Fachhochschule Heidelberg

University of Applied Science

DIPLOMARBEIT

Intrusion Detection und Intrusion Response System mit künstlichen Neuronalen Netzen.

Vorbetrachtung und Analyse

Vorgelegt von:

Robert Gladewitz

bei

Erstkorrektor:
Prof. Walter Hame

Zweitkorrektor:
Jan Maltry

Inhaltsverzeichnis

1 Einleitung

Das Internet hat sich seit seiner Entstehung von einem rein militärisch-wissenschaftlich genutzten Medium zu einem globalem Massenmedium mit breitem Anwendungsspektrum entwickelt. Die Anwendung erstreckt sich von Informationssystemen bis hin zum E-Commerce. Unternehmen, öffentliche Einrichtungen sowie private Anwender nutzen das Internet zur Abwicklung von Geschäftsvorfällen, Austausch von Daten und Information, Werbung beziehungsweise Präsentationen. Das Pflegen von Geschäfts- und Kundenbeziehungen und die weltweite Verfügbarkeit der Datenbestände erweitern das Spektrum und die Möglichkeiten der Anwendung des Internets.

Der Aspekt des freien privaten oder betrieblichen Internetzugangs birgt eine weitere große Gefahr in sich. Jede heruntergeladene Software aus dem Internet kann ein Virus oder ein trojanisches Pferd beinhalten. Auch Skriptsprachen, die in Browsern oder E-Mailprogrammen standardgemäß verfügbar sind, bieten für Angreifer eine Möglichkeit, Makroviren zu verbreiten.

Die Sensibilität der Daten rücken Sicherheitsaspekte verstärkt in den Vordergrund. Der zunehmende Erfolg von Angriffen aus dem Internet zur Gewinnung von vertraulichen Informationen oder zur Störung des Betriebsablaufes stellt die Effektivität bisheriger Sicherheitsmethoden wie Firewalls in Frage.

1.1 Aufgabenstellung

Für eine Firewall mit äußerem und innerem Router sowie einem überwachten Grenznetz ist ein System zu konzipieren und einzurichten, bei dem die Auswertung der Log-Dateien teilweise durch ein künstliches Neuronales Netz und teilweise durch konventionelle Überwachung erfolgt.

1.2 Ziele, Vorgehensweise und Abgrenzung

Diese Arbeit hat zum Ziel, ein System zu konzipieren, das die bisherigen Sicherheitssysteme um den Einsatz eines künstlichen Neuronalen Netzes erweitert. Der Schwerpunkt liegt in der kontinuierliche Überwachung des Gesamtsystems. Dabei werden zunächst die Machbarkeit des angestrebten Ergebnisses und schon vorhandene Lösungen hinsichtlich ihrer Einsatzmöglichkeiten untersucht. Anschließend erfolgt eine Systemanalyse, die die die vorhandenen Systeme und deren Schwächen aufzeigt. Aus den Ergebnissen wird ein erster Entwurf erarbeitet.
Da nicht alle Fehler vorhandener Systeme im Rahmen dieser Diplomarbeit aufgelistet werden können, werden im folgenden nur Angriffe auf die bekanntesten Schwachstellen erläutert. Desweiteren werden nur Systeme vorgestellt, die für die Verwendung von Firewalls und Intrusion Detection Systemen sinnvoll sind.

1.3 Aufbau der Diplomarbeit

Die Diplomarbeit besteht aus drei Teilen. Der erste Teil umfasst die allgemeine Theorie über Netzwerke und Firewall-Umgebungen. Es werden die Grundlagen wie Begriffe und Konzeptionelles abgehandelt und außerdem eine Studie über Machbarkeit und Verfügbarkeit vorhandener IT-Produkte und Systeme erstellt. Der zweite Teil dient zur Darstellung vorhandener Systeme. Hierbei werden die Schwächen und Stärken der Systeme auf neue Anforderungen analysiert. Im dritten Teil wird ein theoretischer Ansatz für ein Intrusion Detection System erstellt.

2 Grundlagen

In den letzten zehn Jahren wurde die Welt der Computer verändert. Insbesondere im Sicherheitsbereich entstanden neue Begriffe und Konzepte. Das permanente Wachstum von Netzwerkstrukturen, das zu einer starken Abhängigkeit von der Funktionsfähigkeit dieser weltumspannenden Netze führte, geht einher mit einem enormen Anstieg von Angriffen aus Gründen der Wirtschaftsspionage oder nur zum Vergnügen von „Freizeit-Hackern“.

Aber nicht nur Hacker sind eine Bedrohung. Sowohl Unerfahrenheit und Unaufmerksamkeit der Benutzer als auch nicht überwachte Clientsysteme stellen weitere Sicherheitsrisiken dar. Auf der Internetseite http://www.sandboxsecurity.de/, unter der Rubrik Sicherheitstests wird beispielsweise demonstriert, welche Möglichkeiten der Manipulation von Rechnern möglich sind.

Das Risiko, ein potenzielles Opfer eines Hackerangriffes zu werden, war noch nie so hoch wie heute. Das FBI verzeichnete im Zeitraum von Januar 1999 bis Januar 2000 über 500 Sicherheitslücken in Programmen, Skripten und Nachrichten. Eine Studie aus dem Jahr 1999 des Computer Security Institute im Auftrag des FBI bezifferte den finanziellen Verlust für Unternehmen durch Computerangriffe im Jahr 1998 auf insgesamt 136 Milliarden US-Dollar.

Aus der erheblichen Zunahme von Presseberichten über erfolgreiche Hackerangriffe lässt sich das wahre Ausmaß aufgrund der hohen Dunkelziffer durch nicht entdeckte Angriffe nur erahnen. Einen Überblick über bekannte Angriffe bietet die Internetseite http://www.ibrixx.de/time/security_news.php3. Die folgende Grafik zeigt eine deutlich steigende Tendenz für Makroviren. [CIA01,FBI01,Sym01]

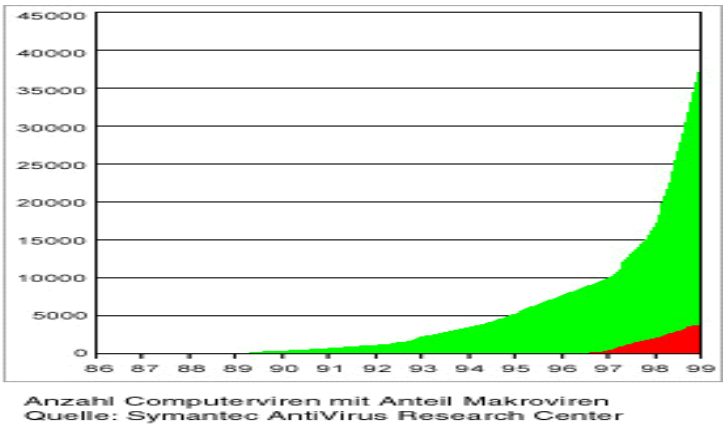


Abbildung 2-1: Steigende Anzahl von Viren

2.1 Begriffe

2.1.1 Firewalls

Systeme, die einen Angreifer aus dem Internet abwehren sollen, nennt man Firewalls. Diese trennen das interne Netzwerk vom Internet.

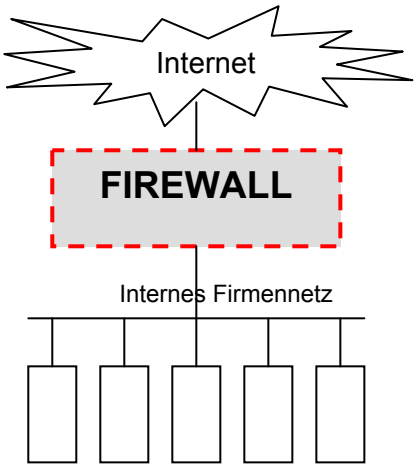


Abbildung 2-2: Grundprinzip Firewall

Firewalls können jedoch nicht alle Angriffe aus dem Internet abwehren. Bei entsprechender Qualität eines Angriffs kann nur die Zeit verlängert werden, die der Angreifer braucht, um in ein System einzudringen. In dieser Zeit muss der lokal verantwortliche Administrator den Angriff erkennen und entsprechende Gegenmaßnahmen einleiten. Die Anforderungen an den Administrator sind sehr hoch, da eine ständige Präsens und Aufmerksamkeit erforderlich sind. Aufzeichnungen, die viele gescheiterte Angriffsversuche enthalten, vermitteln dem Administrator ein trügerisches Sicherheitsgefühl. [HeKa98, ZwCoCh00]

2.1.2 Bastionshosts

Bastionshosts gelten als geopferte Rechner in einer Firewall. Dies können Server sein, die Dienste im Internet anbieten oder Internetdienste für das interne Netz zur Verfügung stellen. Sie sind vom internen Firmennetz getrennt und dienen als Sicherheitsbarriere vor Angreifern aus dem Internet. [ZwCoCh00]

2.1.3 Intrusion Detection Systeme (IDS)

Ein recht junges Gebiet im Bereich der Sicherheit von Netzwerken sind Intrusion Detection Systeme (Angriffs-Erkennungs-Systeme). Diese haben das Ziel, einen Angriff oder andere Sicherheitsverletzungen zu erkennen. Sogenannte Intrusion Detection Systeme sollen als intelligente Alarmanlage dienen und bei Angriffen aller Art Alarm schlagen. Zusätzlich sollen solche Systeme auch Gegenmaßnahmen einleiten können (Intrusion Response Systeme).

Die meisten derzeitigen Intrusion Detection Systeme werten die anfallenden Protokolldateien (Auditdaten) in Echtzeit aus, um einen Angriff zu erkennen. Moderne Systeme arbeiten dabei mit Mustern, die aus bereits vorhergehenden Angriffen bekannt sind.

Die Auditdaten werden mit Hilfe von Expertensystemen ausgewertet. In Ansätzen werden für die Auswertung künstliche Neuronale Netze eingesetzt. [HeKa98]

2.1.4 Künstliche Neuronale Netze

Künstliche Neuronale Netze versuchen die Arbeitsweise des menschlichen Gehirns nachzubilden. Die Fehlertoleranz, die hochgradige Parallelität und die Lernfähigkeit des menschlichen Gehirns sollen dabei annähernd simuliert werden.

Diese Vorteile sprechen für einen Einsatz von künstlichen Neuronalen Netzen im Bereich der Intrusion Detection Systeme. So könnte das System durch künstliche Intelligenz und Lernfähigkeit neue Angriffssituationen erkennen und sich für geeignete Gegenmaßnahmen entscheiden. [Bitt99; HeKa98]

2.1.5 Auditdaten (Log-Dateien)

Jedes System erstellt sogenannte Log–Dateien (Protokolldateien). Die daraus resultierenden Daten bezeichnet man als Auditdaten. In den Protokolldateien werden Systemabläufe und Ereignisse gespeichert. Die Speicherung erfolgt häufig in normalen Textdateien. Unter Unix-Systemen können Log-Dateien auf einem zentralen Server gespeichert werden. Diesen Server nennt man Backlog-Server. [ZwCoCh00,HeKa98]

2.1.6 Intranet

Intranets sind unternehmensinterne Informationsnetze. Diese werden vorwiegend genutzt, um den Mitarbeitern interne Informationen des Unternehmens zur Verfügung zu stellen. Zum Schutz vor Angriffen oder unberechtigten Lesern werden Intranets durch spezielle Router vom Internet getrennt. [Pohl00]

2.1.7 Backlog-Server (Log-Server)

Ein Backlog-Server dient zur zentralen Speicherung der Auditdaten in einem Netzwerk. Hierbei können die Auditdaten schon vorsortiert und gefiltert werden.

2.1.8 Intrusion (Eindringen)

Den Begriff Intrusion haben Herberlein, Levitt und Mukherjee [1991] wie folgt beschrieben: „Eine Menge von Handlungen, deren Ziel es ist, die Integrität, die Verfügbarkeit eines Betriebsmittels zu kompromittieren.“ Ein Angriff ist die vorsätzliche Verletzung der Sicherheitsmaßnahmen eines Systems. Dabei nutzt der Angreifer bekannte Sicherheitslücken oder Konfigurationsfehler aus.

2.1.9 DoS (Denial of Service)

Durch einen Denial of Service-Angriff werden bestimmte Rechner und/oder Dienste drastisch eingeschränkt beziehungsweise zum Absturz gebracht. Meistens wird bei dieser Form von Angriffen versucht, durch das Ausnutzen von Schwachstellen in Betriebssystemen, Programmen und Diensten oder grundsätzlicher Entwurfsschwächen der verwendeten Netzwerkprotokolle, die angegriffenen Systeme zum Absturz zu bringen oder derartig zu überlasten, dass diese Systeme ihre eigentliche Funktionalität nicht mehr erfüllt können. [Pohl00]

2.1.10 Viren

Codefragmente, die sich an Dateien, Bootsektoren und Programme anhängen und sich anschließend bei deren Ausführung oder Verarbeitung vermehren, nennt man Viren. [Sym01]

2.1.11 Trojanische Pferde

Trojanische Pferde sind Programme, die sich nach außen wie normale Anwendungssoftware verhalten können, nach innen aber Anweisungen enthalten, die Schaden anrichten. In vielen Fällen verhält sich ein Trojanisches Pferd wie ein normales Anwendungsprogramm, das Daten zu einem beliebigen Zeitpunkt an einen Angreifer übermitteln oder Veränderungen am System vornehmen kann. Der Angreifer nutzt die Informationen oder die erzeugten Sicherheitslücken, um in ein System einzudringen. [Sym01]

2.1.12 Würmer

Würmer sind Programme, die sich nach ihrer Aktivierung selbst vermehren und weiterverbreiten können. Der Schaden solcher Programme kann sehr groß sein, da in kurzer Zeit ein ganzes Netz durch Selbstreplikation befallen werden kann. [Sym01]

2.1.13 Paketfilter

In Firewalls werden auf Routern und Bastionshosts Paketfilter eingesetzt, um unzulässigen Netzverkehr auszufiltern. Senderadresse, Empfängeradresse, Server-Port, Empfängerport und Headerparameter werden dabei gefiltert. [ZwCoCh00]

2.1.14 IP-V4

IP-V4 ist die heute standardmäßig eingesetzte Protokollfamilie im Internet. Es ist ein verbindungsloses Protokoll, welches den Austausch von Daten zwischen zwei Rechner erlaubt. Durch den geschichteten Aufbau werden die Aktionen der jeweiligen darunter liegenden bzw. darüber liegenden Schichten transparent.

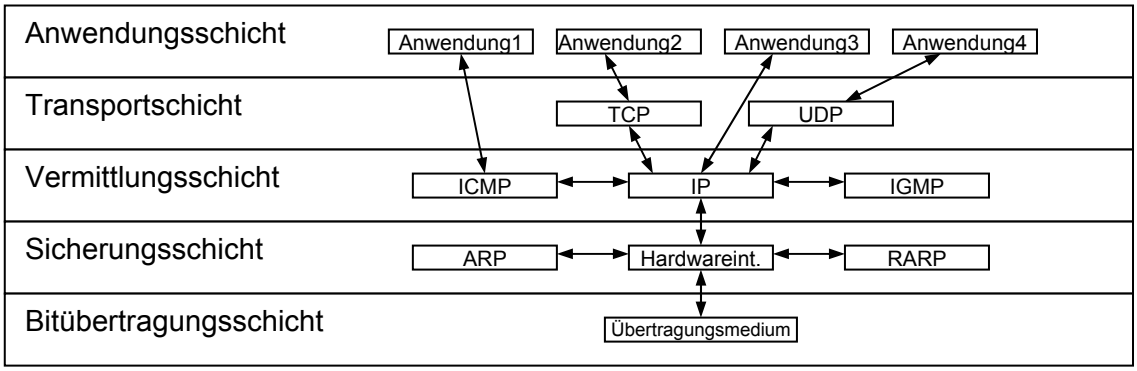


Abbildung 2-3: Schichten im IP-V4

Beim Versenden von Daten wird in jeder Schicht das Paket neu verpackt und ein zusätzlicher Header angefügt.
Die Adressierung von IP-V4 befindet sich auf der IP-Ebene. Durch das bei der Entwicklung von IP-V4 nicht absehbare Wachstum des Internets ist der Adressraum auf 256^4 = 4294967296 Hosts beschränkt. Durch die Klassifizierung und Aufteilung des Netzes in Teilnetze und durch Routing der Netze fallen viele der Adressen weg. Bei weiter ansteigendem Wachstum des Internets ist die Anzahl der Hosts in absehbarer Zeit nicht mehr ausreichend. Der Nachfolger IP-V6 beseitigt diese Beschränkung und korrigiert einige Implementierungsfehler. Dieser ist momentan noch in der Testphase.
[Pohl00,BoWo97]

2.1.15 IP-V6

IP-V6 ist eine Neuentwicklung der Protokollfamilie IP-V4. Mit dieser soll nicht nur das Problem mangelnder Adressierungsmöglichkeiten, sondern auch vorhandene Sicherheitslücken von IP-V4 beseitigt werden. Die neuen Funktionen von IP-V6 sind:

- Adressraum mit 16 Byte Adressierung
- Verringerung der Headerfields von zwölf auf acht
- Erweiterte Unterstützung zur Übertragung multimedialer Inhalte
- Autokonfiguration von neu erkannten Rechnern
- Providerwechsel ohne Änderung der alten Adresse
- Neue Sicherheitsmechanismen

[BoWo97]

2.1.16 RFC (Request For Comment)

Unter dem Stichwort RFC („Anforderung zu Kommentaren“) werden Kommentare zu Netzwerkspezifikationen und die daraus resultierenden Probleme zusammengefasst. RFCs waren ursprünglich Mitteilungen zwischen den Entwicklern des ARPANET, die dazu dienten, Probleme und Problemlösungen zu diskutieren. Im Laufe der Zeit entwickelten sich diese Dokumente zu einem Standard. Heute werden die RFC’s in zwei Gruppen unterteilt:

- Die **FYI-RFCs** dienen als Übersicht und einleitende Themen. RFC 1600 gibt beispielsweise eine Übersicht über alle RFCs von 1 bis 1599 . Dieser dient damit als Inhaltsverzeichnis für alle RFCs mit Nummern kleiner als 1600.

- Die **STD-RFCs** identifizieren die RFCs, welche die wirklichen Internet Standards spezifizieren.

Die Organisation für Verwaltung und Standardisierung solcher Dokumente ist die IETF (The Internet Engineering Task Force).

2.1.17 IP-Sec

IP-Sec ist ein Protokoll, dass die Authentifizierung und Verschlüsselung in IP-Netzen ermöglicht. Im zukünftigen Internetstandard IP-V6 wird IP-Sec integraler Bestandteil sein. Zudem kann IP-Sec als Erweiterung mit der aktuellen Version IP-V4 verwendet werden. Im Gegensatz zu anderen Verschlüsselungen wie zum Beispiel SSL setzt IP-Sec nicht auf das vorhandene Übertragungsprotokoll auf, sondern ist direkt in dieses integriert.

IP-Sec unterstützt zwei verschiedene Modi:

1. Transport-Modus:
   Beim Transport-Modus werden nur die Nutzdaten verschlüsselt, um eine bessere Netzwerkperformance zu erreichen.
2. Tunnel-Modus:
   Im Tunnel-Modus werden zusätzlich die Protokolldaten verschlüsselt. Dies ist zum Beispiel für Virtual Private Networks (VPN) von Bedeutung ist.

Durch den modularen Aufbau von IP-Sec ist die Verwendung kryptographischer Verfahren nicht festgesetzt, weshalb auf Entwicklungen in diesem Gebiet flexibel reagiert werden kann. Die IETF (The Internet Engineering Task Force) hat bestimmte Algorithmen für IP-Sec-Implementierungen festgelegt, um Interoperabilität zwischen den verschiedenen Produkten zu erreichen. Zu den Standard-Verschlüsselungsalgorithmen gehören beispielsweise Secure-Hash, DES und MD5.

IP-Sec definiert Protokolle, deren Sicherungsdienste der Struktur eines IP-V6 Paketes entsprechend durch zwei zusätzliche Header, den ‘IP Authentication Header’ (AH) und den Header ‘IP Encapsulating Security Pay-load’ (ESP), realisiert werden. Das Format dieser Header ist unabhängig von den verwendeten kryptographischen Algorithmen.
[BoWo97]

2.1.18 VPNs (Virtual Privat Networks)

VPN simuliert ein geschlossenes Netzwerk zwischen zwei Netzen. Hierbei werden Daten zwischen zwei Routern verschlüsselt über das Internet geschickt. Dieser Vorgang wird als „tunneln“ bezeichnet. [ZwCoCh00]

2.1.19 Spamming-Mail und Third-Party-Relaying

Third-Party-Relaying ist der Versuch, E-Mails mit falscher Absenderadresse über einen E-Mail-Server zu versenden. Das Protokoll SMTP beinhaltet keine User-Authentifizierung und stellt somit eine Sicherheitslücke in Systemen dar.
Hacker versuchen auf diese Weise, tausende E-Mails an verschiedene Empfänger mit gefälschter Absenderadresse zu versenden. Diese E-Mails nennt man wegen Ihres Inhalts und ihrer Bestimmung Spamming-Mails. Der Empfänger erhält dabei unerwünste Informationen oder Werbung. [ZwCoCh00]

2.1.20 Mail-Relay-Server

Mail-Relay-Server werden eingesetzt, um E-Mails weiterzuleiten. Sie besitzen weder eine E-Mail-Userverwaltung, noch speichern sie lokale E-Mails. Im Normalfall werden diese Server dazu verwendet, E-Mails vom internen E-Mail-Server direkt ins Internet beziehungsweise E-Mails aus dem Internet an den internen E-Mail-Server zu versenden. Bei jedem Sendeversuch wird geprüft, ob es sich um eine Spamming-Mail handelt. [ZwCoCh00]

2.1.21 Maskieren (englisch: Masquerating)

Maskieren erlaubt es, alle Rechner aus einem internen Netzwerk unter Verwendung der äußeren IP-Adresse eines Routers mit gerouteter Adresse für außenliegende Netzwerke, wie zum Beispiel dem Internet, zu präsentieren.
Interne Clients mit nicht gerouteten Adressen können ohne Proxy-Server auf Ressourcen des Internets zugreifen.
Zur Verdeutlichung ein Beispiel:
Ein Client baut eine Verbindung zu einem Server im Internet auf. Im Router wird für jedes Paket die Senderadresse (Source-Address) durch die äußere Adresse des Routers ersetzt. Bei den zurückkommenden Paketen der Verbindung ersetzt der Router seine eigene Zieladresse (Destination-Address) durch die Clientadresse. Für den Ser-

ver im Internet ist es eine Verbindung zwischen dem Router und sich selbst, für den Client ist es eine Verbindung direkt mit dem Internetserver. Der Router fungiert transparent für Clients und Server als Vermittler. [ZwCoCh00]

2.1.22 NAT (Network Address Translation)

Zusätzlich zu den bisherigen Paketfiltern und dem Maskieren kann in einer Firewall NAT eingesetzt werden.

Hiermit ist es im Unterschied zum Maskieren möglich, bestimmte Adressen mit Ports auf andere Adressen beziehungsweise Ports umzuleiten. Dies ermöglicht zum Beispiel den Einsatz transparenter Proxy-Server für bestimmte Dienste in der DMZ.

Eine weitere Möglichkeit, NAT einzusetzen, ist die Weiterleitung von gerouteten öffentlichen Adressen für bestimmte Ports (Dienste) zu inneren privaten Adressen.

Ein Beispiel zur Verdeutlichung:

Eine Firma besitzt nur eine öffentliche Adresse im Internet und möchte trotzdem Dienste auf mehrere Server verteilen. Durch NAT werden Anfragen auf bestimmten Ports an andere Rechner weitergeleitet:

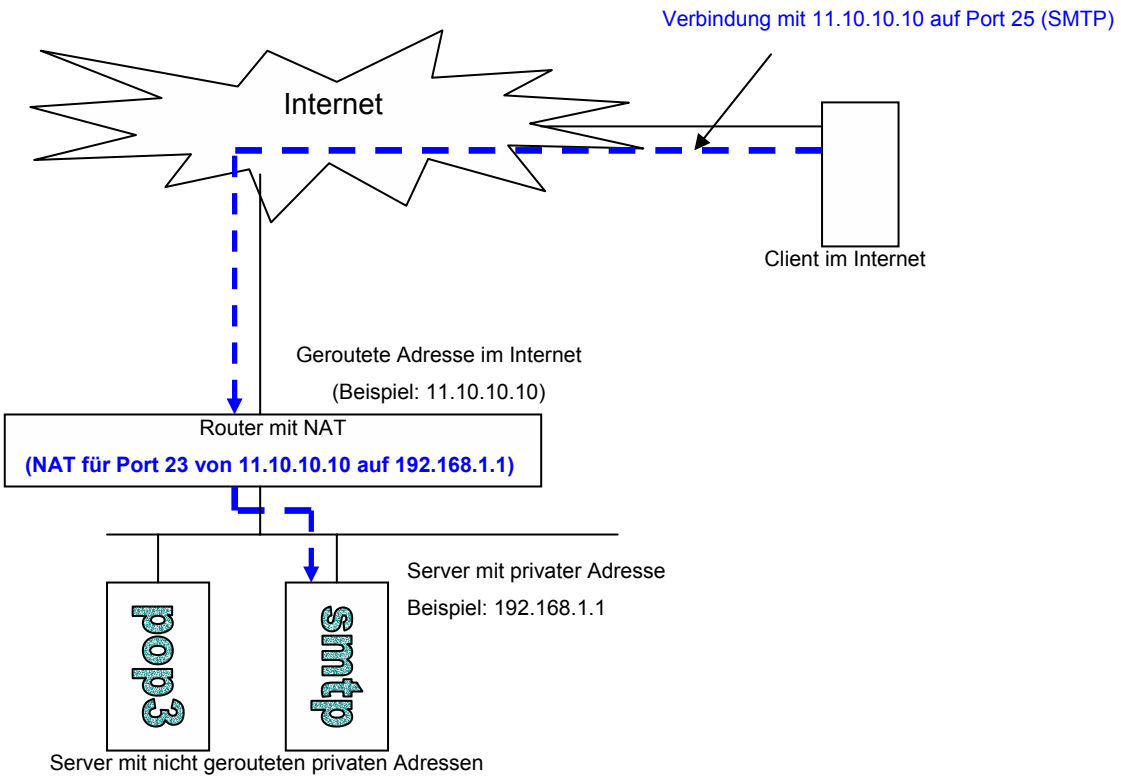


Abbildung 2-4: Verbindung NAT

Ein Client im Internet fordert eine Verbindung mit der IP-Adresse 11.10.10.10 auf dem Port 25 (SMTP) an. Der Router besitzt in der Konfiguration einen NAT Eintrag für den-Port 25 und leitet die entsprechenden Pakete an den zuständigen Server weiter, der im internen Netz liegt (Name: smtp). Hierfür ersetzt der Router seine eigene Empfängeradresse in den Paketen mit der des betreffenden internen Servers. Bei der Rückverbindung ersetzt er die Senderadresse durch seine eigene. Sowohl Client als auch für den Server bleibt die Veränderung der Pakete transparent. [ZwCoCh00]

2.1.23 Proxy-Server (Application-Gateways)

Proxy-Server leiten die Kommandos und Daten von oder an Clients weiter. Die Clients haben keinen direkten Kontakt mit den angefragten Servern im Internet oder anderen Netzen, sondern nutzen den Proxy-Server als Gateway. Ein angefragter Server kommuniziert nur mit dem Proxy-Server. Für ihn ist der Proxy-Server der anfragende Client für diese Verbindung ins Internet. Dabei ist zu berücksichtigen, dass clientseitig nicht alle Anwendungen einen Proxy-Server unterstützen.

Bei einigen Diensten können sogenannte Cache-Speicher eingesetzt werden. Falls Clients mehrere Anfragen an dieselbe Ressource wie zum Beispiel Bilder oder HTML-Seiten im Internet stellen, braucht der Proxy-Server diese nicht mehr direkt aus dem Internet zu laden, sondern nur noch aus seinem Cache.

Ein weiterer Vorteil von Proxy-Servern ist, dass Clients nicht direkte Verbindungen zum Internet aufbauen. Somit benötigen die Clients keine öffentlichen Adressen im Internet und können durch Filter und ACLs beschränkt werden.
[ZwCoCh00]

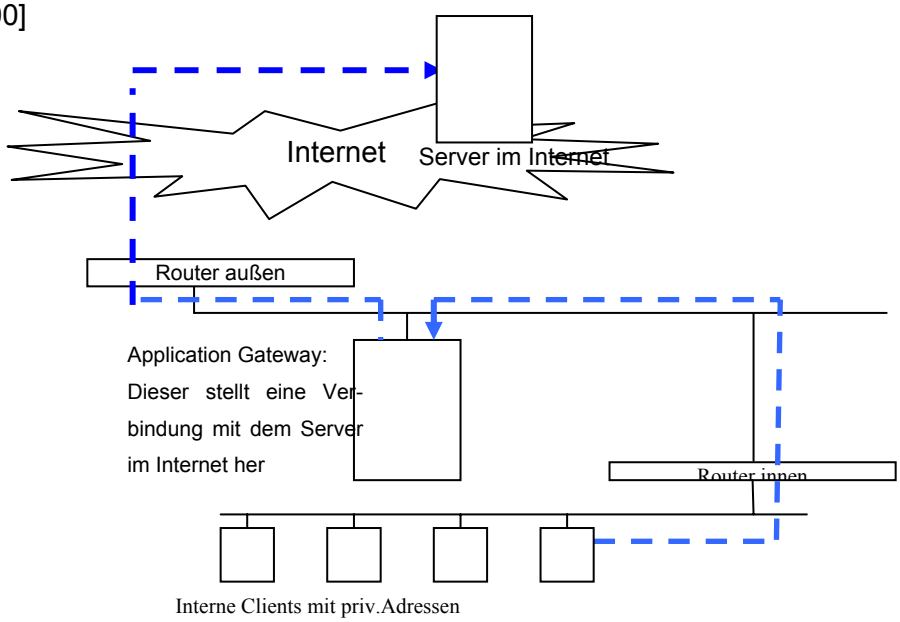


Abbildung 2-5: Verbindung mit Gateways

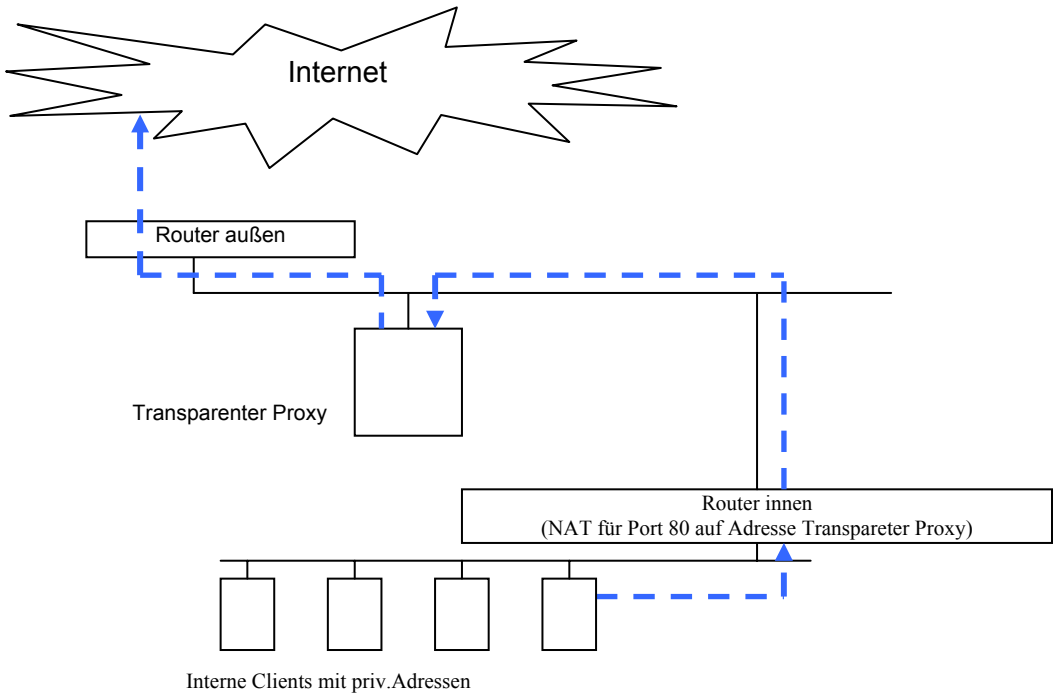
2.1.24 Transparente Proxy-Server

Transparente Proxy-Server können einige Dienste wie zum Beispiel HTTP transparent anbieten, was bedeutet, dass dieser Proxy-Server für den nutzenden Client nicht sichtbar ist.

Beispielsweise werden alle ausgehenden Verbindungen von Clients an WWW-Server im Internet an einen Proxy-Server umgeleitet. Hierfür werden alle Pakete an Port 80, den Standardport für WWW-Server, mit NAT an einen transparenten Proxy-Server geleitet. Der Unterschied zum vorherigen Beispiel ist, dass an den Client-Anwendungen keine besonderen Einstellungen vorgenommen werden müssen.

Der transparente Proxy leitet die Anfrage weiter ins Internet. Für den Client ist es eine

Abbildung 2-6: Verbindung Transparenter Proxy und NAT



direkte Verbindung ins Internet, sie ist für diesen transparent. Der transparente Proxy-Server stellt eine Anfrage an einen WWW-Server und leitet die Antwort den Client weiter. [ZwCoCh00]

2.2 Mögliche Angriffe und dessen Folgen

Jeder Angreifer verfolgt in der Regel ein bestimmtes Ziel. In den meisten Fällen ist dieses der Missbrauch von Ressourcen, Spionage oder das Lahmlegen bestimmter Dienste. Ein erfolgreicher durchgeführter Angriff kann nicht nur einen finanziellen Schaden anrichten, sondern auch das Image beziehungsweise den Ruf einer Firma schädigen. [ZwCoCh00, BoWo97,FBI01]

2.2.1 Angriffspunkte

Ein Angreifer macht sich sowohl die Schwächen als auch die Fehler in einem System zunutze. Folgende Fehler und Schwächen im System sind als Sicherheitsrisiken einzustufen:

- Konfigurationsfehler:
  Falsche Parameter oder Einstellungen der lokalen Administratoren sind häufige Konfigurationsfehler. Beispiele hiefür sind: falsche Berechtigungen, fehlerhafte Zugriffsrechte von Diensten und Programmen sowie eine unbedachte Lücke in Systemdiensten .

- Implementierungs- und Programmierfehler:
  Dienste, Programme und Protokolle wurden fehlerhaft implementiert. Die häufigsten Folgen sind Pufferüberläufe, die den Angreifer befähigen, Systemabläufe auf dem System zu beeinflussen. Auch Fehler bei der Sicherheit von Anwendungen in einem System sind hier berücksichtigen. Fehler in Java, ActiveX und anderen Plugins werden in letzter Zeit häufig aufgedeckt. Diese Fehler können in folgende Kategorien eingeteilt werden:
  - Designfehler im Kommunikationsprotokoll
  - Designfehler in der Dienstspezifikation
  - Designfehler in einer Anwendung

- Fehlverhalten von Benutzern:
  Anwender, die sich nicht an die Sicherheitskriterien des Unternehmens halten, stellen ebenfalls ein Risiko im Netzwerkbetrieb dar. Hierzu gehört zum Beispiel die Verwendung einfach zu erratender Passwörter.

- Andere Schwächen:
  Hiermit sind alle Schwächen oder Fehler gemeint, die nicht zu den vorherigen Kategorien gehören wie zum Beispiel die Möglichkeit eines Portscans trotz äußerem Router mit Paktfilter. Aber auch Schwächen wie zum Beispiel unentdeckte Fehler oder Fehler durch menschliches Versagen, die sich nicht vermeiden lassen, stellen ein Sicherheitsrisiko dar.

Details zu Implementierungsfehlern werden über Mailinglisten und Newsgroups zur Verfügung gestellt. Die bekannteste Mailingliste in Deutschland ist der DFN-Cert. Fast täglich werden hier neue Fehler und Patches bekannt gegeben. [ZwCoCh00,BeWo97,Pohl00,DFN01]

2.2.2 Angriff nach Plan

Ein Angriff erfolgt fast immer geplant und ist durch bestimmte Ereignisse im System zu erkennen. Zunächst muss sich ein Angreifer Informationen über das Netzwerk und dessen Dienste beschaffen. Dazu wird in der Regel ein Portscanner verwendet. Es gibt Hunderte von Portscannern, die auf unterschiedliche Weise einen Netzabschnitt nach bestimmten Diensten durchsuchen. Antwortet ein Server auf eine der Anfragen des Portscanners, weiß der Angreifer, welche IP-Adresse einen bestimmten Dienst anbietet. Der Angreifer versucht mittels Hilfsprogrammen wie finger, netstat, ruser, nbtstat, rwho oder rstat zusätzliche Daten zu ermitteln, um mehr Informationen über das Netzwerk zu erhalten. Anschließend kann der Hacker auf verschiedene Netzwerkressourcen zugreifen, um Fehler in Diensten oder Protokollen auszunutzen und um Benutzerrechte zu erlangen. Hier beginnt der eigentliche Angriff. Wenn ein Fehler gefunden und ausgenutzt wurde, beginnt der Angreifer Daten auf dem Rechner zu modifizieren. Hierbei nutzt er häufig Fehler in Anwendungen oder weiteren Diensten aus. Der Angreifer bekommt häufig die vollen Rechte (root oder Administrator) auf dieser Maschine. Jetzt kann der Angreifer je nach Konfiguration des Netzes weitere Rechner, denkbar wären interne Server, angreifen, um sich so auf noch mehr Rechnern im System Rechte zu verschaffen und um seine Spuren zu verwischen. Im weiteren Verlauf kann er Schaden mit dem Löschen oder dem Ausspionieren von Daten anrichten. Der zeitliche Rahmen für die Abfolge eines Angriffs ist dabei nicht festgelegt. [ZwCoCh00,Pohl00]

2.2.3 Angriffsarten

Angriffe auf Systeme finden auf verschiedenen Ebenen statt. Der Hacker kann einen oder mehrere Fehler in einem System ausnutzen, um seine Ziele zu erreichen. Im folgenden werden die möglichen Angriffsarten basierend auf der im OSI-Modell beschriebenen Schichten unterteilt.

2.2.3.1 Angriffe auf die untere Protokoll-Ebene

Viele Angriffe werden schon auf der *ARP-Ebene (Address Resolution Protocol)* durchgeführt. Da auf dieser Ebene häufig weniger protokolliert werden kann, hat das Intrusion Detection System Schwierigkeiten, Angriffe aus diesem Bereich zu erkennen.
Eine Schwachstelle in diesem Protokoll ist, dass ein Angreifer die Cachespeicher anderer Rechner beeinflussen kann. Normalerweise verschickt ein Rechner einen Broadcast in das Netz „Wer hat die IP-Adresse 192.168.152.1“ und bekommt darauf eine Antwort mit der Mac-Adresse (Hardware-Adresse), der angeforderten TCP/IP-Adresse.
Anschließend sendet der Angreifer eine gefälschte Antwort an den anfragenden Rechner, die dem Host mitteilt, dass zu seiner MAC-Adresse des Angreifers, die IP-Adresse 192.168.152.1 gehört. Der Host „xxx“ trägt diesen gefälschten ARP-Eintrag in seinen ARP-Cache ein. Greift dieser auf die Adresse 192.168.152.1 zu, wird eine Verbindung mit dem Hackerrechner aufgebaut. [HeKa98, Pohl00]

2.2.3.2 Angriffe auf IP-Ebene

Von der dritten Schicht des OSI-Modells sind mehrere Schwachstellen bekannt. Zahlreiche Design- oder Implementierungsfehler sind bis heute gar nicht oder nur zum Teil korrigiert worden. Die folgende Aufzählung bietet eine kurze Übersicht der bekannten Angriffsmöglichkeiten:

- IP Fragmentierung:
  TCP-Header-Informationen können fragmentiert sein. Router suchen häufig nach bestimmten Zeichenketten in einem TCP-Header und können somit leicht überlistet werden, da die gesuchten Informationen nicht vorhanden sind.
- Fälschung der IP-Header:

Ein Hacker kann die Länge oder Quelladresse eines IP-Paketes fälschen. Somit bringt er den Stack des Zielsystems durcheinander und das System kann stehen bleiben.

- SYN Paket mit unerreichbarer Quelladresse:
  Ein Angreifer sendet einen „gewünschten Verbindungsaufbau (SYN)“ an einen Rechner, dabei enthält das Paket eine gefälschte und unerreichbare Quelladresse. Der angesprochene Rechner reserviert Speicher in seinem System und sendet ein SYN-ACK Packet, um den angeforderten Verbindungsaufbau fortzusetzen. Da die ursprüngliche IP-Adresse nicht erreichbar ist, wartet der Rechner vergebens auf die nächste ACK-Bestätigung.
- CPU-Angriffe auf Microsoft Windows NT:
  Durch Implementierungsfehler in Microsoft Windows NT 4.0 Systemen ist es möglich, durch Verbindung auf bestimmte Ports (137,53,135) und das Senden bestimmter Zeichenketten, die CPU Auslastung auf 100% zu erhöhen.
- ICMP-Redirect:
  Mit gefälschten ICMP-Redirect-Paketen können die Routingtabellen von Zielrechnern verändert werden.
- ICMP-Destination Unreachable oder ICPM Time to Live exceeded:
  Durch solche Angriffe können Router falsche Informationen über die Erreichbarkeit anderer Rechner erhalten. Das hat zur Folge, dass ein Zielsystem nicht mehr erreichbar ist.
- ICMP-Tunnel:
  Hat ein Angreifer einen Rechner im Zielsystem, der solche Pakete interpretieren kann, besteht die Möglichkeit, trotz einer Firewall Daten über eine ICMP-Tunnel-Verbindung zu übertragen.

[HeKa98]

2.2.3.3 Angriffe auf die höheren Protokoll-Ebenen

- DNS-Cache Verfälschung:
  Im Aliasfeld falsche Informationen eingetragen
- Kein Reverse-Lookup des Zielsystems:
  Findet der Angreifer heraus, dass kein Reverse-Lookup vom Zielsystem ausgeführt wird, so kann er leichter eine gefälschte DNS-Antwort schicken.

- NIS (Network Information System) – Fälschung der RPC-Anfrage:
  In diesem Fall wird per IP-Spoofing eine falsche Antwort an einen NIS-Client gesendet.
- FTP (File Transfer Protocol) Angriff des Datenkanals bei passiver Verbindung:
  Durch das Erraten der Ports für den Datenkanal erhält ein Angreifer bei einer bestehenden Client-Server Verbindung durch einen Fehler in der Implementierung des FTP-Servers dieselben Daten, die der Server dem Client der ursprünglichen Verbindung übermittelt.
- FTP Brute-Force Angriffe:
  - Passwortangriff:
    Benutzernamen und Passwörter werden durch entsprechende Software entschlüsselt oder ermittelt
  - Benutzerrechte:
    Durch fehlerhafte Benutzerrechte ist es möglich wie zum Beispiel Schreibrechte im FTP-Root Verzeichnis ist es möglich, die Datei .rhost zu übertragen, um erweiterten Zugriff auf das System zu erhalten.
  - TFTP:
    Durch falsche Berechtigungen ist es möglich, die Datei „/etc/passwd“ zu übertragen.
- HTTP – CGI:
  Durch Fehler in der Einrichtung des HTTP-Dämons ist es möglich, Informationen und Systemdateien zu übertragen.
- NFS (Network File System)
  - Fälschung durch IP-Spoofing und damit erlangen von Zugang zur Freigabe
  - Erraten des Filehandels
    Die Filehandels sind bis zum Neuinstallieren des NFS-Servers gültig
  - Falls die Exportliste mehr als 255 Zeichen hat kommt es zum Pufferüberlauf
  - Ältere NFS-Server erlauben es, per „cd ..“ Befehl bis zur Server-Root vorzudringen.

- Mailspoofing bei SMTP-Servern
  Da im Protokoll selbst keine Authentifizierung vorgesehen ist, kann jeder Client die Daten wie zum Beispiel die Senderadresse oder andere Header-Informationen selbst angeben. Eine Datenechtheit ist somit nicht gegeben!

- Verteilter Angriff
  Hierbei werden beispielsweise durch Skripte Verbindungen von verschiedenen Rechnern gleichzeitig aufgebaut. Dadurch kann es bei Überlastung zum Denial-of-Service kommen.

[HeKa98]

2.2.3.4 Angriffe auf Authentifizierungssysteme

Die Gewährleistung, dass Benutzer in einem System sicher und ordnungsgemäß authentifiziert werden, stellt ein großes Problem dar. Von diesem Aspekt kann die Sicherheit eines ganzen Netzwerksystems abhängen. Dabei sind zwei Sicherheitslücken besonders gefährlich:
[HeKa98, DFN01]

Passwörter sind unverschlüsselt

Bei vielen Diensten im Internet werden Passwörter unverschlüsselt übermittelt. Durch sogenannte Netsniffer können die Passwörter leicht ausspioniert werden. Zu den gefährdeten Diensten gehören:

- POP3 (Post Office Protocol)
- Telnet
- FTP (File Transfer Protocol)
- Windows 95 Remoteanmeldung
- Windows NT 4.0 Remoteanmeldung (nur vor Service Pack3)

[CCC01]

Passwörter sind zu einfach (Benutzerfehler)

Viele Benutzer mögen Passwörter nicht oder können sich diese schlecht merken. Aus diesem Grund vergeben viele Benutzer Passwörter, deren Inhalt mit Ihrer unmittelbaren Umgebung in Zusammenhang steht (Name des Partners, Name der Kindes,

Geburtsdaten). Passwordcracker besitzen Wortlisten mit den meist verwendeten Kennwörtern. So kann ein Angreifer leichte Kennwörter leicht herausfinden.
[CCC01]

2.2.3.5 Angriffe auf allen Protokoll-Ebenen (Spoofing)

Die Möglichkeit, einem Rechner wie zum Beispiel einem Router, eine falsche Identität vorzutäuschen, nennt man Spoofing. Dabei gibt es verschiede Möglichkeiten:

- IP-Spoofing :
  IP-Spofing bedeutet die Fälschung der IP-Adresse.
- TCP-Sequenznumme:
  Durch eine gefälschte IP-Adresse und erratene Sequenznummer kann eine vorhande Verbindung übernehmen werden.
- DNS-Spoofing:
  Durch das senden gefälschter Informationen an einen DNS-Server können Adressen und Namen verfälscht werden.
- RIP Spoofing:
  Routen können durch gefälschte Antworten bei RIP-Anfragen gefälscht werden.

2.2.3.6 Viren, Würmer und Trojanische Pferde

In der Regel werden diese Programme oder Programmsegmente in einem Netzwerk von einem Benutzer ungewollt aktiviert. Sie sind eine der größten Gefahren aus dem Internet. Es ist nicht nur möglich, einzelne Rechner oder Netze zu infizieren, sondern es können sicherheitsrelevante Daten an Angreifer verschickt werden. Eine Firewall kann solche Angriffe meistens nicht abwehren. In dem System sollte deshalb eine sich täglich automatisch aktualisierende Antivirensoftware installiert sein. [Sym01]

2.2.4 Folgen von Angriffen

Die meisten Angriffe aus dem Internet verlaufen relativ glimpflich für das attackierte System. Dies liegt daran, dass häufig nur vorgefertigte Angriffsprogramme von unerfahrenen Benutzern eingesetzt werden. Der daraus resultierende Schaden ist aufgrund der schnellen Bekanntheit der Programme meistens gering.
Die größte Gefahr stellen erfahrene Angreifer dar, die auf Kommandozeilenebene ihren Angriffscode selbst schreiben beziehungsweise die Programmierer von Angriffspro-

grammen. Diese verfügen über das notwendige Know-how, Sicherheitsmaßnahmen geschützter Systeme zu umgehen. Der Schaden, den diese Gruppe von Angreifern anrichten kann, reicht von vollständigem Datenverlust über Diebstahl bis hin zur Nutzung der Ressourcen durch Unbefugte.
Aus jüngster Zeit haben mehrere Fälle von Missbrauch gestohlener Daten für Aufmerksamkeit gesorgt. Im Jahr 2000 beklagten einige Kreditinstitute als Folge eines Hackerangriffs auf ihre Netzwerke den Verlust von tausenden Kreditkartendaten inklusive der persönlichen Daten der Betroffenen.
Laut US-Geheimdienst verursacht Wirtschaftsspionage über das Internet Schädenin Milliardenhöhe. Weder die CIA noch das FBI können eine Lösung für vollständigen Schutz in diesem Bereich anbieten. Die NSA entwickelt derzeit auf Basis von LINUX ein Betriebssystem, das einen neuen Sicherheitsstandard setzen soll. Das System soll unter dem Namen SeLINUX (Secure LINUX) mit vollständigem Quellcode veröffentlicht werden. [Sym01;Graf01;CIA01]

2.2.5 Sicherheitsanforderungen an ein Netzwerk

Diese werden in der Fachliteratur genau definiert:

- Zugangskontrollen (Wer darf in das Netzwerk?)
- Authentifizierung (Wer ist der Benutzer?)
- Autorisierung (Wer mit welchen Rechten?)
- Daten-Integrität (Sicherheit der Daten)
- Vertraulichkeit und Verfügbarkeit (Informationen zur Kenntnis nehmen und nutzen)
- Nachweisbarkeit (Beweiskräftig dokumentieren)
- Auditing (Prüfung der Ereignisse)

Nur Systeme, die alle diese Sicherheitskriterien erfüllen, gelten als sicher. Firewalls und spätere Intrusion Detection Systeme sollten zusätzliche Sicherheitskriterien erfüllen. Der Einsatz neuer Systeme wie Intrusion Detection und Intrusion Response wird in den folgenden Jahren immer größeren Einfluss gewinnen. Diese sollen die oben genannten Definitionen in Real-Time überprüfen und bei Verstößen Gegenmaßnahmen einleiten.
Die Sicherheitsanforderungen müssen Bestandteil der Unternehmenskultur werden, um eine korrekte Umsetzung im gesamten Unternehmen zu garantieren. Derzeit ist die Benutzerverwaltung vieler Microsoftnetzwerke in Unternehmen von den lokalen Admi-

nistratoren falsch konfiguriert. Nach Umfragen in mittelständischen Unternehmen gibt es sogar Netzwerke, in dem sich alle Benutzer mit den Rechten von Administratoren anmelden. Dies ist auf die mangelnde Kompetenz der lokalen Administratoren zurückzuführen.[BoWo97,Sym01,ZwCoCh00]

2.3 Bisherige Konzepte

2.3.1 Konzepte für Firewalls

Der derzeitige Entwicklungsstand präferiert zwei Firewall-Konzepte. Alle Konzepte sollten einer einfachen Grundregel folgen: „Alles, das nicht ausdrücklich erlaubt ist, ist verboten“. Bei einer Firewall mit **Dual-Homed-Host** gibt es zwischen internem Netz und dem Internet nur einen Server, der verschiedene Proxy-Dienste anbietet. Auf keinen Fall darf dieser Server Pakete zwischen den beiden Netzen routen. Man benötigt bei der Verwendung dieses Firewall-Konzeptes nur eine öffentliche IP-Adresse; dies ist eine häufig verwendete Lösung für kleinere Firmen.

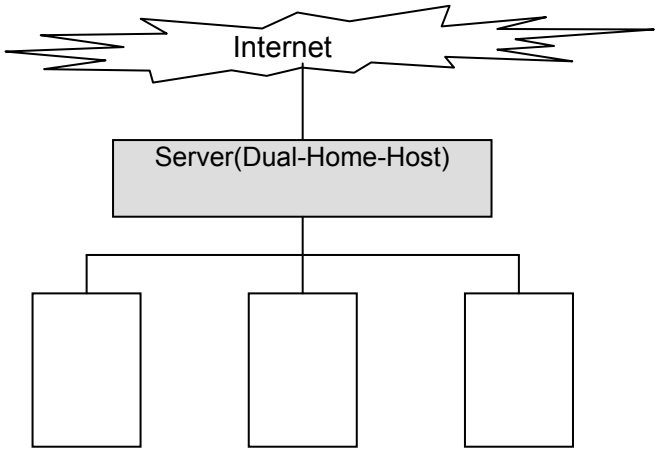


Abbildung 2-7: Firewall Dual-Homed-Host

Das meistverbreitete Firewall-Konzept verwendet ein **Grenznetz**. Dieses Grenznetz nennt man DMZ (**De**-**m**ilitarisierte **Z**one). Die DMZ befindet sich zwischen Internet und dem internen Netz und ist durch zwei Router getrennt.

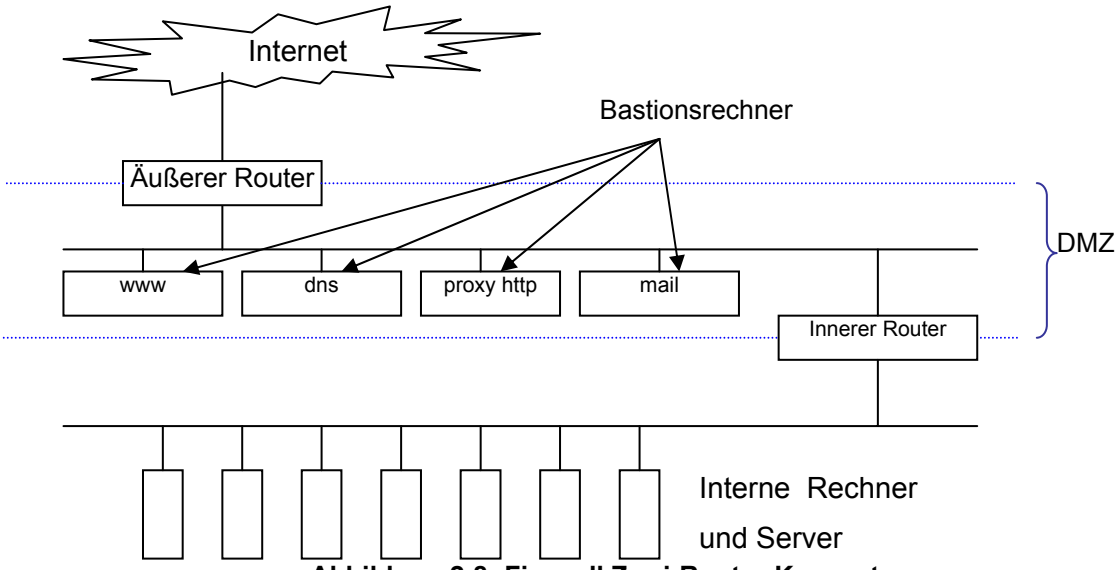


Abbildung 2-8: Firewall Zwei-Router-Konzept

In einem Grenznetz befinden sich alle Server, die Proxy-Dienste oder Dienste im Internet anbieten. Diese Server sind sogenannte Bastionshosts und werden im Falle eines Angriffs als „geopferte Rechner“ eingeordnet.[ChCoCh00]

2.3.2 Der heutige Entwicklungsstand von Intrusion Detection

Auf dem Markt vorhandenen Intrusion Detection Systeme untersuchen lediglich die von den Systemen erzeugten Auditdaten. Da die Daten wegen der umfangreichen Nutzung des Internets schnell sehr groß und damit unhandlich werden, beschreitet die Analyse der Daten neue Wege. Ein Schritt davon ist, dass ein Intrusion Detection System die Auditdaten nach einem bekannten Angriffsmuster auswertet.

Nun können die Daten auf ein überschaubares und trotzdem aussagekräftiges Niveau reduziert werden. Dies birgt jedoch die Gefahr in sich, dass neue Angriffsmuster nicht erfasst werden können.

Viele Administratoren erkannten die Notwendigkeit der Überwachung anderer Systemzustände, die nicht in den Auditdaten vorhandenen sind. Ein Beispiel hierfür ist die Überwachung der Datei- und Ordnerstruktur auf den gefährdeten Rechnern.

Diese Aspekte verraten, dass die Intrusion Detection Systeme noch am Anfang ihrer Entwicklung stecken. [HeKa98]

2.4 Allgemeiner Aufbau eines Intrusion Detection Systems

Laut Definition besteht ein Intrusion Detection System aus drei Hauptkomponenten:

- ***Datensammlung:***
  Die Daten über Ereignisse und Systemzustände der Rechner müssen gesammelt. Diese Daten sollten, wenn möglich, auf einem zentralen Server erfasst werden.

- ***Datenanalyse:***
  Gespeicherte Auditdaten müssen analysiert werden, um mögliche Angriffe zu erkennen. Mögliche einsetzbare Systeme sind künstliche Neuronale Netze oder Expertensysteme.

- ***Ergebnisdarstellung:***
  Die gesammelten Daten müssen in ein für den Benutzer lesbares Format aufbereitet werden.

Eine weitere und feinere Untergliederung der Komponenten ist möglich. [HeKa98]

3 Machbarkeits- und Verfügbarkeitsstudie

Vor der Planung und Umsetzung eines Firewall-Konzeptes ist es erforderlich, den Stand des derzeit technisch Machbaren zu erfassen und bereits vorhandene Lösungen zu betrachten. Das Ziel ist der Aufbau einer soliden Grundlage, auf der eine Erweiterung mittels intelligenter Angriffserkennung und –abwehr für Firewall-Systeme durch neuronale Systeme aufgesetzt werden kann. Dazu ist es notwendig zu wissen, welche Umsetzungsmöglichkeiten die derzeitige Netzwerktechnik hinsichtlich intelligenter Firewall-Systeme ermöglicht. Schließlich ist zu prüfen, welche bereits zur Verfügung stehenden Lösungen zur weiteren Verwendung herangezogen werden können.

3.1 Einsatzziele und Voraussetzungen

3.1.1 Ziele

Das primäre Ziel eines Intrusion Detection Systems ist es nicht nur bekannte Angriffssituationen zu erkennen, sondern auch neue zu analysieren.
In Zukunft soll das System durch künstliche Intelligenz über neue Situationen entscheiden und Maßnahmen zur Gegenwehr ergreifen können. Ein ausgereiftes Intrusion Detection System soll sich selbst organisieren und Entscheidungen über Fehlerbeseitigung treffen können. Die administrativen Aufgaben sollen bis auf einen kleinen Teil vom Intrusion Detection System übernommen werden. Die Administration und zusätzlichen Konfiguration des Systems soll für den Administrator überschaubar sein.

3.1.2 Theoretische Voraussetzungen für Neurocomputer

Der erste erfolgreiche Neurocomputer (Mark I Perceptron) wurde 1957/58 von Frank Rosenblatt, Charles Wightman und Mitarbeitern am MIT entwickelt und für die Mustererkennung eingesetzt. Zu jener Zeit konnte dieser Neurocomputer bereits mit einem 20x20 Pixel großem Bildsensor einfache Ziffern erkennen. Er funktionierte mit Hilfe von 512 motorgetriebenen mechanischen Potentiometern, je einem für jedes der variablen Gewichte.

Im weiteren Verlauf der Entwicklung gab es erst Ende der Achtziger Jahre Fortschritte. Die Zahl der Forscher auf dem Gebiet der Neuroinformatik ist auf mehrere Tausend angestiegen.

Es gibt viele wissenschaftliche Zeitschriften, die als Hauptthema neuronale Netze beinhalten (Neural Networks, Neural Computation, Neurocomputing). Große anerkannte wissenschaftliche Gesellschaften wie die INNS (International Neural Network Society), die ENNS (European Neural Network Society), die IEEE Fachgruppe über neuronale Netze und Fachgruppen nationaler Informatik-Gesellschaften wie die GI (Gesellschaft für Informatik) zeigen, dass die Entwicklung vorangetrieben wird.

Auch deutsche Forscher haben sich auf diesem Gebiet hervorgetan. Zum Beispiel Prof. von Seelen, der durch neuartige neuronale Ansätze zum Stereosehen eines mobilen Roboters bekannt wurde oder Prof. Günter Palm, der durch seine theoretischen Arbeiten über Assoziativspeicher und ihre Hardware-Realisierung wissenschaftliche Bedeutung erlangte. Prof. Alex Waibel ist mit seinen wissenschaftlichen Arbeiten über Time-Delay-Netze zur Spracherkennung hervorgetreten.

Das Unternehmen Siemens betreibt eigenständige Forschungen auf diesem Gebiet, sowohl theoretische Grundlagenforschung, als auch die praktische Entwicklung eines VLSI-Neurocomputer (Ramach), der auch an einigen Hochschulen als Test-Neurorechner im Einsatz ist.

[Rau01; Lipp00]

3.2 Machbarkeitsstudie

Die Soft- und Hardwarehersteller überschlagen sich mit Meldungen über neue Produkte, die mehr Leistung und mehr Komplexität besitzen sollen. Im Berech der künstlichen Neuronalen Netze gibt es im Bereich der nicht wissenschaftlichen Anwendungen wenig Neues. Die Hersteller setzen immer noch auf konventionelle Techniken.

3.2.1 Möglichkeiten der Hardware

Trotz der stetigen Weiterentwicklung im Bereich von Computern haben Rechner und Software heute noch nicht die Leistungsfähigkeit, künstliche Neuronale Netze mit der Leistungsfähigkeit des Gehirns in Echtzeit nachzubilden. Die Architektur der heutigen Rechner basiert auf der Neumanschen Rechnerarchitektur, die nur einen beziehungsweise wenige leistungsstarke Prozessoren enthält. Die Parallelisierung verfolgt ein anderes Konzept, bei dem viele Prozessoren mit weniger Leistung verwendet werden, um eine höhere Geschwindigkeit zu erreichen. An solch einem Neurocomputer arbeiten die Wissenschaftler in den letzten Jahren mit Hochdruck. Dieser soll durch viele kleine Prozesseinheiten und deren Parallelisierung eine höhere Leistung als alle heutigen Rechner besitzen. Einige Ansätze solcher Neurocomputer existieren bereits, sind aber bei Weitem noch nicht ausgreift genug, alle Anforderungen an künstliche Neuronale Netze zu erfüllen. Erst dann wird es möglich sein, Echtzeitsimulationen von künstlichen Neuronalen Netzen zu erzeugen.
Selbst verteilte Systeme sind in ihrer Entwicklung noch nicht so weit ausgereift, um künstliche Neuronale Netze simulieren zu können. Software und Hardware müssen in den nächsten Jahren noch verbessert werden.
[Rau01]

3.2.2 Möglichkeiten der Software

Heute können kleinere künstliche Neuronale Netze mit Software simuliert werden. Eine Software, die es ermöglicht, neuronale Netze für den praktischen Einsatz zu erstellen, ist nicht vorhanden oder reicht noch nicht für ein komplexes Aufgabengebiet wie zum Beispiel der Überwachung einer Firewall aus. Zudem stellt die Selbstorganisation ein Problem dar. Eingeschränkte Möglichkeiten der Komplexität verhindern eine ausreichende Anzahl von Neuronen.

Aus diesem Grund weichen alle Hersteller von Intrusion Detection Systemen auf Expertensysteme aus. Diese können nur einen vorhanden Datenbestand verarbeiten, Selbstorganisation und Lernen neuer Situationen ist unmöglich.

3.3 Verfügbare Systeme

Der Markt für Sicherheitssysteme ist vielseitig. Produkte für Firewalls und Intrusion Detection Systeme sind entweder noch nicht ausgereift oder schwer zu administrieren. Im Rahmen dieser Diplomarbeit wird lediglich auf die populärsten Systeme eingegangen.

3.3.1 Produkte für Firewall-Lösungen

Heutige Firewall-Systeme bestehen meist aus mehreren Produkten, da ein Produkt nicht die volle Unterstützung der gewünschten Funktionen bietet. In den letzten Jahren hat sich in diesem Bereich das Betriebssystem Linux als Grundlage von Firewalls durchgesetzt. Eine schnelle Anpassung an neue Voraussetzungen und Fehlerbeseitigung sprechen für den Einsatz von Linux.

3.3.1.1 Squid (http-Proxy)

Squid ist ein Open-Source Produkt und für verschiedene Unix-Systeme erhältlich. Es wird als HTTP-Proxy eingestuft und bietet eine Reihe von Optionen und Filterregeln. Squid ist für den Einsatz in Firewalls empfehlenswert, da ausreichende Auditdaten zur Verfügung gestellt werden und die Konfiguration bis ins kleinste Detail reicht. Die Verwendung ist allerdings auf WWW-Browser bezogene Dienste beschränkt. Unterstützt werden:

- HTTP
- FTP (nur Browsergestütztes FTP)
- Security (HTTPS)
- Gopher
- Wais

[Squ01]

3.3.1.2 ipchains (Paketfilter)

Ipchains ermöglicht ein einfaches Filtern von Paketen auf Routern oder Servern. Eine zusätzliche Funktion ist das Maskieren. Der Vorteil ist die einfache Konfiguration per Skript.

3.3.1.3 iptables (Paketfilter und NAT)

Seit dem Kernel 2.4 für Linux ist dieses Produkt ausgereift für den kommerziellen Einsatz in Firewalls. Das Produkt unterstützt folgende Funktionen:

- Packetfiltering (Verwerfen, Reject)
- NAT (Network Address Translation)
- Regeln in “Ketten”
- Beschränkung der Paketanzahl

Der Vorteil bei diesem Produkt ist, dass die Filterregeln in Skripten angefertigt werden können. [Ker01]

3.3.1.4 Cisco Secure PIX Firewall-Serie

Von Cisco, dem Markführer im Bereich Netzwerktechnik, werden umfangreiche Firewall-Lösungen angeboten.

Die Secure Firewall PIX Serie bietet eine Sicherheitslösung mit integrierten Hardware- und Softwarekomponenten von Cisco. Hierfür verwendet Cisco ein nicht auf Unix basierendes integriertes, sicheres Echtzeit-Betriebssystem. Das System erbringt eine Leistung von 256000 simultanen Verbindungen und über 6500 Verbindungen pro Minute, wobei ein Datendurchsatz von fast 170 Megabytes pro Sekunde erreicht werden kann.[Cis01]

3.3.1.5 Firewall-1 (Firma CheckPoint)

Firewall-1 ist eine Firewall, die auf der Paketfilterung mit „Statful Inspection“ beruht. Diese Firewall ist hoch flexibel konfigurierbar und auf nicht-standardisierte Dienste anpassbar.

Eine graphische Administrationsschnittstelle ermöglicht eine zentrale Verwaltung mehrerer Rechner oder anderer Hardwarekomponenten. Eine Unterstützung von VPN bietet eine Anbindung mehrerer Firmennetze über das Internet.

Firewall-1 unterstützt folgende Funktionen:

- ANM (Active Network Management)
- Accounting
- Live Connection Report
- Load balancing
- Across the Board Client-Server- Architektur

- Grafische Benutzeroberfläche
- SMTP Support
- FTP Unterstützung
- Erweiterte Authentifizierung und erweiterte Verschlüsselung
- Transparenter Authentifizierungsserver
- Radius für Einwahlserver
- NAT (Network Address Translation)

Firewall-1 ist für alle gängigen Betriebssysteme erhältlich. [BDG01]

3.3.1.6 CyberGuart Firewall

CyberGuart Firewall ist für die Betriebssysteme Unix und Windows NT erhältlich. Das Ziel der Firma ist es, höchstmöglichen Schutz vor Angreifern aus dem Internet zu bieten. Im Paket sind folgende Dienste integriert:

- Statische und dynamische Paketfilter
- Proxy-Gateways

Eine graphische Benutzeroberfläche ermöglicht ein zentrales Verwalten der Konfiguration der gesamten Firewall. [BDG01]

3.3.1.7 TIS FWTK (Proxy/Applicationgateway)

Das TIS Firewall-Toolkit ist nur für Unix-Systeme konzipiert. Seine Funktionsweise basiert auf einem Berkley ähnlichen Socket-Interface. TIS Firewall-Tollkit bietet Application-Gateway-Funktionen für folgende Dienste:

- Telnet
- FTP
- SMTP
- HTTP
- X11
- Syslog

Das Packet entspricht der Philosophie von Firewalls, so wenig Software wie möglich auf einem System zu verwenden. Die flexible Anpassungsfähigkeit an jedes System spricht für den Einsatz zusammen mit anderen Produkten in Firewalls.

Durch Filterregeln und ACLs können alle Arten von Zugriffen festgelegt werden. Eine Aufzeichnung der Ereignisse per Syslog ist möglich. [HeKa01, Tis01]

3.3.1.8 Gauntlet Firewall

Eine Erweiterung des Trusted Information Systems FWTK ist TIS Gauntlet, das nach NCSA sowie ITSEC E3 zertifiziert ist und von der NSA evaluiert wurde. Die kompletten Sourcecodes sind erhältlich, um das Sicherheitsniveau weiter zu verbessern.
Die Erweiterung der Firewall umfasst folgende Dienste:

- Java Guart
- RSH Proxy
- SHTTP Proxy
- Zugriffsbeschränkungen für HTTP und HTTPS Proxy
- SSL Unterstützung
- POP3
- Secure Server (für FTP und HTTP)
- E-Mail-Gateway
- DNS – Server
- Real Audio
- SQL Proxy
- IP Spoof Protection
- Routing Attack Protection
- Transparenter Zugriff für Dienste
- Firewall zu Firewall Verschlüsselung

[HeKa01]

3.3.1.9 Norton Personal Firewall

Die Firma Symantec bietet eine Lösung zum Schutz von Einzelplatzrechnern im Internet an. Dieses Produkt ist für eine Netzwerkumgebung ohne richtige Firewallsysteme konzipiert und kontrolliert lediglich den Netzwerkverkehr auf den Hardwarekomponenten.
Zusätzliche Funktionen wie das Einrichten von Filtern und die Überprüfung der Webdaten sollen den Rechner vor Angriffen ausreichend schützen. Ein zentrales Speichern der Auditdaten im Netzwerk ist nicht möglich.[Sym01]

3.3.1.10 Sandbox Secure4U Enterprise

Secure4U Enterprise schützt Netzwerke bei Angriffen sowohl vor schadhaftem Code als auch vor nicht schadhaftem Code, der unbeabsichtigt das System gefährdet oder eine Sicherheitslücke öffnet.

Das Produkt arbeitet mit einem einzigartigen Verfahren einer Application Firewall. Alle Systemressourcen und -daten können gegen unerlaubte Zugriffe vor lokalen Anwendungen oder schadhaftem Code abgeschirmt werden. Folgende Schutzmechanismen sind Bestandteil dieser Firewall:

- Limitierung und Einschränkung jeglicher Ressourcen
- Überwachung und Auswertung aller Aktivitäten
- Benutzerwarnungen für unsichere Internetanwendungen wie ActiveX und Java
- Cookieüberwachung
- Überwachung von IP Adressen und Ports
- Integration einer Antivirensoftware
- Überwachung von E-Mail

Eine zentrale Auswertungsmöglichkeit der Auditdaten ermöglicht den Einsatz des Produkts in Intrusion Detection Systemen. Da dieses System nur unter Microsoft Windows Systemen eingesetzt werden kann, ist es für den Einsatz in der Firewall ungeeignet. [BeKa01]

3.3.2 Antiviren Software

Der Markt für Antiviren Software ist groß. Viren und Trojanische Pferde werden von Privatanwendern als Bedrohung angesehen und führen zu einer Fülle von Anbietern von Antivirensoftware auf dem Computermarkt.
Dabei muss die Antivirensoftware folgende Bedingungen erfüllen:

- E-Mailüberwachung auf Viren oder Trojanische Pferde
- Automatische Updates
- Client-Server Architektur
- Zentrales Management
- Automatisches Logging (Auswertbare Auditdaten)
- Automatische Benachrichtigung

Da der Markt für Antivirensoftware sich hauptsächlich auf Privatanwender spezialisiert hat, gibt es nicht viele Produkte, die diese Kriterien erfüllen.

3.3.2.1 Symantec AntiVirus Solution 7.5 (All in One)

Dieses Softwarepaket ist eine Gemeinschaftsproduktion der Firmen Symantec, Intel und IBM. Die Symantec AntiVirus Solution 7.5 bietet Unternehmen mit heterogenen Systemlandschaften einen wirksamen Virenschutz. Sie schützt Desktops, Server, Groupware, Firewalls und E-Mail-Gateways vor Viren sowie vor gefährlichen ActiveX-Controls, Java-Applets und Trojanischen Pferden.
Eine Besonderheit an diesem Produkt ist, dass bei auftretenden Problemen das System per HTTPS die infizierten Dateien direkt an das Virenlabor der Firma Symantec verschickt. Dabei werden vorher alle unternehmensrelevanten Daten aus der Datei entfernt und nur der befallende Teil an das Virenschutzlabor „Symantec AntiVirus Response Center“ (SARC) versendet.
Weitere Funktionen, wie das zentrale Verwalten über die Managementkonsole, Benachrichtigung des Administrators bei Fehlern und die automatischen Updates sind bei den Produkten der Firma seit Jahren vorhanden.
Einen Schutz vor E-Mail-Viren bietet Symantec bereits, bevor der Benutzer eine E-Mail erhält. Auf dem Server werden die E-Mails überprüft und kritische Daten isoliert. Folgende E-Mailsysteme werden unterstützt:

- Microsoft Exchange Server

- Lotus Notes Server
- SMTP Server

Ein weiteres Feature ist der Virenschutz für Firewall-Systeme. Dieses Produkt wurde von Symantec von der Firma IBM übernommen. Es unterstützt die Virenprüfung auf den Internetprotokollen HTTP, FTP und SMTP. [Sym01]

3.3.2.2 Trend Micro

Trend Micro bietet einen weitreichenden Schutz vor Computerviren im gesamten Netzwerk. Wie bei Symantec handelt es sich um ein Softwarepaket aus mehreren Einzelkomponenten:

- ScanMail für Microsoft Exchange, Lotus Notes und Lotus cc:Mail
- ServerProtect für MS-Windows NT Server oder Novell Netware Server
- InterScan VirusWall und InterScan WebProtect (Virenscanner http,SMTP,FTP)
- Desktop VirusWall (für lokale Workstations)

Es unterstützt die Systeme Windows NT, Windows 9x, Unix und Novell. Benutzerdefinierte Meldungen und Aktionen können erstellt werden. Die Auditdaten werden in den Systemprotokolldateien gespeichert und sind somit gut für die Verwendung von Intrusion Detection Systemen geeignet.

3.3.3 ID-Systeme und IR-Systeme

Seit cirka zwei Jahren entwickeln viele namhafte Unternehmen Soft- und Hardwarelösungen für Intrusion Detection und Intrusion Response Systeme, um die Netzwerksicherheit im Internet und Intranet zu verbessern. Viele große Unternehmen versuchen auf diesem Gebiet eine gewisse Vorreiterstellung zu erlangen, wobei ein durchschlagender Erfolg bislang ausblieb.

3.3.3.1 Cisco Netranger

Cisco Netranger ist ein Produkt, welches Intrusion Detection und Intrusion Response beinhaltet. Nach einem erkannten Angriff werden in Echtzeit Gegenmaßnahmen eingeleitet. Der Netranger ist eine Soft- und Hardwarelösung und besteht aus zwei Komponenten, einem Sensor und dem Cisco Secure IDS Director.

Der Cisco Secure IDS Director ist ein softwarebasiertes Managementsystem, das alle Aktivitäten mehrerer Cisco Secure IDS-Sensoren in definierten entfernten Netzwerksegmenten zentral überwacht. Die Administration erfolgt über ein zentrales graphisches Management-System. Das System hat durch eine statische Konfiguration der Auswertung keine Möglichkeit, neue Angriffssituationen zu erkennen. Alle 60 Tage wird die Analysedatenbank aktualisiert. Eine Alarmmeldung ist durch Skripte beliebig erweiterbar. [Cis01]

3.3.3.2 Intrusion Detection für Firewall-1

Firewall-1 ist eine Komplettlösung für Firewalls. Die einzelnen Produktteile laufen plattformunabhängig auf jedem gängigen System (auch auf IOS von Cisco). Eine Erweiterung dieses Produkts bildet „Intrusion Detection für Firewall1“. Dabei handelt es sich um einfache Skripte, die auf bestimmte Situationen Aktionen starten, die zum Beispiel Alarm auslösen oder Veränderungen in der Konfiguration vornehmen können, um den Angriff abzuwehren. Die Konfiguration kann zentral und einfach verwaltet werden. [BDG01]

3.3.3.3 ISS RealSecure

Dieses System überwacht den gesamten Netzwerkverkehr und wertet diesen nach bestimmten Mustern aus, um bedrohliche Situationen zu erkennen. Wenn ein Angriff erkannt wurde, werden je nach benutzerdefinierten Vorgaben verschiedene Aktionen durchgeführt. Dies kann in Form von einer E-Mail an den Administrator, oder die Trennung der bedrohlichen Verbindung geschehen.
Als Zusatz können verschiedene aufgezeichnete Sessions später erneut abgespielt werden, um einen eventuellen Schaden schnell finden und beseitigen zu können.[BDG01]

3.3.3.4 eTrust Intrusion Detect

eTrust ist ein Produkt speziell für E-Business Netzwerke im Internet. Ein Expertensystem mit einer Datenbank soll Angreifer aus dem Internet sofort erkennen und Alarm auslösen. Updates der Signaturen in der Datenbank sollen die Aktualität und die Sicherheit gewährleisten. [BDG01]

3.3.3.5 Symantec Intruder Alert

Symantec Intruder Alert entdeckt unautorisierten Netzwerkverkehr und überprüft die Sicherheit von Anwendungen und Daten. Bei Gefahren kann das System verschiedene vorher definierte Aktionen ausführen.
Das Produkt ist für den Einsatz unter den Systemen Unix (Sun Solaris, AIX, HP UX, Tru64 und NCR), Windows NT und Novell konzipiert. Die Regeln für die Policies werden zentral durch graphische Managementwerkzeuge erstellt. Updates in frei

bestimmbaren Zeitabständen aktualisieren die Datenbasis des integrierten Expertensystems automatisch.
Für die Aktualität der Updates wird von dem Unternehmen Symantec garantiert. [Sym01]

3.3.3.6 LIDS (Linux Intrusion Detection System)

Ein aus jüngerer Zeit bekanntes Tool ist LIDS, das als Open Source auf der Internetseite www.lids.org frei zur Verfügung steht. Das internationale Entwicklerteam setzt sich aus unterschiedlichen Gruppen zusammen, denen sowohl Hacker als auch Universitätsprofessoren angehören. Es basiert auf dem Linux Kernel, der, um die Funktionalität zu erweitern, neu kompiliert werden muss. Der Zweck dieses Tools ist es, bekannte Schwächen von Linux zu beheben.
Derzeit erfüllt LIDS die hohen Anforderungen an ein definitionskonformes Intrusion Detection System noch nicht. Folgende Elemente sind in LIDS enthalten:

- Kernel – Access – Control –Listen
- erweitere Kernel-Sicherheit
- Reference-Monitor

Durch eine Erweiterung der vorhandenen Funktionalität soll das System sicherer werden. Die Hauptfunktionen bilden hierbei:

- Sichern und Verstecken von Dateien (wie z.B. die Konfigurationsdateien von lids)
- Sicherung der Lauffähigkeit der Prozesse - nur root kann Prozesse beenden
- Fein abgestimmte Access – Control - Listen
- Extern erweiterbare Kontrolle über das ganze System
- Erweiterter Security-Alarm vom Kernel
- Portscanner-Erkennung vom Kernel

[Lid01]

4 Systemanalyse

Die Planung eines Intrusion Detection System erfordert eine genaue Kenntnis der möglichen Schwachstellen und Angriffssituationen, die in einem Netzwerk auftreten können. Dabei müssen verschiedene Probleme beachtet werden, die durch den Einsatz unterschiedlicher Systemumgebungen innerhalb eines Netzes hervorgerufen werden können.

4.1 Festlegung der Firewall-Umgebung

Für die Implementierung des Intrusion Detection Systems im Rahmen der Diplomarbeit wird eine an das Firewall-Konzept der Fachhochschule Heidelberg angelehnte Umgebung angenommen. Diese beinhaltet eine Firewall mit zwei Routern und einem Grenznetz, welches das innere Netz vom Internet trennt.
Die strikte Abgrenzung von Grenz- und internem Netz ist nach wie vor das am besten geeignete Konzept für eine Firewall. Dieses ermöglicht eine sinnvolle Verteilung der Dienste auf die Bereiche, in denen sie tatsächlich nur gebraucht werden.
Standardgemäße Regeln einer konventionellen Firewall werden im Grundaufbau der Firewall-Umgebung verwendet. Die Namen der Rechner werden nach deren Funktion festgelegt und nur die wichtigsten Dienste betrachtet. Dabei werden nur grundlegende Dienste festgelegt.

Struktureller Aufbau der Firewall-Umgebung

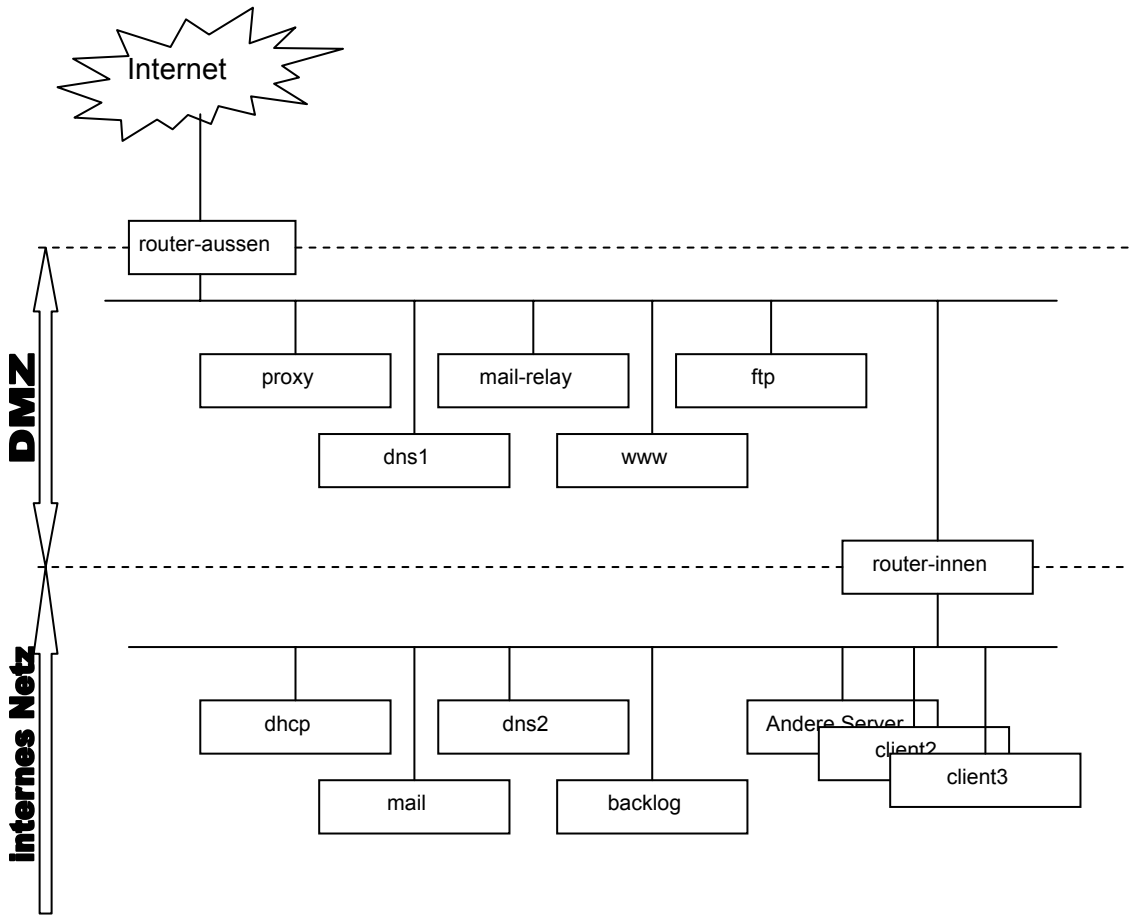


Abbildung 4-1: Beispiel Netz mit DMZ

Die folgende kurze Beschreibung gibt einen Überblick über die Funktionen und Aufgaben der Teilnetze in der angestrebten Firewall-Umgebung:

- DMZ (Demilitarisierte Zone / Zwischennetz)
  In der DMZ befinden sich alle Rechner, die Dienste im Internet anbieten sollen. Außerdem befinden sich dort Application-Gateways, die Dienste für die Clients im internen Netz weiterleiten. Die DMZ dient als Schutzwall gegen Angreifer aus dem Internet.
- Internes Netz
  Im internen Netz befinden sich alle internen Clients sowie ein Backlog-Server, ein Internet E-Mail-Server, ein interner DNS-Server und ein DHCP-Server.

4.1.1 Dienste in den einzelnen Teilnetzen

Durch die Einteilung des Netzes in einzelne Teilnetze können die angebotenen Dienste im Netz verteilt werden. Eine sinnvolle Aufteilung gewährleistet die größtmögliche Sicherheit, da beispielsweise Internetdienste nur im äußeren Grenznetz betrieben werden sollten, wohingegen interne Dienste wie zum Beispiel interne Terminaldienste nur im inneren Netz zur Verfügung stehen dürften.

4.1.1.1 Dienste der DMZ

Die DMZ beinhaltet alle Dienste, die direkt im Internet angeboten werden oder Application-Gateways, die Dienste aus dem Internet anbieten.

DNS *(Server: dns1)*	leitet interne Name-Server-Anfragen an das Internet weiter und antwortet auf DNS-Anfragen aus dem Internet. Dieser DNS-Server kennt nur die Namen der Rechner, die sich im gerouteten Netzbereich befinden. Dieser Name-Server besitzt keine eigene Datenbasis.
FTP *(Server: ftp)*	stellt Dateien im Internet zur Verfügung.
HTTP *(Server: www)*	präsentiert die HTML-Dokumente der Institution.
SMTP *(Server: mail-relay)*	ist ein SMTP-Relay-Server, der E-Mails aus dem Internet zum internen E-Mail-Server leitet und umgekehrt E-Mails vom internen E-Mail-Server direkt ins Internet verschickt.
Application-Gateway *(Server: proxy)*	ist ein Gateway für HTTP, FTP, Gopher und HTTPS und leitet Anfragen interner Clients an das Internet weiter.

4.1.1.2 Dienste im internen Netz

DNS *(Server: dns2)*	bietet Name-Server-Dienste für interne Adressen und Namen. Dieser Name-Server leitet alle Anfragen, die er selbst nicht beantworten kann, an den Server dns1 weiter. Der Name-Server besitzt die aktuelle Datenbasis für die Server der DMZ.
DHCP *(Server: dhcp)*	ist ein Dienst für alle internen Clients im 172.28.x.x Netzwerk.
POP3 *(Server: mail)*	ist ein E-Mail-Server, der die E-Mails der internen Clients speichert und der für den ankommenden und ausgehenden E-Mail-Verkehr über das Internet den Relay-Server in der DMZ verwendet.
SYSLOG *(Server: Backlog)*	speichert zentral die Auditdaten aller überwachten Server ab.

4.1.2 Sicherheitsaspekte und Grundeinrichtung

Verschiedene in der Firewall eingerichtete Schutzmechanismen sollen die Sicherheit in der DMZ und der internen Netze gewährleisten.
Die grundlegenden Schutzmechanismen sind momentan nur statisch und sowohl für den wachsenden Internetgebrauch als auch für die damit verbundenen höheren Gefahren aus dem Internet nicht mehr ausreichend.
Die Implementierung eines Intrusion Detection Systems ist noch nicht umgesetzt. Alle Veränderungen im System müssen vom Administrator vorgenommen werden. Das Erkennen von gefährlichen Situationen ist allein durch die Einschätzung und Kontrolle des Administrators gewährleistet.

4.1.3 Grundlegende Festlegung der Schutzmechanismen in der DMZ

4.1.3.1 Paketfilter

Eine Möglichkeit, einen Angriff auf bestimmte Dienste eines Rechners in einer Firewall zu verhindern, besteht darin, nur die Protokoll-Pakete zuzulassen, die für die jeweiligen Dienstspezifikationen nötig sind. Hauptsächlich werden solche Paketfilter auf Routern eingesetzt.

In der Firewall-Umgebung wird auf den beiden Routern, ROUTER-AUSSEN und ROUTER-INNEN, Paketfilterung eingesetzt. Die Bastionshosts haben keine eigenen Paketfilterungsmechanismen.

Die Paketfilter auf den Routern sind nach den üblichen Prinzipien einer Firewall erstellt worden. Alles, das nicht für die normale Einsatzfähigkeit benötigt wird, ist verboten.

Dazu benötigen die Router für jeden einzelnen Rechner individuelle Filterregeln. Abgelehnte Pakete werden im Syslog-Dienst mitgeloggt. Die hierfür eingesetzte Filtersoftware ist das kernelbasierende „ipchains“.

Die Filterregeln sind nicht nur auf „forward“ beschränkt, um einen unmittelbaren Zugriff auf die Router zu beschränken. Alle „input“ und „output“ Pakete werden ebenfalls auf gültige erlaubte Regeln hin überprüft.

4.1.3.2 SYN und ACK bei TCP-Paketen

Zusätzlich zu den Paketfiltern wird bei den TCP-Paketen einer Verbindung überprüft, ob es sich um einen Verbindungsaufbau (Syn-Bit ist gesetzt) oder um ein Bestätigungspaket (ACK-Bit ist gesetzt) handelt. Viele Hacker versuchen einen Server anzugreifen, indem Sie nach den Filterregeln zwar die richtigen Pakete schicken, aber in Wirklichkeit einen neuen Verbindungsaufbau herstellen. In dieser Firewall werden alle SYN-Pakete verboten, die nach Protokollspezifikation für einen Verbindungsaufbau nicht erforderlich sind.

4.1.3.3 Software und Dienste auf den Bastionshosts

Software und Dienste auf den Servern sind die Hauptangriffspunkte. Durch eine Beschrängung der Software und Dienste auf das Notwendigste wird die Zahl der möglichen Angriffspunkte reduziert.

4.1.3.4 Zentrale Auditdaten

Nach einem erfolgreich durchgeführten Angriff werden zuerst die lokalen Auditdaten vom Angreifer verändert, um den Angriff zu verstecken.
Alle Auditdaten werden zusätzlich zu der lokalen Speicherung über den Syslog-Dienst ungepuffert an den internen Backlog-Server geschickt, der diese Daten zentral speichert. Diese Daten werden durch Skripte oder Programme verdichtet.

4.1.3.5 Verwendung von Proxy-Diensten

Alle internen Clients in der Firewall-Umgebung befinden sich in nicht gerouteten Netzen. Dadurch können diese nur Dienste über Proxy-Gateways nutzen.

4.1.3.6 Nicht geroutete Adressen für interne Clients

Durch Verwendung nicht gerouteter Adressen im internen Netz ist gewährleistet, dass Angreifer aus dem Internet nicht direkt auf die Rechner im internen Netz zugreifen können.
Zusätzlich müssen alle Clients, ohne Verwendung von Maskieren oder NAT auf den Routern, Application-Gateways verwenden, um Dienste im Internet zu nutzen.

4.1.3.7 Schutz für E-Mail-Server (Spamming-Mail und E-Mail-Daten)

Die Anwendung eines Relay-Servers in der DMZ wurde auch in der Firewall-Umgebung implementiert.
Durch den Einsatz eines Mail-Relay-Servers wird gewährleistet, dass der POP3-Server mit gespeicherten E-Mails nicht direkt mit dem Internet kommuniziert. Dies erhöht die Sicherheit vor Missbrauch der Benutzerdaten.

4.1.3.8 Updates von Software und Diensten

Jeden Tag werden neue Implementierungsfehler in verschiedenen Softwarepaketen vom DFN-Cert bekannt gegeben. In der Firewall-Umgebung sind alle aktuellen Updates eingespielt.

4.1.3.9 Zugriffsrechte in der DMZ

Soweit möglich werden auf allen Rechnern der DMZ Zugriffsbeschränkungen der einzelnen Dienste konfiguriert. Hierfür können in den Konfigurationsdateien der meisten Programme oder Dienste ACL's (Access Control Listen) oder andere Zugriffsbeschränkungen definiert werden. Sinnvolle Daten, wie Anmeldungen oder Ablehnungen werden in den Auditdaten gespeichert.
Ein erweiterter Einsatz von TCP-Wrappern kann zum Beispiel gewährleisten, dass inetd-Dienste nur definierte Adressbereiche in Anspruch nehmen können.

4.1.3.10 Sicherung aktueller Konfigurationen der Server

Alle relevanten Konfigurationsdateien der Server in der Firewall-Umgebung werden in bestimmten Zeitabständen durch ein Skript gepackt und als E-Mail an den lokalen Administrator versendet. Beim Auftreten von Hardwarefehlern oder erfolgreichen Hackerangriffen kann somit gewährleistet werden, dass ein ausgefallener Server durch einen neuen ersetzt werden kann, indem die Konfigurationsdateien zurückgesichert werden.

4.2 Auswertung von Schwachstellen

Die Auswertung von Schwachstellen beinhaltet das Kennen und Analysieren derselben, sowie die Eindämmung der Auswirkungen. Sicherheitsrelevante Schwachstellen können in drei Kategorien unterteilt werden:

- Nicht kalkulierbare Schwachstellen und Fehler
  sind alle unbekannten, nicht vorhersehbaren Ereignisse.
- Kalkulierbare Schwachstellen und Fehler
  sind alle bekannten, vorhersehbaren Ereignisse,
  die die Sicherheit einer Firewall tangieren.
- Abhilfe
  umfasst alle Maßnahmen, die zur Eindämmung beziehungsweise Beseitigung der Schwachstellen angewendet werden können.

4.2.1 Nicht kalkulierbare Schwachstellen

4.2.1.1 Abhängigkeit von den Herstellern der eingesetzten Software

Viele auf den Servern angebotene Dienste und eingesetzte Programme einschließlich der verwendeten Betriebssysteme enthalten Fehler, die ein hohes Sicherheitsrisiko darstellen. Wie schnell die Fehler nach den Bekanntwerden seitens der Hersteller beseitigt werden, liegt außerhalb des Einflussbereiches des zuständigen Systemadministrators. Bekannte Zeiträume bewegen sich zwischen einer Stunde und mehreren Monaten. Ein erwähnenswertes Negativbeispiel sind die Firmen Microsoft und HP. Sicherheitspatches wurden in einigen Fällen erst nach über sechs Monaten zur Verfügung gestellt. Im Gegensatz dazu stellen LINUX-Distributoren und Anwendungsentwickler Sicherheitspatches in der Regel innerhalb einer Woche zur Verfügung.

Ebenso ist die Quantität und Qualität der Fehlerbereinigung durch Patches oder Updates nicht vorhersehbar. Oftmals verursacht die vermeintliche Korrektur der jeweiligen Software neue Fehler beziehungsweise werden diese nicht oder nur unvollständig beseitigt.

4.2.1.2 Benutzerabhängigkeit

In jedem System stellt der Benutzer eine potentielle Schwachstellen dar. Durch keine Firewall oder Intrusion Detection System kann gewährleistet werden, dass geheime, firmeninterne Daten an die Öffentlichkeit gelangen.

Zudem stellt die Unfähigkeit und Risikobereitschaft der Benutzer einen sicherheitsrelevanten Faktor dar. Öffnen von E-Mails mit Würmern oder das Starten von Programmen mit jeglicher Art von Virus kann verheerende Folgen haben.

Von Angreifern an das Unternehmen versendete E-Mails mit gefährlichen Dateianhängen und/oder Skripten werden beim leichtfertigen Öffnen der E-Mail ausgeführt und können großen Schaden anrichten. Ein Mitarbeiter startet beispielsweise ein als Spiel getarntes Angriffsprogramm welches sich selbst in die Autostartfunktion des entsprechenden Rechners einträgt. So können nach einem Neustart beispielsweise Passwörter und Zugriffe über das Netzwerk gespeichert werden. Die Daten werden naschließend zu einem definierten Zeitpunkt zum Beispiel per E-Mail an den Angreifer übermittelt.

Der lokale Administrator oder ein Intrusion Detection System erkennt in solchen Fällen keine Sicherheitsverletzung, da das Öffnen und Senden von E-Mails grundsätzlich noch keine Sicherheitsrichtlinien verletzt.

- Der Benutzer bekommt eine E-Mail vom Hacker, wobei die E-Mailadresse nicht verdächtig ist.
- Der Benutzer greift auf das Netzwerk zu.
- Der Benutzer schickt eine E-Mail an den Angreifer. Für das Firewall-System ist dies ein normaler Vorgang.

4.2.1.3 Unbekannte Schwachstellen der eingesetzten Software

Dieses Thema beschäftigt derzeit die Sicherheitsbeauftragten von Regierungen und Unternehmen. Vorher unbekannte Fehler stellen ab dem Zeitpunkt ihrer Entdeckung ein großes Risiko dar.

4.2.1.4 Unentdeckte Angriffe

Nicht entdeckte Angriffe können verschiedene Ursachen und Auswirkungen haben. Grundsätzlich ist es nach einem erfolgreichem Angriff nicht auszuschließen, dass der Angreifer die Systemaufzeichnungen und -programme manipuliert. Dies wird meistens durch Rootkits automatisiert durchgeführt.

Oftmals bleiben Angriffe durch einen mangelnden Detaillierungsgrad der zu protokollierenden Auditdaten unentdeckt.

Angriffe mit Hilfe von E-Mail-Würmern sind nur schwer zu entdecken. Diese führen nach ihrer Einschleusung innerhalb der erlaubten Regeln ungewollte Aktionen aus.

4.2.2 Kalkulierbare Schwachstellen

4.2.2.1 Systemadministrator

Der Systemadministrator trägt die volle Verantwortung für alle Einstellungen im System und der verwendeten Software. Durch ein fehlerhaft konfiguriertes System können Angriffe begünstigt werden. Dies kann in einer mangelnden Restriktion des Systems oder in einer fehlerhaften Konfiguration begründet liegen.

4.2.2.2 Bekannte nicht zu beseitigende Schwachstellen

Durch die Organisation der Netzwerkstrukturen oder durch die Spezifikationen einiger Dienste bleiben immer noch Schwachstellen übrig, die nicht beseitigt werden können.

Ein großes Risiko stellt beispielsweise der FTP-Dienst, der auch zur Veröffentlichung von Webseiten der Benutzer auf den WWW-Servern aktiv ist. Da die Passwörter über das gesamte Internet unverschlüsselt versendet werden, können diese einfach abgefangen werden. Hacker können so ohne Wissen des lokalen Administrators an Ressourcen des Systems herankommen.

4.2.2.3 Passwörter der Benutzer

Viele Benutzer haben in der Systemumgebung Passwörter, die der Administrator nicht beeinflussen kann. Sie vergeben häufig Namen aus der Familie als Kennwörter. Da eingegebene Passwörter nicht auf den Inhalt überprüft werden können, sind Sicherheitsrichtlinien schwer umsetzbar.

4.2.3 Gegenmaßnahmen zur Risikominimierung

Die Abhängigkeit von den Herstellern kann durch Verträge oder Produktauswahl und -wechsel eingeschränkt werden. Sicherheitsrisiken durch die Benutzer und Administratoren können durch eine geeignete Personalauswahl und Schulungen optimiert werden.

Zudem sollte im Rahmen der gesetzlichen Möglichkeiten und der Betriebsvereinbarungen eine Überwachung der Aktionen von Mitarbeitern durchgeführt werden. Gegen unbekannte Softwarefehler ist ein Schutz nicht möglich. Zur Erkennung und Bekämpfung von Angriffen mittels Rootkits oder E-Mail-Würmern schützen nur eigene

Programme oder Anti-Viren-Programme. Der aktuelle Sicherheitsstandart der Software wird durch regelmäßige Patches und Updates gesichert.

Falls eine Schwachstelle zwar bekannt, aber eine Fehlerbeseitigung noch nicht verfügbar ist muss eine Abwägung zwischen Notwendigkeit des Dienstes und dem Sicherheitsrisiko durchgeführt werden.

4.3 Erkennung von Angriffen

Viele Angriffe sind durch eine vorhersehbare Folge von Ereignissen leicht zu erkennen, da diese einem bestimmten Muster folgen. Durch Verwendungen vorgefertigter Programme sind die Abläufe für Standardfälle gleich. Das Erkennen von gehackten Rechnern ist für ein Intrusion Detection System von Bedeutung, zumeist sind diese an ungewöhnlichen Paketen beziehungsweise Aktionen zu erkennen.

4.3.1 Angriffsaktionen und deren Anzeichen

Angriffe können auf mehrere Tage verteilt sein. In der Regel führt der Angreifer zunächst einen Port- oder Netscan durch, um verwundbare Programme oder Dienste zu finden. Anschließend versucht dieser noch mehr Informationen über den Dienst oder das System zu erlangen. Dies kann durch einen E-Mail-Wurm oder dem „finger“ Befehl geschehen.

Der eigentliche Angriff erfolgt erst später. Der Angreifer nutzt dazu erfahrungsgemäß vorgefertigte Programme und dringt in das verletzbare System ein. Dieser Vorgang dauert in den meisten Fällen nur Minuten oder Sekunden.

Die Tatsache, dass ein Angreifer seinen Angriff auf mehrere Tage verteilt, bringt ein großes Problem mit sich: Provider wie zum Beispiel Deutsche Telekom weisen Ihren Clients bei jeder Einwahl eine andere IP-Adresse zu. Es kann also nicht festgestellt werden, ob derselbe Angreifer nach einem vorherigen Portscan oder Netscan versucht, in das System einzudringen.

4.3.1.1 Port- und Netscan

Portscan

Bei einem Portscan werden verschiedene Ports eines Rechners auf genutzte Dienste überprüft. Ist ein Port aktiv, kann eine Verbindung mit einem Service auf dem Server benutzt werden. Antwortet ein Rechner nicht auf dem Port, wird kein Dienst auf diesem angeboten.

Charakteristisch für Portscans sind:

- mehrere versuchte Verbindungen auf verschiedenen Ports eines Rechners
- die Quelladresse ist in allen Fällen gleich oder wiederholt sich

Netscan

Ähnlich einem Portscans versucht der Angreifer, Dienste von Servern ausfindig zu machen. Dabei wird bei einem Netscan in den meisten Fällen der ganze IP-Bereich und dies häufig nur auf einem Port gescannt. Netscans weisen folgende Charakteristika auf:

- Viele nicht zulässige Pakete mit verschiedenen Zieladressen
- Zielport ist gleich oder wiederholt sich
- Die Quelladresse ist in allen Fällen gleich oder wiederholt sich

Die folgende Auflistung zeigt einen Auszug aus einer Logdatei eines LINUX-Servers über einen abgelehnten und geloggten Netscan.

```
...
Jul   8 22:16:18 router-aussen kernel: Packet log: input DENY eth1 PROTO=6
203.75.168.189:3093 x.x.x.1:53 L=60 S=0x80 I=55552 F=0x4000 T=37 SYN (#71)

Jul   8 22:16:18 router-aussen kernel: Packet log: input DENY eth1 PROTO=6
203.75.168.189:3094 x.x.x.2:53 L=60 S=0x80 I=55553 F=0x4000 T=37 SYN (#71)

Jul   8 22:16:18 router-aussen kernel: Packet log: input DENY eth1 PROTO=6
203.75.168.189:3095 x.x.x.3:53 L=60 S=0x00 I=55554 F=0x4000 T=37 SYN (#71)

Jul   8 22:16:18 router-aussen kernel: Packet log: input DENY eth1 PROTO=6
203.75.168.189:3096 x.x.x.4:53 L=60 S=0x00 I=55555 F=0x4000 T=37 SYN (#71)

Jul   8 22:16:18 router-aussen kernel: Packet log: input DENY eth1 PROTO=6
203.75.168.189:3097 x.x.x.5:53 L=60 S=0x00 I=55556 F=0x4000 T=37 SYN (#71)

Jul   8 22:16:19 router-aussen kernel: Packet log: input DENY eth1 PROTO=6
203.75.168.189:3098 x.x.x.6:53 L=60 S=0x00 I=55557 F=0x4000 T=37 SYN (#71)

Jul   8 22:16:20 router-aussen kernel: Packet log: input DENY eth1 PROTO=6
203.75.168.189:3192 x.x.x.7:53 L=60 S=0x00 I=55740 F=0x4000 T=37 SYN (#71)

Jul   8 22:16:20 router-aussen kernel: Packet log: input DENY eth1 PROTO=6
203.75.168.189:3193 x.x.x.8:53 L=60 S=0x00 I=55741 F=0x4000 T=37 SYN (#71)
…
```

Die vorhanden Log-Einträge von ipchains sind wie folgt zu interpretieren:

Zeilenteil	***Information***	***Netscan-Erkennung***
Jul 8 22:16:18	Zeitstempel – in diesem Fall Log-Eintrag vom 8 Juli um 22:16:18 Uhr	
Router-aussen	Servername ist „router-aussen“	
Kernel	Meldung wurde vom Kernel des Systems erstellt	
Packet log	Information über die Art des Ereignisses	X
Input	Regel für ipchains – mögliche Werte sind input, forward, output	X
DENY	Paket wurde „verschluckt“, der Absender erhielt keine Rückantwort	X
eth1	Netzwerkkarte eth1	X
PROTO=6	Protokoll 6 - TCP	X
203.75.168.189	Absender-Adresse 203.75.168.189	X
:3093	Absenderport 3093	
x.x.x.20	Zieladresse x.x.x.20	X(#1)
:53	Zielort 53 (Nameservice)	X(#1)
L=60	Länge des Pakets in Bytes	
S=0x80	TOS	
I=55717	IP-ID	
F=0x4000	16 BIT-Fragment Offset + Flags	
T=37	Time To Live	
SYN(#70)	SYN-Bit ist gesetzt	

Tabelle 4-1: Logeintrag Portscan

#1 : Die ersten drei Adressteile sind bei einem Netscan gleich.

Durch die Wiederholung der gekennzeichneten Auditdaten ist ein Erkennen dieser Angriffe durch ein Intrusion Detection System einfach.
Der folgende Programmablaufplan dient der Erkennung von Port- oder Netscans:

Abbildung 4-2: Ablauf Erkennung Port- und Netscan

Der Programmablaufplan stellt die möglichen Vorgehensweisen auf der Grundlage der Ereignisse und deren Folgen aus Sicht des Erkennungsprogramms dar.

4.3.1.2 Spoofing

Eine Möglichkeit Router mit fehlenden oder fehlerhaften Paketfiltern zu umgehen, ist das Paket-Spoofing. Hierbei sendet der Angreifer Pakete mit falscher Source-Adresse, um diese in ein angegriffenes Netz zu schleusen. Dadurch kann der Angreifer einen sogenannten „blinden Angriff“ auf einen Server in dem angegriffenen Netz ausführen, da ein Router die Pakete ohne spezielle Filterregeln nicht überprüft.
Das Verhindern von solchen Pakete ist durch Filterregeln zu gewährleisten. Bei richtiger Konfiguration speichern Router die abgelehnten Spoofing-Versuche als nicht zugelassenes Paket wie folgt in den Auditdaten:

```
Router mit folgender Konfiguration:
eth0: 192.168.20.0/255.255.255.0
eth1: 192.168.10.0/255.255.255.0

Jul    12  16:06:25  router  kernel:  Packet  log:  input  DENY  eth1  PROTO=6
192.168.20.189:3000 192.168.20.1:53 L=60 S=0x80 I=14 F=0x4000 SYN (#71)
```

(richtiges Zielnetz, gefäschtes Absendernetz)

Zeilenteil	Information	Angriffserkennung
Jul 12 16:06:25	Zeitstempel	
Router	Servername ist „router“	
kernel:	Meldung wurde vom Kernel des Systems erstellt	
Packet log:	Information über die Art des Ereignisses	
Input	Angesprochene Regel ipchains	
DENY	Abgelehntes Paket	X
eth1	Netzwerkkarte ist eth1	X
PROTO=6	Protokoll = TCP	
192.168.20.189	Senderadresse	X
:3000	Senderport	
192.168.20.1	Zieladresse	
:53	Zielport	
L=60	Länge des Pakets	
S=0x80	TOS	

I=14	IP-ID	
F=0x4000	16 BIT-Fragment Offset + Flags	
T=45	Time to Live	
SYN	SYN-Bit ist gesetzt	

Tabelle 4-1: Logeintrag Spoofing

Das folgende Schema zeigt den Ablauf zur Erkennung von Angriffen mittels Spoofing:

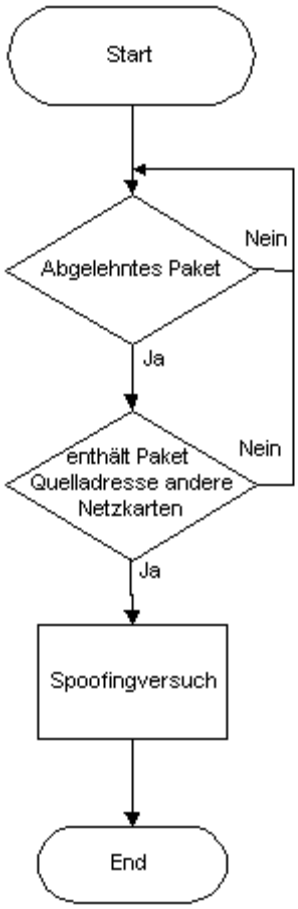


Abbildung 4-3: Ablauf Erkennung Spoofing

4.3.1.3 Falsche Paketlängen und fragmentierte Pakete

Verschiedene Tools wie ipchains können fragmentierte Pakete sowie Pakete mit falscher Länge ablehnen und deren Auftreten in den Auditdaten vermerken. Intrusion Detection Systeme können durch Auswerten der Paketart in den Auditdaten überprüfen, ob es sich um einen Angriff handelt oder nicht.

Ein Erkennungssystem muss den Datensatz der Auditdaten auslesen und Interpretieren. Das folgende Ablaufschema stellt die Vorgehensweise dieses Systems bei entsprechenden Eingangsvoraussetzungen dar:

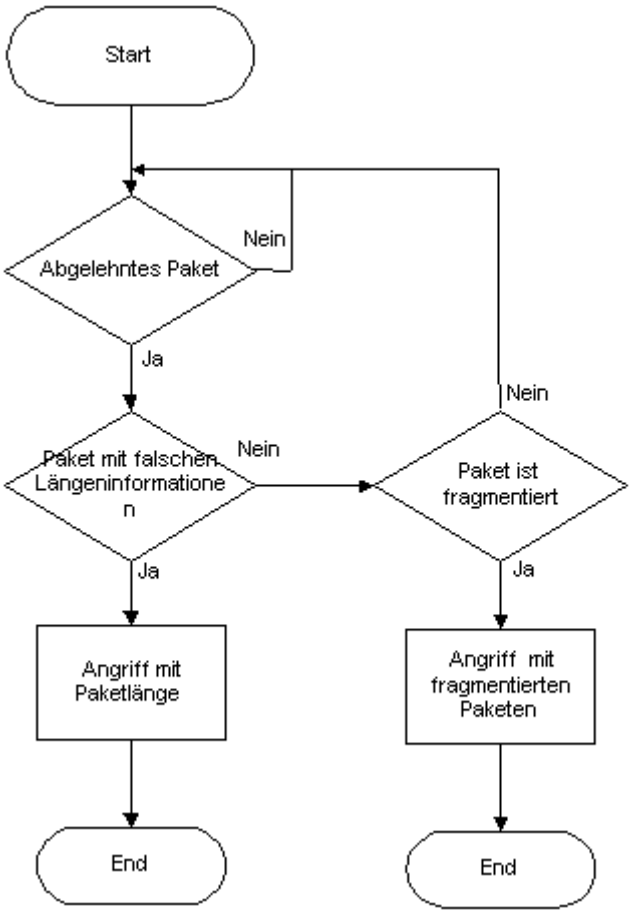


Abbildung 4-4: Ablauf Erkennung Paketfälschung

4.3.1.4 Erfolgreicher Angriff bei Einsatz von Rootkits (Unix-Systeme)

Nach einem erfolgreichen Angriff werden zunächst Aktionen ausgeführt, um den Erfolg des Angriffs zu verstecken. Dabei werden üblicherweise beim Einsatz des **Rootkits** folgende Aktionen am Betriebssystem ausgeführt:

- Veränderung der lokalen Auditdaten
- Veränderung einiger Programme
    - ls (Listen von Orderinhalten)
    - df (Partitionen und dessen Platz anzeigen)
    - cd (Wechseln in ein angegebenes Verzeichnis)
    - md5sum (MD5 Summe von Dateien erkennen)
    - ps (laufende Prozesse)
    - find (Finden von Dateien)
- Veränderung einiger Konfigurationsdateien

Es werden alle Dateien verändert, die das Erkennen des erfolgreichen Angriffes bei Standardsystemaufrufen ermöglichen. Da auch Programme verändert werden, die das Überprüfen von Dateien erlauben, sollten hier selbst programmierte oder umbenannte Tools verwendet werden, die nicht in der Standard-Linux-Distribution vorhanden sind.
Unabhängig davon sollten in regelmäßigen Abständen bestimmte Programm- und Konfigurationsdateien nach der MD5-Summe überprüft werden, um erfolgreiche Angriffe, die vorher noch nicht erkannt werden konnten, aufzudecken. Die Ergebnisse sollten an einen anderen Server übermittelt und ausgewertet werden, da eine lokale Auswertung vom Angreifer verändert werden kann.
Weiterhin kann beim Überprüfen des Verkehrs des Netzwerks festgestellt werden, ob ungewöhnliche Aktivitäten stattfinden. Erhöht sich beispielsweise der Netzwerkverkehr auf dem äußeren Router gegenüber dem inneren Router spürbar, sollte eine Überprüfung der betroffenen Server erfolgen. Hierbei ist zu beachten, dass einige Proxydienste Daten zwischenspeichern, wodurch sich der Datenverkehr in das Internet verringern müsste. Erlaubte Pakete sollten in den Auditdaten gespeichert werden, um eine Überprüfung des Netzwerkverkehrs zu ermöglichen.
Falls die MD5-Summen bei der Auswertung nicht mehr übereinstimmen, ist dieser Systemzustand als kritisch anzusehen, folglich müssen Gegenmaßnahmen sowie ein Alarm ausgelöst werden.
Beispiel für die Verwendung von MD5:

Mit dem Programm md5sum unter Unix wird die Datei /bin/ls überprüft.
Befehl:
#> md5sum /bin/ls
Ausgabe:
193d7df20197e30bc67d5d4fd2f7c7b2 /bin/ls

Wird die Datei nun trojanisiert oder modifiziert, verändert sich immer die MD5-Prüfsumme. Ein möglicher Ablauf zur Erkennung von trojanisierten Dateien kann in einem Angriffserkennungsprogramm wie folgt dargestellt werden:

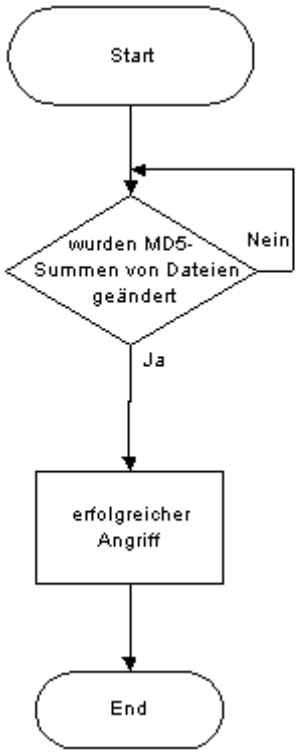


Abbildung 4-5: Ablauf Erkennung Angriff Rootkit

4.3.1.5 BackOrifice (BO) (Windows-Systeme)

BackOrifice ist ursprünglich ein Werkzeug zur Fernadministration eines Microsoft-Windows-Servers oder einer Arbeitsstation. Das Programm funktioniert bei allen Microsoft Betriebssystemen ab Windows 95 und Windows NT 4.0. Voraussetzung für die Verwendung ist, dass das serverseitige Programm in den Startmechanismus des Rechners eingebunden wird. Der Angreifer muss hierfür Schreibzugriff auf die Festplatte(n) des Rechners bekommen, um ein BackOrifice fern installieren zu können.

Der Angreifer benutzt gewöhnliche Netzwerkscanner, die große Bereiche von IP-Adressen nach bestimmten Ports abscannen (Ports 137-139). Diese Werkzeuge überprüfen auch, ob die Festplatten für den Angreifer beschreibbar sind oder nicht. Innerhalb weniger Minuten kann eine große Anzahl von Rechnern mit BackOrifice infiziert werden.

BackOrifice und das BackOrifice zugrunde liegende Programm NetBUS sind inzwischen im Quellcode verfügbar und funktionieren durch Firewalls hindurch, sofern diese Programme von UDP auf TCP Protokoll umgeschrieben wurden. BackOrifice Scanner finden nur das ursprüngliche Programm BO.EXE, nicht aber die neukompilierten Derivate von BackOrifice.

Ein BackOrifice-Angriff ist durch seine Angriffsspezifikation leicht zu erkennen und abzulehnen. Router sperren in allen Fällen die Ports 137 bis 139 für den Zugriff aus dem Internet.

Ein Angriff ist in der Regel leicht aus den Auditdaten zu erkennen, da ein Netscan oder Portscan ausgeführt wird.

```
…
Jul   8 21:10:20 router-aussen kernel: Packet log: input DENY eth1 PROTO=17
204.5.64.209:137 x.x.x.7:137 L=78 S=0x80 I=45784 F=0x0000 T=107 (#71)
Jul   8 21:10:20 router-aussen kernel: Packet log: input DENY eth1 PROTO=17
204.5.64.209:137 x.x.x.8:137 L=78 S=0x80 I=45784 F=0x0000 T=107 (#71)
…
```

Zur Analyse der Auditdaten wird der Inhalt dieser Zeile ausgewertet:

```
Jul   8 21:10:20 router-aussen kernel: Packet log: input DENY eth1 PROTO=17
204.5.64.209:137 x.x.x.7:137 L=78 S=0x80 I=45784 F=0x0000 T=107 (#71)
```

Die folgende Tabelle schlüsselt die oben aufgeführte Zeile aus den Auditdaten nach den für ein Angriffserkennungsprogramm notwendigen Informationen auf:

Zeilenteil	***Information***	***Bo-Angriffs-Erkennung***
Jul 8 21:10:18	Zeitstempel – in diesem Fall Log-Eintrag vom 8 Juli um 21:10:20 Uhr	
router-aussen	Servername ist „router-aussen“	
Kernel	Meldung wurde vom Kernel des Systems erstellt	
Packet log	Information über Art vom Ereignis	X
Input	Regel für ipchains – mögliche Werte sind input, forward, output	X
DENY	Paket wurde „verschluckt“, der Absender erhielt keine Rückantwort	X
Eth1	Netzwerkkarte eth1	X
PROTO=17	Protokoll 17 – UDP (Siehe Anhang)	X
204.5.64.209	Absender-Adresse 203.75.168.189	X
:137	Absenderport ist 3093	X
x.x.x.7	Zieladresse 141.19.228.20	X(*)
:137	Zielort 53 (Nameservice)	X(**)
L=78	Länge des Pakets in Bytes	
S=0x80	TOS	
I=45784	IP-ID	
F=0x0000	16 BIT-Fragment Offset + Flags	
T=107	TIme To Live	
(#71)	Undokumentiert	

Tabelle 4-2: Logeintrag BO – Portscan/Netscan

(*/**) Ein Port- oder Netscan können anhand der sich ändernden Werte für den Zielport oder die Zieladresse eindeutig unterschieden werden.
Weitere Merkmale für Port- und Netscans befinden sich im Kapitel 4.3.1.1.

Aus der Auswertung der Auditdaten lässt sich ein allgemeingültiges Schema für Angriffe mittels BackOrifice auf Netzwerksysteme ableiten. Die folgende Graphik veranschaulicht den möglichen Angriffsablauf und das jeweilige Verhalten eines Angriffserkennungsprogramms:

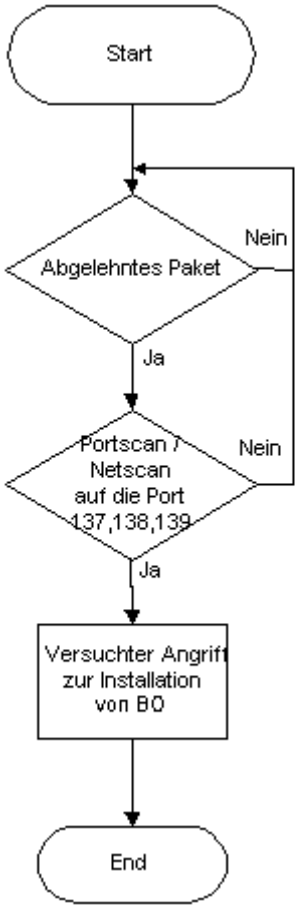


Abbildung 4-6: Ablauf Erkennung Portscan/Netscan BO

4.3.1.6 Mail-Spamming

Bei den meisten SMTP-Servern kann Mail-Spamming nach der Installation ohne Abänderung der Konfiguration durchgeführt werden. Bei richtiger Konfiguration wird ein Spamming-Versuch als Ablehnung in den Auditdaten registriert. Die Meldung ist von der Server-Software abhängig. Bei den häufig verwendeten Mail-Relay-Servern POST-FIX und SENDMAIL wird der Eintrag in den Auditdaten als „Relay access denied“ gespeichert. Das Programm Postfix vermerkt einen Spamming-Versuch wie folgt in den Auditdaten:

Jun 24 23:52:30 dns postfix/smtpd[22164]: reject: RCPT from dnsfh.foo.de [x.x.x.49]: 554 <glade@fh-heidelberg.de>: Recipient address rejected: Relay access denied; from=<admin@test.de> to=admin@foo.de

Die folgende Tabelle verdeutlicht den Zusammenhang zwischen der Interpretation der Auditdaten von Postfix und der Angriffserkennung durch ein Intrusion Detection Programm:

Zeilenteil	Information	Erkennung für Angriff
Jun 24 23:52:30	Zeitstempel	
Dns	Servername	
postfix/smtpd[22164]:	Dienst und Prozess-Pid	
reject:	Zurückgewiesene E-Mail	X
RCPT from dnsfh.foo.de [x.x.x.49]:	Sendender Server/Rechner	X
554 <glade@fh-heidelberg.de>: Recipient address rejected: Relay access denied;	Meldung an den Sender der E-Mail	X
from=<admin@test.de>	Angegebene Absenderadresse der E-Mail	X(*)
to=admin@foo.de	Angegebene Empfängeradresse der E-Mail	X(*)

Tabelle 4-3: Logeintrag Mail-Spamming

(*) – gelten als zusätzliche Informationen für die Angriffserkennung

Für die Prüfung in Skripten und Programmen ist folgender Ablauf zu berücksichtigen:

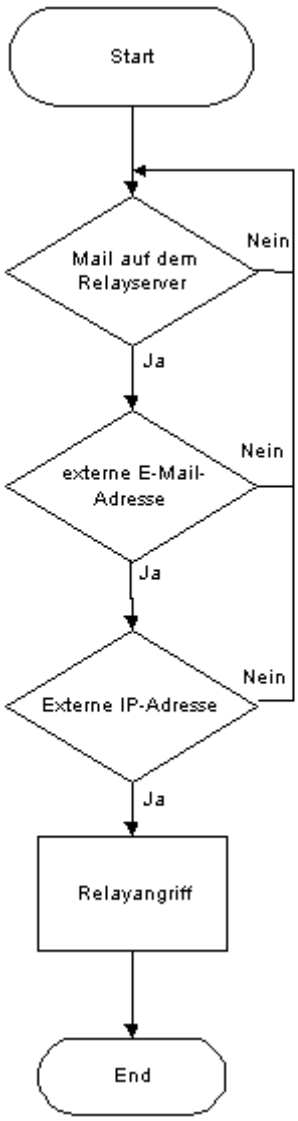


Abbildung 4-7: Ablauf Erkennung Mail-Spamming

Diese Art des Angriffes hat durch die Konfiguration des Systems keine negativen Auswirkungen auf die Systemsicherheit. Postfix erkennt, dass es sich um einen Mail-Spamming-Versuch handelt und lehnt diesen bei richtiger Konfiguration ab. Dennoch sollte eine Warnung als Vermerk an den Administrator gesendet werden.

4.3.1.7 Denial of Service-Angriffe

Der Angreifer versucht mehrfach mit gefälschter nicht vorhandener Quelladresse auf einen Dienst zuzugreifen, um eine Verbindung anzufordern. Der Server versucht zu antworten und wartet auf Antwort auf seine Antwort.

Diese Angriffe sind nur zu erkennen, wenn auf den Routern auch Pakete geloggt werden, die erlaubt sind:

...

```
Jul  8 22:16:18 router-aussen kernel: Packet log: forward ACCEPT eth1
PROTO=6 203.75.168.189:1077 x.x.x.1:80 L=60 S=0x80 I=55552 F=0x4000
T=37 SYN (#71)

Jul  8 22:16:18 router-aussen kernel: Packet log: forward ACCEPT eth2
PROTO=6 x.x.x.2:80 203.75.168.189:1077 L=65 S=0x80 I=55553 F=0x4000
T=45

Jul  8 22:16:18 router-aussen kernel: Packet log: forward ACCEPT eth1
PROTO=6 203.75.168.189:1078 x.x.x.1:80 L=60 S=0x80 I=55558 F=0x4000
T=37 SYN (#71)

Jul  8 22:16:18 router-aussen kernel: Packet log: forward ACCEPT eth2
PROTO=6 x.x.x.2:80 203.75.168.189:1078 L=65 S=0x80 I=55559 F=0x4000
T=45
Jul  8 22:16:18 router-aussen kernel: Packet log: forward ACCEPT eth1
PROTO=6 203.75.168.189:1078 x.x.x.1:80 L=60 S=0x80 I=33333 F=0x4000
T=37 SYN (#71)

Jul  8 22:16:18 router-aussen kernel: Packet log: forward ACCEPT eth2
PROTO=6 x.x.x.2:80 203.75.168.189:1079 L=65 S=0x80 I=33334 F=0x4000
T=45
```

...

In der folgenden Tabelle werden zwei sich wiederholende und zusammenhängende Pakete dargestellt, wobei die ersten beiden Zeilen des Auszugs der Logdaten ausgewertet werden:

Zeilenteil Packet (Syn)	Zeilenteil Packet (Ack)	Bermerkung	Merkmal für Erkennung
Jul 8 22:16:18	Jul 8 22:16:18	Zeitstempel für Logeintrag	
router-aussen	router-aussen	Rechnername ist „router-aussen“	
kernel:	kernel:	Meldung wurde vom Kernel des Systems erstellt	
Packet log:	Packet log:	Zusätzliche Informationen über die Art der Meldung	
Forward	forward	Regel für ipchains (input,forward oder output)	X
ACCEPT	ACCEPT	Ist ein erlaubtes Paket	
eth1	eth2	Ziel auf Netzwerkkarte	X
PROTO=6	PROTO=6	Protokoll 6 = TCP	
x.x.x.2	203.75.168.189	Absenderadresse	X
:80	:1077	Absenderport	X
203.75.168.189	x.x.x.2	Zieladresse	X
:1077	:80	Zielport	X
L=60	L=66	Länge des Pakets in Bytes	
S=0x80	S=0x80	TOS	
I=55553	I=55554	IP-ID	
F=0x4000	F=0x4000	16 BIT-Fragment Offset + Flags	
T=37	T=45	Time To Live	
SYN(#71)	---	Syn-Bit ist gesetzt	X

Tabelle 4-4: Logeintrag DOS

Aus den Informationen der Auditdaten ist ein Denial of Service-Angriff wie folgt zu analysieren:

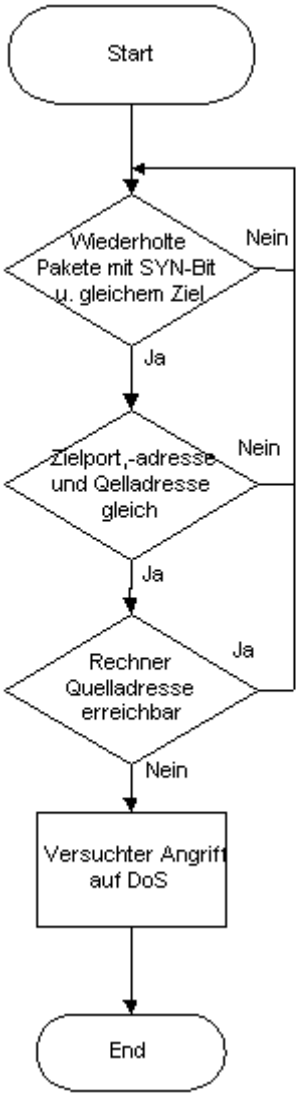


Abbildung 4-7: Ablauf Erkennung DoS

Diese Angriffe sind als kritisch anzusehen und es sind sofortige Gegenmaßnahmen zu ergreifen, um die Verfügbarkeit des Systems zu gewährleisten. Dabei ist zu berücksichtigen, dass Angriffe dieser Art nur durch eine Prüfung der Absenderadresse zu verhindern sind. Ein Angriffserkennungsprogramm muss dafür spezielle Funktionen zur Verfügung stellen, die das Ablaufmuster erkennen, und darauf entsprechend reagieren.

4.3.1.8 Bufferoverflow-Angriffe

Bufferoverflows gehören mit zu den gefährlichsten Angriffen. Betroffen sind fast alle Dienste. Zunehmend benutzen Angreifer Bufferoverflows für Angriffe auf Server in verschiedenen Unternehmen.

Die Fehler, die einen Bufferoverflow verursachen, liegen zumeist in der jeweiligen Programmimplementierung, wodurch es kaum möglich ist, diese zu erkennen. In den meisten Fällen geben weder die Auditdaten der Router und von diesen geloggte Pakete, noch die Auditdaten des angegriffenen Dienstes über solch einen Angriff Auskunft. Dadurch ist es durch ein Angriffserkennungsprogramm nur schwer oder gar nicht zu gewährleisten, dass diese Angriffe erkannt werden. Die folgende Ablaufdarstellung zeigt eine Möglichkeit für die Erkennung eines Angriffes auf:

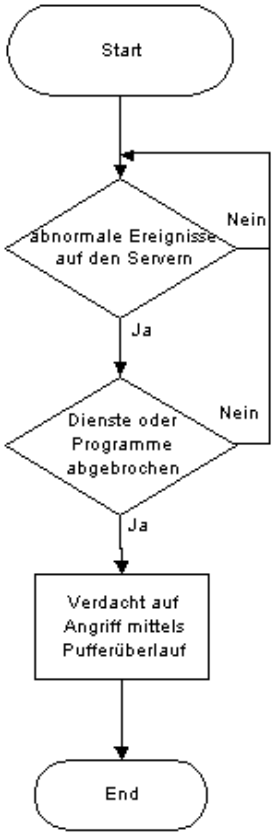


Abbildung 4-9: Ablauf Erkennung Bufferoverflow

Zusätzlich sollten noch die in Kapitel 4.3.1.4 aufgeführten Maßnahmen ergriffen werden, um die tatsächliche Ursache der nicht schlüssigen Auditdaten zu ermitteln.

4.3.1.9 E-Mail-Würmer

E-Mail-Clients wie Outlook von der Firma Microsoft ermöglichen das Ausführen von Skripten in E-Mails. Da Skripte auch für die Erstellung von E-Mail-Würmern verwendet werden können, sollten auf allen Clients die Optionen für das Ausführen von allen Skriptarten deaktiviert sein.

Ein Antivirenprogramm sollte alle E-Mails vor dem Empfang durch den Benutzer überprüfen und gefährdete E-Mail-Teile wie angehängte Programme oder Dokumente entfernen, um sich vor dieser Art von Angriffen zu schützen. Diese Antivirensoftware speichert die Aktionen in den Auditdaten und verschickt den infizierten E-Mail-Teil an den Administrator.

Ein Angriffserkennungsprogramm kann zwar den Angriff erkennen, aber als Gegenmaßnahme lediglich eine Mitteilung an den Administrator leiten, da durch die sendenden E-Mail-Server nicht zu lokalisieren ist, wer der wahre Absender der E-Mail ist.

Durch Auswertung und Analyse der Auditdaten des Antivirenprogramms können nachträglich Aktionen ausgeführt wie Warnungen oder Sperrungen ausgeführt werden. Das folgende Schema zeigt einen beispielhaften Erkennungsprozess für E-Mail-Würmer und –Viren durch ein Antivirenprogramm.

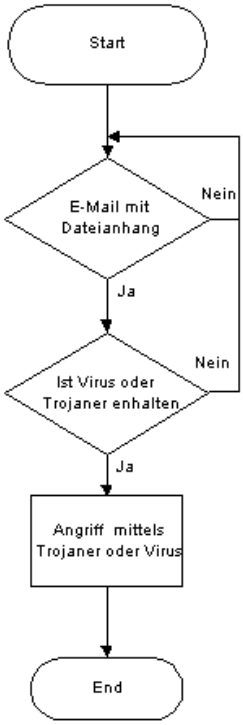


Abbildung 4-10: Ablauf Erkennung E-Mail-Wurm/E-Mail-Virus

4.3.1.10 Verbrauch der Festplattenressourcen

Ein Angreifer versucht, den Speicherplatz von Festplatten aufzubrauchen, um ein System oder einen Dienst zum Absturz zu bringen. Erzeugt dieser beispielsweise durch sich wiederholende Ereignisse umfangreiche Auditdaten in den lokalen Logdateien, kann er damit die Festplattenpartition zum Überlaufen bringen.

Der freie Festplattenplatz aller Partitionen der Systeme in einer Firewall-Umgebung muss regelmäßig überprüft und in den Auditdaten vermerkt werden. Der Standardbefehl „df“ liefert zum Beispiel folgende auswertbare Daten:

```
Filesystem           1k-blocks      Used Available Use% Mounted on
/dev/hda1               233336     66148    155141  30% /
/dev/sda1              1020968    159228    809876  16% /home
/dev/hda7              1628612   1244368    301512  80% /usr
/dev/hda6               139986     48757     84002  37% /var
```

In der folgenden Tabelle wird die logische Auswertung der für das Angriffserkennungsprogramm erforderlichen Daten am Beispiel der eingerahmten Zeile dargestellt:

Zeilenteil	Information	Für Erkennung notwendig
/dev/hda6	Partition (IDE-Controller a, Partition 6)	
139986	Größe der Partition angegeben in 1K-Byte-Blöcken (139986 KiloByte)	X
48757	Verbrauchter Platz der Partition angegeben in 1K-Byte-Blöcken (139986 KiloByte)	
84002	Verfügbarer Platz der Partition angegeben in 1K-Byte-Blöcken (139986 KiloByte)	X
37%	Prozentangabe des verbrauchten Festplattenplatzes	
/var	Einhängepunkt der Partition	X

Tabelle 4-5: Ausgabe Partitionen

Die so gewonnenen Auditdaten können wie folgt zur Angriffserkennung ausgewertet werden:

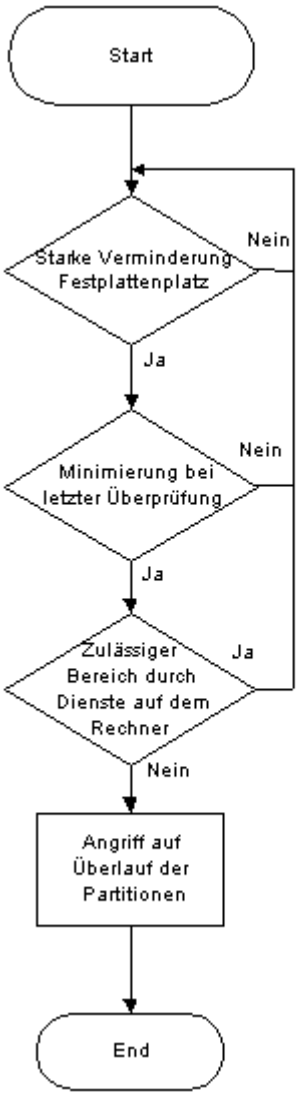


Abbildung 4.11: Erkennung Plattenverbrauch

4.3.2 Übersicht aller zu erfassenden Auditdaten

Grundsätzlich gilt, dass alles geloggt werden muss. Alle Aktionen wie Pakete und Zugriffe auf die überwachten Server müssen in den Auditdaten gespeichert werden, um eine sichere Firewall im Zusammenarbeit mit einem Angriffserkennungssystem zu erlangen. Dabei ist es unwichtig, ob ein Zugriff als erlaubt oder verboten gilt.
Alle Auditdaten müssen auf einem zentralen Server, dem Backlog-Server, gespeichert und ausgewertet werden.

4.4 Einarbeiten in die neuen Anforderungen

Das Ziel der Arbeit soll ein Netz mit größtmöglicher Sicherheit zur Abwehr von Angreifern sein. Dabei soll das System auf mögliche Schwachstellen im System überwacht und bei Gefahren die entsprechenden Gegenmaßnahmen eingeleitet werden.
Das System muss hierfür nicht nur bekannte Schwachstellen erkennen und abwehren, sondern auch neue Situationen analysieren, auswerten und erlernen. Zusätzlich müssen für ein sicheres System in kürzester Zeit Updates für Schwachstellen zur Verfügung stehen. Eine Zusammenfassung aller Anforderungen an das System:

- zentrale Speicherung der Auditdaten
- zentrale Auswertung aller Auditdaten mittels künstlichen Neuronalen Netz
- selbstständiges Erkennen von neuen gefährlichen Situationen
- sofortige Gegenmaßnahmen einleiten, falls Situation dies erfordert
- Warnungen, Zusammenfassungen und Empfehlungen für den Administrator erstellen
- Stabiles Betriebssystem
- Programm- und Betriebssystemhersteller oder Entwickler müssen schnell auf Fehler reagieren und Updates bereitstellen

4.5 Einarbeiten physikalischer Restriktionen

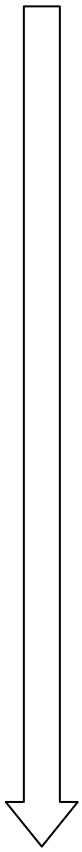
Viele Rechnersysteme stoßen schnell an die Grenzen ihrer Leistungsfähigkeit. Nicht nur die Rechengeschwindigkeit spielt eine große Rolle, sondern auch die exponentiell wachsende Entwicklung neuer Einsatzmöglichkeiten des Internets, die beispielsweise durch die Übertragung multimedialer Inhalte die Ressourcenanforderungen erhöhen.
Dies führt zu einer Erhöhung des Netzwerkverkehrs und der zu loggenden Vorgänge. Deshalb müssen zur Bewältigung der Datenmengen und deren Auswertung die verwendeten Rechnersysteme entsprechend leistungsfähig sein.

4.5.1 Netzwerkverkehr zum Backlog-Server

Alle Aktionen in der DMZ müssen protokolliert werden, um die Sicherheit zu gewährleisten. Zu den aufgezeichneten Auditdaten gehören:

- die Logdaten der Dienste aller Bastionshosts
- alle Pakete, die zum Datenverkehr auf innerem und äußerem Router gehören
- zusätzliche Informationen über den Zustand aller überwachten Server und dessen Dienste

Aus den Vorgaben entwickelt sich folgende Berechnung für die Bandbreite:



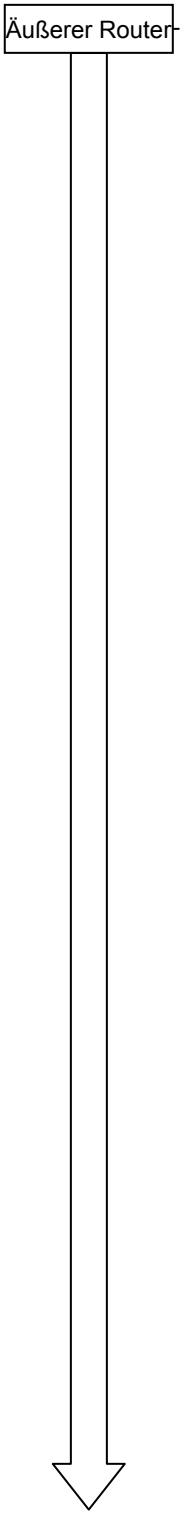
Bandbreite = 2 Megabit = 2000000 Bits/Sekunde pro Richtung
= 4000000 Bytes/Sekunde beider Richtungen

→ Bandbreite beide Richtungen
= Bandbreite Bits / 8
= 4000000 / 8
= 500000 Bytes / Sekunde

durchschnittliche Paketlänge Daten = 230 Bytes/Paket
durchschnittliche Paketlänge Syslog = 160 Bytes/Paket

→ Pakete pro Sekunde vor äußeren Router
= Bandbreite Bytes / durchschnittliche Paketlänge
= 5000000 / 230
= 2174 Pakete/Sekunde

→ zusätzliche Anzahl an Syslogpaketen
= 6522



Daten innere Karte vom äußeren Router:

→ **Paketanzahl**

= Pakete Syslog + Pakete Daten

= 6522 + 2147

= 8696 Pakete / Sekunde

→ *Bandbreite Syslog:*

= Pakete Syslog * Größe Pakete Syslog

= 6522 * 160

= 1043520 Bytes / Sekunde

→ *Bandbreite Daten:*

= Pakete Syslog * Größe Pakete Syslog

= 2174 * 230

= 500020 Bytes / Sekunde

→ **Bandbreite innere Karte vom äußeren Router gesamt**

= Bandbreite Syslog + Bandbreite Daten

= 1043520 + 500020

= 1881780 Bytes / Sekunde

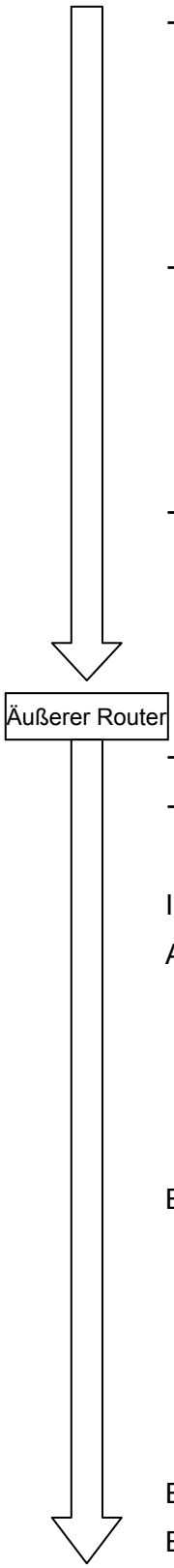
Zusätzliche Daten in der DMZ

→ + 25 % Datenverkehr - Pakete

= Datenverkehr Internet + (0.25 * Datenverkehr Internet)

= 2174 + 2174 * 0.25

= 2718 Pakete



→ + 25 % Datenverkehr – Bytes

Pakete * durchschnittliche Paketlänge

= 2718 * 230

= 625140 Bytes / Sekunde

→ Zusätzlicher Syslog-Daten

= ca. 100 Pakete (getestet bei maximaler Auslastung)

= 100 * 160

= 1160 Bytes / Sekunde

→ Zusammenfassung der Daten zum inneren Router

→ 2718 Pakete Daten (230 Bytes/Paket)

→ 6622 Pakete Syslog (160 Byte/Paket)

→ 9340 Pakete Gesamt

Äußerer Router

→ 9340 * 3 = 28020 neue Syslog-Pakete

→ Syslog-Pakete gesamt

Innere Karte vom inneren Router

Anzahl Syslog-Pakete

= Syslog-Pakete neu + Syslog-Pakete alt

= 28020 + 6622

= 34642

Bandbreite Syslog-Pakete

= Anzahl Syslog-Pakete * 160

= 34642 * 160

= 5542720 Bytes / Sekunde

= ca. 5,29 Megabytes / Sekunde

Bandbreite Daten unverändert = 625140 Bytes / Sekunde

Bandbreite gesamt: 6167860 Bytes/Sekunde = 5,9 MB/Sekunde

Das folgende Diagramm fasst alle Bandbreiten maßstabsgerecht zusammen:

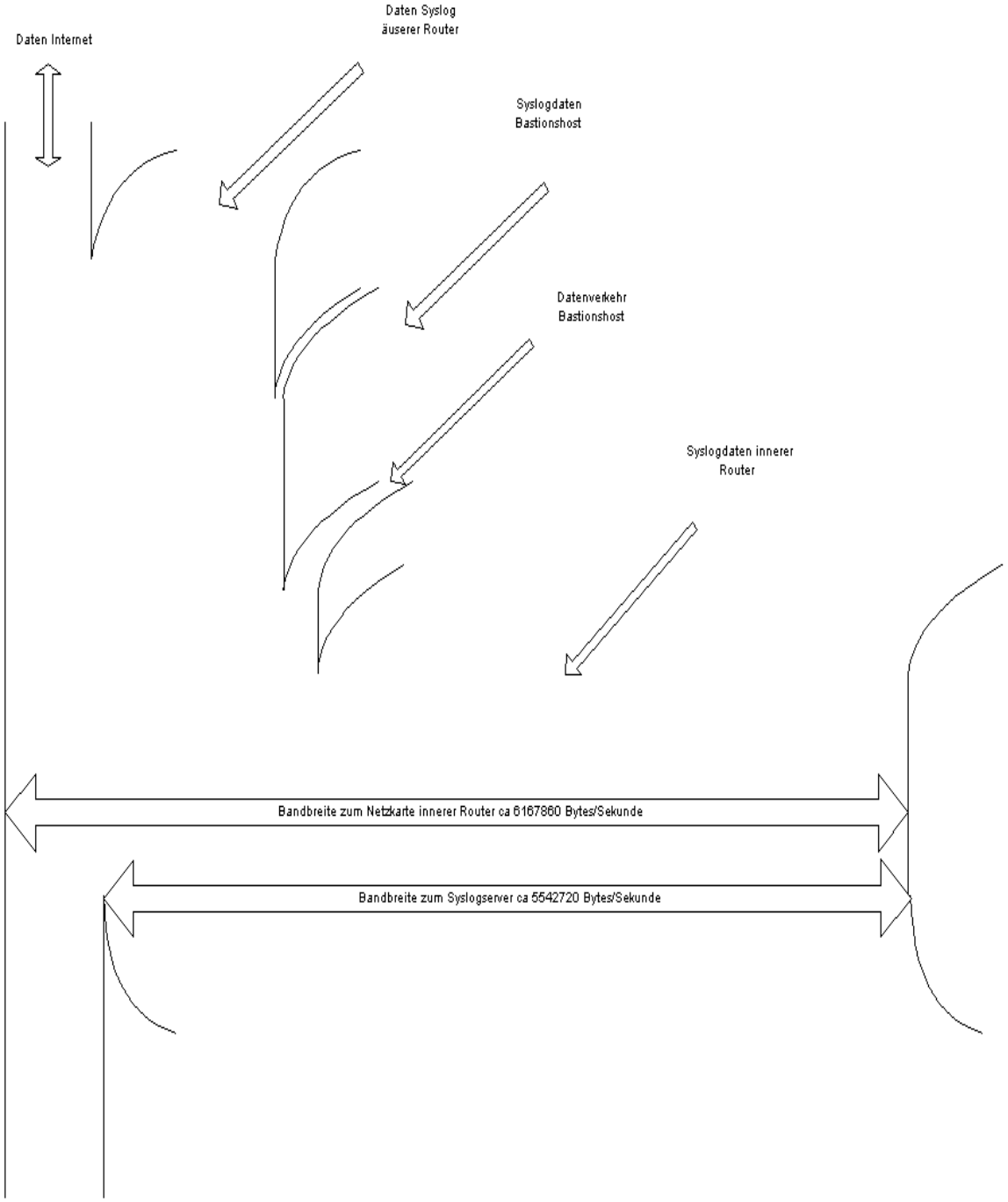


Abbildung 4-12: Diagramm Bandbreite Syslog

4.5.2 Ressourcen verwendeter Rechner in der DMZ

Die Größe der Auditdaten stellt in diesem Konzept für die meisten Server in der DMZ kein Problem dar, dass heißt die Ressourcen der Server sind ausreichend für die Verarbeitung der Ereignisse und dem Erstellen beziehungsweise Verschicken der Auditdaten. Engpässe sind bei den Servern innerer Router und dem Backlog-Server zu erwarten, die durch entsprechende Hardwarebestückung ausgeglichen werden müssen.

4.5.2.1 Ressourcen innerer Router

Alle Pakete aus und in die DMZ werden über den inneren Router versendet. Die Last auf dem Router bei voller Internetnutzung liegt bei ca. 5,9 MB pro Sekunde (innere Karte inklusive eigener Syslog-Pakete). Die Anzahl der Pakete beträgt 9340. Der Router muss alle Pakete überprüfen, ob es nach seinen Regeln (input, forward und output) ein zulässiges Paket ist. Hinzu kommt, dass der Router für alle Pakete ein neues Syslog-Paket erstellen und versenden muss.
Tests mit einem Pentium 4 mit 1,3 GHz Taktfrequenz und 256 MB Rambus hatten bei diesem Datenverkehr keine Einschränkungen des Routers zur Folge.

4.5.2.2 Ressourcen Backlog-Server

In der Errechnung aus dem Kapitel 4.5.1 werden 34642 Ereignisse an den Backlog-Server gesendet. Dies entspricht einer Datenmenge von 5,3 MB pro Sekunde. Diese Daten müssen vom Backlog-Server sinnvoll verarbeitet werden:

- Filtern von unkritischen Ereignissen
- Zusammenfassen von sich wiederholenden Ereignissen
- Zusammenfassen und Auswerten von zusammenhängenden Ereignissen
- Auswertung der Daten auf Gefahren für das Netzwerk
- Aufbereiten der Daten in einen Ereignisraum für das Neuronale Netz
- Auswerten des Ereignisraumes in einem Neuronalem Netz

Bei diesem Datenumfang ist ein sehr schneller Rechner für die Verarbeitung und Verdichtung der Informationen erforderlich. Nicht nur die Prozessorleistung stellt einen Engpass dar, sondern auch die Leistung der Speichermedien.

4.5.3 Schlussfolgerung für die Vorbereitung der Auditdaten

Bei Einhaltung aller Regeln für eine sichere Firewall-Umgebung reichen die heutigen Ressourcen für die Verarbeitung der Auditdaten nur bei Verwendung hochwertiger Hardware aus. Zusätzlich können Maßnahmen für die Informationsverdichtung der Auditdaten angewendet werden. Dabei dürfen keine relevanten Informationen für das Intrusion Detection System verloren gehen.

Zur Verdichtung der Informationen von Auditdaten müssen folgende Anforderungen betrachtet werden:

1. Unwichtige Informationen herausfiltern
2. Zusammenhängende Ereignisse zusammenfassen
3. Wiederholung von gleichen Ereignissen zusammenfassen
4. Ereignisinformationen in einem Schlüsselsystem kodieren

Der Standarddienst für die Verarbeitung und Speicherung in Unix- und Linux-Systemen unterstützt keine der oben festgelegten Anforderungen. Dies hat zur Folge, dass die Informationen aus dem Syslog-Dienst per eigenem Dienst den Ansprüchen entsprechend verarbeitet werden müssen.

Windows-Systeme stellen ein noch größeres Problem dar. In diesen Systemen muss ein zusätzlicher Dienst für die zentrale Speicherung der Auditdaten zur Verfügung gestellt werden. Darüber hinaus bieten erweiterbare Tools aus dem Internet keine vollständige Lösung nach dem hier geforderten Muster.

Erst die Entwicklung eines neuen Dienstes würde die Grundlage schaffen, die gestellten Anforderungen zu erfüllen.

5 Entwurf des Netzes

5.1 Zwischenstand

Die Angriffsmöglichkeiten auf ein Netzwerk aus dem Internet sind zahlreich. Die bisherigen Konzepte zur Angriffsabwehr sind statisch und nicht mehr zeitgemäß. Derzeitige Ansätze für ein Intrusion Detection System beinhalten Expertensysteme mit intelligenter Angriffserkennung und –abwehr. Diese sind jedoch nicht ausreichend, um mit der ständig steigenden Anzahl neuer Angriffsmethoden fertig zu werden. Neuronale Netze sollen diese ablösen und selbstständig auf neue Angriffssituationen reagieren. Ausgangssituation für die Einführung eines intelligenten Intrusion Detection Systems im Rahmen dieser Arbeit ist die Simulation eines Neuronalen Netzes aufgrund des zur Verfügung stehenden finanziellen Rahmens.

5.2 Aufbau des Netzes

Der Aufbau des Gesamtnetzes entspricht der Erarbeitung aus dem vierten Kapitel. Die Simulation des Neuronalen Netzes soll als Anwendung auf dem Backlog-Server integriert werden. Weitere benötigte Dienste sollen die geforderten Anforderungen an ein Intrusion Detection System vervollständigen.

5.2.1 Struktur des Netzes

Als Grundgerüst für den Entwurf des Netzes dient das in Kapitel 4.1.1 erarbeitete Muster als Vorlage. Vereinfacht kann der Aufbau folgendermaßen dargestellt werden:

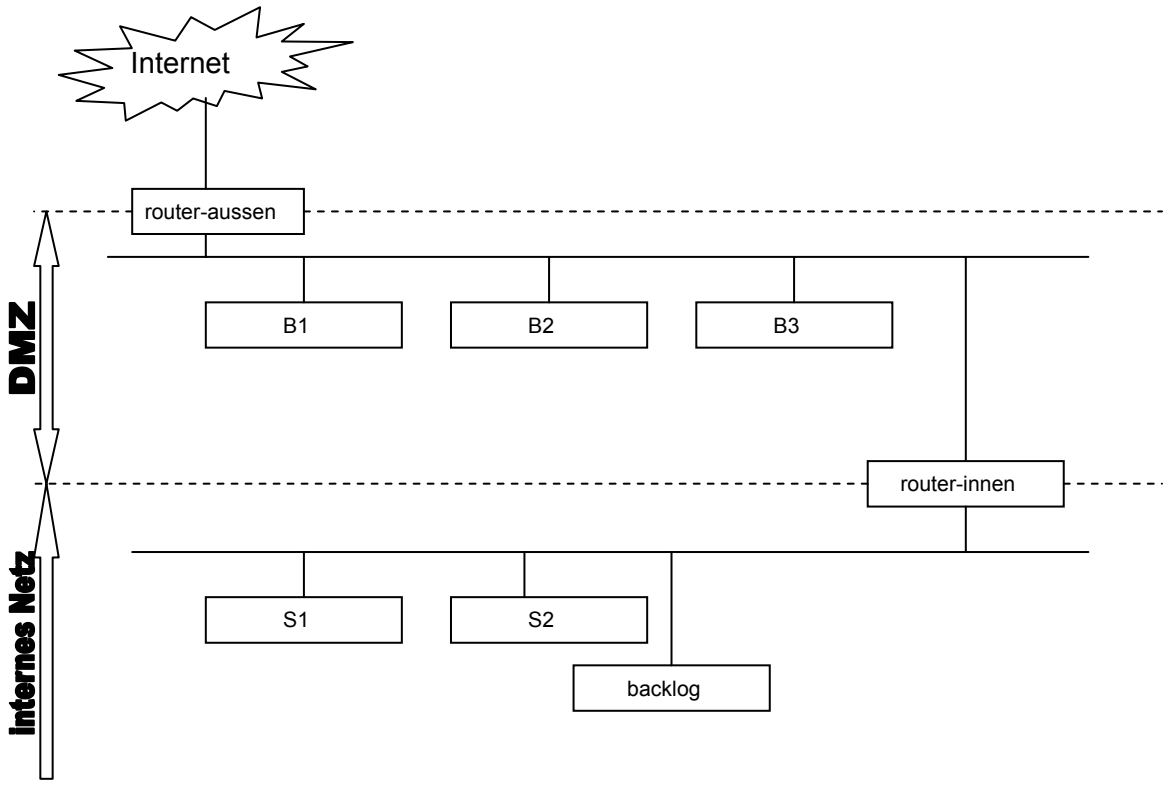


Abbildung 5-1: Grundstruktur Netz mit DMZ

5.2.2 Struktur der Dienste

5.2.2.1 Syslog-Dienst

Der Syslog-Dienst soll alle Ereignisse und Zustände an den Backlog-Server schicken. Das folgende Schaubild zeigt den Datenstrom der Informationen zum Backlog-Server

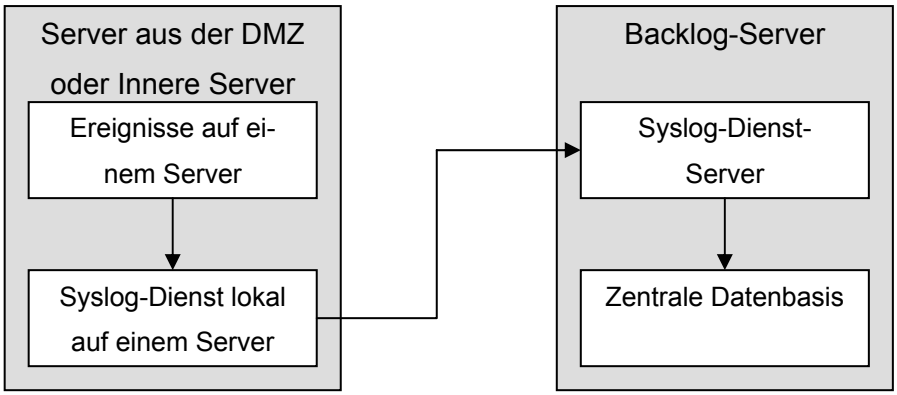


Abbildung 5-2: Informationsstrom Ereignisse

5.2.2.2 Dienst zur Aufbereitung der Audit-Daten

Die Aufbereitung der Audit-Daten soll mittels eines neuen Dienstes vorgenommen werden. Hierbei werden die Informationen für das Neuronale Netz vorbereitet und die Daten in einer sinnvollen Form gespeichert:

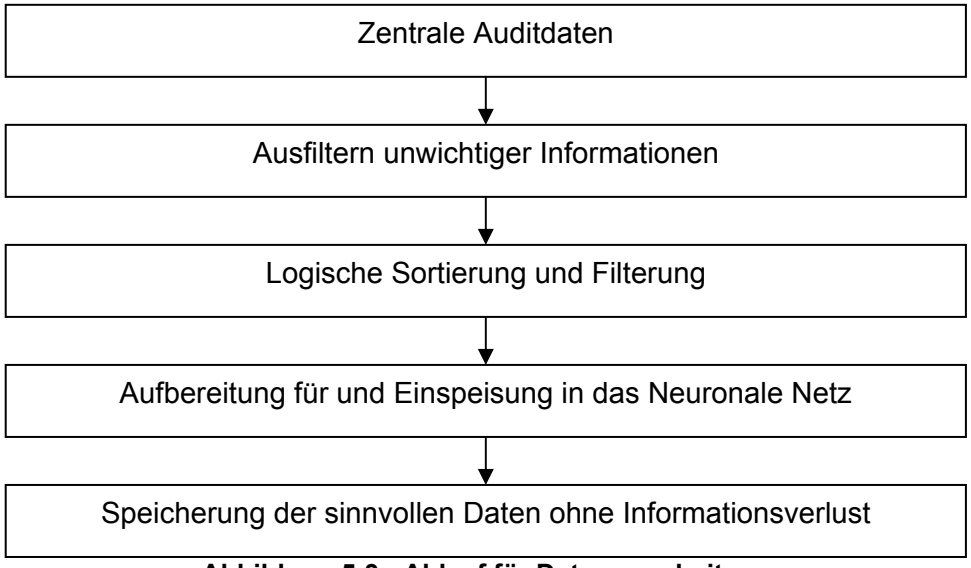


Abbildung 5-3: Ablauf für Datenverarbeitung

5.2.2.3 Einbindung des Neuronalen Netzes

Die aufbereiteten Informationen werden durch das Neuronale Netz nach folgendem Schema verarbeitet:

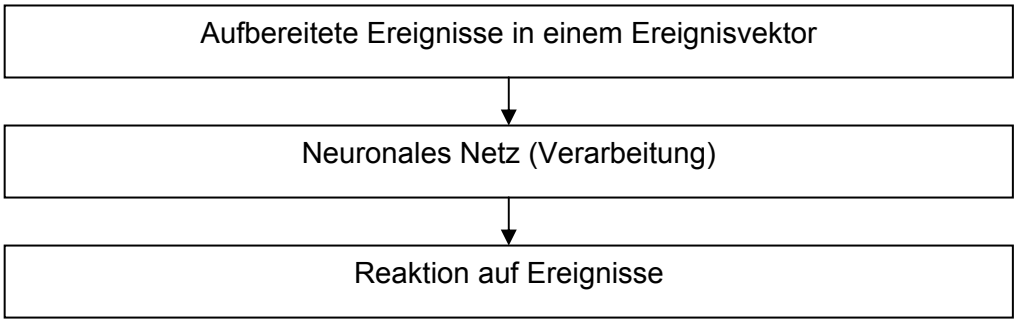


Abbildung 5-4: Ablauf mit Neuronalem Netz

5.3 Hard- und Softwarebedarf

5.3.1 Hardware

Grundvoraussetzung für alle Server in der DMZ ist die Verwendung einer stabilen Hardware. Ausgesuchte Komponenten mit ausreichender Leistung sollen die Stabilität des Systems gewährleisten.
Besondere Anforderungen an die Rechnerleistung ist bei folgenden Servern erforderlich.

5.3.1.1 Besondere Hardwareanforderungen des Backlog-Servers

Dieser Server muss alle Syslog-Daten auswerten und speichern. Hierfür wird eine erhöhte Rechenleistung und ausreichender Speicherplatz benötigt. Geeignet sind Mehrprozessormaschinen mit einem Raid-System für die Festplatten, um Probleme mit Engpässen der Speichermedien zu verringern.

5.3.1.2 Besonderer Hardwarebedarf Innerer Router

Dieser Router ist durch eine komplexe Paketanzahl und deren Kontrolle auf die Zulässigkeit stark belastet. Die Kontrolle der Gültigkeit der Pakete erfordert eine hohe Rechenleistung.

5.3.2 System- und Anwendungssoftware

5.3.2.1 Betriebssysteme

Auf allen überwachten Rechnern können sowohl auf Microsoft Windows als auch auf Unix/LINUX basierende Systeme zum Einsatz kommen. Oftmals bestimmt das Einsatzgebiet das zu verwendende Betriebssystem.
Für den Backlog-Server empfiehlt sich der Einsatz von LINUX als Betriebssystem. Gründe hierfür liegen in dem im Gegensatz zu Microsoft Windows bereits integrierten Dienstes für Syslog-Server und -Client und der durch das OpenSource-Prinzip offen liegenden Quellcodes, um eine bessere Anpassung zu gewährleisten.

5.3.2.2 Anwendungssoftware für Dienste der überwachten Server

UNIX/LINUX-Systeme beinhalten den Dienst zur zentralen Speicherung der Auditdaten. Für kritische Ereignisse werden vom Backlog-Server Aktionen durchgeführt, die die Sicherheit des Gesamtsystems gewährleisten soll. Hierbei soll ein neuer verschlüsselter Remote-Control-Dienst eingesetzt werden.

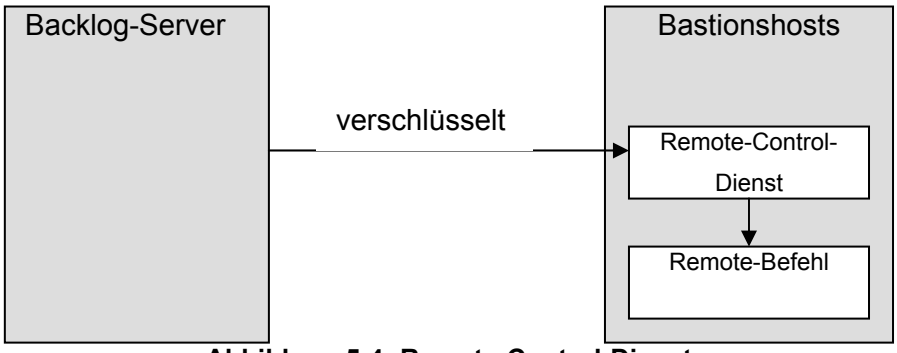


Abbildung 5-4: Remote-Control-Dienst

Für auf Microsoft Windows basierende Server muss zusätzlich ein neuer Dienst (Client-Dienst) für die zentrale Speicherung der Auditdaten auf einem Backlog-Server programmiert werden.

5.3.2.3 Anwendungssoftware für Dienste des Backlog-Servers

Für das Sammeln der Auditdaten soll der standardgemäße Syslog-Dienst von LINUX verwendet werden. Diese Auditdaten sollen dann nach den oben genannten Kriterien gefiltert und aufbereitet und in das Neuronale Netz eingebunden werden. Dieser Dienst soll neu implementiert werden. Ebenso soll der Dienst für die Remote-Control-Funktionen neu implementiert werden. Das Neuronale Netz soll mit Hilfe dieser Dienste die genannten Anforderungen erfüllen.

5.3.2.4 Aufbau des künstlichen Neuronalen Netzes

Ein simuliertes Neuronales Netz soll als eigenständige Anwendung auf dem LINUX-Backlog-Server laufen. Dieses ist vollständig neu zu implementieren. Zu einem späteren Zeitpunkt kann dieses simulierte künstliche Neuronale Netz durch eine geeignete Hardwarelösung ersetzt werden.

Die aufbereiteten Daten sollen in das künstliche Neuronale Netz eingespeist werden, welches über durchzuführende Abwehraktionen entscheidet, die beispielsweise durch Remote-Control-Funktionen andere Rechner beeinflussen können.

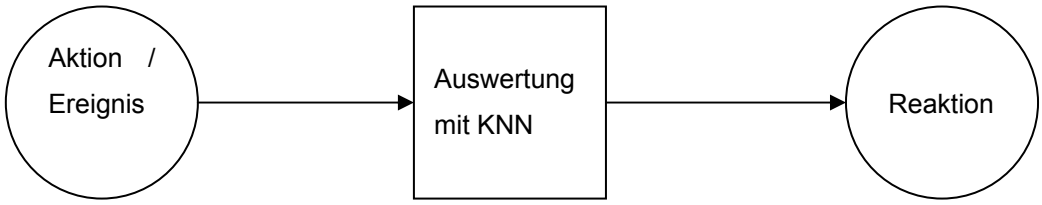


Abbildung 5-5: Aufbau und Ablauf Neuronales Netz

5.4 Entwurf der Datenstrukturen

5.4.1 Struktur des Systems

Alle Informationen aus den Auditdaten sollen komprimiert werden, das heißt, nach den Forderungen in Kapitel 4.5.3 verdichtet werden. Folgende Graphik bildet den Informationsfluss auf dem Backlog-Server ab:

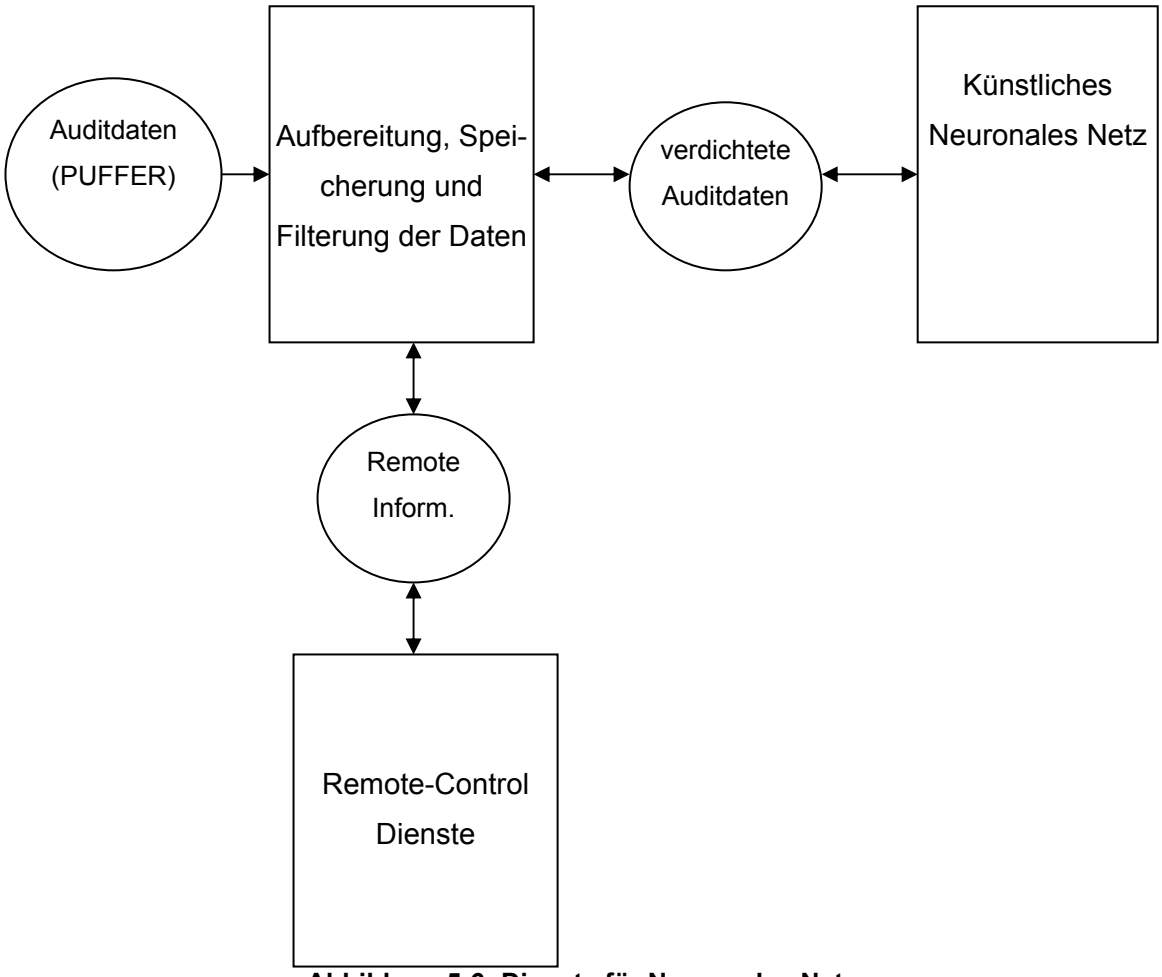


Abbildung 5-6: Dienste für Neuronales Netz

5.4.2 Merkmalsraum für das Neuronale Netz

Folgende Eingangsinformationen werden als Merkmalsraum an das Neuronale Netz gesendet:

Nr	Informationen	Anzahl Bits
1	Router Aussen	1
2	Router Innen	1
3	Bastionshost 1	1
4	Bastionshost 2	1
5	Bastionshost 3	1
6	Bastionshost ...	1
7	DMZ (Grenznetz)	1
8	Netz Innen	1
9	Gleiche Absenderadresse	1
10	Gleiche Zieladresse	1
11	Gleicher Quellport	1
12	Gleicher Zielport	1
13	Paket mit ungültiger Länge	1
14	SYN-Bit gesetzt	1
15	ACK-Bit gesetzt	1
16	Quellhost nicht erreichbar	1
17	Paketweg in beide Richtungen gleich	1
18	E-Mail hat externe E-Mail-Zieladresse	1
19	Abnahme Festplattenplatz	1
20	Zu geringer Festplattenplatz	1
21	MD5-Summen von Dateien geändert	1
22	Virenprogramm meldet Virus in E-Mail	1
23	E-Mail hat Dateianhang	1
24	Erkennbare Auditdaten für Pufferüberlauf	1
25	Erlaubte Aktion	1
26	Erkennbare Informationen für den Angreifer	1
27	Zähler (für Wiederholungen)	16
28++	...	

Tabelle 5-1: Merkmalsraum Input Neuronales Netz

Mit diesem definierten Merkmalsraum lassen sich alle bisher abgehandelten Reaktionen des künstlichen Neuronalen Netzes abbilden. Es folgen zwei Beispiele für die Abbildung des Merkmalsraumes.

Nr	Informationen	Gesetzte Merkmale Netscan	Gesetzte Merkmale DoS-Angriff
1	Router Aussen	X	X
2	Router Innen		
3	Bastionshost 1	X	
4	Bastionshost 2		X
5	Bastionshost 3		
6	Bastionshost ...		
7	DMZ (Grenznetz)	X	
8	Netz Innen		
9	Gleiche Absenderadresse	X	X
10	Gleiche Zieladresse		X
11	Gleicher Quellport		
12	Gleicher Zielport	X	X
13	Paket mit ungültiger Länge		
14	SYN-Bit gesetzt	X	X(Erstes Paket)
15	ACK-Bit gesetzt		X(Antwortpaket)
16	Quellhost nicht erreichbar		X
17	Paketweg in beide Richtungen gleich	X	X
18	Mail hat externe E-Mail-Zieladresse		
19	Abnahme Festplattenplatz		
20	Zu geringer Festplattenplatz		
21	MD5-Summen von Dateien geändert		
22	Virenprogramm meldet Virus in E-Mail		
23	E-Mail hat Dateianhang		
24	Erkennbare Auditdaten für Pufferüberlauf		
25	Erlaubte Aktion		
26	Erkennbare Informationen für den Angreifer	X	
27	Zähler (für Wiederholungen)	50	100

Tabelle 5-2: Beispiel Merkmalsraum Input Neuronales Netz

5.4.3 Reaktionen des künstlichen Neuronalen Netzes

Als ausgehende Zustände und Reaktionen soll folgender Ereignisraum definiert werden:

1	Kritisch 1	betroffenes Netz abschalten und den Administrator sofort verständigen
2	Kritisch 2	betreffenden Rechner abschalten und den Administrator sofort verständigen
3	Kritisch 3	betreffenden Dienst abschalten und den Administrator sofort verständigen
4	Kritsch 4	den Administrator sofort verständigen
5	Fraglich	dem Administrator mitteilen
6	Unkritisch	Nichts tun
7	Auswertung	Portscan
8	Auswertung	Netscan
9	Auswertung	Maschine gehackt
10	Auswertung	DOS
11	Auswertung	Mail-Spamming-Versuch
12	Auswertung	E-Mail-Wurm
13++	Auswertung	... (weitere neue Merkmale)

Tabelle 5-3: Merkmalsraum Output Neuronales Netz

Nach der Auswertung durch das Neuronale Netz sollen die gewonnenen Informationen in den Auditdaten vermerkt und Maßnahmen zum Schutz des Netzes ergriffen werden. Beide Merkmalsräume (In- und Output) sollen dynamisch erweiterbar sein, um neue Kriterien festlegen zu können.

5.4.4 Struktur der komprimierten und gefilterten Auditdaten

Alle Daten müssen so aufbereitet werden, dass keine wichtigen Informationen über Ereignisse im System verloren gehen, jedoch die Größe und Anzahl der gespeicherten Daten auf ein Minimum reduziert werden.

Zuerst sollen alle unnötigen Informationen herausgefiltert werden. Ein Beispiel für unnötige Informationen sind die „marks“ in den Auditdaten. Der Syslog-Dämon setzt in bestimmten Zeitabständen Markierungszeilen zur besseren Übersicht.

Allen Ereignissen soll eine Ereignisnummer eines Nummernsystems zugewiesen werden. Die Texthinweise können so als Informationen wegfallen und durch eine global festgelegte Nummern ersetzt werden.
Anschließend sollen zusammenhängende Ereignisse zusammengefasst werden. Zum Beispiel entstehen bei einer zulässigen Standardverbindung viele Auditdaten über die gesendeten und empfangenen Pakete. Hier soll ein Filter einsetzen, der nur noch die Verbindungsteilnehmer und den Port speichert.

5.5 Entwurf der Dienste

5.5.1 Syslog-Dienst für Microsoft-Systeme (Client-Dienst)

In Microsoft Windows-Systemen werden standardmäßig alle Auditdaten nur lokal in einer Datenbank gespeichert. Ein neuer Dienst soll diese Informationen an den Backlog-Server versenden, um einen Einsatz in der definierten Systemumgebung zu gewährleisten. Die Informationen sollen vorab im festgelegten Nummernsystem verschlüsselt werden.

Als Programmiersprache empfiehlt sich C oder C++ zum Einsatz kommen, um betriebssystemnahe Schnittstellen ansprechen zu können.

5.5.2 Dienst zur Aufbereitung der Auditdaten

Die Aufbereitung der Auditdaten dient der Informationsverdichtung und Informationskontrolle. Die Algorithmen für die Informationsverdichtung sollen in externen Klassen definiert werden, um auf Systemveränderungen mit neuen, einfach strukturierten Klassen zu reagieren. Zusätzlich sollen variable Datenbankinformationen gewährleisten, dass Veränderungen an der Datenstruktur des Syslog-Dämons oder anderer Dienste ausgeglichen werden können.

C oder C++ soll als Programmiersprache eingesetzt werden. Bei diesem Dienst ist nicht nur eine systemnahe Programmierung erforderlich, sondern auch eine hohe Geschwindigkeit aufgrund der umfangreichen Datenmengen ein entscheidender Faktor.

5.5.3 Remote-Control-Dienst

Es werden zwei Remote-Control-Dienste benötigt. Auf dem Backlog-Server wird ein Server-Dienst benötigt, der die Remote-Control-Verbindung steuert. Auf den anderen Servern des Gesamtsystems werden Client-Dienste benötigt, die auf das Remote-Control-Signal des Backlog-Servers „horchen“.

Alle Verbindungen des Remote-Control-Systems sollen mit einem Ticket-System verschlüsselt werden, um Sicherheitsrisiken zu minimieren. Als Verschlüsselungssystem kann Kerberos verwendet werden.

Die Implementierung des Systems soll in der Programmiersprache C oder C++ vorgenommen werden, um systemnah programmieren und um schon vorhandene C-Bibliotheken aus den entsprechenden Systemen (Windows- und Unix/LINUX-Systeme)

verwenden zu können. Dabei muss für jedes Betriebssystem ein eigener Client-Dienst programmiert werden.

6 Resümee

Der Staat, die gesamte Wirtschaft und als Ganzes betrachtet das globale System sind abhängig von einer Internetanbindung ihrer Netze. Die Börsen in ihrer heutigen Funktion wären undenkbar ohne eine globale Verbindung untereinander. Die Menschheit hat sich komplex vernetzt, um regelmäßige und unregelmäßige Geschäftsabläufe auf staatlicher, wirtschaftlicher und zunehmend auch privater Basis zu ermöglichen, zu verwalten und zu optimieren. Die Vorteile liegen auf der Hand: Im Optimalfall wird in Zukunft jeder von überall aus fast alle Vorgänge aus dem Geschäfts- und Privatleben abwickeln können. Doch jeder Komfort hat seinen Preis. Weltweit über das Internet zugängliche Computer sind grundsätzlich ‚rein physikalisch gesehen, erst einmal öffentlich für jeden zugänglich. Erst die eingesetzten Protokolle, Dienste und Systeme beschränken diesen Generalzugriff auf das erforderliche Minimum. Diese können wegen des weltweiten Einsatzes nicht ohne erheblichen Einsatz an Ressourcen verändert werden, um gestiegene Sicherheitsaspekte zu erfüllen.

Der Missbrauch von Daten privater Personen sowie Unternehmen ist in den letzten Jahren explosionsartig gestiegen. Die meisten Staats- und Unternehmensnetzwerke sind deshalb durch Firewalls gesichert. Alle Firewalls können letzten Endes als Aufsatz auf die bestehenden Systeme interpretiert werden, um den Zugriff auf bestimmte Teile dieses weltumspannenden Netzes auf diejenigen einzugrenzen, die dazu berechtigt sind. Die konventionellen Firewall-Konzepte sind aus heutiger Sicht nicht mehr ausreichend, um mit der Vielzahl der neuen Angriffsmethoden fertig zu werden. Selbst die heutigen Expertensysteme können in diesem Rahmen nur teilweise als erfolgreich angesehen werden. Zukunftsweisende Intrusion Detection Systeme auf Basis Neuronaler Netze zeigen einen Ausweg aus der schier unlösbar erscheinenden Situation. Heute hat sich die Angreiferseite derart weiter entwickelt, dass es sogar komplette Konstruktionswerkzeuge für Viren und qualitativ hochwertige Software für Angriffe auf Netzwerke gibt, die auch von Laien bedienbar sind. Verändert ein etwas erfahrenerer Benutzer beispielsweise eine Schleife innerhalb eines auf diese Art und Weise konstruierten Virus, erkennt diesen im Normalfall kein einziges Antivirenprogramm, dass derzeit auf dem Markt ist. Intelligente Angriffserkennung ist die einzige Chance Systemveränderungen dieser Art anhand des unterschiedlichen Laufverhaltens des Systems überhaupt festzustellen. Allein die

Tatsache, dass der amerikanische Geheimdienst NSA mit der Eigenentwicklung einer „sicheren“ Systemumgebung auf Basis von LINUX tätig wird, spricht für die verheerende Ausgangssituation auf Seiten der Netzbetreiber. Es gibt derzeit kein als hundertprozentig sicher anzusehendes System. Es bleibt zu befürchten, dass selbst zukünftige Intrusion Detection Systeme keinen absoluten Schutz bieten werden. Letzten Endes wird vermutlich ein Kompromiss gefunden werden müssen, der die Zahl der angebotenen Dienste auf ein sinnvolles Maß reduziert, um wenigstens in diesen Bereichen eine sehr hohe Sicherheit gewährleisten zu können.

Summary (englisch)

The state, the entire economy and looking at the global system as a whole are depending on an internet-connection with their networks. The world stock market in their today's function would be unimaginable without a global connection. The human race has become connected to manage and optimise regular and irregular state, economic and private businesses. The advantages are obviously: in the future everyone will be able to settlement everything from everywhere. There's a price to pay for everything. Worldwide are fundamental all computers accessible without a limit from everywhere. Just the protocols, services and systems keep this access to a minimum.

The abuse of data by private persons as well as businesses exploded in the last year. Therefore most of state and businesses networks are secured through firewalls. All firewalls can be seen as top part of the existing systems to enclose the action of specific parts of the whole network for people who are authorized. The conventional firewall-concepts are not sufficient anymore to handle the huge number of attacks. Even the today's expert-systems can be seen in this way just as partially successful. Intrusion Detection Systems on basis Neuronal Net that point the way ahead show a way out of this insoluble seeming situation. Today the attackers have been developed to such an extent that even complete construction-tools for viruses and qualitative high-grade software for intruders of networks exist which can even serve layman. Changes an experienced user for instance a loop inside of that kind of way constructed virus, recognizes this normally no single debug program, that is at the moment on the market. Intelligent intrusion detection is the only chance system-changes this way because of the different serial-behaviour of the system actually find out.

The fact of the matter is that the American secret service NSA with its own development works with a "secure" system on basis of LINUX, shows the disastrous situation on side of the network-provider. At the moment there is no system which is 100 percent save. It is feared that future Intrusion Detection Systems cannot offer an absolutely protection. In the end there has to be find a compromise, to reduce the offered services and their protection of a sensible standard and to offer a high security in the necessary parts.

7 Anhang

A Ehrenwörtliche Erklärung

Ich versichere,

dass ich die Kapitel der Diplomarbeit, für die ich als Verfasser genannt werde, selbständig verfasst habe,

dass ich keine anderen, als die angegebenen Quellen und Hilfsmittel benutzt habe,

dass ich diese Arbeit bei keinem anderem Prüfungsverfahren vorgelegt habe.

Heidelberg	**12. September 2001**	
Abgabeort	Abgabedatum	Unterschrift des Verfassers

B Literaturverzeichnis

[Bitt99]
Prof. Dr Bittel, O.: Neuronale Netze. Konstanz 1999.

[HeKa98]
Dr. von Helden, Josef; Dr. Karsch, Stefan: Grundlagen, Vorderungen und Marktübersicht für Intrusion Detection Systeme (IDS) und Intrusion Response Systeme (IRS). Debis IT Security Service, Bonn 1998.

[BoWo97]
Bonnard, Andreas; Wolff, Christian: Gesichtere Verbindung von Computernetzen mit Hilfe von Firewalls. Siemens AG, München 1997

[Pohl00]
Pohlmann, Norbert: Firewall-Systeme. 4. Auflage; MITP-Verlag, 2000

[ZwCoCh00]
D. Zwicky, Elisabeth; Cooper, Simon; Chapman, Brent: Einrichten von Internet-Firewalls. O'reilly, 2001

[Lipp00]
Prof. W.-M. Lippe: Einführung in Neuronale Netze. SoftComputing

[Rau01]
Judith Rauch: Neuroinformatiker: Gehirn dient als Vorlage für den Computer. Computer Zeitung 11.01.2001

[CCC01]
Computer Chaos Club: Meldungen und Hilfestellungen. Internet-News 2001

[Sym01]
Symantec Informationen: Produktinfo Symantec: www.symantec.de

[Graf01]
Marcus Graf: Ohne Konzepte keine Sicherheit. Internetartikel 02.2001. FOX Marcom & Media Verlag GmbH

[DFN01]
DFN Cert Veröffendlichungen: DFN-Cert http://www.cert.dfn.de

[CIA01]
CIA *Veröffendlichungen:* CIA http://cia.com und http://www.cia.gov

[FBI01]
FBI Veröffendlichungen: FBI Computer Intrusion Squad (2000/2001). FBI http://www.fbi.gov

[Cis01]
Cisco Produktinformationen: Cisco Internet. http://www.cisco.com und http://www.cisco.com/de/, 2001

[BDG01]
BDG GmbH & Co. KG: BDG Internet. http://www.bdg.de/bdg/produkte.htm,

[TIS01]
TIS - Firewall: Internet. http://www.fwtk.org

[Ker01]
Linux Kernes Information: Internet. http://www.kernel.org

[Squ01]
Squid – Proxy: Internet www.squid-cache.org

C Abkürzungsverzeichnis

ACK	Acknowledgement
ACL	Access Control List
AFT	Authenticated Firewall Traversal
AH	Authentication Header
AIX	UNIX-Betriebssystem von IBM
API	Application Programming Interface
ARP	Address Resolution Protocol
AS	Autonome Systeme
ASC	Application Sharing Component
ASCII	American Standard Code for Information Interchange
ATM	Asynchronous Transfer Mode
BSD	Berkeley Software Distribution
BSI	Bundesamt für Sicherheit in der Informationstechnik
CGI	Common Gateway Interface
CHAP	Challenge-Handshake Authentication Protocol
CLNP	Connectionless Network Protocol
COM	Component Object Model (von Microsoft)
DMZ	Demilitarisierte Zone
DNS	Domain Name System
DSS	Digital Signature Standard
EBCDIC	Extended Binary Coded Decimal Interchange Code
ECB	Electronic Codebook Mode
EIT	Enterprise Integration Technologies
EOT	End of Transmission
ESP	Encapsulation Security Payload
FDDI	Fiber Distributed Data Interface
FF	Form Feed
FIN	Final
FSP	File Service Protocol
FTP	File Transfer Protocol
Ftpd	FTP-Dämon

FW	Firewall
FWTK	Firewall Toolkit
GIF	Graphics Interchange Format
GUI	Graphical User Interface
SMTP	Simple Transfer Protocol (E-Mailübertragung im Internet)

D Tabellenverzeichnis

E Abbildungsverzeichnis