeit zu schützen. Sie benötigen deshalb Sicherheitssysteme, um sich gegen Angriffe aus dem Internet zu schützen, zum Beispiel Firewall-Systeme. Damit diese wirklich effektiv eingesetzt werden können, sind nachvollziehbare Aussage über deren Möglichkeiten und Grenzen im Sinne von Sicherheit und Vertrauenswürdigkeit wichtig.

2 Ausgangssituation

Es gibt eine Vielzahl von Komponenten, um Firewall-Lösungen aufzubauen: Packet Filter, Stateful Inspection, Application Gateways, Proxies, Adaptive Proxies und andere. Die letzen Jahre haben aber gezeigt, daß zwar viele Organisation Firewall-Komponenten nutzen, diese aber nicht in der Lage sind, Aussagen über die Sicherheit und Vertrauenswürdigkeit ihrer Firewall-Lösung zu machen.

Da aber gerade dieser kritische Übergang vom zu schützenden Netz in das Internet ein großes Risiko darstellt, ist eine Aussage über die Möglichkeiten und Grenzen im Sinne von Sicherheit und Vertrauenswürdigkeit von Firewall-Systemen für die Verantwortlichen der Organisationen von fundamentaler Bedeutung, um eine Einschätzung über das Risiko der Anbindung an das Internet zu erhalten.

Eine 100%ige Sicherheit ist in der Praxis nicht realisierbar – auch nicht mit aufwendigen, bestens geplanten und optimal betriebenen Firewall-Systemen! Es kann nämlich keine absolute Sicherheit von Sicherheitssystemen nachgewiesen werden.

Daher ist es zweckmäßig, die Betrachtung auf die Unsicherheit des Internet-Anschlusses über ein Firewall-System zu lenken. Ziel muß es sein, diese Unsicherheit umfassend zu kennen und zu minimieren, denn durch ein sinkendes Maß an Unsicherheit steigt die Sicherheit über die Einschätzung des Risikos der Anbindung an das Internet.

Zur Erhöhung der technischen Sicherheit von Firewall-Systemen werden mit theoretischen Erkenntnissen und praktischen Erfahrungen mögliche Ursachen, Zusammenhänge, Pfade und Szenarien für „Unsicherheit“ erfaßt und beleuchtet. Dann können, im Sinne von technischem, technologischem und organisatorischem Wissen, Aussagen über die kausalen Abläufe der signifikanten Koalarationen über die Möglichkeiten und Grenzen der Wirkung von Firewall-Systemen getroffen werden.

3 Theoretische Grundlage von Firewall-Systemen

Im folgenden wird ein theoretisches Modell vorgestellt, mit dessen Hilfe die Definition von einheitlichen Kriterien über die Aussagen der Möglichkeiten und Grenzen im Sinne der Wirkung von Sicherheit und Vertrauenswürdigkeit von Firewall-Systemen abgeleitet und klassifiziert werden können /Pohl00b/.

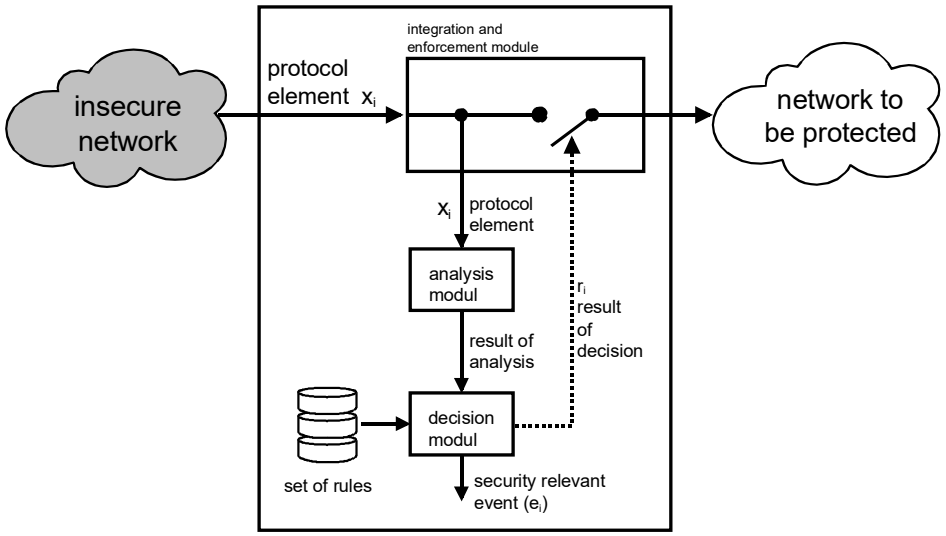
3.1 Definition eines Firewall-Elements

Ein Firewall-System besteht aus Firewall-Elementen, die aktiv in die Kommunikation zwischen dem zu schützenden und dem unsicheren Netz eingreifen sowie einem Security Management, das für die Verwaltung des aktiven Firewall-Elementes verantwortlich ist.

Grundsätzliches:

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

Im folgenden wird der prinzipielle Aufbau der aktiven Firewall-Elemente, die in die Kommunikationsschnittstelle zwischen dem unsicheren Netz und dem zu schützenden Netz eingefügt werden, definiert. Ein so umrissenes Firewall-Element kann Packet Filter, Stateful Inspection, Application Gateway, Proxies und Adaptive Proxies repräsentieren.



Firewall Element

Einbindungs- und Durchsetzungsmodul:

Das Einbindungs- und Durchsetzungsmodul realisiert die Einbindung des aktiven Firewall-Elements in das Kommunikationssystem sowie die Durchsetzung der im Regelwerk festgehaltenen Sicherheitspolitik.

Die Einbindung in das Kommunikationssystem muß so realisiert werden, daß die Kommunikationsdaten nicht am Einbindungsmodul vorbeifließen können, ohne einer Analyse und einer Entscheidung unterzogen worden zu sein. Aus diesem Grund ist die Einbindung besonders sicherheitskritisch. In Abhängigkeit des verwendeten Protokollelementes wird das Einbindungsmodul an unterschiedlichen Stellen der Protokollarchitektur eingebunden.

Analysemodul -> *analysis*(x_i):

Im Analysemodul werden die Kommunikationsdaten des Protokollelementes (x_i) den Möglichkeiten des aktiven Firewall-Elements entsprechend analysiert. Die Ergebnisse der Analyse werden an das Entscheidungsmodul weitergeleitet. Im Analysemodul können mit Hilfe von Zustandsautomaten Statusinformationen (z.B. Verbindungsaufbau, Transfertzustand oder Verbindungsabbau) der Kommunikation festgehalten werden.

Entscheidungsmodul

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

Result of the decision module:

$$\mathbf{r_i} = \textit{result-of-decision}(\ \textit{analysis}(\mathbf{x_i}),\ \textit{security-management}(\mathbf{rules})\ )$$

r_i = true

das Protokollelement x_i wird weitergeleitet, evtl. als Beweissicherung der Aktion in einem Logbuch festgehalten

r_i = false

das Protokollelement x_i wird nicht weitergeleitet, und es wird ein sicherheitsrelevantes Ereignis e_i erzeugt.

Regelwerk -> *security-management* (rules):

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

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

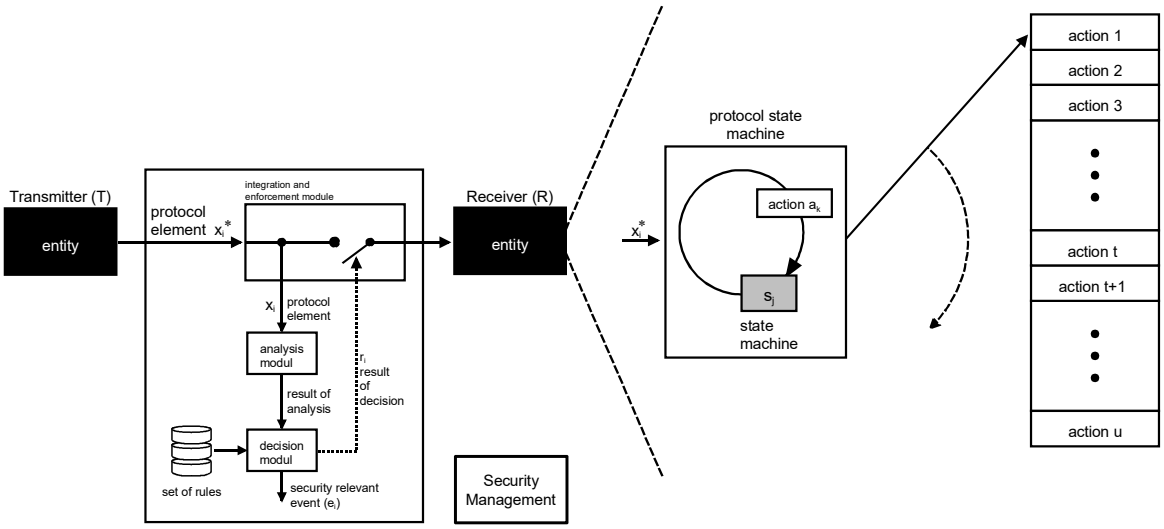
3.2 Definition des Kommunikationsmodells mit integriertem Firewall-System

Im folgenden wird das Kommunikationsmodells mit integriertem Firewall-System definiert. Das Firewall-System soll den Receiver $\{r_1, ... r_m\}$ vor Angriffen auf seine Werte aus dem unsicheren Netz schützen.

Es wird davon ausgegangen, daß mit Hilfe eines Security-Managements die Rechte in das Firewall-System, in Übereinstimmung mit der vorher festgelegten Sicherheitspolitik, eingetragen worden sind, die es ermöglichen sollen, die erlaubten Protokollelmente $\{x_1, ... x_t\}$ über das Firewall-System übertragen zu können. Bei einer fehlerfreien Implementierung des Firewall-Systems und der Kommunikationsprotokolle und -dienste auf der Empfängerseite, werden auch nur erlaubte Aktionen $\{a_1, ... a_t\}$ beim Receiver $\{r_1, ... r_h\}$ ausgeführt.

Bei dem Kommunikationsmodell mit integriertem Firewall-System müssen beliebig viele Transmitter und Receiver berücksichtigt werden.

Kommunikationsmodell mit integriertem Firewall-System



Firewall Systems

Mit Hilfe der Betrachtung der möglichen Einflußfaktoren auf die Auswahl und Durchführung der Aktionen beim Receiver sollen Kriterien abgeleitet werden, mit deren Hilfe eine Aussage über die Möglichkeiten und Grenzen im Sinne der Sicherheit und Vertrauenswürdigkeit des Kommunikationsmodell mit integriertem Firewall-Systemen gemacht werden kann.

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

a_k = *action-select*(*protocol-state-machine*(**x_i^*, s_j**),
authenticity(**x_i**),
result-of-decision(*analysis*(**x_i^***), *security-management*(**rules**)),
functionality-of-the-firewall-system())

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

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

3.3 Grundsätzliche Einflußfaktoren für die Auswahl und Durchführung der Aktion auf der Empfängerseite

Im folgenden werden die Funktionen und deren grundsätzlichen Einflußfaktoren aufgezeigt, die bei der Kommunikation des Kommunikationsmodells mit integriertem Firewall-System eine Rolle spielen. Es werden die Gründe festgehalten und erläutert, die sich für ein mögliches Fehlverhalten der Kommunikationsabläufe trotz integriertem Firewall-System herauskristallisiert haben.

3.3.1 Fehlerquellen durch Angriffe aus dem Netz

- **Funktion:** *authenticity*(**x_i**)

Für den richtigen Kommunikationsablauf ist wichtig, daß sowohl der Transmitter(t_l) authentisch/echt ist als auch das Protokollelement x_i^* authentisch/echt und unversehrt übertragen worden ist.
Einflußfaktoren:
- Vertrauenswürdigkeit des Netzes
- Vertrauenswürdigkeit des Kommunkationsteilnehmers

oder/und

- Gewährleistung der Authentikation des Kommunikationspartners
- Gewährleistung der Authentikation des Ursprungs der Daten

3.3.2 Fehlerquellen der Kommunikationslösung beim Receiver

3.3.2.1 Verantwortung des Anwenders

- **Funktion:** protocol-state-machine(**x_i^*, s_j**)

Einflußfaktoren:

- **Konfiguration beim Empfänger:**
  Die Konfiguration des Kommunikationsprotokolls oder –dienstes haben Fehler, die zur Folge haben, daß trotz erlaubten Protokollelementen (x_i) eine nicht erlaubte Aktion auf der Empfängerseite durchgeführt wird.

3.3.2.2 Verantwortung des Herstellers

- **Funktion:** protocol-state-machine**(x_i^*, s_j)**

Einflußfaktoren:

- **Implementierung beim Empfänger**
  Die Implementierung des Kommunikationsprotokolls oder –dienstes hat Fehler, die zur Folge haben, daß trotz erlaubten Protokollelementen (x_i) eine nicht erlaubte Aktion auf der Empfängerseite durchgeführt wird.

3.3.3 Fehlerquellen des Firewall-Systems

3.3.3.1 Verantwortung des Anwenders

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

Einflußfaktoren:

- **Sicherheitspolitik**
  - Es wird mehr erlaubt, als für die eigentliche Aufgabenstellung der einzelnen Nutzer erforderlich ist.
  - Die unbeabsichtigte falsche Eingabe der Regeln führt zu einem Fehlverhalten des Firewall-Systemes.
  - Die beabsichtigte falsche Eingabe der Regeln verfolgt das Ziel, das Firewall-System zu umgehen.
  - Die Einschränkung der Protokollelemente kann, z.B. durch Unwissenheit oder nicht richtige Vorgabe, unzureichend sein.
  - Neue Angriffsmethoden, die dem Verantwortlichen der Firewall-Systems nicht bekannt sind, könne daher auch nicht durch eine explizite Einschränkung verhindert werden.

3.3.3.2 Verantwortung des Herstellers

- **Funktion:** *analysis*(x_i)

Einflußfaktoren:

- **Tiefe der Analyse:**
  Die Analyse der Protokollelemente kann nicht detailliert genug Aussagen treffen, und damit nur eingeschränkt Aktionen verhindern. Sie kann in der Feststellung der Entscheidungskriterien und in deren Verdichtung zur Entscheidung Durchlaß oder Sperren zu sehr begrenzt sein. Bei der Analyse der Protokollelemente können wichtige und/oder neue Entscheidungskriterien unberücksichtigt bleiben. Bei der Synthese der Kriterien zu Entscheidungen können

Entscheidungregeln nicht ausgereift oder nicht umfaßend umgesetzt sein. .
Dieser Punkt geht einher mit der Komplexität der möglichen Einschränkungen.

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

Einflußfaktoren:

- **Vertrauenswürdige Implementierung:**

Unzureichende Qualität der Realisierung des Firewall-Systems:

- Die Qualität der Realisierung eines Firewall-Systems ist derart, daß in bestimmten Situationen ein Fehlverhalten auftritt.
- folgende Komponenten müssen betrachtet werden
  - Betriebssystem, auf dem die Firewall-Applikation läuft
  - Firewall-Applikation
  - Security Management
  - Hardware der Firewall-Elemente und des Security-Management
  - Authentikationskomponenten der Kommunikationspartner

3.3.4 Sicherheitsdienste eines Firewall-Systemes

- **Funktion:** functionality-of-the-firewall-system()

Die folgende Tabelle beschreibt die Standardsicherheitsdienste eines Firewall-Systems. Für jeden Dienst wird aufgelistet, welche Informationen vom Firewall-Systemen überprüft werden, welche Festlegungen und Maßnahmen getroffen werden, was geprüft wird und welchen Einfluß das für Sicherheit und Vertrauenswürdigkeit von Firewall-Systemen hat.

Sicherheitsdienst	**Überprüfung / Fest-legung / Maßnahme**	**Was wird geprüft?**	**Einfluß auf Sicherheit und Vertrauenswürdigkeit**
Zugangskontrolle auf Netzwerkebene	Welche Rechnersysteme (Transmitter, Receiver) dürfen über das Firewall-System miteinander kommunizieren?	• IP-Adressen der beteiligten Rechnersysteme • Zeit, zu der eine Aktion zulässig ist	• Vertrauenswürdige Implementierung • Vertrauenswürdigkeit des Netzes • Vertrauenswürdigkeit des Kommunikationspartners • Sicherheitspolitik
Zugangskontrolle auf Benutzerebene	Welche Benutzer dürfen über das Firewall-System eine Kommunikation aufbauen?	• Identität des Benutzers • Authentikation des Benutzers • Zeit, zu der eine Aktion zulässig ist	• Vertrauenswürdige Implementierung • Gewährleistung der Authentikation des Kommunikationspartners • Sicherheitspolitik
Zugangskontrolle auf Datenebene	Dürfen die Daten eines definierten Benutzers über das Firewall-System	• Identität des Absenders der Daten	• Vertrauenswürdige Implementierung

	übertragen werden?	• Authentikation des Absenders der Daten • Integrität der Daten • Zeit, zu der eine Aktion zulässig ist	• Gewährleistung der Authentikation des Ursprungs der Daten • Sicherheitspolitik
Rechteverwaltung	Festlegung, mit welchen Protokollen und Diensten und zu welchen Zeiten über das Firewall-System eine Kommunikation stattfinden darf.	• Header-Informationen auf den verschiedenen Schichten • Zeit, zu der eine Aktion zulässig ist	• Vertrauenswürdige Implementierung • Gewährleistung der Dantenunversehrheit • Tiefe der Analyse • Sicherheitspolitik
Kontrolle auf Anwendungsebene	Überprüfung, ob Kommandos genutzt oder Dateninhalte übertragen werden, die nicht zur durch die Anwendung definierten Aufgabenstellung gehören.	• Kommandos und Dateninhalte der verschiedenen Anwendungen • Zeit, zu der eine Aktion zulässig ist	• Vertrauenswürdige Implementierung • Gewährleistung der Dantenunversehrheit • Tiefe der Analyse • Sicherheitspolitik
Entkoppelung von Diensten	Entkoppeln verhindert, daß Implementierungsfehler, Schwachstellen und Konzeptionsfehler der Dienste Möglichkeit für Angriffe bieten.	• Kommandos • Zeit, zu der eine Aktion zulässig ist	• Vertrauenswürdige Implementierung • Konzept der Entkopplung
Beweissicherung und Protokollauswertung	Verbindungsdaten und sicherheitsrelevante Ereignisse werden protokolliert und können für die Beweissicherung von Benutzerhandlungen und für die Erkennung von Sicherheitsverletzungen ausgewertet werden.	• Aktionen und sicherheitsrelevanten Ereignisse • Zeit, zu der eine Aktion zulässig ist	• Vertrauenswürdige Implementierung • Sicherheitspolitik • Konzept der Beweissicherung und Protokollauswertung
Alarmierung	Besonders sicherheitsrelevante Ereignisse werden an ein Security Management gesendet, damit bei Sicherheitsverletzungen schnell reagiert werden kann.	• Zeit, zu der eine Aktion zulässig ist	• Vertrauenswürdige Implementierung • Vertrauenswürdigkeit des Netzes • Sicherheitspolitik
Verbergen der internen Netzstruktur	Die Struktur des zu schützenden Netzes soll gegenüber dem unsicheren Netz verborgen werden. Es nicht sichtbar sein, ob im zu schützenden Netz 10, 100, 1.000 oder 10.000 Rechnersysteme vorhanden sind.	• IP-Adressen	• Vertrauenswürdige Implementierung • Konzept des Verbergens der internen Netzstruktur (dual-homed Gateway)

4 Konzeptionelle Möglichkeiten und Grenzen von Firewall-Systemen

4.1 Konzeptionelle Möglichkeiten von Firewall-Systemen

In diesem Abschnitt werden die konzeptionelle Möglichkeiten, die die Einbindung eines Firewall-System erbringt dargestellt.

4.1.1 Common Point of Trust-Konzept

Ein Firewall-System stellt den „Common Point of Trust“ für den Übergang zwischen unterschiedlichen Netzen dar. Mit anderen Worten: Der einzige Weg ins interne Netz führt kontrolliert über das Firewall-System, das als Pförtner fungiert. Die Vorteile dieses „Common Point of Trust“-Konzepts sind:

- **Kosten:**
  Die Realisierung von Sicherheitsmechanismen in einem zentralen Firewall-System ist wesentlich effizienter als die Realisierung von Sicherheitsmechanismen auf jedem einzelnen Rechnersystem, das im zu schützenden Netz steht.
- **Umsetzung der Sicherheitspolitik:**
  Mit Hilfe eines zentralen Firewall-Systems kann die Sicherheitspolitik einer Organisation auf einfache Weise zentral durchgesetzt werden. Zum Beispiel werden die Dienste und Protokolle, die über ein Firewall-System möglich sein sollen, an einer zentralen Stelle für alle Benutzer definiert und überprüft.
- **Sicherheitsinfrastruktur:**
  Eine kryptographische (starke) Authentikation von Benutzern ist nur auf einem Firewall-System zu realisieren und nicht auf jedem einzelnen Rechnersystem im zu schützenden Netz, damit die Benutzer sicher identifiziert und authentisiert werden können. Für heterogene Rechnerlandschaften gibt es z. Zt. keine Konzepte und Realisierungen, wie kryptographische Authentikation auf den unterschiedlichen Rechnerbetriebssystemen (VMS, Unix, Windows, OS/2, ...) praktisch realisiert werden kann.
- **Sicherheit durch Abschottung:**
  Durch die reduzierte Funktionalität, die ein Firewall-System anbietet, existieren weniger Angriffspunkte für Angreifer aus dem unsicheren Netz. Der Aufwand für Sicherheitsmechanismen konzentriert sich auf das Firewall-System. Dadurch wird erreicht, daß die Rechnersysteme des zu schützenden Netzes nicht mehr von einem Rechnersystem aus dem unsicheren Netz (z. B. Internet) angegriffen werden können, sondern Rechnersysteme von außerhalb durch das Firewall-System abgeblockt werden. Rechnersysteme können nicht mehr zum Ziel von Angreifern aus dem unsicheren Netz werden, wenn sie falsch installiert oder konfiguriert sind. Alle Sicherheitsmechanismen sind in dem Firewall-System konzentriert realisiert.
- **Überprüfbarkeit:**
  Durch den klaren Übergang (Common Point of Trust) zwischen zwei Netzen ist eine einfache und vollständige Protokolliermöglichkeit vorhanden, da die gesamte Kommunikation über das Firewall-System läuft.

4.1.2 Reduzierung des Risikos eines Schadens

Durch die Reglementierung der Kommunikationsmöglichkeiten mit Hilfe eines Firewall-Systems kann das Risiko eines Schadens und damit die Reduzierung der Verwundbarkeit einfach ermöglicht werden.

4.2 Konzeptionelle Grenzen eines Firewall-Systems

Die Firewall-Systeme, die die Sicherheitsdienste für die Kommunikation im Internet und Intranet bereitstellen, sind sehr komplexe technische Sicherheitsmaßnahmen. Dennoch können auch aufwendige Firewall-Systeme keine hundertprozentige Sicherheit gewährleisten.

Im folgenden werden einige Aspekte aufgezeigt, die beim Einsatz von Firewall-Systemen zu beachten sind:

Hintertüren:

Ein Firewall-System schützt genau die Kommunikationsverbindungen, die darüber erfolgen. Gibt es Kommunikationsübergänge am Firewall-System vorbei (backdoors), hat das System keine Sicherheitswirkung mehr. Deshalb ist es absolut wichtig, daß keine weitere Verbindung zwischen dem unsicheren Netz und dem zu schützenden Netz besteht, damit das »Common Point of Trust«-Konzept realisiert werden kann. Dafür sind entsprechende personelle und organisatorische Sicherheitsmaßnahmen nötig.

Interne Angriffe:

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

Angriffe auf Datenebene:

Ein Firewall-System ist ursprünglich nicht in der Lage, im Bereich der erlaubten Kommunikation Angriffe auf der Datenebene zu erkennen. Dazu gehören: Angriffe durch das Senden von Malware wie E-Mail-Attachments, Downloads vom Web, Java Applets und Active-X-Controls.

Wissen und Hypothese:

Mit einem Firewall-System können durch theoretisches Wissen und praktische Erfahrungen Fehlerursachen verhindert werden. Gerade bei innovativen Anwendungen und Technologien wie dem Internet wird mit einer Vielzahl von Hypothesen gearbeitet. Daher gibt es einen Bereich des Neuen, Unbekannten und auch Unerwünschten und Unvorhersehbaren, was wir mit Hilfe eines Firewall-Systems nicht beherrschen können, weil dieses nur auf Ereignisse reagieren kann, die wir bereits eindeutig kennen. Hier liegt eine Grenze von Firewall-Systemen. Diesem können wir nur mit weiteren, modular ergänzten Sicherheitsmechanismen entgegenwirken. Zum Beispiel vermag Intrusion Detection auch neuartige Angriffsversuche zu erkennen.

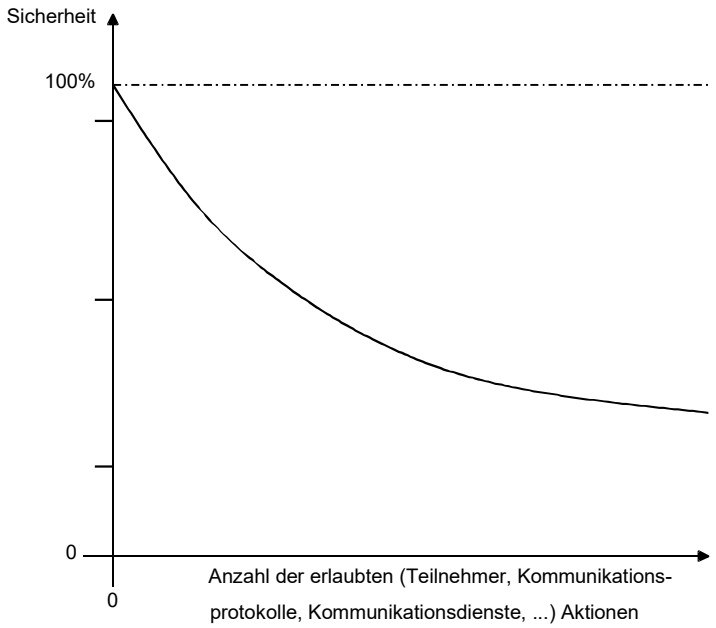
Richtige Sicherheitspolitik und richtige Umsetzung der Sicherheitspolitik:

Ein Firewall-System kann nur die Sicherheitsdienste erbringen, die eingerichtet sind. Deshalb ist es von besonderer Bedeutung, daß eine Sicherheitspolitik erarbeitet wird, die darstellt, welche

Ressourcen (Rechnersysteme, Kommunikationseinrichtungen, Daten usw.) im zu schützenden Netz einen hohen Schutzbedarf haben und wie sie geschützt werden sollen. Außerdem muß definiert werden, auf welche Weise die Sicherheitsmechanismen für die Aufrechterhaltung des sicheren Betriebs eines Firewall-Systems periodisch überprüft werden.

security versus connectivity ⇔ Risiko versus Chance

Je kleiner die Menge erlaubter Aktionen ist, um so geringer ist das Risiko, daß ein Schaden auftreten kann. Jeder Teilnehmer, jeder Rechner, der über ein Firewall-System kommunizieren darf, stellt ein zusätzliches Risiko dar. So stellen z.B. auch die erlaubten Kommunikationspartner ein Risiko dar, falls sie unberechtigte Kommunikationsverbindungen nutzen. Aus diesem Grund ist zu beachten: so wenig wie möglich/nötig über das Firewall-System zulassen, damit ein Höchstmaß an Sicherheit erreicht werden kann.



Je mehr erlaubt ist, um so größer ist das Risiko der Verwundbarkeit. Wenn nichts erlaubt ist, kann über das Netz auch kein Schaden auftreten. Hier wird das Spannungsfeld zwischen „security und connectivity“ deutlich. Mit Hilfe eines Firewall-Systems sollen die Vorteile der Kommunikation nach außen genutzt werden, aber der mögliche Schaden durch diese Handlungen begrenzt werden.

Die Teilnehmer, die zur Erfüllung ihrer Aufgabenstellung kommunizieren müssen, sollen mit den Kommunikationsprotokollen und -diensten, die sie für ihre speziellen Aufgaben benötigen, zu den entsprechenden Zeiten dies tun dürfen – aber nur so weit, wie dafür nötig ist.

Vertrauenswürdigkeit des Kommunikationspartners und der empfangenden Daten

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

5 Das richtige Firewall-Konzept für jeden Anwendungsfall

Um eine einschätzbare Aussage über Firewall-Systeme treffen zu können, ist die Sicherheitseinstufung von Firewall-Konzepten sehr hilfreich. Dabei werden Einsatzfälle definiert, die nach den Kriterien Vertrauenswürdigkeit des Netzes und des Kommunikationspartners und Angriffpotential in Abhängigkeit des Einsatzfalles

1. das unsichere Netz ist innerhalb der eigenen Organisation oder
2. das unsichere Netz ist außerhalb der eigenen Organisation

betrachtet.

Die wichtigste Motivation für den Einsatz eines Firewall-Systems ist also die Reduzierung des Risikos der Verwundbarkeit, wenn ein Schutzbedarf der eigenen Werte besteht. Wenn das zu schützende Netz keinen Schutzbedarf hat, muß auch kein Firewall-System eingesetzt werden. Wenn aber ein Schutzbedarf vorliegt, dann muß der Einsatzfall entsprechend berücksichtigt werden und ein angemessenes Firewall-Konzept ist auszuwählen.

Im folgenden wird eine Methode erläutert, wie dies in der Praxis mit den gewonnenen Erkenntnissen geschehen kann.

Definition des Einsatzfalles:

Im folgenden werden zwei Einsatzfälle von Firewall-Systemen definiert:

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

Die Wirkung der unterschiedlichen Firewall-Konzepte

In der folgenden Tabelle wird die Wirkung der unterschiedlichen Firewall-Konzepte auf die Angriffe dargestellt /Pohl00a/. Es wird davon ausgegangen, daß die Lösungen über ein sicheres Betriebssystem, ein sicheres Security Management und Firewall-Schutzmechanismen verfügen.

Angriffsart	**Firewall-Konzepte**	Packet Filter	Application Gateway	Packet Filter und single-homed Application Gateway	Packet Filter und dual-homed Application Gateway	zwei Packet Filter als Screened Subnet und ein single-homed Application	High-level Security Firewall-System
Angriffe durch einen Dritten	Wiederholen o. Verzögern von Protokollelementen	◔	◕	◔	◕	◔	◕
	Einfügen o. Löschen von Daten in den Protokollelemten	◔	◕	◑	◕	◑	◕
	Modifikation der Daten in den Protokollelementen	○	◕	◑	◕	◑	◕
	Boykott des Receivers	◔	◑	◔	◑	◔	◕
	Trittbrettfahrer	◔	◑	◔	◑	◔	◑
	Empfangen von Malware (Viren, Wurmer, Trojanische Pferde,...)	◔	◕	◑	◕	◑	◕
Angriffe durch den Transmitter	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	○	◑	◔	◑	◔	◑
Vorbe-reitung für Angriffe	Social Engieering	○	○	○	○	○	○
	Analyse mit Hilfe von Scannerprogrammen	○	●	◑	●	◑	●
Angriffe auf das Firewall-System	Manipulation des Firewall-Systems	○	○	◔	◕	◑	●
	Einbau einer Trap-Door	○	○	○	○	○	○
	Nutzung einer falschen Konfiguration des Firewall-Systems	○	◔	◔	◕	◑	●
	Nutzung von Implementierungsfehlers des Firewall-Systems	○	◔	◔	◕	◑	●
	interne Angriffe	○	○	○	○	○	○

● sehr große Wirkung ◕ große Wirkung ◑ Wirkung

◔ gering Wirkung ○ keine Wirkung ◆ Grundlage für die Wirkung

Die nächste Tabelle zeigt, wie in Abhängigkeit des Schutzbedarfes und des Einsatzfalles welches aktive Firewall-Elementen oder Kombination aktiver Firewall-Elemente verwendet werden soll. Die Definition des Schutzbedarfes ist an das Grundschutzhandbuch des BSI /BSI99/ angelehnt.

Entscheidungsmatrix für das Firewall-Konzept:

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

Falls überhaupt ein Schutzbedarf besteht, ist für die Kommunikation mit einem unsicheren Netz außerhalb des eigenen Verantwortungsbereiches immer ein dual-homed Application Gateway im Firewall-Konzept notwendig.

Dem Schutzbedarf entsprechend, kann dann entweder nur ein dual-homed Application Gateway oder in Kombination mit einem Packet Filter bzw. einem Screened Subnet zum Einsatz kommen.

Falls das unsichere Netz innerhalb des eigenen Verantwortungsbereiches liegt, wie z.B. das Intranet, genügt es, abhängig des Schutzdarfs, nur Packet Filter oder Kombinationen mit single-homed Application Gateways zu verwenden. Eine Alternative in diesem Anwendungsbereich sind Stateful Inspection oder Adaptiv Proxy Lösungen, die auch auf der Anwendungsebene Sicherheitsfunktionen zur Verfügung stellen.

Durch die Kombination eines dual-homed Application Gateway mit Packet Filter oder Screened Subnet ist eine sehr hohe Sicherheit zu erreichen.

Stets muß der Leitsatz sein: „Das passende Firewall-Konzept für den jeweiligen speziellen Anwendungsfall“.

Grundlegende Einflußfaktoren von Firewall-Systemen

Durch die Diskussion des Kommunikationsmodell mit integriertem Firewall-System können grundlegenden Einflußfaktoren von Firewall-Systemen herausgearbeitet werden.

Im folgenden werden die Ergebnissen und die strukturellen Zusammenhänge über Angriffe und Wirkung der verschiedenen Einflußfaktoren eines Firewall-Systems beschrieben und in Form von Tabellen umfassend dargestellt.

Es wird gezeigt, daß neben den eigentlichen Sicherheitsdiensten eines Firewall-Systems weiter Einflußfaktoren eine große Wirkung auf die Sicherheit von Firewall-Systemen haben.

Die Einflußfaktoren eines umfassenden Firewall-System werden unterteil in:

- Firewall-Konzept (hier als Beispiel eines High-level Security Firewall-Systems)
- die Vertrauenswürdigkeit (Evaluierung und Zertifizierung) des Firewall-Systems und
- die Einflußfaktoren der eigenen Organisation durch die richtige Sicherheitspolitik und den sicheren Betrieb eines Firewall-Systems.

Außerdem werden weitere Aspekte mit Hilfe zusätzlicher Sicherheitsmechanismen wie Verschlüsselung, Intrusion Detection, Anti-Virus-/Anti-Malware-Systeme, Personal Firewall und Audits bewertet, die dann als umfassendes Firewall-System eine insgesamt höhere Gesamtsicherheit garantieren.

Die Wirkung von umfassenden Firewall-Systemen

In der folgenden Tabelle wird die Wirkung eines umfassenden Firewall-System auf die Angriffe in Ihrer Gesamtheit dargestellt.

Angriffsart	**Sicherheitsaspekte eines umfassenden Firewall-Systems**	High-level Security Firewall-System	Vertrauenswürdigkeit	Verschlüsselung	PFW	Anti-Malware-System	Intrusion Detection	Audits	nichttechnische Sicherheitsmaßnahmen	Sicherheitspolitik	sicherer Betrieb
Angriffe durch einen Dritten	Wiederholen o. Verzögern von Protokollelementen	◕	◆	◕	○	○	○	◆	○	◆	◆
	Einfügen o. Löschen von Daten in den Protokollelemten	◕	◆	●	○	○	○	◆	○	◆	◆
	Modifikation der Daten in den Protokollelementen	◕	◆	●	○	○	○	◆	○	◆	◆
	Boykott des Receivers	◕	◆	○	○	○	◑	◆	◕	◆	◆
	Trittbrettfahrer	◑	◆	●	○	○	○	◆	○	◆	◆
	Empfangen von Malware (Viren, Wurmer, Trojanische Pferde,...)	◕	◆	◕	●	◕	○	◆	◕	◆	◆
Angriffe durch den Transmitter	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	◑	◆	○	○	○	○	◆	◕	◆	◆
Vorbe-reitung für Angriffe	Social Engieering	○	○	○	○	○	○	◆	●	◆	◆
	Analyse mit Hilfe von Scannerprogrammen	●	◆	○	○	○	◑	◆	○	◆	◆
Angriffe auf das Firewall-System	Manipulation des Firewall-Systems	●	◆	○	○	○	◑	●	◕	◆	◆
	Einbau einer Trap-Door	○	●	○	○	○	◔	○	○	○	○
	Nutzung einer falschen Konfiguration des Firewall-Systems	●	○	○	○	○	◑	●	◕	◆	◆
	Nutzung von Implementierungsfehlers des Firewall-Systems	●	◆	○	○	○	◑	●	◕	◆	◆
	interne Angriffe	○	○	○	●	○	◕	◔	◕	◆	◆

● sehr große Wirkung ◕ große Wirkung ◑ Wirkung

◔ gering Wirkung ○ keine Wirkung ◆ Grundlage für die Wirkung

Die Wirkung von High-level Security Firewall-Systeme ist auf die meisten Angriffe groß bis sehr groß.

Die Vertrauenswürdigkeit durch Evaluierung und Zertifizierung, die Durchführung von Audits, die Erabeitung einer richtigen Sicherheitspolitik und der sichere Betrieb eines umfassenden Firewall-System stellen Randbedingungen der Sicherheit der Nutzung eines Firewall-Systems dar und ist somit Grundlage für die Wirkung auf die entsprechenden Angriffsarten.

Die Verschlüsselung erhöht die Schutzwirkung bei Angriffen durch Dritte deutlich.

Die Anti-Malware-Systeme sind notwendig, um mit einer großen Wirkung gegen Viren, Würmer und Trojanische Pferde einen entsprechenden Schaden verhindern zu können.

Ziel einer Personal FireWall ist es, die Lücken zu schließen, die bei einem zentralen Firewall-System und bei den bekannten Virenscannern noch vorhanden sind, damit die elektronischen Werte auf einem PC umfassend geschützt sind.

Dazu wird neben der Reglementierung der Kommunikation auf dem PC eine sichere Umgebung nach dem Sandbox-Modell realisiert um jede Anwendung, die innerhalb des Betriebssystem läuft, zu isolieren. Alle schützenswerten Systemressourcen und Dateien können gegen unerwünschte Zugriffe durch lokale Applikationen oder Malware, die in das System eindringen, abgeschirmt werden. Hierdurch wird eine sehr große Wirkung gegen das Empfangen von Malware sowie gegen Java, ActivX, ... Angriffen erzielt /Pohl00c/. Außerdem kann auch eine sehr große Wirkung gegen interne Angriffe, d.h. auf Daten, die auf den PCs stehen, erreicht werden.

Intrusion Detection-Systeme haben eine große Wirkung gegen interne Angriffe und helfen, Unregelmäßigkeiten zu erkennen und dann entsprechend schnell realgieren zu können.

Nichttechnische Sicherheitsmaßnahmen haben eine große Wirkung gegen einige Angriffe und sind besonders wichtig, um gegen „Social Engeneering“ etwas entgegenzusetzen.

6 Zusammenfassung

Die Ergebnisse dokumentieren, daß Firewall-Systeme prinzipiell geeignet sind, um sich an unsichere Netze wie das Internet risikoärmer anzukoppeln.

Da die Diskussion über Firewall-Systeme aufzeigt, daß man keine 100%tige Sicherheit erreichen kann, ist es zweckmäßig, die Betrachtung eines Firewall-Systems auf den Schwerpunkt der „Unsicherheit“ zu legen. Ziel muß es sein, diese Rest-Unsicherheit zu minimieren. Denn durch die sinkende Zahl der Unsicherheiten steigt die Resistenz eines Firewallsystems. Unsicherheiten sind all diejenigen Zustände, welche zu illegalen oder unerwünschten Zuständen eines Firewall-Systems führen.

Auch hier muß einem bewußt sein, daß immer ein Restrisiko bestehen bleibt, das mit der Hilfe von weiteren – modular zu ergänzenden – Sicherheitsmechanismen wie Intrusion Detection, Antivirus-Konzepten, Personal FireWalls und Verschlüsselung weiter reduziert werden muß, um so zu einer praktischen Sicherheit zu gelangen.

Wichtig sind ebenso periodische Audits und Revisionen, die Erarbeitung einer richtigen Sicherheitspolitik, die Aufrechterhaltung eines sicheren Betriebs und Vertrauenswürdigkeit der Realisierung.

Durch den Einsatz eines umfassenden Firewall-System kann die Verwundbarkeit minimiert werden, was die Chancen einer risikoärmeren Internet-Ankopplung erhöht.

7 Literatur

/Comm98/ ISO/IEC SC27 N2161
„Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and gerneral model“ 1998

/BSI99/ BSI: »IT-Grundschutzhandbuch«, BSI 7152, Köln: Bundesanzeiger-Verlag, 1999

/Pohl00a/ N. Pohlmann
„Firewall-System – Sicherheit für Internet und Internat, VPN, E-Mail Security und Intrution Detection System“, 3. Auflage, Thomson Publishing, Bonn 2000

/Pohl00b/ N. Pohlmann
„Möglichkeiten und Grenzen von Firewall-Systemen“, KES – Kommunikations- und EDV-Sicherheit; SecMedia Verlag, Ingelheim 3/2000

/Pohl00b/ N. Pohlmann
„Personal FireWall“, KES – Kommunikations- und EDV-Sicherheit; SecMedia Verlag, Ingelheim 4/2000