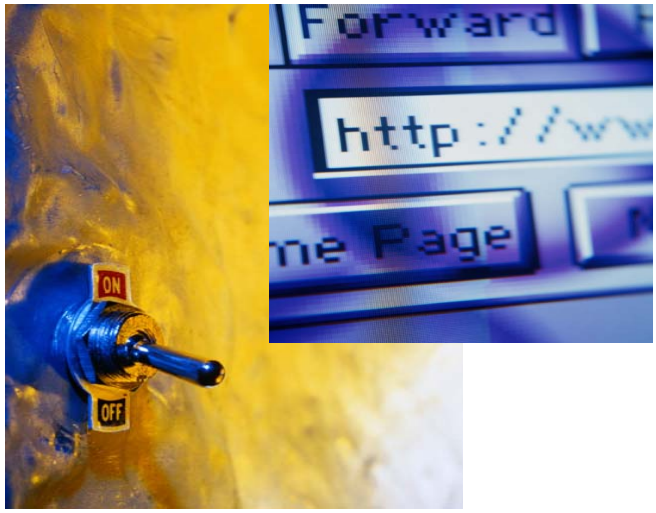
Firewalls in Kürze

Kleine Psychologie der Netzwerk (Un-)Sicherheit.



Fürchtet sich Ihr Unternehmen vor Angriffen aus dem Internet? Wenn ja, dann sind Sie nicht allein. Es gibt viele User, die das Internet nicht verwenden, aus der Angst heraus, einem Hackerangriff zum Opfer zu fallen. Die Zeitschrift Infosecurity News hat kürzlich in einer Umfrage festgestellt, dass 25% aller Unternehmen bereits nicht autorisierte Zugriffe aus dem Internet auf Ihr Netzwerk festgestellt haben.

Auch das Mysterium der Computer Hacker hält manche Unternehmen vom Gebrauch des Internets ab. Hacking ist eine neue Art der Kriminalität. Aber was verursacht den Medienhype um dieses Thema und was macht Computer Hacker so mysteriös? In der Hauptsache ist es einfach ein Mangel an fundamentalem Verständnis für diese Technologie. Dazu kommt noch die Komplexität der Netzwerksicherheit insgesamt. Andererseits kann kaum Unternehmen heute noch ohne das Internet effektiv arbeiten.

Viele Unternehmen ignorieren das Thema einfach. Leider ignoriert so manche Geschäftsleitung auch gleich sämtliche Sicherheitsvorschläge Ihres Netzwerkadministrators. Das geht immer so lange gut, bis der Schaden entstanden ist. Der immer gleiche Kommentar lautet dann: „Wir haben bereits Schritte unternommen, dass so etwas nie wieder passieren kann“. Für diese Unternehmen ist die Informationssicherheit teuer geworden. Zu den Kosten, die durch den Angriff entstanden sind, kommt nun noch zusätzlich der Aufwand für die Gegenmassnahmen, Häufig nimmt auch der Ruf des Unternehmens Schaden, so dass weitere Kosten durch entsprechende Marketing Massnahmen entstehen.

Letztendlich ist ein Netzwerk nur so sicher, wie es angewandt und gewartet wird. Das heisst, wenn Sie mit dem Internet arbeiten, müssen Sie sich schützen. Am besten funktioniert das mit einer Firewall. Im folgenden haben wir einige wichtige Informationen zu Firewalls zusammengestellt.

Was ist eigentlich eine Firewall?

Eine Firewall ist eine Sicherheitseinrichtung. Es gibt sie als Hardware oder als Software. Die Firewall separiert zwei oder mehr Netzwerke, die auf unterschiedlichen Sicherheitsniveaus operieren. Die Firewall hält dabei nicht berechtige Zugreifer aus externen Netzen wie z.B. dem Internet fern. Gleichzeitig haben die User im internen Netzwerk Zugriff auf externe Ressourcen.

Telefon 0811/5541-0 • Telefax 0811/5541-499
E-Mail: techsupp@black-box.de • Internet: www.black-box.de

Warum benötigt man eine Firewall?

Sobald ein Server oder Host an ein externes Netzwerk angeschlossen sind, ist die Gefahr eines Angriffs von aussen gross. Dieser kann böswillig oder zufällig, durch Hacker oder andere Eindringlinge erfolgen. Wie der Zugriff erfolgt, kann variieren. Absichern sollten Sie sich aber gegen:

- **Social Engineering:** Ein Hacker gibt vor ein autorisierter User zu sein. Der Hacker kommt dabei in den Besitz eines Zugangsgerät von einem autorisierten User. Möglich ist auch das berechtigte User Ihre Passworte und/oder potentielle Sicherheitslöscher im Netzwerk verraten haben.

- **Lauschangriff:** Hacker hören ein Netzwerk ab und kommen so in den Besitz von Passwörtern, Dateien und Nachrichten.

- **War Dialling:** Hacker wählen zufällige Telefonnummern, in der Hoffnung ein Modem zu finden, dass Ihren Anruf beantwortet und den Zugang in das angeschlossene Netzwerk ermöglicht.

- **Hostangriff:** Ein Server oder Host, der nicht ordnungsgemäß aufgesetzt ist oder dessen Betriebssystem nicht korrekt verwaltet wurde, ist ein leichtes Opfer für Hacker.

- **Passwort Vermutung:** Systemadministratoren können diese Angriffe verhindern, indem sie Regeln und Anforderungen an die Passwörter stellen, die schwer zu vermuten sind z.B. alphanumerische Passwörter.

- **Denial-of-Service (DoS):** Sobald eine TCP-Verbindung startet, setzt der Hacker sein SYN-Identifizierungssignal in den TCP-Header. Anschliessend macht der Hacker seine IP Adresse unerreichbar, sodass der Server die Verbindung nicht komplettieren kann. Dabei reserviert er aber im System noch Ressourcen für diese Adresse. Wenn eine solche Verbindung aufgebaut wird, sollte der Server den nicht berechtigten Client erkennen und den angeforderten Dienst verweigern.

- **Protokoll-basierende Angriffe:** Hacker verwenden sogenannte Port-Scanning Programme und suchen damit nach UDP- oder TCP Ports. Sobald ein aktiver Port gefunden ist, kann er dazu verwendet werden, Schwachstellen in Protokollen zu finden die wiederum Zugriff auf Ihr internes Netzwerk ermöglichen.

Welche Arten von Firewalls gibt es ?

Firewalls können grundsächlich auf zwei Arten unterschieden werden:

- Auf Netzwerkebene oder

- Auf Anwendungsebene

Telefon 0811/5541-0 • Telefax 0811/5541-499
E-Mail: techsupp@black-box.de • Internet: www.black-box.de

Firewalls auf Netzwerkebene

Auf der Netzwerkebene gibt es zwei verschiedene Kategorien: Paket-Filterung und Schaltkreisweg (Circuit Gateways).

Firewalls mit Paket Filterung
arbeiten auf der Netzwerkschicht und überprüfen die Header der IP-Pakete. Anhand dieser Header entscheiden Sie, ob sie ein Paket weiterleiten oder nicht weiterleiten. Dabei gibt es 3 Unterkategorien zur Paket-Filterung

- **Statische Paket Filterung:** Die Sicherheitsregeln werden manuell konfiguriert und können auch nur manuell durch den Systemadministrator geändert werden.
- **Dynamische Paket Filterung:** Die Firewall trifft Ihre Entscheidungen anhand der Aktivität des verbundenen Routers. Beginnt zum Beispiel ein User im internen Netzwerk eine FTP-Sitzung, dann leitet die Firewall die FTP-Pakete durch. Dynamische Firewalls erstellen Schalttabellen, um die Sicherheitsregeln der jeweiligen Aktivität anzupassen.
- **Sateful Inspection:** Dies ist eine Technik, bei der die Firewall jedes Paket genau überprüft, bevor sie ihre Sicherheitsentscheidung trifft. Auch hier werden zur Anpassung der Sicherheitsregeln Schalttabellen erstellt.

Firewalls mit Circuit Gateways
arbeiten ähnlich wie Firewalls mit Paket Filterung. Sie treffen Ihre Entscheidungen anhand der IP-Adressen. Circuit Gateways arbeiten auf der Transportschicht und überprüfen in der Hauptsache die Aktivität der TCP-Ports. Sie können zwar nicht den Datenverkehr selbst überprüfen, wohl aber eine direkte Verbindung zwischen zwei Netzwerken verhindern.

Firewalls auf Anwendungsebene

Dieses sind gewöhnlich Proxy-Server, die auf der Applikationsebene arbeiten und die Pakete analysieren, idem sie nach FTP oder http Kommandos suchen. Diese Kommandos verwenden Sie als Basis für Ihre Sicherheitsentscheidung.
Firewalls auf Anwendungsebene erlauben eine direkte Verbindung zwischen zwei Netzwerken erst dann, wenn der gesamt Datenverkehr geloggt und überprüft ist.
Die Firewall kann hier auch als Network Address Translator (NAT) agieren, der Netzwerk IP-Adressen verbirgt. Sobald ein Paket eine Applikation durchlaufen hat, verschleiert der Proxy-Server den Ursprung der Adresse und externe User haben keine Möglichkeit die IP-Adressen aufzuspüren.

Implementierung

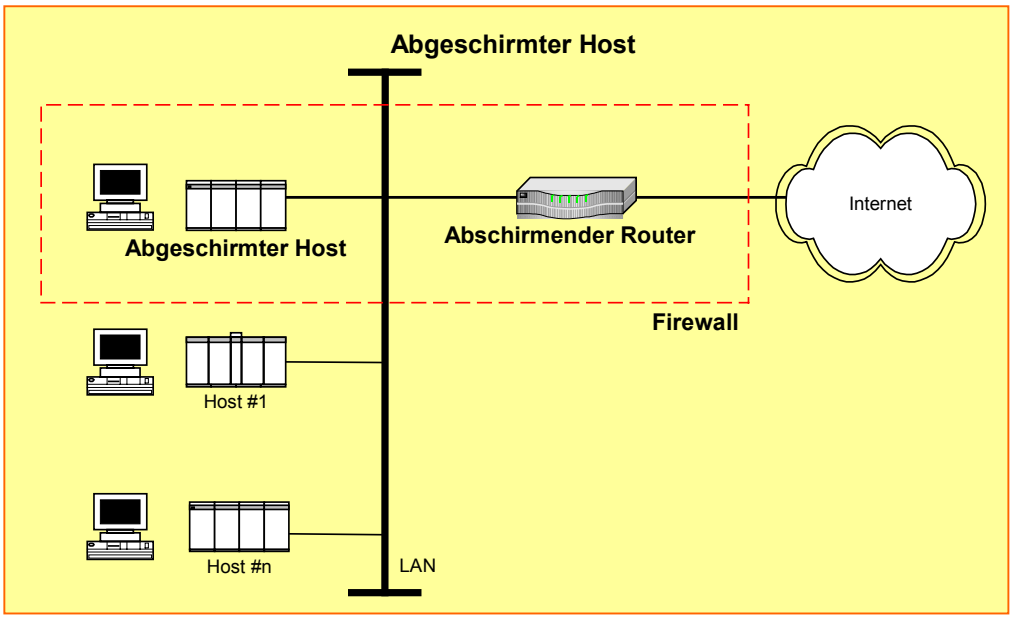
Hardware Architekturen

Hier gibt es eine Vielzahl. Die wichtigsten sind:

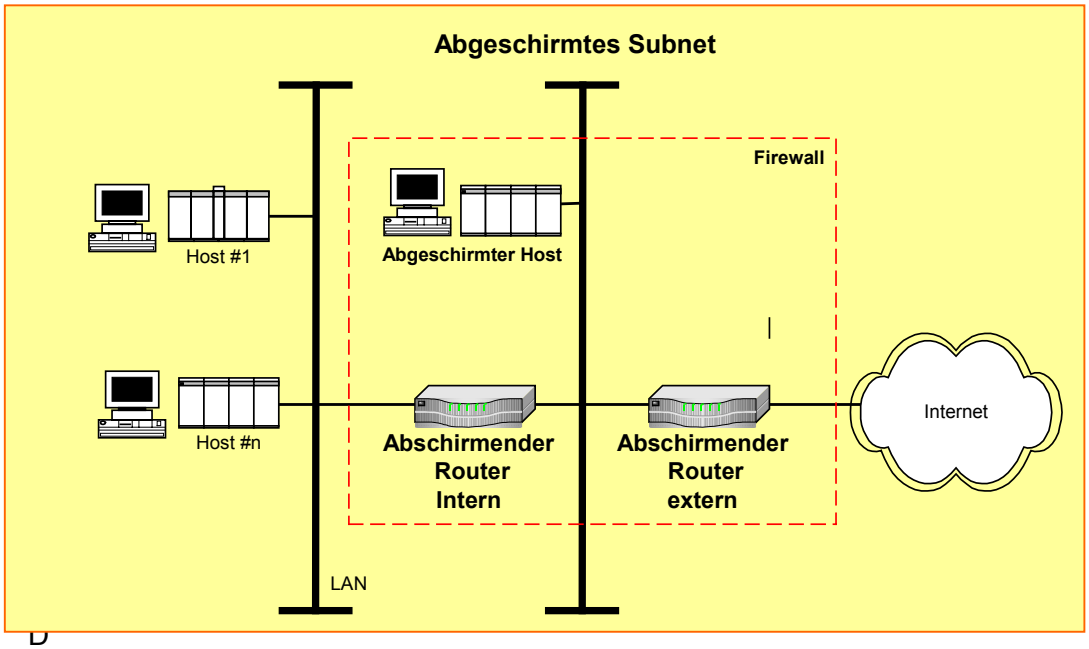
- Abgeschirmter Host
- Abgeschirmtes Subnet
- Dual-homed Host

Telefon 0811/5541-0 • Telefax 0811/5541-499
E-Mail: techsupp@black-box.de • Internet: www.black-box.de

Eine **abgeschirmte Host-**Architektur verwendet einen Abschirmungs-Router zwischen dem Haupt-LAN und Internet. Dieser verhindert das Datenverkehr von einem gewöhnlichen Host direkt ins Internet gelangt. Lediglich der abgeschirmte Host im Haupt-LAN kann von einem Internet-User gesehen werden. Dieser abgeschirmte Host ist dann das einzige Gerät, dass von Hacker und Eindringlingen angegriffen werden kann. Jeder andere Host im Haupt-LAN erhält den Internet-Zugang ausschliesslich über den abgeschirmten Host.



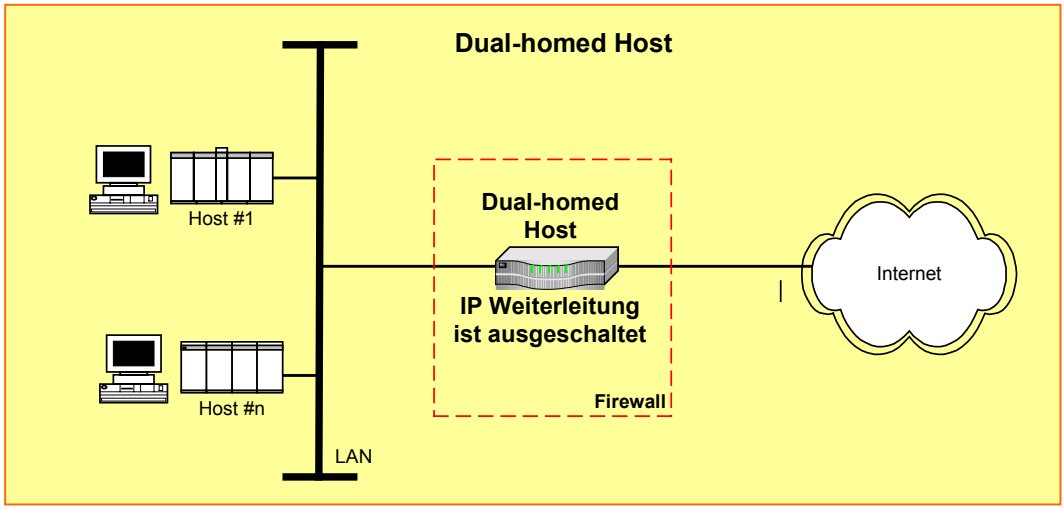
Die **abgeschirmte Subnet**-Architektur funktioniert ähnlich wie der abgeschirmte Host, weil auch Sie keine direkte Verbindung eines Hosts zum Internet erlaubt.
Sie verwendet aber zwischen dem LAN-Segment und dem abgeschirmten Host noch einen weiteren Router zur Abschirmung. Dadurch erhält man ein zusätzliches LAN-Segment auch Perimeter Network genannt, dass ein Eindringlich erst passieren muss, bevor er Zugriff ins Haupt-LAN erhält.



D

Telefon 0811/5541-0 • Telefax 0811/5541-499
E-Mail: techsupp@black-box.de • Internet: www.black-box.de

ie **Dual-home Host** Architektur verbietet Host/Internet-Verbindungen über einen Proxy-Dienst im Host komplett. Daher scheint diese Architektur momentan die sicherste zu sein. Sollte jedoch diese Firewall versagen, haben Eindringlinge Zugang zum kompletten Haupt-LAN.



Auf **Software**

basierende Lösungen gibt es viele im Handel. Sie sind für kleine Unternehmen mit knappen Budgets oder private Internet-User mit einem xDSL- oder Modemzugang ideal geeignet.
Die typische Software-Firewall erlaubt dem End-User nur einen bestimmten Programmtyp, um als LAN- oder Internetserver zu agieren. Sie erlauben zum Beispiel den Netzwerk-Zugang externer User nur über spezielle TCP oder UDP-Ports. Die Firewall kann auch so konfiguriert werden, dass sie Alarm schlägt, wenn sie unbekannte Pakete aufspürt. In diesem Fall kann man von Alarm zu Alarm selbst entscheiden, ob das Paket passieren darf oder nicht.

Die BLACK BOX Lösung zum Schutz Ihrer Daten: Firewall B5000

Telefon 0811/5541-0 • Telefax 0811/5541-499
E-Mail: techsupp@black-box.de • Internet: www.black-box.de

Einige Tipps wie Sie Ihren PC zuhause absichern können

Auch ohne Firewall sollten sie auf jeden Fall die folgenden Punkte beachten:

- Wenn Sie sich über ein Modem ins Internet einwählen, trennen Sie auf jeden Fall am Ende der Sitzung die Verbindung.
- Wenn Sie eine xDSL oder Festverbindung haben, die immer aktiv ist, dann schalten Sie Ihren PC aus, wenn sie ihn nicht brauchen.
- Überwachen Sie Ihren PC und achten Sie auf Ihre aktivierten Dienste. Schalten Sie File-Sharing nur dann ein, wenn Sie es benötigen und setzen Sie in jedem Fall ein Passwort.
- Nutzen Sie Anti-Viren Software und halten Sie sie auf dem neuesten Stand! Eine veraltete Anti-Viren-Software nutzt gar nichts.

Trotz dieser Sicherheitsmassnahmen empfehlen wir Ihnen dringend auch daheim eine Firewall-Software zu verwenden. Die Software ist nicht teuer. Es gibt sogar ein Firewall-Paket namens ZoneAlarm, dass man sich unter www.zonelabs.com herunterladen kann. Dieses Programm ist für den privaten nicht kommerziellen Gebrauch kostenlos.
Unsere Experten empfehlen auch die Filterung der ausgehenden Aktivitäten. Dieser sind jedoch im privaten Gebrauch Grenzen gesetzt. Den Filter für ausgehende Aktivitäten zu konfigurieren, ist etwas kompliziert und eine falsch konfigurierte Firewall ist schlimmer als keinerlei Firewall.
Ist Ihr Virenschutz auf dem neuesten Stand, ist die Filterung ausgehender Aktivität weniger dringlich.
Auch die Firewall selbst sollte in kurzen Abständen immer wieder auf den neuesten Stand gebracht werden. Alle Hersteller von Firewalls für den privaten Gebrauch, bieten auf Ihren Websites dafür Updates an. Nutzen Sie diesen Service zu Ihrem Vorteil.

Hilfe im Web

Wenn Sie noch mehr über Sicherheit im Web wissen möchten, dann bieten die folgenden Seiten nützliche Informationen für Sie:

www.mcaffee.de www.secinf.de

www.grc.com www.networkice.com

www.happyhacker.org

Oder wenden Sie sich an den FREE TECH SUPPORT von BLACK BOX. Unsere Experten informieren und beraten Sie gerne.

Telefon 0811/5541-0 • Telefax 0811/5541-499
E-Mail: techsupp@black-box.de • Internet: www.black-box.de