Thema: Sicherheit in offenen Netzen

- Gefahren, Angriffe, Risiken
- Analysen der Bedrohung
- Sicherheitsdienste
- Sicherheitsmechanismen
- Firewall - Systeme

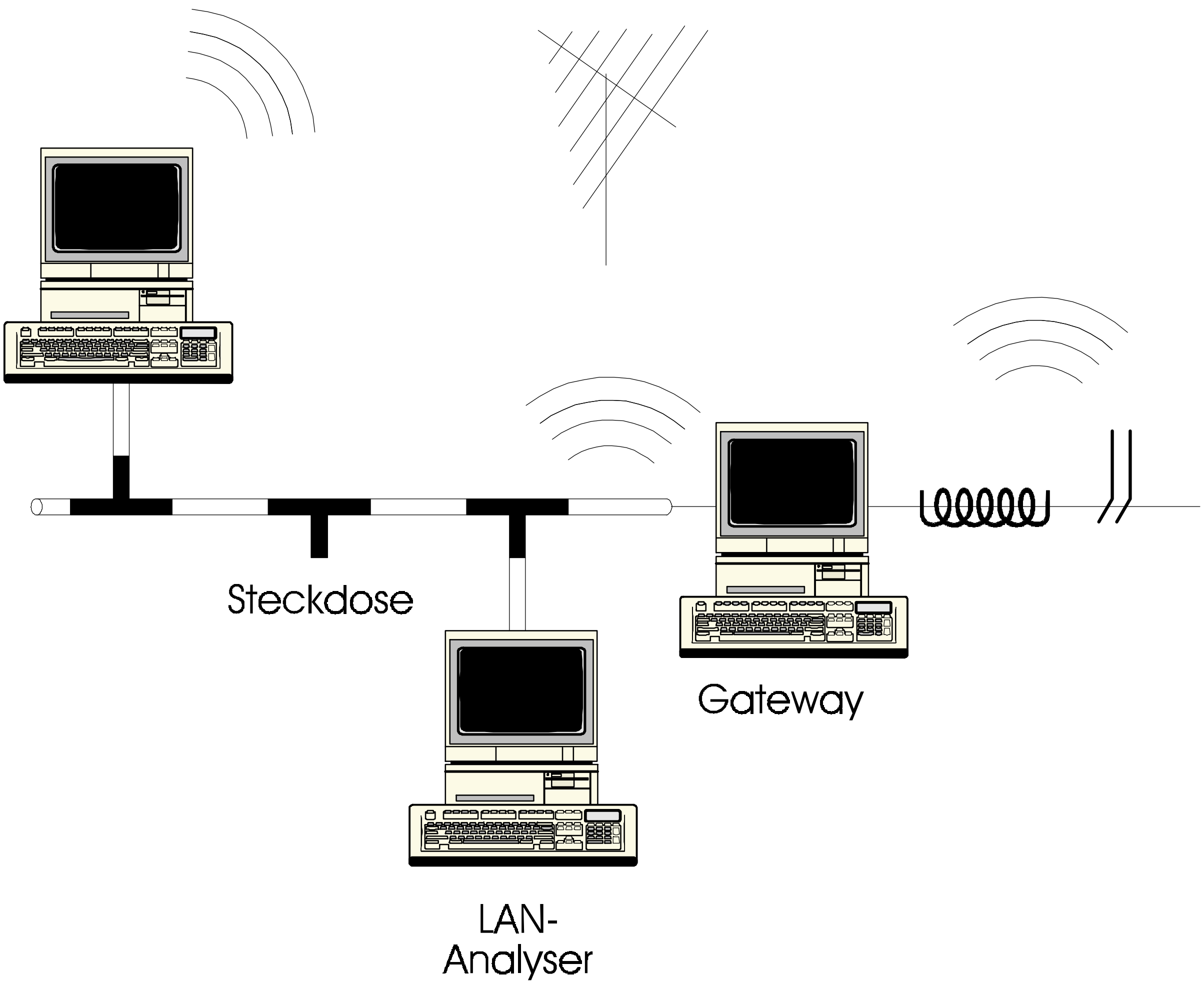
Gefahren, Angriffe, Risiken

passive Angriffe

➔ keine Verfälschung, aber Bedrohung der Vertraulichkeit der Daten

Bsp.: Ausnutzung der elektromagnetischen Abstrahlung; akustische Analysen von Typenraddruckern; Klemmen und Induktionsschleifen; Antennen zum Abhören drahtloser Verbindungen; beugen von Lichtwellenleitern; flexible Kommunikations-Infrastruktur von Gebäuden

- Abhören der Vermittlungsinformation
  Teilnehmer, Verbindung, Leistungen
- Abhören der Benutzerinformationen
  Inhalt
- Verkehrsflußanalyse
  wann, in welchem Umfang und Struktur der Kommunikation



aktive Angriffe

➔ mit Hilfe von Zwischengeräten, welche die Übertragungsprotokolle verstehen und bedienen können. Eine kurzzeitige Zwischenspeicherung und Manipulation der Nachrichten ist möglich, ohne das dies von den befugten Stationen bemerkt wird.

- Wiederholung oder Verzögerung einer Information
  wesentliche Beeinflußung des Empfangsprozesses, d.h. es kann dazu führen, daß Aktionen verhindert oder wiederholt ausgelöst werden
- Einfügen, Modifikation und Löschen bestimmter Daten
  jegliche Softwaremanipulation, wie z.B. das Einpflanzen von Viren
- Vortäuschen einer falschen Identität
  Angriff des Benutzers, indem er sich für jemand anderen ausgibt
- Nutzung fremder Betriebsmittel
- Boykott des Kommunikationssystems
  blockieren von Anschlüssen
  herabsetzen der Durchsatzrate durch unnötige Übertragungen
  physikalische Störungen
- Aktive Angriffe auf gespeicherte und archivierte Informationen
- Modifikation von Rechten und Attributen

zufällige Gefährdungen

dazu gehören z.B.: Rauschen, Übertragungsfehler oder Leitungsunterbrechungen

Analyse der Bedrohung

Folgende Fragen sollte man sich bei der Bedrohungsanalyse stellen, da nicht alle im vorangegangenen Abschnitt genannten Gefahren gleichzeitig und jedem System drohen. So ist es möglich den Sicherheitsaufwand auf das notwendige einzuschränken.

1. Frage: Welche Objekte müssen geschützt werden?
   Welche gespeicherten Informationen?
   Welche übertragenen Informationen?
   Welche Betriebsmittel?
2. Frage: Wovor müssen die Objekte geschützt werden?
   Vor welchen passiven Angriffen?
   Vor welchen aktiven Angriffen?
   Vor welchen zufälligen Gefahren?
   Welche Schäden ergeben sich durch Fehlbedienung, Sabotage oder Boykott?
3. Frage: Wer sind die potentiellen Angreifer?
   Frage 3.1.: Wer kommt als Innentäter in Frage?
   - Welche autorisierten Personen?
   - Über welche Prozesse und Peripheriegeräte?
   - Wie werden Wartungstechniker kontrolliert?
   - Welche nicht-autorisierten Personen und Prozesse sind möglich?
   - Kommen Handwerker, Putzpersonal oder andere als Angreifer in Frage?

   Frage 3.2.: Wer kommt beim entfernten Kommunikationspartner als Innentäter in Frage?
   - siehe Frage 3.1.
   - Bestehen Gefahren durch „falsche“ Kommunikationspartner?

   Frage 3.3.: Wer kommt im Transitsystem (Gateways, Netzknoten, Übertragungsstrecken) als Täter in Frage?
   - Welche autorisierten und nicht-autorisierten Personen?

   Frage 3.4.: Wer kommt beim Hersteller der verwendeten Hard- und Software als Gefahrenursache in Frage?
4. Frage: Mit welchen Mitteln werden die Angriffe ausgeführt?
   Ausprobieren?
   Schwachstellen nutzen?
   Software-Manipulation?
   Hardware-Manipulation?
   Automatisch generierte Vorgänge?

5. Frage: Wie groß ist für den Angreifer jeweils der Aufwand, um die Angriffe durchzuführen?
   Wieviel Zeit benötigt er für den Angriff?
   Wie hoch sind die Kosten?
   Welches und wieviel Personal benötigt er?
   Welches Know-how ist erforderlich?
6. Frage: Wie groß ist das Risiko für einen Angreifer, daß der Angriff erkannt wird?
   Kann der Angriff entdeckt werden?
   Kann der Angreifer erkannt werden?
   Kann der Angreifer gefaßt werden?
   Wie hoch wird das voraussichtliche Strafmaß sein, falls der Angreifer gefaßt wird?
7. Frage: Wie groß ist der Nutzen für einen Angreifer?
   Ist der gewonnene Vorteil für ihn direkt verwertbar?
   Wieviel ist der gewonnene Vorteil für ihn direkt wert?
   Kann er den Vorteil verkaufen?
   Wenn er den gewonnenen Vorteil verkaufen kann, wieviel ist er wert?
   Kann er den gewonnenen Vorteil zur Erpressung verwenden?
8. Frage: Wie hoch ist der mögliche Schaden?
   Gering?
   Gravierend?
   Existenzgefährdend?
9. Frage: Gibt es spezielle Bedrohungen?

Sicherheitsdienste

Die aufgezeigten Gefahren verlangen wirkungsvolle Sicherheitsmaßnahmen. Diese werden im ersten Schritt Technologie-unabhängig formuliert, um flexibel zu bleiben. Diese Technologie-unabhängigen Sicherheitsmaßnahmen sind die Sicherheitsdienste, welche modulartig miteinander kombiniert werden können.

Vertaulichkeit

Vertraulichkeit ist der wichtigste Sicherheitsdienst. Er dient dem Schutz vor passiven Angriffen. Da der Kommunikationsdienst verbindungsorientiert oder verbindungslos erfolgen kann, muß es entsprechende Dienste geben.

Verhinderung der Verkehrsflußanalyse

Dieser Sicherheitsdienst soll vor Informationsgewinn auf Grund einer Verkehrsflußanalyse schützen.

Erkennung der Datenunversehrtheit
Dieser Dienst sorgt für eine Überprüfung der Daten. Dabei wird das Löschen, Verändern, Einfügen, Wiederholen, Vertauschen, Verzögern aller Dateneinheiten erkannt. D.h., die Erkennung auf Datenunversehrtheit bezieht sich auf den gesamten Datenstrom, wenn eine verbindungsorientierte Kommunikation stattfindet.

Authentifikation des Kommunikationspartners
Ein weiterer Angriff besteht darin, daß der Kommunikationspartner eine falsche Identität vortäuscht. Diese „Maskerade“ soll durch die Authentifikation des Kommunikationspartners, den Nachweis seiner Identität verhindert werden.
Es wird zwischen einseitiger und gegenseitiger Authentifikation unterschieden.

Authentifikation des Ursprungs der Daten
Es ist ebenfalls notwendig, sicherzustellen, daß die Daten, die nach dem Authentifikationsprozeß ausgetauscht werden, wirklich von dem echten Kommunikationspartner stammen.

Zugangs- und Zugriffskontrolle
Dieser Sicherheitsdienst schützt vor dem unbefugten oder unsachgemäßen Nutzen von Beriebsmitteln.

Urhebernachweis
Die „Authentifikation des Ursprungs der Daten“ ermöglicht dem Empfänger nur zu überprüfen, ob die Daten von dem angenommenen Ursprung stammen, während der Urhebernachweis den Empfänger in die Lage versetzt, objektiv und für Dritte nachvollziehbar nachzuweisen, daß die Daten von einem bestimmten Urheber erzeugt wurden.

Empfängernachweis
Er schützt den Sender einer Nachricht davor, daß der Empfänger abstreitet, diese Nachricht mit genau dem ihm übermittelten Inhalt empfangen zu haben.

Aufrechterhaltung des Betriebs
Sicherheitsdienst, der einen unterbrechungsfreien Betrieb gewährleistet, Sabotage- und Boykottaktionen erkennt und umgeht.

Sicherheitsmechanismen

Verschlüsselung

Eine geeignete Methode, Vertraulichkeit zu erreichen, ist die Verschlüsselung. Entsprechend den Ergebnissen der Bedrohungsanalyse wird entschieden, auf welche Teile sich die Vertraulichkeit beziehen muß, und welche Daten somit zu verschlüsseln sind.

Verhinderung einer Verkehrsflußanalyse

Durch Senden von Fülldaten in den Sendepausen zwischen den Nutzdaten wird ein Nachrichtenstrom erzeugt, dessen Struktur nicht mehr dem Strom der Nutzdaten entspricht. Die Verschlüsselung wird in gleicher Weise auf Nutz- und Fülldaten angewendet. Außerdem dürfen zwischen den Nutz- und Fülldaten keine Lücken entstehen, da sonst ein Rückschluß auf die Struktur möglich ist.
Die vollständige Verhinderung einer Verkehrsflußanalyse ist nur auf synchronen, durchgeschalteten Verbindungen möglich.
→ Probleme bei Paketvermittlungsnetzen !!!

Erkennung der Datenunversehrtheit

Es werden ähnliche Mechanismen eingesetzt wie zur Datensicherung während der Datenübertragung.
Der Nachricht werden Prüfsummen angehängt, an denen der Empfänger den korrekten Empfang erkennt. Die Ansprüche sind aber höher, da es dem Angreifer nicht möglich sein soll, die Nachricht oder die Prüfsumme zu ändern oder auszutauschen. Als Schutz müssen Laufnummern, Zeitstempel, Zufallszahlen oder andere Informationen hinzugefügt werden, die mit in die Berechnung der Prüfsumme eingehen.

Authentifikation der Kommunikationspartner

1. Einfache Authentifikation

   Passwortmethode

   Jede Instanz wird mit einem Paßwort versehen, das bei jeder Kommunikation geprüft wird. Die Stärke beruht auf der Geheimhaltung des Paßwortes. Wenn eine Verschlüsselung verwendet wird, muß das Paßwort bei jeder Übertragung anders verschlüsselt und nur einmal gültig sein.

   Rückrufmethode

   Um die Teilnehmernummer des Anrufers mit Hilfe des Netzdienstes zu überprüfen, ruft der Angerufene den Anrufer zurück. Dadurch erfolgt eine einseitige Authentifikation.

2. Starke Verfahren mit asymmetrischen Algorithmen

2.1. Einseitige Authentifikation

One Pass

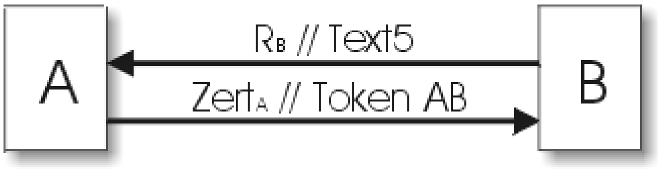
In einem einzigen Schritt weist der Sender A einer Nachricht spontan seine Identität nach. Er sendet das Token AB. Die Einmaligkeit und Zeitrichtigkeit werden über einen Zeitstempel oder eine Reihenfolgenummer gewährleistet. Außerdem kann der Empfänger B überprüfen, daß die Authentifikation für ihn erfolgt ist.

Token AB=TVP_A // B // Text2 // d_A(TVP_A // B // Text1)
TVP = Time Variant Parameter (Zeitstempel oder Reihenfolgenummer)
d_A(M) = elektronische Unterschrift von A unter die Nachricht M

Two Pass

Auch hier wird nur die Identität des Teilnehmers A nachgewiesen, aber erst auf Anforderung durch den Teilnehmer B und nach Vorgabe einer Zufallszahl R_B durch den Prüfer, die die Einmaligkeit und Zeitrichtigkeit gewährleisten soll.

Token AB=R_A // B // R_B // Text2 // d_A(R_A // B // R_B // Text1)



2.2. Gegenseitige Authentifikation

Two Pass

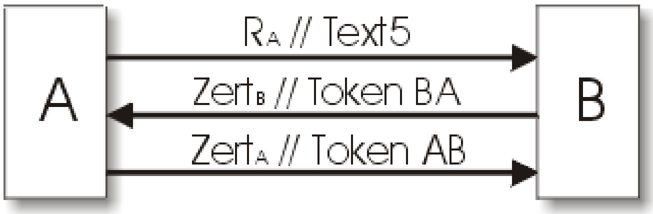
Das Token AB das von A an B gesendet wird, ist identisch mit dem der einseitigen Authentifikation, das Token BA in der Gegenrichtung ist symmetrisch aufgebaut.

Token AB=TVP_A // B // Text2 // d_A(TVP_A // B // Text1)
Token BA=TVP_B // A // Text4 // d_B(TVP_B // A // Text3)

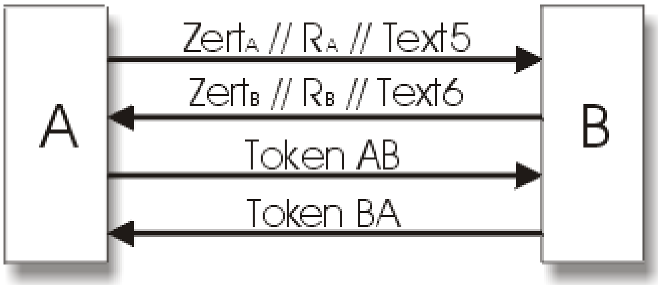
Three Pass

In diesem Fall wird die Einmaligkeit und Zeitrichtigkeit durch gegenseitig vorgelegte Zufallszahlen R_A und R_B gewährleistet.

Token BA=R_B // A // R_A // Text2 // d_B(R_B // A // R_A // Text1)
Token AB=R_A // B // R_B // Text4 // d_A(R_A // B // R_B // Text3)



Two Pass Parallel



<u>Authentifikation des Ursprungs der Daten</u>

Erfolgt ähnlich wie die Erkennung der Datenunversehrtheit, wobei aber die elektronische Unterschrift eingesetzt werden muß, da sonst kein objektiver

Nachweis möglich ist. Das Verfahren besteht daher aus der Berechnung des Hashcodes über die Daten mit anschließender elektronischer Unterschrift unter den Hashcode. Außerdem müssen den Daten zusätzliche Parameter hinzugefügt werden, damit Wiederholungen und Verzögerungen erkannt werden.

Firewall-Systeme

Bevor man sich an die Realisierung von Firewall-Lösungen begibt, sollte man sich mit einigen grundlegenden Strategien für den Aufbau von Firewalls und die Durchsetzung von Sicherheitsmaßnahmen verdeutlichen. Diese beruhen nicht auf großartigen Erkenntnissen, sondern beinhalten einfache Konzepte.

1. Konzepte:

Minimale Zugriffsrechte

Im Grunde besagt das Prinzip der minimalen Zugriffsrechte, das jede Einheit - ob Benutzer, Verwalter, Programm, System etc. - gerade so viele Zugriffsrechte erhält, wie für die Erfüllung der anstehenden Aufgaben erforderlich sind. Es verkleinert die Angriffsfläche.

Mehrschichtige Verteidigung

Sofern nur ein geringer Mehraufwand damit verbunden ist, sollte man immer zusätzliche Abwehrmaßnahmen ergreifen.
Bsp.:

- zwei gleichkonfigurierte Paketfilter nacheinander
- wenn man nicht möchte, daß elektronische Post an einen Rechner geschickt wird, sollte man nicht nur Pakete herausfiltern, sondern auch das Mail-Programm löschen.

Die Passierstelle

Eine Passierstelle zwingt den Angreifer dazu, einen schmalen Pfad zu benutzen,den man überwachen und kontrollieren kann. Im Zusammenhang mit Netzwerksicherheit stellt der Firewall zwischen einem Unternehmen und dem Internet eine solche Passierstell dar, sofern dort die einzige Verbindung besteht.

Das schwächste Glied

Eine Kette ist nur so stark wie ihr schwächstes Glied und eine Mauer wie ihre schwächste Stelle. Geschickte Angreifer versuchen, diese Stelle ausfindig zu machen. Man sollte sich dieser Stelle bewußt sein, da es immer eine schwächste Stelle gibt.

Sollte es in einem Netzwerk keine Passierstelle geben, so muß man davon ausgehen, daß sehr viele Verbindungen existieren, von denen sich wiederum viele als sehr schwach erweisen können.

Fehlersicherheit

Das Prinzip Fehlersicherheit bedeutet, daß wenn einmal ein Fehler in einem System auftritt, dieses den Angreifern den Zugriff verweigert, anstatt ihnen dadurch den Zugang zu ermöglichen. Dies kann dazu führen, daß berechtigte Benutzer ebenfalls ausgeschlossen werden, was aber für gewöhnlich akzeptiert wird.

Die einschränkende Grundhaltung:
„Alles ist verboten, was nicht ausdrücklich erlaubt ist"
➔ fehlersicherer Standpunkt: alles Unbekannte ist möglicherweise gefährlich
jedes Programm wird einer Analyse unterzogen und zur Benutzung freigegeben, falls ungefährlich

Die freizügige Grundhaltung:
„Alles ist erlaubt, was nicht ausdrücklich verboten ist"
➔ kein fehlersicherer Standpunkt: unbekannte Probleme tauchen in der Liste der Schutzmaßnahmen nicht auf; aber sie bestehen, bis sie (meistens durch entstandenen Schaden) entdeckt werden

Allumfassende Beteiligung

Es ist notwendig, daß sich alle Benutzer am aktiven Schutz beteiligen. Nur ein einziger Benutzer, der sich aus den Sicherheitsmechanismen ausklinken kann genügt, die ganze Verteidigung zum Einsturz zu bringen. Dazu ist es nötig, den Betroffenen die Lage begreiflich zu machen.

Vielfalt der Verteidigung

Dieses Prinzip basiert auf der Idee, das verschiedene Systeme im Sinne einer mehrschichtigen Verteidigung einzusetzen sind. Allerdings müssen dafür mehr Komplexität und höhere Kosten in Kauf genommen werden.
Oft kommt man dann zu dem Schluß, das es mehr Nachteile als Vorteile gibt, und das der potentielle Nutzen dazu nicht im Vergleich steht.

Einfachheit

Komplexe Programme enthalten mehr Fehler, wobei jeder von ihnen zu einer Sicherheitslücke werden kann. Selbst wenn Fehler an sich nicht zu Sicherheitsproblemen führen, akzeptieren Anwender jedoch beinahe jedes Verhalten eines Systems, sobald sie es als unberechenbar kennengelernt haben.

Einige Definitionen zu Firewalls:

Firewall
Eine oder mehrere Komponenten, die den Zugriff zwischen einem geschützten Netz und dem Internet oder zwischen beliebigen anderen Netzen beschränken.

Host
Ein Computersystem, das an ein Netz angeschlossen ist.

Bastion Host
Ein Computersystem, das besonders geschützt werden muß, da es für Angriffe prädestiniert ist - in der Regel, weil es dem Internet offensteht und eine wichtige Anlaufstelle für Benutzer interner Netze ist.

Dual-Homed-Host
Ein für verschiedene Aufgaben ausgelegtes Computersystem mit mindestens zwei Netzschnittstellen.

Paket
Die elementare Kommunikationseinheit im Internet.

Paketfilterung
Die Aktion, bei der ein Gerät den Datenfluß von und zu einem Netz selektiv steuert. Dies geschieht meist nach Regeln, die festlegen, welche Pakettypen zugelassen sin und welche aufgehalten werden (z.B. Pakete von oder zu einer bestimmten IP-Adresse).

Grenznetz
Ein Netz, das zwischen ein geschütztes und ein externes Netz eingefügt wird, um eine weitere Schutzschicht zu schaffen. Ein Grenznetz wird auch manchmal DMZ genannt, was für De-Militarisierte-Zone steht.

Proxy-Server
Ein Programm, das stellvertretend für interne Clients mit externen Servern kommuniziert. Proxy-Clients unterhalten sich mit Proxy-Servern, die bestätigte Client-Anfragen an die eigentlichen Server weiterleiten und die Antworten zurück an die Clients übermitteln.

2. Paketfilter und Proxy-Dienste - Zwei für den Aufbau von Firewalls wesentliche Konzepte

Paketfilterung

Ein normaler Router sieht sich einfach die Zieladresse eines jeden Paketes an und wählt den besten ihm bekannten Weg aus. Weiß der Router nicht wie er das Paket in Richtung seines Bestimmungsortes senden kann, so gibt er das Paket an den Ursprungsort zurück.

Paketfilter-Systeme routen Pakete zwischen internen und externen Rechnern, gehen dabei aber selektiv vor. Der in einem Paketfilter-Firewall verwendete Routertyp wird Überwachungsrouter genannt. Er routet oder blockiert Pakete entsprechend der Sicherheitspolitik des Standorts.

Beispiel Überwachungsrouter zu programmieren:

- Blockieren aller Verbindungen von Systemen außerhalb des internen Netzes. Lediglich eintreffende SMTP-Verbindungen passieren, um E-Mail empfangen zu können.

Proxy-Dienste

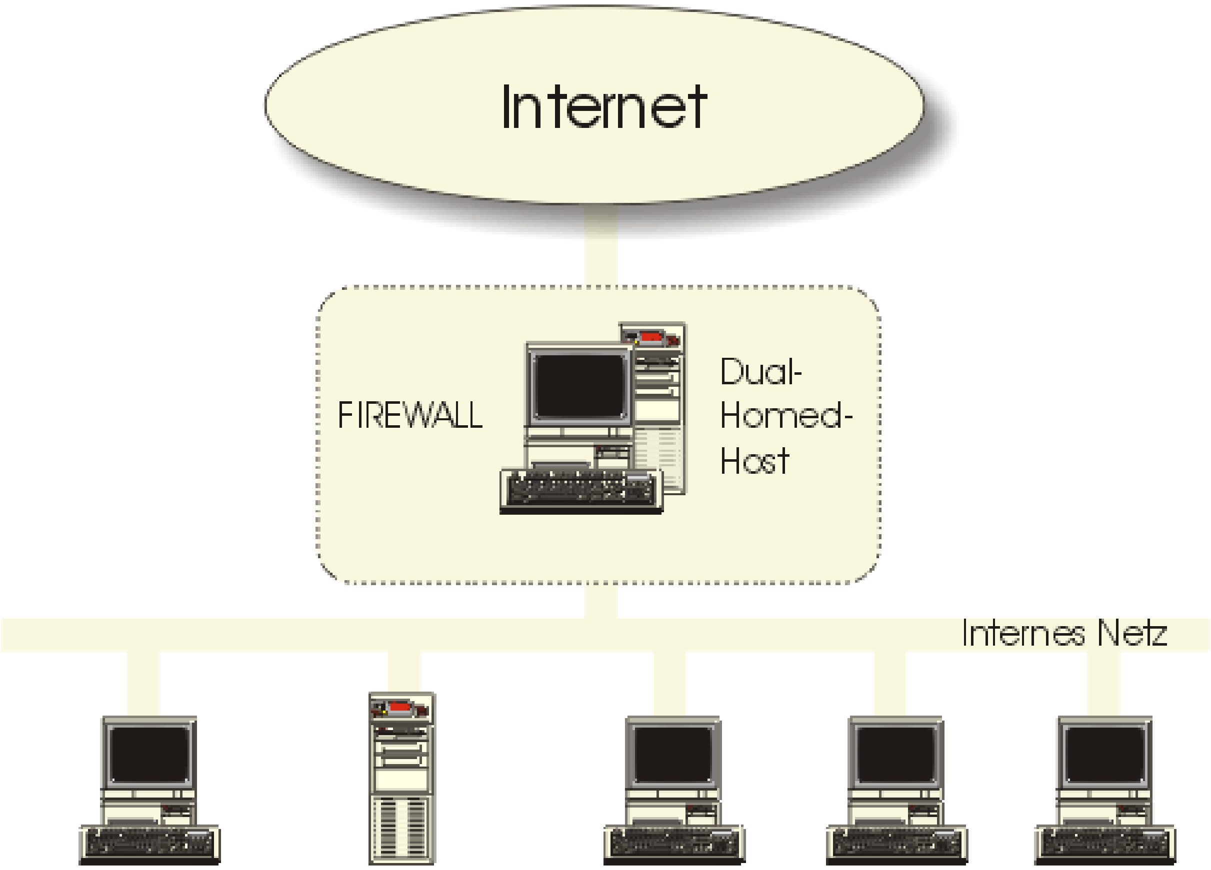
Proxy-Dienste sind spezielle Anwendungs- oder Serverprogramme, die auf einem Firewall-Host ablaufen. Sie befinden sich zwischen dem Benutzer im internen Netz und einem Dienst im Internet. Benutzer und Dienst verständigen sich über einen Proxy, der die gestellten Anfragen an die eigentlichen Dienste weiterleitet, sofern sie sich mit der Sicherheitspolitik des Standorts vereinbar sind.
Ein Proxy-Dienst ist eine Software-Lösung und nicht an sich schon eine Firewall-Architektur.

➔ Die „richtige Lösung“ für den Aufbau eines Firewalls besteht selten aus einer einzigen Technik. Die meisten Firewalls verwenden eine Kombination aus Proxy-Diensten und Paketfilterung.

3. Architekturen für Firewalls

Architektur mit Dual-Homed-Host

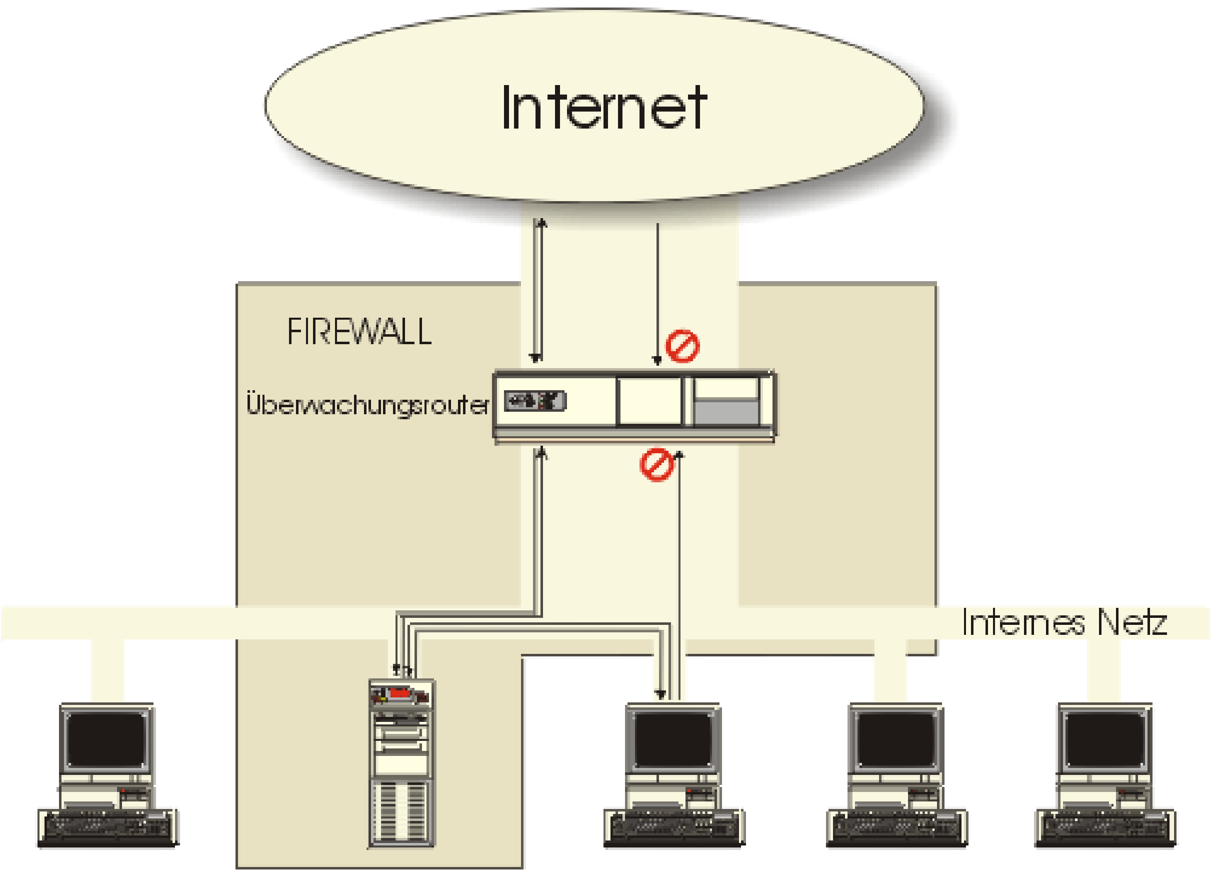
Eine Architektur mit Dual-Homed-Host wird um den Dual-Homed-Host herum aufgebaut. Ein solcher Host ist als Router zwischen den Netzen einsetzbar, an den die Schnittstellen angeschlossen sind, da er IP-Pakete von Netz zu Netz routen kann. Für die Firewall-Architektur jedoch deaktivieret man diese Routing-Funktion, so daß Systeme innerhalb und Systeme außerhalb des Firewalls jeweils mit dem Dual-Homed-Host, aber nicht direkt miteinander kommunizieren können. Ein Dual-Homed-Host kann Dienste nur anbieten, indem er Proxies einsetzt oder Benutzer direkt bei sich einloggen läßt. Für die meisten Benutzer ist es unbequem, einen solchen Host zu nutzen, indem sie sich bei ihm einloggen.



<u>Architektur mit überwachtem Host</u>

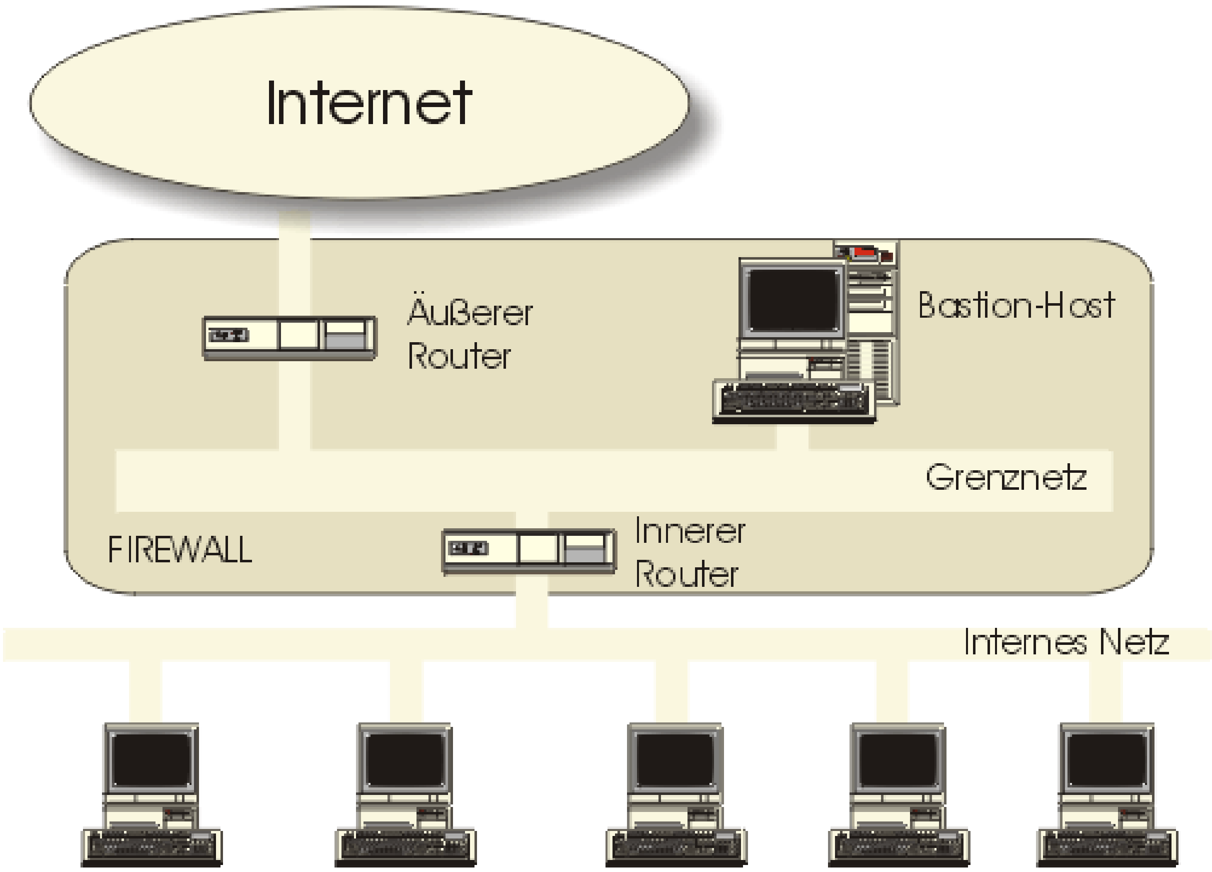
Eine Architektur mit Dual-Homed-Host bietet Dienste von einem Rechner an, der an mehrere Netze angeschlossen ist, wobei das Routing abgeschaltet ist. Die Architektur mit überwachtem Host dagegen bietet Dienste von einem Rechner an, der nur an das interne Netz angeschlossen ist, wobei ein getrennter Router verwendet wird. Bei dieser Architektur wird Sicherheit in erster Linie über Paketfilterung gewährleistet.

Der Bastion-Host ist das einzige System, zu dem Rechner aus dem Internet Verbindungen aufbauen können.



Architektur mit überwachtem Teilnetz

Die Architektur mit überwachtem Teilnetz erweitert die Architektur mit überwachtem Host um eine Sicherheitsschicht, und zwar ein Grenznetz, das das innere Netz weiter vom Internet isoliert.
Indem man den Bastion-Host in einem Grenznetz isoliert, schwächt man die Auswirkungen eines Einbruchs in den Bastion-Host ab.



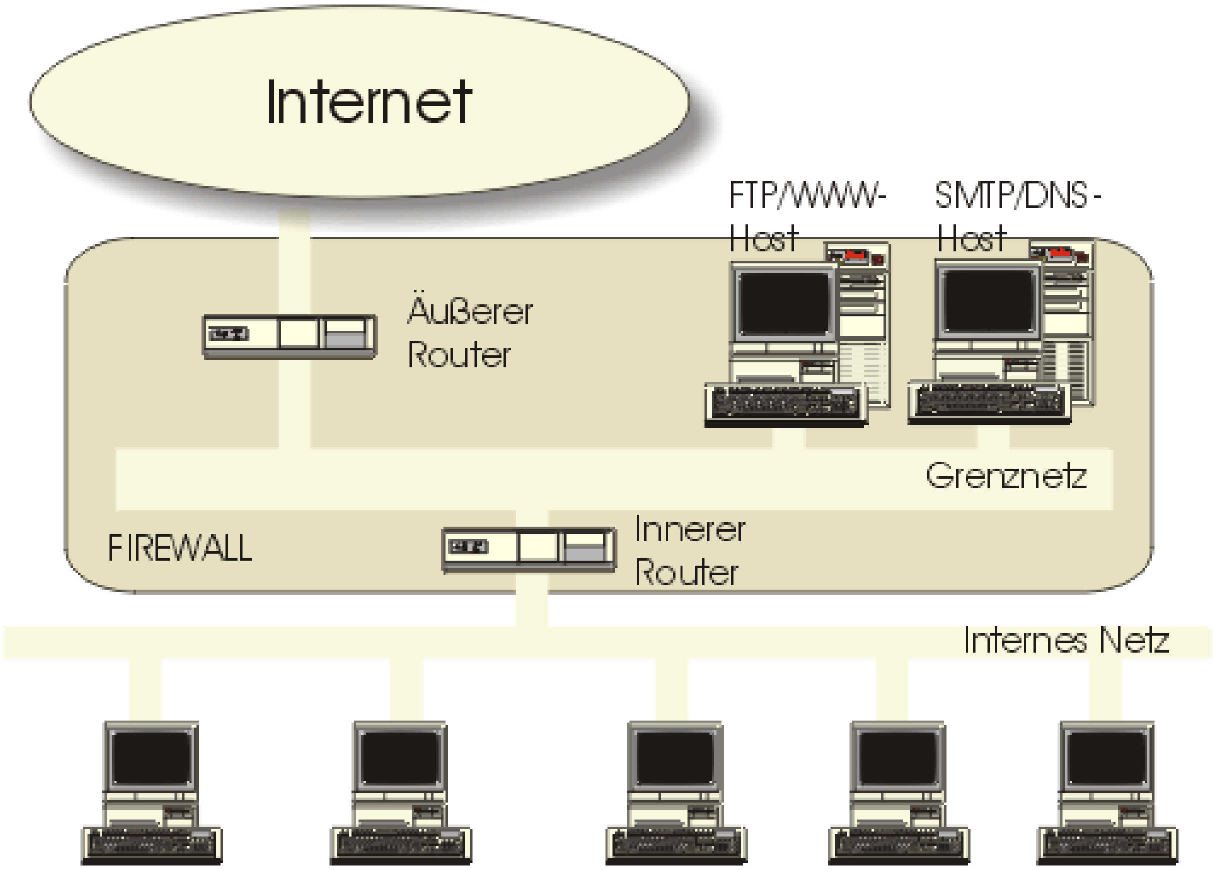
Varianten von Firewall-Architekturen:

- Mehrere Bastion-Hosts

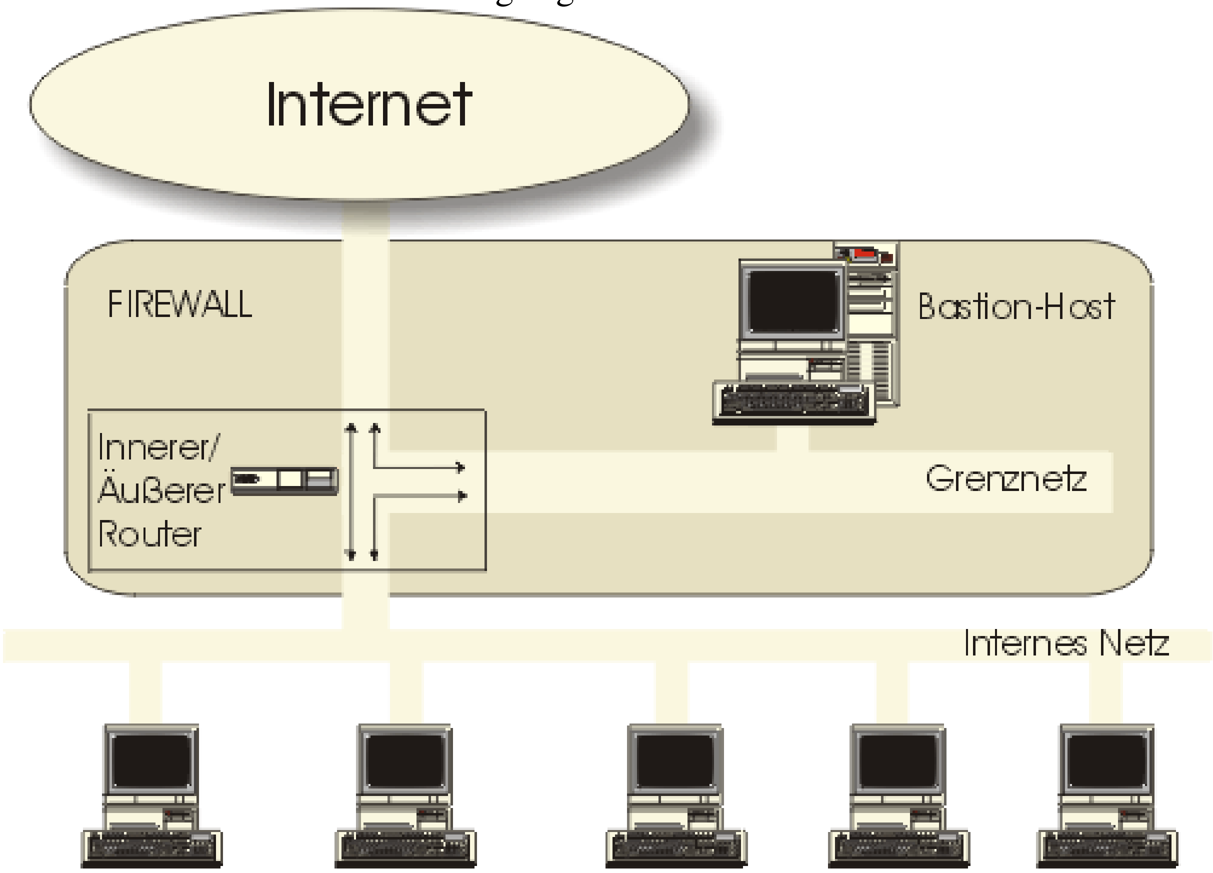
Durch den Einsatz mehrerer Bastion Hosts ist es möglich, z.B. die Leistung zu steigern, Daten getrennt zu halten oder Redundanz zu schaffen.

- Zusammenlegen des inneren und äußeren Routers

Wenn man den inneren und den äußeren Router zusammenlegt, gibt es immer noch ein Grenznetz (an der einen Routerschnittstelle) und einen Anschluß an das interne Netz (an einer anderen Router-Schnittstelle). Ein Teil des Verkehrs fließt direkt zwischen dem internen Netz und dem Internet. Das ist der Verkehr, den die für den Router definierten Regeln zur Paketfilterung zulassen. Ein anderer Teil erfolgt zwischen dem Grenznetz und dem Internet oder dem Grenznetz und dem internen Betz. Dieser Verkehr wird von Proxies gehandhabt.



oben: Architektur mit zwei Bastion-Hosts
unten: Architektur mit zusammengelegtem inneren und äußeren Router



Weitere Varianten:

- Zusammenlegen des Bastion-Hosts und des äußeren Routers
- Mehrere äußere Router
- Mehrere Grenznetze

Gefahren:

- Zusammenlegen des Bastion-Hosts und des inneren Routers
  Bastion-Host und äußerer Router haben unterschiedliche Schutzfunktionen; sie ergänzen einander, unterstützen einander jedoch nicht direkt. Der innere Router fungiert teilweise als Absicherung der beiden.
  Eine der wichtigsten Aufgaben des Grenznetzes besteht darin, zu verhindern, daß der Bastion-Host internen Verkehr ausspionieren kann. Wenn man den Bastion-Host in den inneren Router verlagern würde, wäre er in der Lage den gesamten inneren Verkehr zu verfolgen.
- Mehrere innere Router
  Die grundlegende Gefahr besteht darin, daß die Routing-Software an einenem internen System entscheidet, daß der schnellste Weg zu einem anderen internen System über das Grenznetz führt. Wenn man Glück hat, funktioniert dieser Ansatz einfach deshalb nicht, weil er durch die Paketfilterung auf einem der Router blockiert wird. Wenn man Pech hat, ist er erfolgreich und der Verlehr mit vertraulichen und rein internen Daten fließt über das Grenznetz. Dort kann er von jemandem mitgehört werden, dem es gelingt, in den Bastion Host einzudringen.

Literatur, Quellenangaben:

Informationssicherheit in Datennetzen
Ch. Ruhland
DATACOM-Verlag, 1993

Sichere Netze
M. Wojcicki
Hanser Verlag, 1991

Einrichten von Internet
FIREWALLS
D.B. Chapman, E.-D. Zwicky
O`Reilly Intern. Thomson Verlag, 1996