Internet Sicherheit - Firewall und IDS

abc Information GmbH
PO Box 130208
13601 Berlin
Germany

+49-700-ITBROKER
http://www.Broker.de
email:contact@Broker.de

abc Information GmbH
PO Box 130208
13601 Berlin
Germany

+49-700-ITBROKER
http://www.Broker.de
email:contact@Broker.de

1 Sicherheit (Kurzfassung)

Wenn man heute von Internet spricht, so stösst man meist auf Begriffe wie WWW, Surfen, FTP, eMail und vielleicht sogar noch auf Sicherheit im Internet. Letzteres ist für den einzelnen Privatbenutzer des Internets nicht von grosser Bedeutung. Für Anbieter kommerzieller Dienste und Industriebetriebe auf dem Internet ist Sicherheit meist von höchster Priorität. Kleinbetriebe koppeln z.B. Teilnetze der verschiedenen Filialen über das Internet oder ermöglichen Aussendienstmitarbeitern Fernsitzungen auf ihrem lokalen Rechenzentrum abzuhalten. Bei Grossbetrieben ist die Problematik ähnlich, auch sie nutzen die vielen Möglichkeiten, welche das Internet bietet. Dabei sind die nötigen Vorkehrungen zu treffen, damit firmeninterne Daten vor unerlaubtem Zugriff oder gar Zerstörung geschützt sind. Man versucht also, sich vom Internet abzuschotten, quasi eine dicke Mauer zwischen das interne Netz (Intranet) und das Internet zu stellen.

Solche Mauern nennt man "Firewall". Firewalls sind Gebilde, welche sich an die Anforderungen des jeweiligen zu schützenden Netzes anpassen lassen. Sie überwachen dann den Datenverkehr von und zum Internet.

Nach der Installation des Firewalls kann man sich aber nicht darauf verlassen, dass das System für immer und ewig vor "Einbrecher" sicher ist. Darum muss ein Tool eingesetzt werden, welches das System ständig überwacht. Ein solches Tool nennt man IDS (Intrusion Detection System). Bei uns wird Real Secure 5.0 von ISS (Internet Security Systems) eingesetzt.

Das Sicherheitssystem (Firewall+IDS) kann man sich vorstellen, wie wenn die Firewall die Türe zu einem Haus ist und das IDS die Alarmanlage. Zur Tür (Firewall) kommen nur erwünschte Teilnehmer rein. Kommt aber jemand von Fenster ins Haus muss die Alarmanlage (IDS) einspringen und die nötigen Massnahmen ergreifen.

Nach der Durchführung dieses Praktikums sollten Sie folgende Lernziele erreicht haben:

- Notwendigkeit von Sicherheit kennen
- Wichtige Sicherheitsaspekte kennen
- Ein einfaches Sicherheitskonzept erstellen können
- Das Prinzip eines Firewalls kennen
- Den Unterschied zwischen Proxy/Paket-Filter kennen
- Einige Evaluationskriterien für Firewall-Systeme kennen
- Einen Firewall konfigurieren und testen können
- Das Prinzip eines IDS kennen
- Real Secure beherrschen
- Anwendungsmöglichkeiten eines IDS kennen

abc Information GmbH
PO Box 130208
13601 Berlin
Germany

+49-700-ITBROKER
http://www.Broker.de
email:contact@Broker.de

2 Theorie und Grundlagen

Mit zunehmender Verbreitung des Internets wächst nicht nur die Zahl der ehrlichen Internet-Benutzer. Leider bekommen auch dunkle Gestalten einen einfacheren Zugriff zu Computer und -netzen. Darum ist es wichtig, sich mit "Sicherheit im Internet" auseinanderzusetzen. Dieses Kapitel zeigt einige wichtige Aspekte zur Sicherheit auf und motiviert zugleich, aktiv zur Sicherheit beizutragen.

Sicherheit wir oft als Oberbegriff für zwei Themengebiete verwendet:

Datensicherheit

> Datenintegrität und Betrieb gewährleisten: Dazu gehören Massnahmen wie Stromversorgung, Backup, Mirroring, Redundante System etc.

Datenschutz

> Missbrauch von Daten verhindern: Dazu gehören Massnahmen wie Firewalls, Verschlüsselung etc.

Im weiteren werden wir den Begriff Sicherheit allgemein für den Bereich des Datenschutz verwenden. Hier noch einige Beispiele die zeigen, was geschehen kann, wenn ein Netz ungenügend geschützt ist:

Elektronische Einbrüche

> In New York wurden fünf Männer beschuldigt, im Juli 1992 in Computersysteme mehrerer regionaler Telefonfirmen und Grossunternehmen, Universitäten und Kreditforschungsinstituten wie TRW eingebrochen zu haben. Bei TRW sollen sie 176 Konsumentenkreditberichte gestohlen haben. Dabei zapfte die Regierung erstmals mit gerichtlicher Bewilligung Leitungen an, um Gespräche und Datenübermittlungen von Hackern festhalten zu können.
> *Quelle: Computerworld Schweiz, Nr. 17/93, p. 13.*

Pentagon-Hacker

> Die britische Polizei verhaftet mit Schützenhilfe der US-Fahnder den 16-jährigen Pentagon-Hacker mit Vulgo "Datastream". Der junge Brite hat im Juli 1995 im Computer des amerikanischen Verteidigungsministeriums unter anderem geheime Mitteilungen zum amerikanisch-koreanischen Atomstreit entdeckt. Dateien zu Raketenforschung, Besoldung, Personaldaten und E-Mail wurden über Internet verbreitet. Dann jedoch lief er in eine elektronische Falle: Aufgeflogen ist der Jugendliche, weil er über Nacht vergass, die Verbindung zum Pentagon-Computer abzubrechen.
> *Quelle: The Independent, January 3, 1995, 2766.*

abc Information GmbH
PO Box 130208
13601 Berlin
Germany

+49-700-ITBROKER
http://www.Broker.de
email:contact@Broker.de

3 Sicherheit realisieren

Um Bedrohungen zu bestimmen was ein Sicherheitssystem leisten soll müssen zuerst die Anforderungen definiert werden

3.1 Anforderungen

An Daten und Informatiksysteme werden allgemein folgende Anforderungen gestellt:

- Verfügbarkeit
- Authentizität und Integrität
- Vertraulichkeit

dazu kommt je nach Anwendung:

- Beweisbarkeit von Vorgängen
- Überwachung der Ressourcenbenützung

Verfügbarkeit

Fragestellungen:

- Wie lange kann ein Unternehmen ohne seine Daten leben?
- etc.

Die Erhöhung der Verfügbarkeit ist das Hauptziel der meisten Sicherheitsmassnahmen wie Redundante System, Backups etc. Wie kritisch diese Grösse für ein Unternehmen ist kann sich je nach Anwendung stark unterscheiden. (Bsp. Ein Börsenmakler braucht aktuelle Daten innerhalb von Minuten für die Steuerung einer Maschine dagegen entscheiden Sekunden usw.)
Jeder Benutzer merkt üblicherweise sofort ob sein System und seine Daten verfügbar sind.

Authentizität und Integrität

Fragestellungen:

- Was geschieht wenn falsche Daten weiterverarbeitet werden?
- Was geschieht wenn auf Grund modifizierter oder gefälschter E-Mail Entscheidungen getroffen werden?
- etc.

Authentizität und Integrität wird teilweise von Sicherheitsmassnahmen wie Checksummen etc. gewährleistet. Dies Massnahmen schützen üblichweise vor Hard- und evtl. Softwarefehlern für einen Schutz gegen Angriffe muss meist aber noch mehr getan werden.
Kaum ein Benutzer macht sich Gedanken über die Authentizität und Integrität der Daten; was der Computer liefert wird meist als wahr und richtig angenommen.

Vertraulichkeit

Fragestellungen:

abc Information GmbH
PO Box 130208
13601 Berlin
Germany

+49-700-ITBROKER
http://www.Broker.de
email:contact@Broker.de

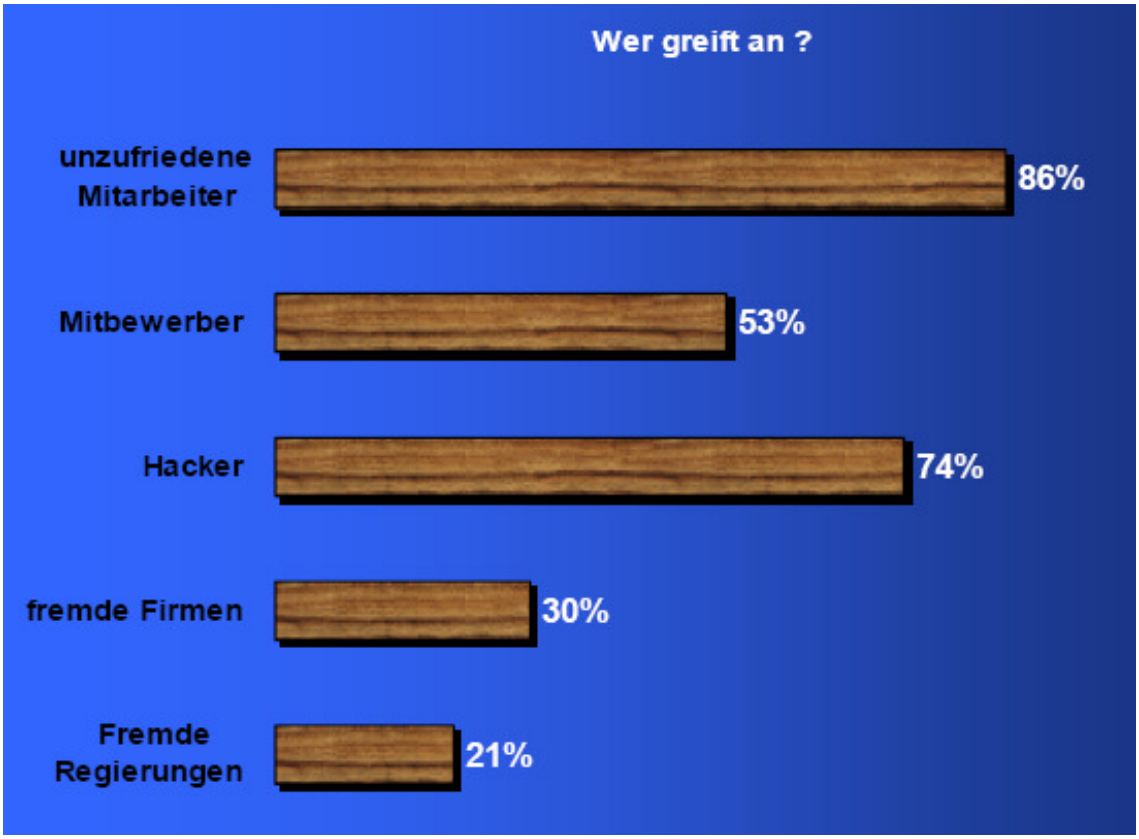
- Was geschieht wenn Konkurrenten Einsicht in interne Daten erhalten?
- Was geschieht wenn Entscheide zu früh publik werden?
- etc.

Zur Wahrung der Vertraulichkeit dienen Methoden wie Kryptographie und Zugangsschutz.
Die meisten Benutzer sind sensibilisert für Vertraulichkeit weil sie dies auch bei nicht IT-Anwendungen (z.B. Briefpost) beachteten.

3.2 Bedrohungen

Gefahren (beabsichtigt oder unbeabsichtigt) droht primär von den eigenen Mitarbeitern!

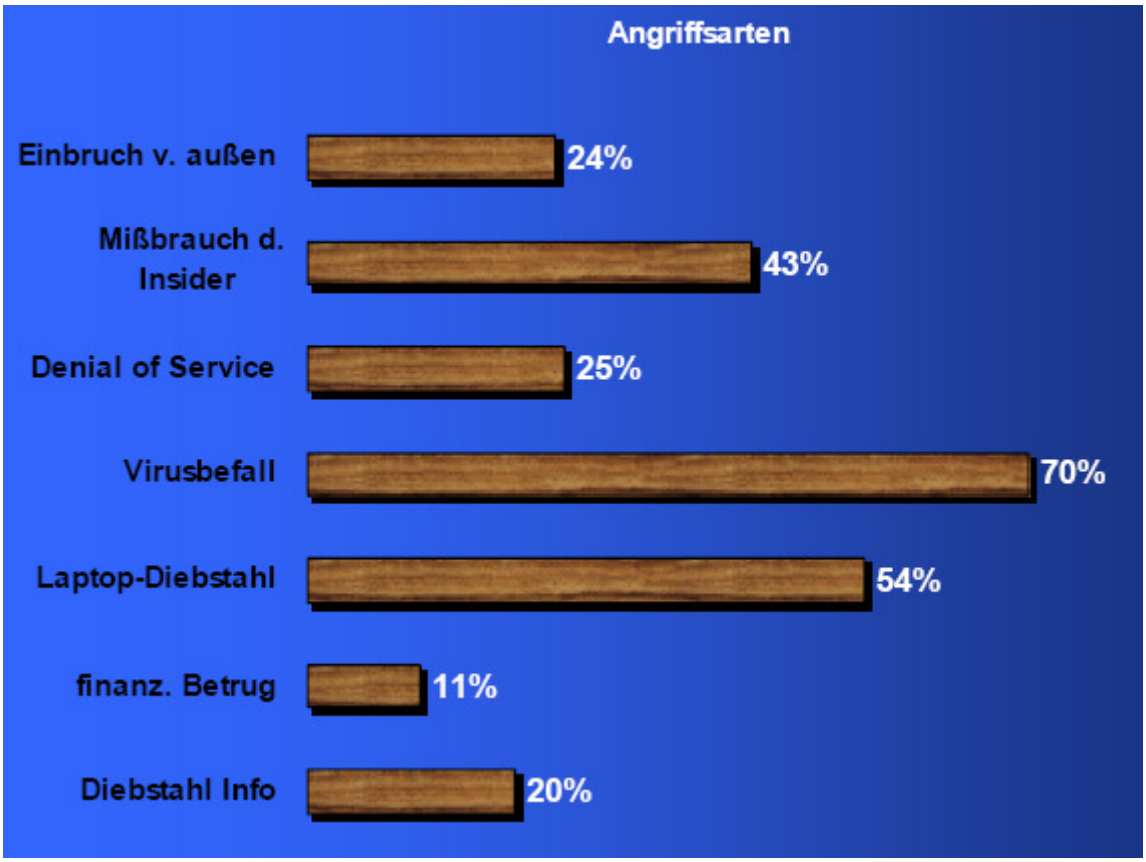
Wer greift an



abc Information GmbH
PO Box 130208
13601 Berlin
Germany

+49-700-ITBROKER
http://www.Broker.de
email:contact@Broker.de

Häufigkeit der Angriffe



Welche Bedrohungen sind zu erwarten? Man unterscheidet zwei Varianten:

Aktive Angriffe:

- Eindringen nichtauthorisierter Personen
- Beeinträchtigung und Störung des Netzwerkbetriebes
- Vortäuschen einer falschen Identität
- Moifikation von Daten

Passive Angriffe:

- Abhören von Teilnehmer-Identitäten und Passwörtern
- Abhören von Daten
- Verkehrsflussanalyse

abc Information GmbH
PO Box 130208
13601 Berlin
Germany

+49-700-ITBROKER
http://www.Broker.de
email:contact@Broker.de

Wer sind die Angreifer:

- Mitarbeiter des eigenen Unternehmens
- Personen aus dem Konkurrenz/Wettbewerbs-Umfeld
- Hacker/Cracker aus der Computer-Untergrundszene
- professionelle Hacker/Industriespione

Je nachdem, in welchem Bereich eine Firma tätig ist, wird sie auch stärker von einer bestimmten Personengruppe besucht und leider auch attackiert. Die überwiegende Anzahl von Angriffen und **Gefahren (beabsichtigt oder unbeabsichtigt) droht von den eigenen Mitarbeitern!** (ca. 86%). Diese Tendenz ist steigend. So waren es noch vor ca. 5 Jahren ca 70% von eigenen Mitarbeitern.
Aus Statistiken ist zu sehen, dass sehr viele Angriffe aus dem Internet von Universitäten und Schulen ausgehen. Vermehrt stellt man jedoch fest, dass professionelle Hacker für Industriespionage eingestellt werden

3.3 Schwachstellen

Wie aber gelangen Angreifer auf fremde Systeme? Man kann die Schwachstellen in folgende Kategorien unterteilen:

Mangelhafte Software:

Keine Software ist 100%ig fehlerfrei. Es ist bereits vorgekommen, dass Angreifer Softwarefehler auf entfernten Systemen ausgenutzt haben, um höher privilegierte Benutzerrechte zu erhalten.

Schlecht konfigurierte und administrierte Systeme:

Die beste Firewall nützt nichts, wenn sie nicht richtig konfiguriert ist. In Zeitnot wird vielfach vergessen Sicherheitsmechanismen nach der Administration wieder einzuschalten oder nach dem Einbau einer neuen Komponente die Gesamtsicherheit des Systems neu zu überdenken. Daraus ergibt sich ein wichtiger Grundsatz aller Sicherheitssysteme: Die Einhaltung der Sicherheitspolitik ist **nicht** Sache der Systemadministratoren sondern sollte wo immer möglich an eine andere Stelle delegiert werden.

Sicherheitsprobleme der Kommunikationsprotokolle:

UDP und TCP garantieren keine sicheren Kommunikationspfade. Bei der Datenübertragung mit Hilfe von TCP/IP lässt sich nicht vorhersagen, über welche Knoten die Übertragung der Pakete erfolgt. Sitzt ein Angreifer am Terminal eines Vermittlungsknotens, so kann er die Daten, welche dort vermittelt werden, lesen.

Passwörter:

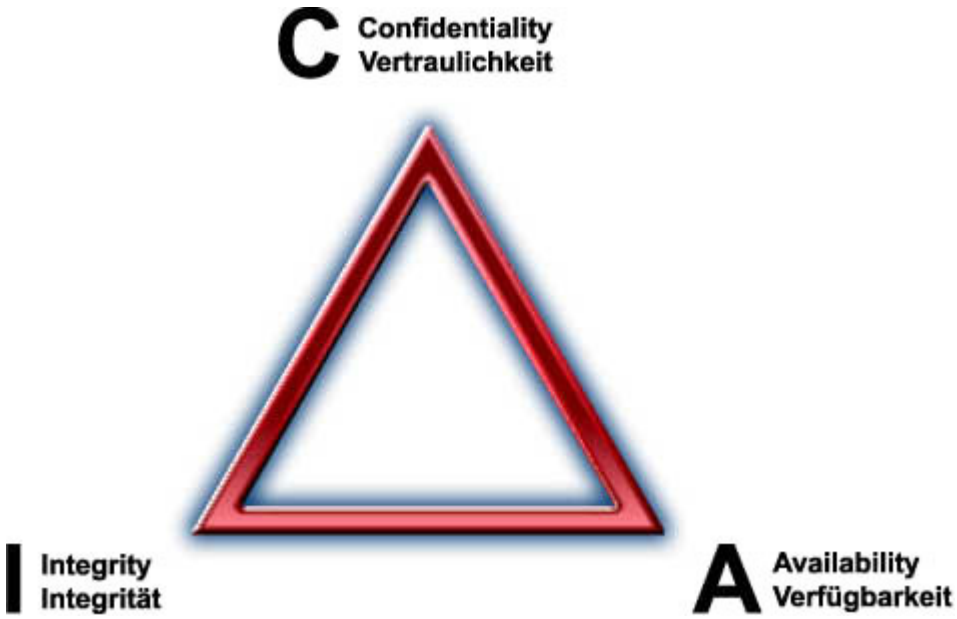
Die Wahl und Verteilung von Passwörtern hat einen grossen Einfluss auf die Sicherheit des Systems. Was nützt es, wenn jeder Benutzer das Passwort des Systemverwalters kennt oder die Passwörter so schlecht sind, dass man sie mit einem Taschenrechner knacken kann?

abc Information GmbH
PO Box 130208
13601 Berlin
Germany

+49-700-ITBROKER
http://www.Broker.de
email:contact@Broker.de

3.4 CIA-Dreieck

Bei allen Bemühungen um Sicherheit darf man folgendes aber nicht vergessen: Werden Massnahmen zur Erhöhung der Vertraulichkeit eingesetzt leidet darunter die Verfügbarkeit, erhöht man die Verfügbarkeit leidet darunter die Integrität usw.
Man kann diesen Zusammenhang in einem Dreieck darstellen (CIA-Dreieck, siehe Abbildung) mit den drei Kriterien Vertraulichkeit, Integrität und Verfügbarkeit als Eckpunkte und die Eigenschaften eines Systems oder die Anforderungen an ein System darin als Fläche eintragen.



Oder mit einem Beispiel ausgedrückt: Das sicherste System wäre ein Computer ohne Netzwerkanschluss und Stromzufuhr eingeschlossen in einem Safe: Man hätte damit fast ein Maximum an Vertraulichkeit gewonnen - wie aber kann man jetzt darauf aktuelle Daten nachführen (Integrität) und wie ermöglicht man den Zugriff für Benutzer (Verfügbarkeit)?

3.5 Sicherheitskonzept

Bevor man etwas absichern will, muss man wissen, wie man was vor was genau absichern will. Dieses Wie, Was und Wovor definiert man als eine Reihe von Entscheidungen in einem "Sicherheitskonzept" oder in "Sicherheitsrichtlinien".
Dieses Kapitel zeigt, worauf beim Erstellen eines Sicherheitskonzepts geachtet werden muss und stellt dabei ein einfaches Gerüst zur Verfügung.

Was muss geschützt werden?

Als erstes müssen die zu schützenden Objekte identifiziert werden. Dies ist ein sehr wichtiger Teil. Wird nur eine Workstation vergessen, kann schon ein Angriff darauf ein ganzes Netz lahmlegen!

- Hardware
- Software

abc Information GmbH
PO Box 130208
13601 Berlin
Germany

+49-700-ITBROKER
http://www.Broker.de
email:contact@Broker.de

- Daten
- Dokumentation
- Zubehör

Wovor wird geschützt?

Nach der Zusammenstellung der zu schützenden Objekte kann man sich nun überlegen, wovor die Objekte geschützt werden sollten. Grundsätzlich fragt man sich, welche Mitarbeiter welche Zugriffsrechte haben. Dazu definiert man Benutzergruppen:

- Gäste
- Aushilfen
- Mitarbeiter
- Systemadministrator
- Service-Personal
- externe Benutzer

Ein Mitarbeiter kann dabei in keiner Gruppe, einer oder mehreren Benutzergruppen angehören. Gehört er keiner Benutzergruppe an, so hat er keine Zugriffsrechte. Sind Zugriffsrechte verteilt, kann man unterscheiden, ob authorisierte oder nicht authorisierte Zugriffe erfolgen.

Wie gut wird geschützt?

Grundsätzlich unterscheidet man zwischen zwei Denkweisen:

- Alles, was nicht ausdrücklich erlaubt ist, ist verboten
- Alles, was nicht ausdrücklich verboten ist, ist erlaubt

Eine 100%ige Sicherheit wird nie erreicht[Murphy]! Man kann aber eine hohe Sicherheit erreichen, wenn die 1. Denkweise angewendet wird und einige Regeln eingehalten werden

Minimale Zugriffsrechte und Datensicht

> Nur die zur Erfüllung einer Aufgabe absolut notwendigen Rechte dürfen vergeben werden. Dieses Prinzip verkleinert die Angriffsfläche und begrenzt den Schaden bei gezielten Attacken. Was der Mitarbeiter nicht probiert er auch nicht aus und kann damit keinen unbeabsichtigten Schaden anrichten.

Mehrschichtige Verteidigung:

> Man sollte sich nie auf nur einen Schutzmechanismus verlassen. Es müssen Mechanismen eingesetzt werden, die sich gegenseitig unterstützen oder verstärken.

Die Passierstelle:

> Die Passierstelle zum geschützten Bereich sollte möglichst eng sein. Zum Beispiel beim Anschluss des Firmennetzes an das Internet verwendet man darum nur eine Schnittstelle. Diese Schnittstelle kann genau überwacht werden. Werden dagegen mehrere Schnittstellen verwendet, kann man sich zuwenig auf die einzelnen konzentrieren und es geschehen schneller Fehler.

abc Information GmbH
PO Box 130208
13601 Berlin
Germany

+49-700-ITBROKER
http://www.Broker.de
email:contact@Broker.de

Das schwächste Glied:

Eine Kette ist nur so stark wie ihr schwächstes Glied. Dies gilt auch für ein Schutzsystem. Ein Angreifer sucht immer nach dem schwächsten Glied, um so schnell wie möglich die Mauer zu durchbrechen. Deshalb sollte man sich genau überlegen, worauf man sich bei der Überwachung besonders konzentrieren muss.

Zuverlässigkeit:

Es ist bekannt, dass jede Software Fehler hat. Es muss darauf geachtet werden, dass bei einem Softwarefehler ein Angreifer nicht plötzlich Zugang erhält, wo er sonst abgewiesen würde. Es kann sich unter Umständen auch lohnen mehrer Firewallsysteme gestaffelt hintereinander einzusetzen damit nicht beim Auftreten eines Softwarefehlers in einem System die ganze Verteidigung weg ist.

Umfassende Beteiligung:

Jeder Mitarbeiter muss mitmachen wollen und darum für die Sicherheit motiviert werden.

Einfachheit:

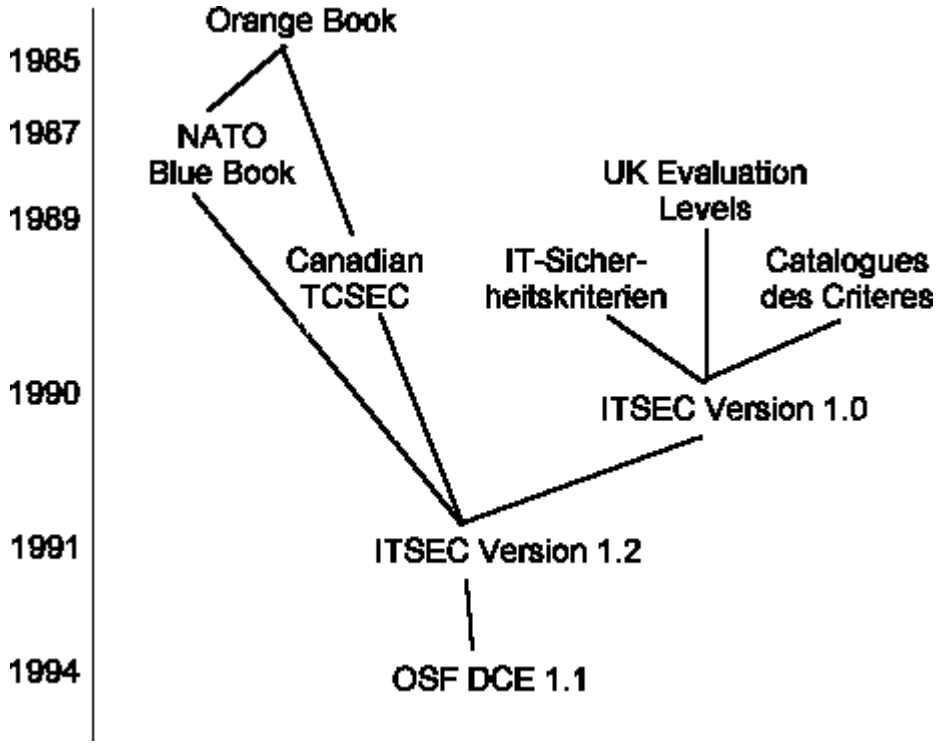
Die Sicherheitssysteme sollten einfach und übersichtlich gestaltet werden. Nur so ist es möglich, eine Kontrolle darüber zu haben.
Bsp.: Zwingt man die Benutzer dazu jede Woche ein neues 15stelliges Passwort zu verwenden, werden sie es sicher irgendwo aufschreiben...

3.6 Sicherheitsklassen

Mit zunehmender Abhängigkeit heutiger Unternehmen von der Funktionsfähigkeit der Informationssysteme werden auch die Sicherheitsaspekte zu einem wichtigen Faktor. Um die Sicherheit von Informationssystemen auch nach objektiven Kriterien einheitlich beurteilen zu können, wurden Richtlinien geschaffen.
Der erste bedeutende Kriterienkatalog war das sogenannte (TCSEC - Trusted Computer System Evaluation Criteria), welches vom amerikanischen Verteidigungsministerium herausgegeben wurde. Darauf aufbauend folgten weitere, wie aus folgender Abbildung zu sehen ist.

abc Information GmbH
PO Box 130208
13601 Berlin
Germany

+49-700-ITBROKER
http://www.Broker.de
email:contact@Broker.de



Das Orange Book

Im Orange Book werden Informationssysteme (auch IT-Systeme genannt) in die sieben Sicherheitsklassen D, C1, C2, B1, B2, B3 und A1 unterteilt.

Das Orange Book ist das "militärische" Modell von Sicherheit mit dem primären Ziel der Einhaltung der Vertraulichkeit und betrifft nur die Sicherheit eines Hosts und nicht eines Netzwerks. Das Modell umfasst immer Systeme d.h. die ganze Hard- und Software inkl. aller Anschlüsse, den Ort an dem sich das System befindet und die komplette Dokumentation. Es ist deshalb nicht möglich ein Betriebssystem zu kaufen welches z.B. C2 sicher ist; Software ist allenfalls C2 zertifizierbar im Rahmen eines kompletten Systems!

In der **Klasse D** sind alle Systeme eingeordnet, welche die Anforderungen für die Klassen C bis A nicht erfüllen. Das System kann zwar sehr sicher sein, erfüllt aber mindestens eine Anforderung der anderen Klassen nicht. Die Klasse D beschreibt den geringsten Sicherheitsstandard.
Die **Klasse C** wird in die zwei Sicherheitsebenen C1 und C2 unterteilt.
C1 beschreibt die Sicherheitsmechanismen, welche normalerweise auf einem typischen Unix-System verfügbar sind. Die Benutzer müssen sich dem System gegenüber mit einem Loginnamen und einem Passwort legitimieren. Durch diese Kombination werden auch die Zugangsrechte für die Benutzer festgelegt.
C2 verlangt zusätzlich zu den Sicherheitsmechanismen von C1, dass alle oder bestimmte Operationen der einzelnen Benutzer überwacht und gespeichert werden können.
Die **Klasse-B**-Kriterien fordern zusätzliche Mechanismen zu den Kriterien der Klasse C. Die Klasse B wird in die drei Sicherheitsebenen B1, B2 und B3 unterteilt.
In **B1** werden verschiedene Sicherheitsniveaus wie nicht vertraulich, vertraulich, geheim oder streng geheim unterschieden. Die Rechte der Besitzer und Benutzer können nur durch den Systemoperator verändert werden.
B2 verschärft die Sicherheitskriterien der Ebene B1 weiter und fordert zusätzlich:

- Zugangskontrollen zu allen Komponenten des Systems

abc Information GmbH
PO Box 130208
13601 Berlin
Germany

+49-700-ITBROKER
http://www.Broker.de
email:contact@Broker.de

- gesicherter Kommunikationspfad zwischen Benutzer und System
- Abschirmung gegen elektromagnetische Abstrahlung nach aussen
- Unterscheidung zwischen Operator und Systemverwalter
- Markierung aller Einrichtungen mit der jeweiligen Geheimhaltungsstufe
- Formelle Beschreibung des Sicherheitsmodells

B3 Systeme erfüllen noch höhere Kriterien und müssen in der Regel von Grund auf als solche konzipiert und entwickelt werden. Dabei sind unter anderem zusätzliche Mechanismen zur Wiederherstellung des ursprünglichen Systemzustands nach Systemfehlern zur Verfügung zu stellen.
Die **Klasse-A**-Kriterien fordern keine zusätzliche Systemerweiterung. Um diese Sicherheitsklasse jedoch zu erhalten, müssen alle Bedingungen der unteren Klassen erfüllt und zusätzlich bis auf das kleinste Detail dokumentiert sein.

Der ITSEC-Kriterienkatalog

Auch in Europa wurde ein Kriterienkatalog für die Beurteilung der Sicherheit von Informationssystemen geschaffen. ITSEC (Information Technology Security Evaluation Criteria) wurde in Anlehnung an das Orange Book auch in sieben Klassen aufgeteilt , welche in der Definition auch ungefähr mit dem Orange Book übereinstimmen, wie aus folgender Tabelle zu entnehmen ist:

Übersicht über die Sicherheitsklassen

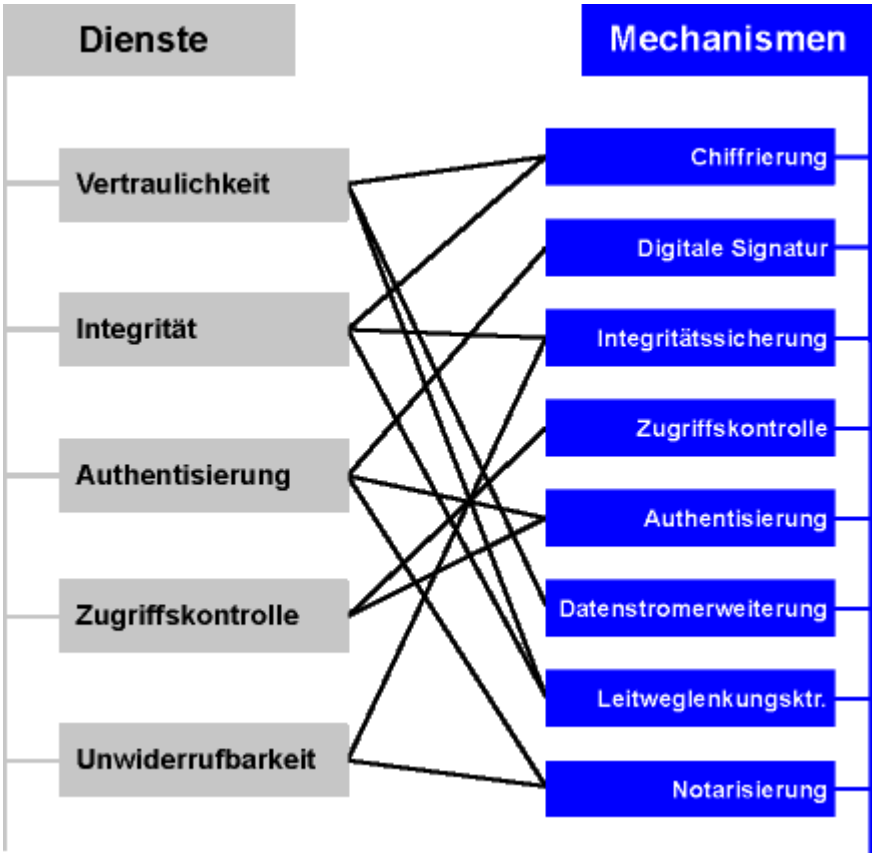
Orange Book	ITSEC	Sicherheit
D	E0	unzureichend
C1	E1	getestet
C2	E2	methodisch getestet, Konfigurationskontrolle und kontrollierte Verteilung
B1	E3	teilanalysiert (Schaltpläne, Quellcode)
B2	E4	formales Sicherheitsmodell, Spezifikation in semi-formaler Notation
B3	E5	nachvollziehbare Abbildung von Spezifikation/Quellcode
A1	E6	Anforderungen und Grob-Spezifikation in formaler Notation, Konsistenz mit dem formalen Sicherheitsmodell nachweisen

Sicherheit im OSI-Modell

ISO hat zusammen mit IEC, JTC1 und SC21 ebenfalls eine Sicherheitsarchitektur [ISO 7498-2] entwickelt. In dieser Sicherheitsarchitektur werden verschiedene Sicherheitsdienste defininiert, welche mittels Sicherheitsmechanismen realisiert werden können.
Untenstehende Abbildung zeigt die Zusammenhänge:

abc Information GmbH
PO Box 130208
13601 Berlin
Germany

+49-700-ITBROKER
http://www.Broker.de
email:contact@Broker.de



Ein Problem ist allerdings, dass OSI die Sicherheitsarchitektur für offener Systeme definiert hat. Dies führt dazu, dass die Definition so offen ist, dass man sie genauer definieren muss, um überhaupt damit arbeiten zu können. In der Industrie werden meist sog. Subsets definiert. Diese genaueren Definitionen sind nun die Sicherheitsdienste in obiger Abbildung. Das Zusammenwirken aller Sicherheitsdienste gewährleistet schlussendlich die Gesamtsicherheit eines Systems.

3.7 Sicherheitszukunft IPng (IPv6)

An einer neuen Version des Internet Protocols (IP) wird schon längere Zeit gearbeitet. Das Internet Protocol Next Generation (IPng) oder auch IP Version 6 (IPv6) enthält neben dem um vielfaches grösseren Adressraum, den verbesserten Multicast-Adressfunktionen und der neuen Anycast- Adressen auch stark verbesserte Sicherheitsfunktionen. So wurde in IPng die Authentifizierung und die Sicherheitseinkapselung (Encapsulating Security Payload, ESP) eingebaut

Security Parameters Index

Der Security Parameters Index (SPI) wird aus der Zieladresse und einer sogenannten Security Association (Sicherheitskombination) berechnet. Die Security Association gibt unter anderem an, welcher Authentifizierungsalgorithmus und im Falle der Sicherheitseinkapselung, welcher Schlüssel für die Verschlüsselung verwendet wird.

Authentifizierung

abc Information GmbH
PO Box 130208
13601 Berlin
Germany

+49-700-ITBROKER
http://www.Broker.de
email:contact@Broker.de

Mit dem Authentifizierungs-Header, welcher eine Art fälschungssichere Unterschrift darstellt, wird bezeugt, dass ein IP-Paket wirklich vom richtigen Absender stammt und unterwegs nicht verfälscht wurde. Dies wird Angriffe wie IP-Spoofing verunmöglichen.
Die Schlüsselverwaltung für die Authentifizierung wird nicht in IPng integriert, damit es für unterschiedliche Schlüsselverteilungsverfahren offen bleibt. Der Zielrechner kann aber den Algorithmus und den Schlüssel immer aus der Security Association bestimmen, welche aus der eigenen Adresse und dem SPI berechnet werden kann.

Sicherheitseinkapselung

Die Sicherheitseinkapselung (ESP) ermöglicht es, entweder nur die Nutzdaten eines Datenpakets oder ein komplettes Datagramm zu verschlüsseln. Wird ein komplettes Datagramm verschlüsselt, so wird dem verschlüsselten Datagramm ein neuer, unverschlüsselter Header vorangestellt. Somit können vertrauliche Daten wie Kreditkartennummern und Geschäftsberichte sicher durch das Internet geschickt werden.

Zukunft

IPng wird in nächster Zukunft mehr und mehr anzutreffen sein. Einerseits ist das Verlangen nach einem grösseren Adressraum sehr gross und andererseit sind alle Internetbenutzer sehr an einer sicheren Datenübertragung auf dem Internet interessiert, um zum Beispiel Waren über das Internet einzukaufen und mit Kreditkarte sicher zu bezahlen. Die IETF hat die Spezifikationen von IPng als "Proposed Internet Standard" verabschiedet. Momentan wird an den Details des neuen Protokolls gefeilt. Es sind bereits Implementationen von IPng verfügbar.

abc Information GmbH
PO Box 130208
13601 Berlin
Germany

+49-700-ITBROKER
http://www.Broker.de
email:contact@Broker.de

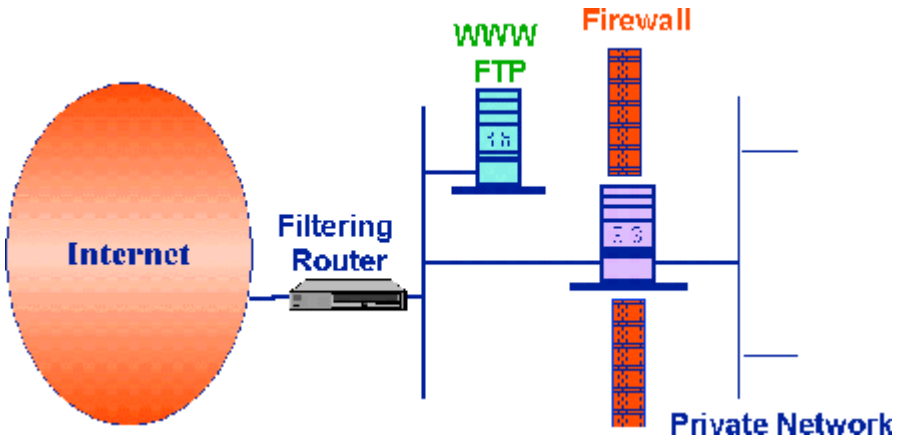
4 Firewalls (Theorie)

In diesem Abschnitt lernen Sie die Grundlagen zu Internet-Firewalls kennen. So wird das Prinzip von Firewalls erklärt und aufgezeigt, wozu sie gebraucht werden. Ein Modell zeigt deren Einordnung im OSI-Referenzmodell. In einer Tabelle finden Sie eine Übersicht über die wichtigsten Begriffe, welche im Zusammenhang mit Firewalls oft gebraucht werden.

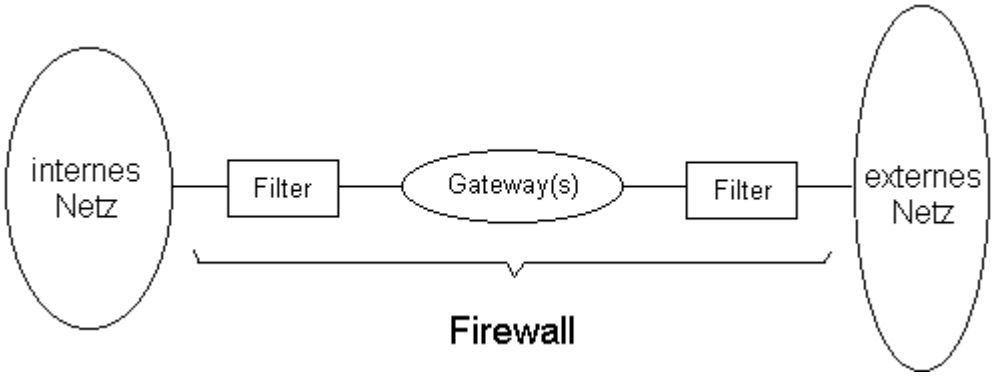
Des Weiteren werden die Eigenschaften der verschiedenen Firewall-Architekturen erläutert und zum Schluss aufgeführt, was Internet-Firewalls nicht leisten

4.1 Prinzip

Ein Firewall setzt sich aus einer oder mehreren Komponenten zusammen. Sie überwacht oder beschränkt den Zugriff zwischen dem Internet und einem privaten Netz.



Man unterscheidet im Allgemeinen zwischen Filtern (manchmal auch "Screens" genannt) und Gateways. Filter schleusen nur ausgewählte Klassen von Verkehr durch, während Gateways als Relais für bestimmte Dienste dienen, welche durch die Filter blockiert werden. So kann ein Systemadministrator einen bestimmten Dienst erlauben, solange dieser über "sein" Gateway geführt wird. Ein Gateway besteht aus einer oder mehreren Maschinen



abc Information GmbH
PO Box 130208
13601 Berlin
Germany

+49-700-ITBROKER
http://www.Broker.de
email:contact@Broker.de

4.2 Definitionen und Begriffe

In folgender Liste sind die wichtigsten Begriffe aufgeführt, welche im Zusammenhang mit Firewalls oft verwendet werden. Hinterher finden Sie zu jedem Begriff die entsprechende Beschreibung

Firewall

Eine oder mehrere Komponenten, welche zwischen einem geschützten Netz und dem Internet (oder einem anderen Netz) den Zugriff überwachen resp. beschränken.

Host

Ein eigenständiges Computersystem mit Anschluss an einem Netz (PC, Workstation, etc.).

Bastion-Host

Bastion -> Bastei, Bollwerk, Verteidigungsanlage: Besonders geschützte Computeranlage, da diese in der Regel eine wichtige Anlaufstelle für interne Benutzer und gegenüber dem Internet offen ist.

Dual-Homed-Host

Computersystem mit mindestens zwei Netzschnittstellen.

Dämon

Ein Programm, welches beim Bootvorgang oder beim Starten einer Anwendung gestartet wird und im Hintergrund aktiv bleibt. Es läuft also unsichtbar ab, deshalb der Name *Dämon* -> Geist, Spuk.

Proxy

Proxy -> Stellvertreter: System oder Prozess, welcher für Maschinen ohne Zugang eine Zugangsmöglichkeit bietet.

Proxy-Server

Ein Programm, welches stellvertretend für interne Clients mit externen Servern kommuniziert. Es stellt eine Art Verbindungspunkt für diese Kommunikation dar, denn nur so ist ein Server von einem Client erreichbar.

Proxy-Dienst

Einzelner Teil eines Proxy-Systems, welches für einen einzelnen (Internet-)Dienst benötigt wird (Bsp.: FTP-, Telnet-, HTTP-Proxy).

Paketfilterung

Prozess, welcher Pakete gemäss gegebenen Regeln passieren lässt oder sperrt. Filterung wird z.B. in lokalen Netzen von Bridges ausgeführt, um Pakete nicht mehr ins Ursprungssegment zu schicken, die als Ziel ein anderes Netzsegment haben als deren Ursprungssegment.

DMZ (Grenznetz)

DMZ: De-Militarisierte Zone. Netz, das als Schutzschicht zwischen ein geschütztes und ein externes Netz eingefügt wird.

Innerer Router

abc Information GmbH
PO Box 130208
13601 Berlin
Germany

+49-700-ITBROKER
http://www.Broker.de
email:contact@Broker.de

Der innere Router (manchmal auch Choke-Router genannt) schützt das interne Netz vor der DMZ (Grenznetz) und vor dem Internet. Der innere Router liegt somit zwischen dem internen Netz und der DMZ.

Äusserer Router

Der äussere Router (manchmal auch Access-Router genannt) schützt die DMZ und das interne Netz vor dem Internet. Meistens wird dieser Router vom Internet-Provider angeboten. Falls hohe Sicherheit verlangt wird, ist der äussere Router ein firmeninternes Gerät. Die Hauptaufgabe ist dann das Blockieren von Paketen mit gefälschten Ursprungsadressen. Diese Pakete behaupten, vom internen Netz zu kommen, werden aber auf dem Internet-"Port" vom Router empfangen-> Diskrepanz.

4.3 Wozu braucht man Internet-Firewalls?

Ein internes Netz (Intranet) gar nicht ans Internet anzuschliessen, ist eine Möglichkeit. Eine andere ist ein Anschluss mit kontrollierbarer Sicherheit. Hier wird eine Einrichtung benötigt, die es ermöglicht, das Netz ans Internet anzuschliessen und dabei ein bestimmtes Mass an Sicherheit beizubehalten. Diesen Schutz bieten Firewalls, sofern diese gewissenhaft eingerichtet werden.

Im Allgemeinen gibt es verschiedene Modelle, ein Firmennetz zu schützen:

- **Keine Sicherheit** ist der einfachste Ansatz. Dabei werden lediglich die Sicherheitsmechanismen eingesetzt, welche ein Hersteller standardmässig bereitstellt.
- **Sicherheit durch Unsichtbarkeit** geht davon aus, dass niemand von der Existenz der bestimmten Ressource weiss.
- **Netzsicherheit**, wobei die Sicherheit beim Netzzugang gewährleistet wird. Dieses Konzept beinhaltet Firewalls, Authentifizierungsverfahren und Verschlüsselung.
- **Hostsicherheit** Könnte man davon ausgehen, dass moderne Betriebssysteme genügen Sicherheitsmechanismen beinhalten und zudem die Möglichkeit gesicherter Host-Host Kommunikation bieten müssten keine anderen Methoden eingesetzt werden. Man kann zwar einzelne Hosts sichern, verteilt damit aber die Administration und erhöht den Aufwand. Meistens wird man deshalb einen Ansatz mit gesicherten Teilnetzen verbunden über Netzsicherheitselemente als Lösung wählen.

Es gibt jedoch kein Sicherheitsmodell für alle Fälle. Jedes Modell muss der entsprechenden Netzumgebung sowie dem zu verwirklichenden Sicherheitskonzept angepasst werden

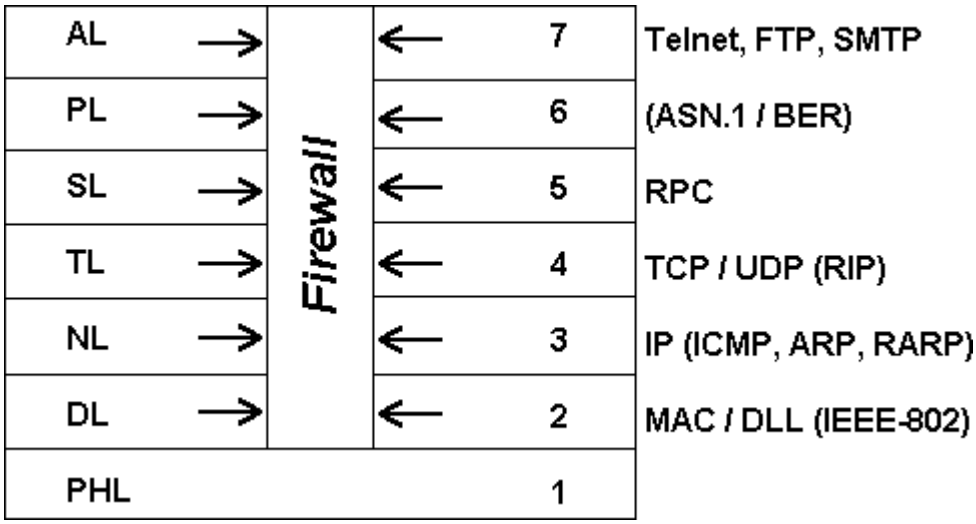
4.4 Firewalls im OSI-Modell

Firewalls werden eingesetzt, um Systeme vor unerlaubtem Zugriff zu schützen. Ein Zugriff kann physikalisch oder logisch geschehen. Physikalisch, wenn z.B. eine Anschlussleitung angezapft wird und logisch, wenn der Zugriff z.B. softwaremässig geschieht.
Das OSI-Referenzmodell beschreibt ein Kommunikationssystem allgemein. Der Kommunikationsvorgang wird in sieben aufeinanderliegende Schichten zerlegt, wobei jede Schicht gewisse Funktionen realisiert. Diese Funktionen oder Dienste werden jeweils der nächst höheren Schicht zur Verfügung gestellt.
Die Schicht 1 ist die physikalische Schicht, welche beim physikalischen Zugriff auf das Übertragungsmedium

abc Information GmbH
PO Box 130208
13601 Berlin
Germany

+49-700-ITBROKER
http://www.Broker.de
email:contact@Broker.de

massgeblich ist. Die verschiedenen Funktionen eines Firewalls liegen in den Schichten 2 bis 7. Untenstehende Abbildung veranschaulicht die Einbettung von Firewalls ins OSI-Referenzmodell.



Aus der Abbildung wird ersichtlich, wo der Firewall seinen Einsatz findet. Ab Schicht 2 nämlich kontrolliert er jeglichen Protokollverkehr zweier kommunizierender Schichten.

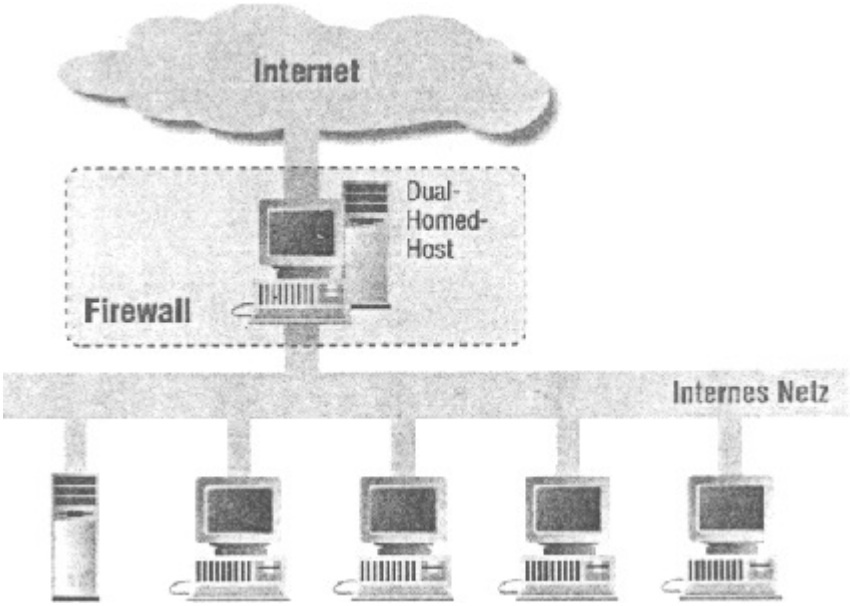
4.5 Firewall-Architekturen

Dual-Homed-Host Architektur

Eine Dual-Homed-Host Architektur wird um den Dual-Homed-Host herum aufgebaut. Dieser Host wird zwischen dem internen und dem kritischen Netz (Internet) plaziert. Der Host könnte somit das Routen zwischen den beiden Netzen übernehmen, die Routingfunktion wird für den Einsatz in der Firewall-Architektur jedoch deaktiviert. Auf diese Weise werden IP-Pakete nicht direkt von einem ins andere Netz geroutet. Ein Rechner ausserhalb des Firewalls und ein Rechner innerhalb des Firewalls können somit nur mit dem Dual-Homed-Host kommunizieren, nicht aber direkt miteinander. Folgende Abbildung zeigt die Netzkonfiguration einer Dual-Homed-Host Architektur:

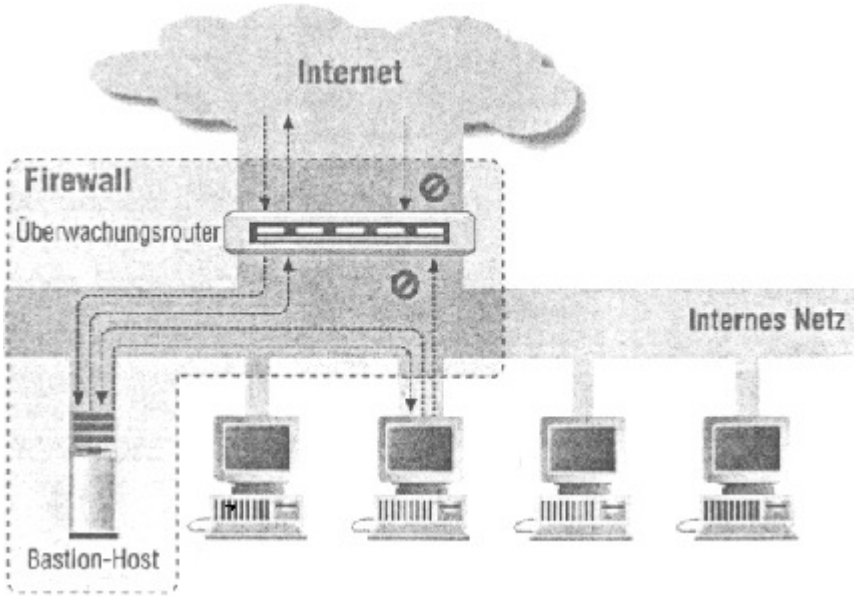
abc Information GmbH
PO Box 130208
13601 Berlin
Germany

+49-700-ITBROKER
http://www.Broker.de
email:contact@Broker.de



Architektur mit überwachtem Host (screend-host architecture)

Diese Architektur bietet Dienste über einen getrennten Router an, welcher als Paketfilter wirkt. Die Dienste werden von internen Maschinen angeboten, meist vom Bastion-Host selbst. Die Paketfilterung auf dem Überwachungsrouter wird so eingerichtet, dass aus dem Internet Verbindungen nur zum Bastion-Host aufgebaut werden können.
Deshalb muss dieser auch höchste Rechnersicherheit bieten.



Architektur mit überwachtem Teilnetz (screend-subnet architecture)

Diese Architektur wird gegenüber der Architektur mit überwachtem Host um ein Grenznetz ergänzt. D.h. zwischen dem Internet und dem internen Netz befindet sich hier das Grenznetz (auch DMZ genannt). Es

abc Information GmbH
PO Box 130208
13601 Berlin
Germany

+49-700-ITBROKER
http://www.Broker.de
email:contact@Broker.de

können auch mehrere Grenznetze zwischen die Aussenwelt und das interne Netz gelegt werden. Diese Massnahme ist jedoch nur sinnvoll und wirksam, wenn sich die verschiedenen Schichten auch unterscheiden. Bei der einfachsten Art dieser Architektur gibt es zwei Überwachungsrouter, die am Grenznetz angeschlossen sind. Man unterscheidet zwischen dem inneren Router und dem äusseren Router. Ein Angreifer muss also an beiden Routern vorbeikommen, um auf das interne Netz zu gelangen. Bei der Architektur mit überwachtem Host ist nur ein Router zu überwinden.

4.6 Paketfilterung

Eine Firewall-Konfiguration besteht meist aus mehreren Komponenten: ein oder mehrere Filter sowie ein oder mehrere Gateways. Paketfilterung ist eine billige Möglichkeit, Gateways zu schützen. Sie kann mit einem Router, welcher entsprechende Mechanismen unterstützt oder mit spezieller Software realisiert werden. Für die Paketfilterung eignen sich "normale" Router, da auf diesen dienötigen Mechanismen meist schon standardmässig implementiert sind. Zudem braucht man für den Anschluss ans Internet meistens sowieso einen Router

Wozu braucht man Paketfilterung?

Mit Paketfilterung kann der Datentransfer gesteuert, zugelassen oder unterbunden werden. Dazu werden folgende Kriterien verwendet:

- Quelladresse, von der die Daten (angeblich) stammen.
- Zieladresse, zu der die Daten gelangen sollen.
- verwendete Sitzungs- und Anwendungsprotokolle.

Die Daten selbst werden meist nicht ausgewertet. So lassen sich Filterregeln definieren, welche z.B. folgende Bedingungen erfüllen:

- Weise jeden Versuch ab, eine Telnet-Verbindung von aussen aufzubauen.
- Ermögliche jedem, uns mit E-Mail (SMTP) erreichen zu können.

Diese Regeln lassen sich relativ einfach realisieren. Schwieriger wird es wenn man mehrfache Kombinationen von Regeln ausdrücken will welche sogar voneinander abhängig sein können. Sinvollerweise setzt man dann ein entsprechendes Konfigurationswerkzeug (z.B. vom Routerhersteller) ein.
Folgendes Beispiel ist mit Paketfilterung jedoch nicht realisierbar, da ein Paketfilter keine Benutzer identifizieren kann:

- Ein bestimmter Benutzer kann sich von aussen mittels Telnet anmelden, alle anderen nicht.

Gewisse Schutzmechanismen lassen sich nur durch Router mit Paketfilterung realisieren. Dazu kommt, dass sich der Router dabei an einer bestimmten Stelle im Netz befinden muss. So ist es beispielsweise sinnvoll, alle Pakete mit interner Quelladresse abzuweisen. Dadurch können Pakete eines Angreifers, welcher als Quelladresse eine interne Adresse angegeben hat, leicht erkannt und eliminiert werden. Der Router alleine weiss nämlich, an welcher physikalischen Netzschnittstelle das externe Netz (z.B. Internet) bzw. das interne Netz angeschlossen ist.

abc Information GmbH
PO Box 130208
13601 Berlin
Germany

+49-700-ITBROKER
http://www.Broker.de
email:contact@Broker.de

Vorteile der Paketfilterung

Einfacher Schutz für ein ganzes Netz durch einen einzigen Überwachungsrouter:

Ein geschickt plazierter Router kann ein ganzes Netz schützen, wenn dieser als einziger Zugang zum Internet wirkt. Dabei ist die Netzsicherheit unabhängig von der Grösse des Netzes.

Einfache Handhabung resp. Transparenz für Anwender:

Für den Einsatz eines Paketfilters sind keine Software-Anpassungen und Konfigurationen auf den Client-Rechnern nötig. Eine spezielle Schulung der Anwender und eine etwaige Anmeldeprozedur fallen auch weg. Der Paketfilter "erscheint" dem Anwender transparent, so nimmt er diesen höchstens im Falle eine kritischen Prozedur wahr.

Standardmässige Implementation der Filtermechanismen:

In den meisten Hard- und Software-Routern ist die Funktionalität der Paketfilterung bereits standardmässig enthalten. So lässt sich ein bereits im Betrieb stehender Router problemlos zu einem Paketfilter "erweitern".

Nachteile der Paketfilterung

Implementation der Paketfilter:

- Paketfilterregeln sind meist schwer formulierbar.
- Paketfilterregeln sind oft nur mühsam zu testen.
- Paketfilterfunktionen sind unvollständig und erschweren oder verunmöglichen oft die Realisierung von bestimmten Filtern.
- Ein fehlerhaftes Paketfilterungsprogramm kann Pakete passieren lassen, welche es hätte sperren müssen.

Paketfilterung ist nicht für alle Protokolle geeignet:

Die r-Befehle von BSD-UNIX sowie NFS und NIS/YP sind sicherheitskritische Protokolle, welche mit Paketfilterung nicht sicher genug abgefangen werden können.

Aktionen, welche normale Router mit gegebener Information nicht ausführen können:

Pakete geben Auskunft über ihren Ursprungsrechner. Von welchem Benutzer das Paket kommt, lässt sich jedoch nicht ausfindig machen. Weiter ist der verwendete Port ersichtlich, aber nicht die Anwendung, zu welcher das Paket gehört. Somit lässt sich ein bestimmter Dienst nur über dessen Portnummer kontrollieren. Und diese Portbelegung kann wiederum manipuliert werden.

Protokollierung

Wie bei allen Überwachungsaktivitäten werden auch bei der Paketfilterung Ereignisse protokolliert. Was wie zu protokollieren ist, entscheidet der Systemadministrator selbst. So kann er z.B. nur die potentiell "bösartigen" oder alle Pakete protokollieren. Hier gilt es ein vernünftiges Mass zu finden. Anhand der Protokolle ist es z.B. möglich, sich einen Überblick über eingehende oder abgehende Verbindungen zu verschaffen.

Antwort auf ICMP-Fehlermeldungen

abc Information GmbH
PO Box 130208
13601 Berlin
Germany

+49-700-ITBROKER
http://www.Broker.de
email:contact@Broker.de

ICMP (Internet Control Message Protocol) dient dazu, Hosts günstigere Routen zu einem Ziel bekanntzugeben, über Routing-Probleme zu informieren oder Verbindungen bei Problemen im Netz abzubrechen
Es stehen folgende zwei Gruppen von ICMP-Fehlermeldungen zur Auswahl:

- Das Ziel ist nicht erreichbar: "host unreachable" oder "network unreachable".
- Das Ziel ist aus administrativen Gründen nicht erreichbar: "host administratively unreachable" oder "network administratively unreachable".

Es gibt mehrere Punkte, die zu beachten sind bei der Entscheidung, ob der Überwachungs-Router ICMP-Fehlermeldungen zurückgibt oder nicht:

- Welche Meldungen werden zurückgeschickt?
- Ist der Zusatzaufwand akzeptabel, welcher beim Versenden der Fehlermeldungen entsteht?
- Erhalten Angreifer durch die Fehlermeldungen zu viele Informationen über Ihr System?

Wo werden Paketfilter plaziert?

Grundsätzlich sollte die Paketfilterung überall dort eingesetzt werden, wo es möglich ist. Die mögliche Anzahl Stellen im Netz hängt aber von der gewählten Firewall-Architektur ab. Bei der Architektur mit überwachtem Host und der Architektur mit überwachtem Teilnetz liegt die Lösung auf der Hand, da sowieso nur ein Router vorhanden ist. Sobald jedoch mehrere Router vorhanden sind, kann die Paketfilterung auch auf mehreren Routern vorgenommen werden. Es empfiehlt sich, die Paketfilterung an möglichst vielen Orten zu nutzen. Damit findet das Prinzip der minimalen Zugriffsrechte Anwendung: alles was nicht explizit erlaubt ist, ist verboten.

4.7 Proxy-Systeme

Proxy steht für Stellvertreter. Rechner mit Zugriffsmöglichkeiten dienen als Stellvertreter (Proxies) für Maschinen ohne Zugang, für die sie die gewünschten Aufgaben erledigen Will ein interner Rechner z.B. Verbindung mit einem Rechner im Internet aufnehmen, nimmt er, der Proxy-Client, Kontakt mit dem Proxy-Server auf. Der Client wendet sich also nicht direkt an den "echten" Rechner, sondern kommuniziert über den Proxy-Server mit diesem. Für den Benutzer ist nicht zu unterscheiden, ob er es mit dem "echten" Server oder dem Proxy-Server zu tun hat. Umgekehrt nimmt der "echte" Server an, er arbeite mit dem Benutzer direkt, obwohl für ihn nur der Proxy-Server sichtbar ist.
Damit Proxy-Systeme effektiv arbeiten, sind sie in Kombination mit Verfahren einzusetzen, welche den Netzverkehr zwischen den Clients und den eigentlichen Servern auf IP-Ebene einschränken. Ansonsten ist es möglich, den Proxy-Server zu umgehen

Wozu braucht man Proxy-Dienste?

Proxy-Dienste werden eingesetzt, um vielen Benutzern den Zugriff auf das Internet zu ermöglichen und gleichzeitig ein bestimmtes Mass an Sicherheit beizubehalten. Der Benutzer erhält nur Zugriff mit Diensten (resp. Protokollen), für die auf dem Gateway entsprechende Proxies installiert sind.
Ein Proxy-System agiert somit als Kontrollstelle, da es nur jene Funktionen zulässt, welche in den installierten Proxy-Diensten realisiert sind. Ein Proxy- Prozess läuft völlig im Hintergrund ab, sodass die Verbindung ins Internet für den Benutzer scheinbar transparent ist. Daraus ergibt sich die einfachste Handhabung von Benutzerseite her.

Vorteile von Proxy-Diensten

abc Information GmbH
PO Box 130208
13601 Berlin
Germany

+49-700-ITBROKER
http://www.Broker.de
email:contact@Broker.de

Bieten Benutzern "direkten" Zugriff auf Internet-Dienste:

Proxy-Dienste gestatten Benutzern, von ihren eigenen Systemen aus auf Internet-Dienste zuzugreifen. Sie vermitteln den Benutzern den Eindruck, direkt mit den Internet-Diensten zu kommunizieren, obwohl im Hintergrund einige Prozesse ablaufen.

Bieten effektive Möglichkeiten zur Protokollierung:

Proxy-Server kennen die zu "vertretenden" Protokolle. Dadurch kann z.B. ein FTP-Proxy-Server nur die abgesetzten Kommandos protokollieren anstelle der gesamten Daten. Die Aufzeichnungen werden somit nicht so umfangreich und bleiben meist recht übersichtlich.

Nachteile von Proxy-Diensten

Software nicht immer leicht zu finden:

Es ist oft ein Problem, stabile Software für neue oder spezielle Dienste zu besorgen. Zudem vergeht meist viel Zeit, bis für einen neu eingeführten Dienst ein entsprechender Proxy-Server verfügbar ist.

Unter Umständen für jeden Dienst eigener Server nötig:

Es sind jedoch einige Produkte erhältlich, bei welchen mehrere Server integriert sind.

Clients und/oder Prozeduren müssen abgeändert werden:

Jede Änderung hat gewisse Nachteile. So lassen sich entsprechende Anweisungen auf einmal nicht mehr wie gewohnt verwenden und es wird eine zusätzliche Fehlerquelle geschaffen.

Proxies nicht für alle Dienste möglich:

Es gibt Dienste wie **talk**, welche komplizierte und verwickelte Interaktionen aufweisen. Für solche Dienste wird es wahrscheinlich nie einen Proxy-Dienst geben.

Kein Schutz vor Schwächen im Protokoll:

Proxy-Dienste überwachen oder ersetzen sicherheitskritische Protokolloperationen. Bei manchen Protokollen ist es aber sehr schwierig, diese kritischen Operationen ausfindig zu machen und diese zu überwachen. Dabei darf die Funktionsfähigkeit nicht eingeschränkt werden. X11 beispielsweise besitzt zahlreiche unsichere Operationen.

Wie funktionieren Proxies?

Die Funktionsweise eines Proxys ist vom Dienst abhängig. Manche Dienste funktionieren mit den Standardservern, bei anderen wird eine Anpassung der Clients oder Server nötig. Auf der Client-Seite unterscheidet man zwischen angepasster Client-Software und modifiziertem Verfahren für die Benutzer. Bei ersterer Alternative muss der Quellcode zur Verfügung stehen, ansonsten lassen sich keine Änderungen an den Clients anbringen. Beim modifizierten Verfahren kann der Benutzer die Standard-Client-Software verwenden, da der Proxy-Server in diesem Fall mit diesen zusammenarbeitet. Bei der Vorgehensweise jedoch wird vom Benutzer ein spezielles Vorgehen verlangt.

Verschiedene Arten von Proxy-Servern

Application-Level-Proxy

Application-Level-Proxy-Server kennen den Dienst und dessen Protokoll, für welchen sie eingesetzt werden. Sie werden meist in Verbindung mit modifizierten Verfahren verwendet, da sie zusätzlich benötigte Informationen mit Kenntnis des Anwendungsprotokolls oder aus den Benutzerdaten

abc Information GmbH
PO Box 130208
13601 Berlin
Germany

+49-700-ITBROKER
http://www.Broker.de
email:contact@Broker.de

beziehen können (z.B. Zieladresse des "echten" Servers). Sie interpretieren also das Protokoll des entsprechenden Dienstes.

Circuit-Level-Proxy

Circuit-Level-Proxy-Server interpretieren das Anwendungsprotokoll nicht. Sie benötigen vom Benutzer also zusätzliche Informationen zum Verbindungsaufbau und verwenden dazu angepasste Clients. Im Allgemeinen fungiert ein Circuit-Level-Proxy-Server quasi als Vermittlungsstelle für die entsprechenden Protokolle.

Intelligente Proxy-Server

Intelligente Proxy-Server verfügen über zusätzliche Funktionalität. Beispiel: Ein HTTP-Proxy-Server hält Daten in einem Cache, um Anfragen nach denselben Daten nicht erneut ins Internet leiten zu müssen.

4.8 Authentifikation

Authentifikation kann als *Beweisen der eigenen Identität* umschrieben werden. In diesem Abschnitt wird auf die Benutzer- und die Host-Host- Authentifikation eingegangen.

Benutzerauthentifikation

Passworte

Die Authentifikation mittels Passwort fällt in die Kategorie "Wissen". Sie hat den Vorteil, dass dazu keine besonderen Ausrüstungen gebraucht werden. Dass Wissen aber verraten oder mitgehört werden kann, ist ein Nachteil. Passworte zählen daher auch nicht zu den starken Authentifikations-Mechanismen.

Einmal-Passworte

Die Einmal-Passwort-Authentifikation verwendet, wie der Name es schon sagt, nur einmal das gleiche Passwort. Dies bewirkt eine effektive Verteidigung gegenüber Mithören oder Verrat. Es gibt verschiedene Einmal-Passwort-Verfahren. Beispielsweise das Verfahren mit einer Streichliste oder jenes, welches einen Taschenauthentifikator verwendet.
Beim ersteren ist der Benutzer im Besitze einer Liste von Passwörtern, welche er der Reihe nach anwendet. Nach Gebrauch wird das eben verwendete Passwort gestrichen. Für die nächste Sitzung ist dann das folgende Passwort zu gebrauchen.
Authentifikation mittels Taschenauthentifikator beruht auf einer internen Uhr und einem geheimen Schlüssel. Die aktuelle Zeit und der geheime Schlüssel werden durch eine Funktion miteinander verknüpft. Das Resultat dieser Verknüpfung dient dem Benutzer als Passwort, das sich von Minute zu Minute jeweils ändert. Der Host nimmt nun die Authentifikation anhand seiner eigenen Uhr und einer Kopie des geheimen Schlüssles vor. Stimmt das Resultat mit der Eingabe des Benutzers überein, so erhält dieser Zugang zum System.

abc Information GmbH
PO Box 130208
13601 Berlin
Germany

+49-700-ITBROKER
http://www.Broker.de
email:contact@Broker.de

Smart Cards - "Intelligente" Chipkarten

Chipkarten oder Smart Cards sind heute weitverbreitet. Sie verfügen meist über eine CPU, einen I/O-Kanal und einige Kilobytes ROM. Die Verwendung von Chipkarten ist sehr einfach und in der Öffentlichkeit oft angewandt. Chipkarten fallen in die Kategorie "Gegenstände" und werden mit der PIN um "Wissen" ergänzt. Ein Angreifer benötigt in diesem Fall wie beim Verfahren mit Einmal-Passwörtern die PIN (Persönliche Identifikationsnummer) oder Benutzerkennung sowie das entsprechende Gerät (Chipkarte oder Taschenauthentifikator), um einen Benutzer zu verkörpern.

Biometrik

Diese Methode verwendet benutzerspezifische Eigenschaften, um eine Authentifikation durchzuführen. Übliche Biometriken sind: Fingerabdruck, Stimmmuster oder Unterschrift. Der Vorteil von Biometriken ist, dass diese nicht verloren oder gestohlen werden können. Ein Nachteil dieses Verfahrens ist jedoch, dass spezielle Hardware benötigt wird.
Bei der Erkennung von Biometriken sind Grenzen gesetzt. So wird ein Benutzer niemals zwei 100%ig übereinstimmende Unterschriften produzieren können. Dies verlangt nach Toleranzen bei der Erkennung. Und, würden Sie einem Benutzer ein Login auf Ihrem System erlauben, der (nur) zu 85% dieser bestimmte Benutzer ist?

Host-Host-Authentifikation

Datennetz-basierte Authentifikation

Die überwiegende Form der Hos-Host-Authentifikation verlässt sich (noch) auf das Netz. Das Netz transportiert die Identität des Benutzers und verlässt sich zudem auf die Sicherheit im Netz. Bei der Datennetz-basierten Authentifikation gibt es zwei Varianten: adressbasiert und namensbasiert. Die adressbasierte Variante verlässt sich auf die numerische IP-Adresse. Die namensbasierte Variante überprüft nebst der Adresse auch noch den damit verknüpften Namen. Dies eröffnet einem Angreifer jedoch die Möglichkeit, einen Mechanismus, der IP-Adresse in Host-Namen umsetzt, zu unterwandern.

Kryptografische Verfahren

Kryptografische Verfahren werden in symmetrische und asymmetrische Verfahren unterteilt. Symmetrische Verfahren verwenden zur Verschlüsselung und Entschlüsselung jeweils an beiden Seiten (Sender und Empfänger) den gleichen geheimen Schlüssel. D.h. beide, Sender und Empfänger, müssen den geheimen Schlüssel kennen. Eines der bekanntesten symmetrischen Verfahren ist DES (Data Encryption Standard). Asymmetrische Verfahren verwenden zur Verschlüsselung und Entschlüsselung jeweils verschiedene Schlüssel. Dabei ist einer dieser Schlüssel öffentlich (bekannt) und der andere geheim. Die Verschlüsselung erfolgt mit dem öffentlichen Schlüssel. Die Entschlüsselung wird mit Hilfe des geheimen Schlüssels ermöglicht, d.h. nur der berechtigte Empfänger kann die Daten richtig entschlüsseln. Ein bekanntes asymmetrisches Chiffrierverfahren ist RSA (von Rivest, Shamir und Adleman).
Eine Anwendung, die sehr oft für die Verschlüsselung von E-Mail verwendet wird, ist PGP (Pretty Good Privacy).

abc Information GmbH
PO Box 130208
13601 Berlin
Germany

+49-700-ITBROKER
http://www.Broker.de
email:contact@Broker.de

4.9 PGP - Pretty Good Privacy

PGP ist ein Verschlüsselungsverfahren von Phillip Zimmermann. PGP ist ein Public-Key-Verfahren, das mit zwei Schlüsseln arbeitet: einem öffentlichen und einem privaten. Beide Schlüssel werden einmal gemeinsam generiert. Das Verfahren bietet folgende Möglichkeiten:

- Eine Nachricht wird so codiert, dass nur ein Empfänger, dessen Public Key man selbst besitzt, sie lesen kann.
- Es wird sichergestellt, dass eine Nachricht von einem bekannten Adressat stammt. Dazu muss der eigene Public Key dem Mail-Verteiler vorher bekanntgegeben worden sein.
- Durch die Verschlüsselung der Nachricht beim Absender wird eine mögliche Änderung auf dem Weg vom Absender zum Empfänger ausgeschlossen. Eine entsprechende Modifikation am chiffrierten Text würde das Programm sofort anzeigen.

Der öffentliche Schlüssel kann also als Adresse oder Telefonnummer angesehen werden. Dabei kann der Inhalt einer Nachricht verschiedenen Formats sein: nur Text, Grafik oder Programme.

Beispiel einer digitalen Unterschrift mit PGP:

```
-----BEGIN PGP SIGNATURE-----

Version: 3.3.3i

Charset: latin1


iQCVAgUBMP41DbCfd7bM70R9AQFOjQQAgjP7RkaLaDFeh0iHBKYH0iKqo+xAEMre

/4QizPhGRlUTCqaATg5bz72Gn2MGrCNFJ2LeFoDE5LDHsF3TWYd12Hp2ZTrLpLXD

cm9iCUJJRKO6aGuQRY27sJQiy00N04G691PniuFAh9oMuQeh/SakhqRYjWD8v7kC

zTXqqt4uhbc=

=JVWt

-----END PGP SIGNATURE-----
```

4.10 Was Firewalls nicht leisten

Firewalls sind ein starkes Werkzeug zum Schutz von Datennetzen. Dennoch bieten sie nur Schutz mit beschränkten Möglichkeiten. Es ist also auch wichtig zu wissen, was Firewalls nicht leisten resp. wo ihre

abc Information GmbH
PO Box 130208
13601 Berlin
Germany

+49-700-ITBROKER
http://www.Broker.de
email:contact@Broker.de

Grenzen liegen.
Wenn Sie von den üblichen Netzwerkschichten (Schichten 2-4) ausgehen, dann stellt der Firewall einen guten Schutz dar. Adressfälschung oder verbotene Dienste können relativ problemlos erkannt werden. Falls eine Attacke jedoch auf höherer Ebene ansetzt, muss der Firewall deren Paketinhalt durchsuchen. Es lohnt sich zu überlegen, ob z.B. der kritische X11-Dienst nicht besser von Anfang an zu sperren ist.
Ein bekanntes Beispiel ist auch *sendmail*. Beim Interpretieren des Inhalts von bestimmten Mail-Headern liess es sich manchmal zu übelgesinnten Aktionen verleiteten. Es verdeutlicht also gut, dass in Fällen, wo der Programmcode einer Anwendung schon fehlerhaft und unsicher ist, auch der beste Firewall als nutzlos erscheint.
Selbst wenn alle bekannten Schlupflöcher gestopft sind, können durch neue Anwendungen oder Dienste bereits wieder neue Schlupflöcher entstanden sein, die man noch gar nicht kennt

abc Information GmbH
PO Box 130208
13601 Berlin
Germany

+49-700-ITBROKER
http://www.Broker.de
email:contact@Broker.de

4.11 Produkte

Dieses Kapitel gibt eine Übersicht über einige auf dem Internet bekannten Firewall-Produkte.

Kommerzielle Firewall-Produkte

Produkt	Firma	Beschreibung
Actane Controller	Actane	Proxy
ANS Interlock	ANS	Proxy
BorderWare Firewall	Borderware	Proxy
Firewall-1	Checkpoint	Packet-Filter
AltaVista Firewall	DEC	Packet-Filter
Gauntlet Firewall	Trusted Information Systems	Proxy
GFX Internet Firewall	GFX	Proxy & Packet-Filter
IBM Firewall	IBM	Proxy
SecureIT	Milkyway Systems	Proxy
Raptor Firewall	AXENT	Proxy
NetGate Firewall	SmallWorks	Packet-Filter
SunScreen	Sun	Packet-Filter
InterGate	Vicomsoft	Packet-Filter

Freeware Firewall-Toolkits

Produkt	Beschreibung
tcpwrapper	Protokollierung und Filterung
portmapper	Protokollierung und Filterung
Socks	Proxy
TIS FWTK	Proxy

abc Information GmbH
PO Box 130208
13601 Berlin
Germany

+49-700-ITBROKER
http://www.Broker.de
email:contact@Broker.de

5 Intrusion Detection System (IDS) (Theorie)

Selbst das beste Sicherheitssytem kann nicht mit letzter Sicherheit ausschliessen, dass es jemanden gelingt, sich unerlaubt Zutritt in das zu schützende Computersystem zu verschaffen. Damit ein erfolgreicher Angriff möglichst schnell erkannt werden kann wurden Intrusion Detection Systeme (IDS) entwickelt. Solche Systeme sind in der Lage mögliche Systemeinbrüche durch Überwachen einer Vielzahl von Netzaktivitäten (Verkehrslast, Aktivitäten an bestimmten Ports, ...) zu erkennen.

5.1 Hauptaufgaben des IDS

Das Ziel der Intrusion Detection-Systeme ist die Erkennung von Sicherheitsverletzungen und eine angemessene, schnelle Reaktion darauf. Hauptaufgaben des IDS sind:

Missbrauchserkennung auf der Netzwerkebene

Erkennung von Angriffen (Denial of Service, SYN-Flooding, PING-Flooding, Pre Attack Probe (Information über Netzwerke, Angriffe über Portscan-Verfahren), Angriffe über World Wide Web-Dienste (Aktive X, Java,..))

Rechnersystem-basierte Angriffserkennung

Alle wichtigen Audit-Dateien auf dem System werden überwacht und ausgewertet. Bei Erkennung von Angriffen werden Alarme ausgelöst.

Erkennung von Anomalien

Erkennung von untypischen System- und Benutzerverhalten.

Intrusion Response

Bei Angriffen können verschiedene Gegenmassnahmen (z.B Alarme über E-Mail, SMS, Unterbrechung der Verbindung, Protokollierung des Angriffs) eingeleitet werden.

Ereignismeldungen

Alle Ereignismeldungen können nach verschiedenen Prioritäten (High, Medium, Low) zugeordnet und angezeigt werden.

Protokolierung / Berichterstattung

Es werden Log-Dateien geführt und nach verschiedenen Kriterien ausgewertet (grafische Auswertung).

5.2 Angriffsarten

Möglichkeiten der Signalerkennung

Um Angriffe erkennen zu können, muss man wissen wonach man suchen muss. Angreifer setzen häufig bestimmte Techniken ein, um Angriffe vorzubereiten. Diese Angriffe erfolgen nach bestimmten Mustern. Kennt man das Muster, Signatur genannt, des Angriffs ist eine Erkennung (Detection) des Angriffs möglich. Einige typische Auswirkungen, die einen Angriff kennzeichnen und deutliche Signaturen hinterlassen, sollen hier als Beispiele kurz vorgestellt werden. Viele dieser Signaturen können nur als Anzeichen für einen Angriff gewertet werden, wenn sie gehäuft oder in ungewöhnlichem Zusammenhang auftreten (ein Einlogversuch mit

abc Information GmbH
PO Box 130208
13601 Berlin
Germany

+49-700-ITBROKER
http://www.Broker.de
email:contact@Broker.de

falschem Passwort ist sicher kein Angriff, bei mehreren hundert Versuchen, ist es eindeutig einer). In den folgenden Unterkapiteln werden einige der häufigsten Angriffsarten beschrieben.

TCP-Portscan

Ein TCP-Portscan ermöglicht es festzustellen, welche TCP-basierten Dienste ein Zielrechner anbietet. Ein TCP-Verbindungsaufbau geschieht normalerweise in drei Schritten:

- Angreifer sendet SYN an zu testenden Port des Zielrechners
- Zielsystem antwortet mit SYN/ACK
- Angreifer sendet ACK an Zielsystem

Nun ist eine aktive Verbindung aufgebaut, die vom Zielsystem normalerweise protokolliert werden sollte, so dass sie leicht entdeckt werden kann. Verzichtet der Angreifer auf den dritten Schritt, weiss er trotzdem, dass dieser Dienst existiert. Der versuchte Verbindungsaufbau wird jedoch häufig nicht in die Log-Dateien übertragen. Programme wie Tcplog sind allerdings in der Lage, auch fehlgeschlagene Verbindungsaufbauten zu protokollieren. Werden häufige (fehlgeschlagene) Verbindungsaufbauten in relativ kurzer Zeit beobachtet, ist dies ein sicheres Zeichen für einen Angriff. Es gibt allerdings auch Portscans, die von Tcplog nicht erkannt werden.

UDP-Portscan

UDP ist ein verbindungsloses Protokoll und besitzt demnach keine Verbindungsaufbauprozedur, die Informationen über angebotene Dienste geben kann. Schickt der Angreifer jedoch UDP-Anfragen an einen inaktiven UDP-Port, so antwortet der Zielrechner mit "ICMP Port unreachable", so dass der Angreifer von den inaktiven auf die aktiven Ports schliessen kann. Die Vielzahl der Anfragen kann einem IDS als Signatur dienen.

Finger- und r-Dienste

Diese und einige weitere Dienste können Informationen über die Benutzer eines Systems liefern, die eventuell für einen Angriff genutzt werden können. Werden diese Dienste auffällig häufig benutzt, deutet dies auf einen bevorstehenden Angriff hin.

IP mit falschen Parametern

Diese Angriffsart wird häufig benutzt, um den Betrieb eines Rechners zu stören (Denial of Service). Die IP-Pakete sind allerdings an ihren falschen Parametern zu erkennen, so dass sie als eindeutige Signatur für einen Angriff dienen können. Beispielsweise stürzen viele Rechner aufgrund einer fehlerhaften Implementierung ab, wenn die Quell- und die Zieladresse sowie Quell- und Zielport übereinstimmen.

Überflutung

Dieser Angriff basiert darauf, einen Rechner oder Dienst dadurch auszuschalten, dass man ihn mit Daten "überflutet". Sendet man beispielsweise E-Mail in grossen Mengen an einen Rechner, so wird das Spool-Verzeichnis überlaufen und kann keine weiteren Daten entgegennehmen. Bei einigen Implementierungen kann es auch zu einem Totalabsturz des Rechners kommen. Diese Angriffsart funktioniert auch mit einigen anderen Diensten, als Indiz kann einem IDS der gehäufte Bedarf an Resourcen dienen.
Ist die Quelladresse eines SYN-Pakets (das normalerweise dem Verbindungsaufbau dient) unerreichbar, weil sie gefälscht ist, wird trotzdem Arbeitsspeicher für die gewünschte Verbindung reserviert. Wird die Anfrage in schneller Folge wiederholt, bindet der Angriff im Rechner zuviel Betriebsmittel und kann seine normalen Aufgaben nicht mehr im vollen Umfang bewältigen.

ICMP-Echo-Request

abc Information GmbH
PO Box 130208
13601 Berlin
Germany

+49-700-ITBROKER
http://www.Broker.de
email:contact@Broker.de

Ein ICMP-Echo-Request (ping) dient normalerweise dazu, die Erreichbarkeit bestimmter Rechner zu überprüfen. Übersteigen diese ICMP-Pakete eine bestimmte in der Spezifikation vorgesehene Maximalgrösse können sie aufgrund einer falschen Implementierung den Zielrechner zum Absturz bringen. Die ICMP-Echo-Request-Pakete können durch ein IDS analysiert werden, so dass auch dieser Angriff automatisch erkannt werden kann.
Mit ICMP-Echo-Requests ist es leicht möglich, die Netzinfrastruktur des Opfers zu untersuchen, indem man alle Netzadressen, die in dem Zielnetz vorkommen können, anspricht. Ping-Pakete an alle vorhandene und sogar an nicht vorhandene Rechner sind ein starkes Indiz für die Vorbereitung eines Angriffs.

Einkapselung/Tunneln

Fast jedes Transportprotokoll lässt es zu, dass in seinem Datenfeld bestimmte Daten untergebracht werden, die auf der Empfängerseite interpretiert werden können. So kann beispielsweise SMB über IP übertragen (getunnelt) werden. Natürlich kann auch IP in IP eingekapselt und so getunnelt werden. Firewalls überprüfen häufig die in Datenfeldern stehenden Informationen nicht. Bestimmte getunnelte Protokolle können jedoch durch Überwachung des Netzverkehrs aufgedeckt werden.

WWW-Spoofing

Der Betreiber eines WWW-Servers hat die Möglichkeit, als Angreifer dem Opfer ein Dokument mit ausschliesslich gefälschten URLs zuzuspielen. Der Benutzer kann diesen Angriff leicht entdecken, indem er die Statusanzeige des Browsers beobachtet. Auch ist es notwendig, dass der Benutzer die WWW-Seiten des Angreifers anwählt. Als Signatur können die für diesen Angriff notwendigen verlängerten URLs leicht von einer IDS entdeckt werden.

5.3 Vor- und Nachteile

Vor- und Nachteile der Signalerkennung

Vorteile sind:

- Häufig werden Angriffe auf Basis von Angriffsskripten durchgeführt, aus denen sich leicht Signaturen ableiten lassen, so dass eine hohe Entdeckungswahrscheinlichkeit gegeben ist.
- Stehen die Signaturen zur Verfügung, ist der Aufwand zur Installation und Wartung gering.

Nachteile sind:

- Der Erfolg hängt unmittelbar von der Güte der Signaturdatenbank ab. Existiert für einen Angriff keine Signatur, wird er nicht erkannt.
- Eine Anpassung der Signaturdatenbank an lokale Gegebenheiten oder eine Definition neuer Signaturen ist meist sehr aufwendig. Aufgrund der speziellen Anpassung sind Signaturdatenbanken nur beschränkt portabel.
- Die Signatur muss regelmässig an neu entdeckte Angriffssignaturen angepasst werden (ähnlich dem Vorgehen bei einem Virenscanner). Die neuen Angriffssignaturen sollten vom Hersteller zur Verfügung gestellt werden.

5.4 DoS-und DDoS-Attacken

DoS-Attacken und DDoS-Attacken

abc Information GmbH
PO Box 130208
13601 Berlin
Germany

+49-700-ITBROKER
http://www.Broker.de
email:contact@Broker.de

Seit den Anfängen des Internets existieren sie, die sog. "Denial-of-Service" (DoS) Angriffe, deren Ziel ist es, die Verfügbarkeit bestimmter Rechner und/oder Dienste einzuschränken. Meist wird bei dieser Form von Angriffen über das Internet versucht, durch das Ausnutzen von Schwachstellen in Betriebssystemen, Programmen und Diensten bzw. das Ausnutzen grundsätzlicher Entwurfsschwächen der verwendeten Netzwerkprotokolle, die angegriffenen Systeme zum Absturz zu bringen, oder derartig zu überlasten, dass diese Systeme ihre eigentliche Funktionalität nicht mehr erbringen können. Reine DoS-Angriffe haben also nicht das Ziel, vertrauliche Daten zu stehlen oder Benutzer-Authentisierungs-Mechanismen zu umgehen, sondern Diensteanbieter lahm zu legen.

DoS-Attacken

Als Denial-of-Service bezeichnet man Attacken, bei welchem ein Benutzer soviel Systemresourcen belegt, dass für die anderen Benutzer keine Ressourcen mehr zur Verfügung stehen. Dadurch kann ein Server oder eventuell nur ein Dienst, der auf dem Server läuft, empfindlich beeinträchtigt werden. Die Ressourcen können Prozesse, Plattenplatz oder die Auslastung der CPU sein. Es gibt zwei Arten von DoS-Attacken:

- Die erste zielt darauf ab, das System unbrauchbar zu machen. Das kann zum einen durch einen herbeigeführten Disk-Crash oder zum anderen durch Löschung wichtiger Kommandos erreicht werden.

- Die zweite Art überlastet irgendeine Ressource im System, um so den anderen Benutzern die Verwendung dieser Ressource unmöglich zu machen.

DDoS-Attacken

Ein neuer Trend in Denial-of-Service Angriffen wird seit Mitte 1999 beobachet und hat Anfang 2000 bei Angriffen auf Firmen, wie Yahoo, Buy.com, eBay, Amazon, Datek, ETrade und CNN für weltweites Aufsehen gesorgt.
Bei einem "Distributed Denial-of-Service"-Angriff wird im Vergleich zu einem Denial-of-Service-Angriff, wie der Name schon sagt, nicht nur von einem einzelnen Rechner attackiert, sondern von einer grossen Anzahl unterschiedlicher Systeme. Diese grossflächig verteilten Angreifer attackieren, zentral koordiniert, einzelne Systeme oder Netzwerke. Die Anzahl der an einem Angriff beteiligter Systeme wurde bereits beobachtet. Da die an einem Angriff beteiligte Rechner oft über grosse Teile des Internets verteilt sind, spricht man deshalb von einem sogenannten Distributed Denial-of-Service (DDoS) Angriff. Momentan sind unzählige solcher Tools unter Namen wie "Trible Flood Network", "Stacheldraht", "trinoo", "Shaft" oder "MStream" im Internet aufgetaucht.

5.5 Beispielaufbau

abc Information GmbH
PO Box 130208
13601 Berlin
Germany

+49-700-ITBROKER
http://www.Broker.de
email:contact@Broker.de

5.6 IDS Produkte

Dieses Kapitel gibt eine Übersicht über einige auf dem Internet bekannten IDS-Produkte.

Kommerzielle Auditing-Produkte

Produkt	Firma	Beschreibung
eTrust	Computer Associates	Netzwerk Analyzer (Windows)
EnGarde T-Sight	En Garde Systems	Netzwerk Analyzer (Windows)
ICEcap Security Suite	Network ICE	Netzwerk Analyzer, Host- und Netzwerkbasierend (Windows)
NetRanger	Cisco	Netzwerk basierendes IDS mit Sensor und Director (Unix)
Dragon Intrusion Detection	NSW	Netzwerk basierendes IDS mit Sensor, Squire und Server (Unix)
Centrax 2.3	CyberSafe	Hostbasiert, Netzwerk, Netzwerkknoten intrusion detection (Unix+Win)
Intruder Alert 3.0 und NetProwler	Symantec	Netzwerk basierendes IDS mit Interface, Agent, Manager (Unix+Win)
Real Secure 5.0	ISS	Netzwerk basierendes IDS mit Console und Sensor (Unix+Win)
CyberCop Monitor	Network Associates	Hostbasierende IDS (Unix+Windows)

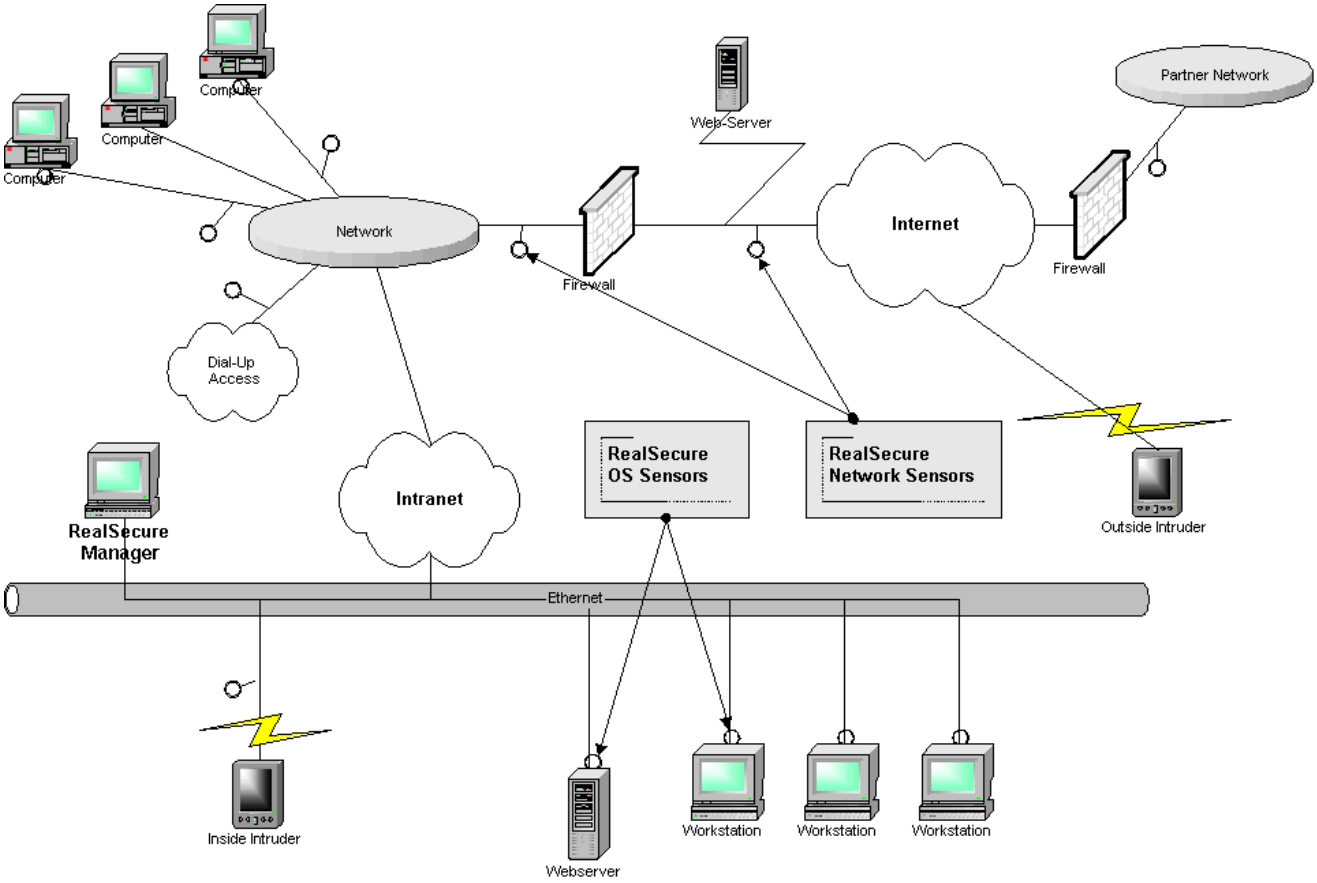
Freeware Auditing-Toolkits

Produkt	Beschreibung
TAMU	Schwachstellenanalyse
COPS	Schwachstellenanalyse
SATAN	Netzschwachstellenanalyse
Crack	Passwort-Cracker

abc Information GmbH
PO Box 130208
13601 Berlin
Germany

+49-700-ITBROKER
http://www.Broker.de
email:contact@Broker.de

6 Beispiel (Theorie)



abc Information GmbH
PO Box 130208
13601 Berlin
Germany

+49-700-ITBROKER
http://www.Broker.de
email:contact@Broker.de