Planung einer Firewall

Von der Theorie zur Praxis

Rainer W. Gerling, München*

Es mag sie ja noch geben, die Manager und EDV-Leiter, die den Kauf einer Firewall gleichsetzen mit dem Kauf einer Textverarbeitung oder eines PCs. Leider ist es nicht so einfach. Eine Firewall kann man kaufen, in Betrieb nehmen und vergessen. Eine Firewall muss sorgfältig geplant werden. Diese Planung ist das A und O des erfolgreichen Betriebes einer Firewall. Dieser Aufsatz soll einen Leitfaden geben, was bei der erfolgreichen Planung einer Firewall zu beachten ist.

1 Firewalltypen

Firewalltypen gibt es viele. In dem vorliegenden Artikel geht es um die einfachste Variante einer Firewall: ein Paketfilter. Gerade die guten aktuellen Statefull Inspection Firewalls bieten einen vernünftigen Kompromiss zwischen Kosten, erreichbarem Sicherheitsniveau und Handhabbarkeit. Eine Hochsicherheitslösung stellt dies aber nicht dar, für viele Firmen auch nicht erforderlich. Aber ein vernünftiger Grundschutz sollte trotzdem von jedermann realisiert werden. Eine Paketfilter-Firewall kontrolliert ausschließlich über Rechneradressen und Dienste (Protokolle). So kann z.B. das ftp-Protokoll zu einem Rechner oder einer Rechnergruppe erlaubt oder verboten werden.

Ein Application Level Gateway, ein anderer Firewalltyp, bietet detaillierte Kontrollmöglichkeiten auf Anwendungsebene, da auf dem Firewallrechner für jeden Dienst (Protokoll) ein spezielles Programm läuft, das das Anwendungsprotokoll versteht und analysiert. Mit einem Application Level Gateway kann dann z.B. beim ftp-Protokoll genau unterschieden werden, ob Dateien geholt (get) oder verschickt werden (put). Und man kann, wenn es für die Sicherheitspolitik notwendig ist, das „get“ erlauben und das „put“ verbieten.

Application Level Gateways sind auf gleicher Hardware deutlich langsamer als Paketfilter Firewalls. Deshalb ist ein Application Level Gateway bei gegebener Leistung teurer als eine Paketfilter Firewall. Welche Variante für ein Unternehmen sinnvoll ist, kann nur nach einer detaillierten Analyse des Schutzbedarfes und der erforderlichen Kommunikationsflüsse entschieden werden. Sehr häufig wird man sich für eine Statefull Inspection Paketfilterlösung entscheiden, da sie einen vernünftigen Kompromiss darstellt.

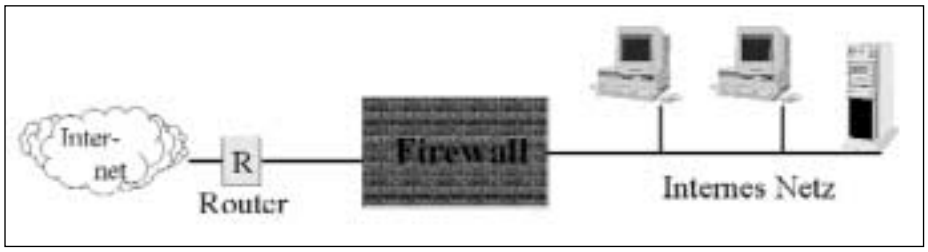

Abbildung 1: Schematische Anbindung einer Firewall als Gateway mit zwei Netzwerkinterfaces.

2 Gateway und Bastion

Abbildung 1 zeigt die typische Konfiguration eines Gateways. Das Netzwerkkabel zwischen Unternehmen und Internet wird aufgetrennt und die Firewall dazwischen gehängt. Die Firewall schaufelt (und kontrolliert dabei) alle Daten von dem einen Netzwerkinterface zu dem anderen. Wenn der Durchsatz durch die Firewall eine Rolle spielt, so ist ein Gateway etwas leistungsfähiger als eine Bastion, da der Netzwerkverkehr genau einmal durch jedes Netzwerkinterface muss. Eine Firewall mit zwei 10 Mbit Netzwerkinterfaces schafft also 10 Mbit Durchsatz, wenn die Firewall-Hardware schnell genug ist.

Im Gegensatz dazu zeigt die Abbildung 2 eine Lösung mit einer Bastion. Hier bilden der Router und die Bastion-Firewall ein Gesamtsystem. Der Router wird so konfiguriert (Stichwort: Access Listen), dass er nur Datenverkehr von und zur Bastion durchlässt. Dadurch werden alle Teilnehmer im internen Netz gezwungen, den Datenverkehr nach außen über die Firewall abzuwickeln. Der Vorteil einer Bastion ist, dass sie überall im Netz stehen kann. Im Gegensatz dazu muss ein Gateway in der unmittel-

INHALT:

* Rainer W. Gerling ist Datenschutzbeauftragter der Max-Planck-Gesellschaft

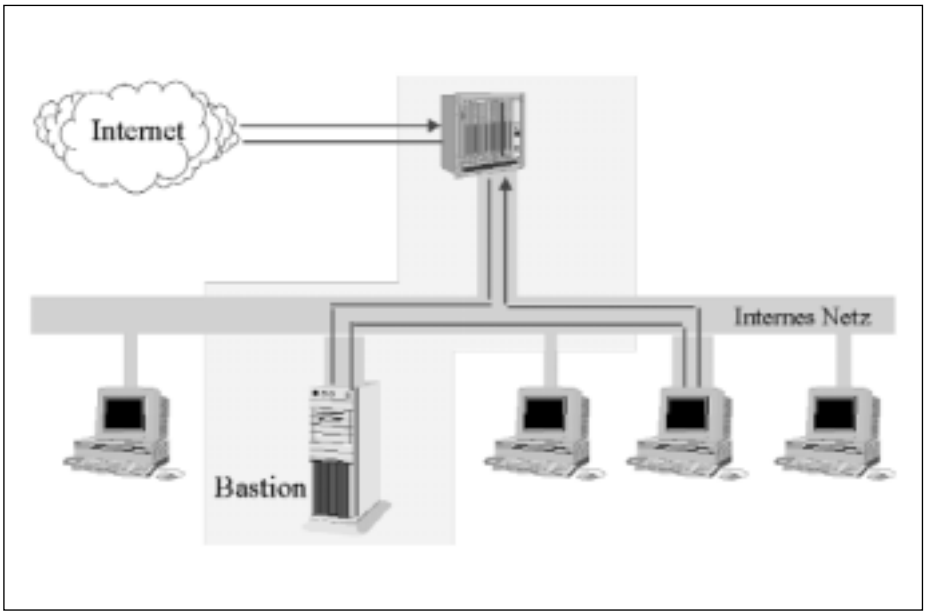

Abbildung 2: Schematische Anbindung einer Firewall als Bastion mit einem Netzwerkinterface. Die Kombination aus Router und Bastion stellt das Firewallsystem (grau unterlegt) dar. Rote Verbindungen sind verboten, grüne jedoch erlaubt.

baren Nähe der zentralen Netzwerkkomponenten stehen, also zwischen Router und zentralem Switch.

Ein Nachteil einer Bastion ist, dass der gesamte eingehende und ausgehende Netzwerkverkehr über ein Netzwerkinterface geleitet wird. Wenn eine Bastion ein 10 Mbit Netzwerkinterface hat, kann sie nur maximal 5 Mbit Durchsatz schaffen.

Auch der Firewallrechner sollte geschützt werden. Deshalb ist es notwendig, zusätzlich auch die Access Listen (Filterregeln) im Router zu nutzen. Jeder Dienst, den die Firewall nicht durchlässt, sollte auch im Router gesperrt sein. Dies führt dazu, dass jeder, der die Firewall über einen speziellen (gesperrten) Dienst angreifen will, erst einmal den Schutz im Router überwinden muss. Jedes Datenpaket, das bereits im Router verworfen wird, belastet die Firewall nicht mehr. Der Router sollte allerdings ein Protokoll erzeugen können, da sonst alle vom Router verworfenen Datenpakete nicht mehr protokolliert werden (auf der Firewall kommen diese ja nicht mehr an).

3 Firewall Backup

Auch ein Firewall Rechner kann einmal ausfallen. Dies ist netztechnisch ein GAU, da der gesamte Netzwerkverkehr des Unternehmens damit zum Erliegen kommt. Als Notfallmaßnahme kommt ein „Überbrücken“ der ausgefallen Firewall nicht in Frage, da dadurch das interne Netz ohne Schutz bleibt. Das Ziel muss sein, die Firewall so schnell wie möglich wieder in Betrieb zu nehmen. Hierzu sollte ein zweiter Firewallrechner identisch konfiguriert im Cold Standby zur Verfügung stehen. Ist die aktive Firewall ausgefallen, werden die Netzwerkkabel an die Standby-Maschine umgesteckt, und diese wird dann eingeschaltet. Nachdem sie hochgefahren ist, läuft die Firewall wieder. Diese Prozedur kann von jedem EDV-Mitarbeiter durchgeführt werden, da keine Anmeldung (Login) an der Firewall erforderlich ist.

Natürlich sollte dieses Verfahren getestet werden, schon manche Backup Lösung scheiterte, weil der geplante Automatismus auf Grund eines kleinen Konfigurationsfehlers nicht funktionierte. In regelmäßigen Abständen (mindestens einmal im Jahr) sollte das Anlaufen der Standby Maschine getestet werden.

Bei Versionsupdates der Firewallsoftware und bei dem Einspielen von aktuellen Sicherheitspatches können diese zuerst auf der Standbymaschine durchgeführt werden. Wenn alles funktioniert, geht diese dann in Betrieb. Danach könne alle Updates und Patches auf der bisherigen Produktionsmaschine nachgezogen werden.

4 Platzierung der Proxies

Ein Proxy Cache hat die Aufgabe, den Daten-Verkehr zu verringern, indem er wiederholte Anfragen nach den gleichen Daten direkt aus seinem Zwischenspeicher beantwortet und nicht durch eine erneute Weiterleitung der Anfrage an den eigentlichen Server (automatische und vorübergehende Zwischenspeicherung auf Grund einer Nutzerabfrage). Werden bestimmte Seiten häufig von Mitarbeitern aufgerufen, kann ein Proxy-Cache den Datenverkehr erheblich reduzieren und somit Kosten sparen. Die Frage ist nun, wo ein solcher Proxy-Cache platziert wird. Vor der Firewall oder hinter der Firewall?

Wenn der Proxy Cache hinter der Firewall ist, also im internen Netz, erspart er der Firewall viel Datenverkehr. Damit steigert er letztendlich den Durchsatz der Firewall. Das Problem der internen Platzierung ist allerdings, dass ein Angreifer, der den Proxy-Cache infiltriert, sich im internen Netz befindet. Der Proxy-Cache wird allerdings auch durch die Firewall geschützt.

Ist der Proxy-Cache vor der Firewall, ist dieser Schutz nicht gegeben. Dafür muss jemand, der den Proxy-Cache erfolgreich übernommen hat, noch die Firewall überwinden, bevor er im inneren Netz ist. Außerdem erspart ein so platzierter Proxy-Cache der Firewall keinen Datenverkehr, da alle Daten, die zwischen Proxy-Cache und internem Netz ausgetauscht werden, durch die Firewall müssen.

Je nach Leistungsvermögen der Firewall und Sicherheitsbedarf ist der Proxy-Cache geeignet zu platzieren. Als erster Denkansatz sollte von der Platzierung des Proxy-Caches in der DMZ (zum Begriff der DMZ siehe weiter unten) ausgegangen werden.

5 Geheimhaltung der Firewall-Regeln

Die Kenntnis der detaillierten Firewallregeln und des Sicherheitskonzeptes erlauben es einem Angreifer, einen maßgeschneiderten Angriff zu planen. Deshalb sind die Details geheim zu halten. Beim Abschluss einer Firewall-Betriebsvereinbarung führt dies jedoch zu einem Problem. Der Betriebsrat möchte die Firewall in den Anlagen zu der Betriebsvereinbarung gern möglichst detailliert beschreiben. Da eine Betriebsvereinbarung betriebsöffentlich ist, gefährdet dies jedoch die Sicherheit der Firewall. Es sollte aber vereinbart werden, dass der Betriebsrat einen Vertreter benennt, der Einsicht in die detaillierten Regeln der Firewall erhält. Dieser Vertreter des Betriebsrats wird auf eine besondere Verschwiegenheit bezüglich der Firewallregeln, auch gegenüber anderen Betriebsratsmitgliedern, verpflichtet. Aus der EDV-Abteilung sollten auch nur der EDV-Leiter und die Administratoren der Firewall Zugriff auf die Firewall-Regeln haben.

6 DMZ

Der völlig unglücklich gewählte Name „demilitarisierte Zone“ (DMZ) beschreibt einen Zwischenbereich, der weder dem internen noch dem externen Netz zugeordnet werden kann. Neutrale Zone wäre eine sehr viel bessere Bezeichnung dafür. Häufig wird die DMZ durch einen dritten Netzwerk-Anschluß an der Firewall realisiert (Abb. 3). Es ist auch möglich, die DMZ als Zwischenbereich zwischen zwei Firewalls zu realisieren (Abb. 4). Brauchen wir für unser Firewallkonzept eine DMZ?

Typischerweise stellt man in der DMZ die Server auf, auf die von außen zugegriffen werden soll. Würde es

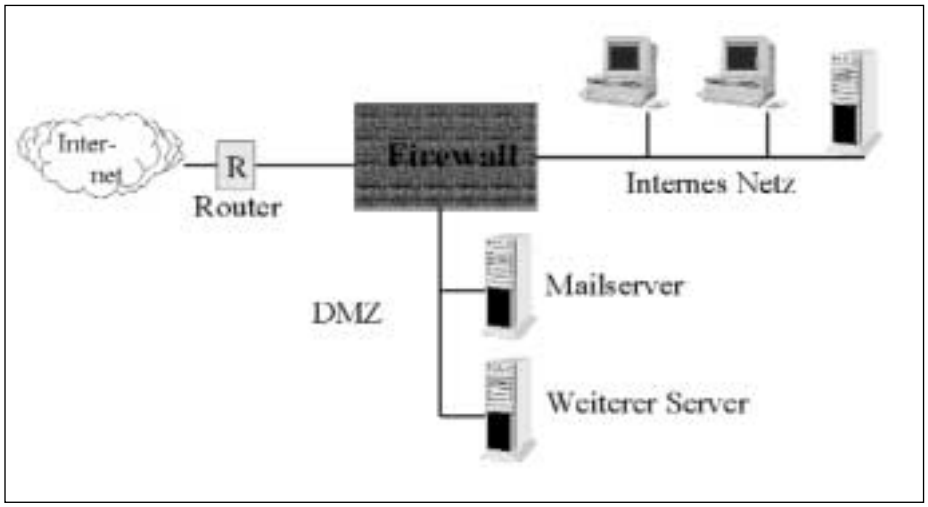

Abbildung 3: Die demilitarisierte Zone wird über ein drittes Netzwerkinterface an der Firewall realisiert.

ein Angreifer schaffen, einen solchen Server zu hacken, so wäre er noch nicht im internen Netz.

Wenn es keine extern-sichtbaren Server gibt, weil diese beispielsweise bei einem Provider stehen, so ist eine DMZ nicht erforderlich. Aber schon ein eigener Mailserver rechtfertigt eine DMZ. Auch der externe DNS-Server bei dem so genannten Split-DNS sollte in der DMZ stehen. Proxy-Caches stehen ebenfalls vorzugsweise in der DMZ.

Eine DMZ ermöglicht es, dass der Datenfluss nur noch extern->DMZ und DMZ->intern stattfinden kann. Jedweder Datenfluss extern->intern kann unterbunden werden. Es muss lediglich noch überlegt werden, wie der Datenfluss von intern nach extern stattfindet. Wird er direkt erlaubt, oder wird er ausschließlich über Proxies in der DMZ abgewickelt. Aus Sicherheitsgründen spricht viel für die Proxy-Lösung.

7 Verschlüsselte Tunnel (VPN)

IPsec, Secure Shell, SSL/TLS und andere auf verschlüsselter Kommunikation beruhende Protokolle erlauben einen sicheren Remote Zugriff ins interne Firmennetz. Da der externe Tunneleingang Bestandteil des internen Netzes wird, muss er genauso geschützt werden, wie das interne

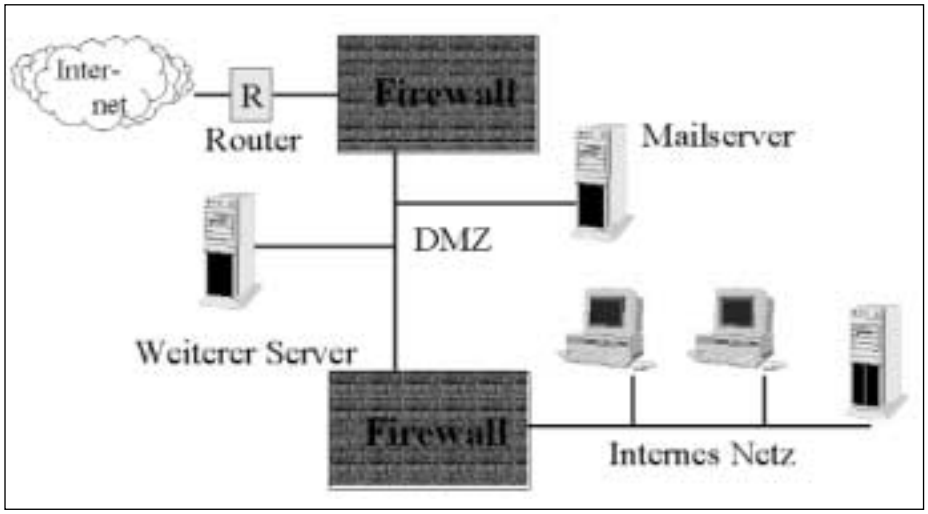

Abbildung 4: Die demilitarisierte Zone, realisiert als Bereich zwischen zwei Firewalls.

Netz. In letzter Konsequenz heißt dies, dass das Notebook oder der Privat-PC des Mitarbeiters, der zum Remote Zugriff genutzt wird, auch durch eine Firewall geschützt werden muss. Zu diesem Zweck wurden die sogenannten Desktop- oder Personal-Firewalls geschaffen. Dieser Firewalltyp (im Allgemeinen ein Paketfilter) schützt genau den Rechner, auf dem er läuft. Eine Übersicht über verfügbare Personal-Firewalls siehe bei Gerling.[1]

Die Zusammengehörigkeit einer Firewall mit einem VPN Produkt zeigt sicherlich z.Z. die Firma NAI am deutlichsten mit der aktuellen Version von PGP 7.[2] Hier sind die IPsec-kompatible Netzwerkverschlüsselung und eine Personal-Firewall in einem Modul integriert und nur gemeinsam installierbar.

Bei der Auswahl einer Personal-Firewall ist insbesondere auf gute Möglichkeiten zur zentralen Administration zu achten. Sonst hängt die Sicherheit von den persönlichen Einstellungen an der Firewall des Mitarbeiters ab. In diesem Sinne ist der Begriff persönliche Firewall nicht gemeint.

8 Betriebskonzept

Eine weitere wichtige Entscheidung ist das Betriebskonzept der Firewall. Es gibt zwei Möglichkeiten:

- ❒ Alles was nicht verboten ist, ist erlaubt.
- ❒ Alles was nicht erlaubt ist, ist verboten.

EDV-Leute neigen zu dem ersten dieser beiden Konzepte, da es den eingefahren Betrieb am wenigsten beeinträchtigt. Auch Vorstellungen der Art „Erst installieren wie die Firewall völlig offen, und dann drehen wir sie langsam zu“ gehören in diese Kategorie. Die Gefahr dieses Konzeptes liegt darin, dass alle Dienste, die man vergessen hat zu verbieten, erlaubt sind. Es ist eine ständige Beobachtung neuer Angrifftechniken und Sicherheitslücken erforderlich, um die Verbotsliste zu verlängern.

Diese Probleme umgeht man mit dem zweiten Betriebskonzept. Die Firewall lässt nur die Dienste durch, die gewollt und explizit freigegeben sind. Diese Variante des Betriebskonzepts erfordert allerdings eine sorgfältige Planung. Nichts wäre schlimmer als ein Totalzusammenbruch der EDV durch eine fehlerhaft oder unvollständig konfigurierte Firewall.

Ein bewährtes Konzept für die Firewall ist:

1. Der Zugriff auf die Rechner innerhalb des Unternehmens von außen soll nur durch Berechtigte erfolgen und auf das notwendige Maß eingeschränkt werden.
2. Alle Dienste, die Passworte im Klartext über das Netz übertragen, werden durch Varianten mit verschlüsselter Übertragung der Passworte ersetzt. Durch Blockierung der Dienste ohne verschlüsselte Übertragung der Passworte wird dieser Übergang erzwungen.
3. Die Firewall soll dem Benutzer nur dann auffallen, wenn er etwas Unerlaubtes zu tun gedenkt.

9 Konfiguration

Zur genauen Festlegung der Konfiguration muss die EDV-Nutzung der Firma detailliert analysiert werden, Auch hierbei kann die Firewall bereits gute Dienste tun. Sie wird vorübergehend mit der Regel „Alles durchlassen“ in Betreib genommen, und der gesamte Datenverkehr wird protokolliert. Eine Analyse dieses Protokolls ergibt, welche Dienste regelmäßig benutzt werden. Dienste die selten genutzt werden, erscheinen in diesem Protokoll natürlich nur, wenn sie während der Protokollierungsphase auch genutzt wurden. Gehen wir im Folgenden die wichtigsten Standarddienste einmal durch. Dabei geht es nicht um das detaillierte Erstellen des Regelwerks, sondern um eine Checklisten-Aufstellung der Dienste, damit keiner vergessen wird.

DNS

Damit Kommunikation möglich ist, muss den Rechnern des Unternehmens Zugriff auf den Namensdienst ermöglicht werden. Es empfiehlt sich, einen internen DNS-Server aufzusetzen. Nur dieser erhält dann Zugriff nach außen. Die Rechner im Unternehmen richten ihre Anfragen an den internen DNS-Server, der diese Anfragen dann nach außen weiter reicht. Wenn das Unternehmen eine eigene Domaine besitzt und auch den DNS-Server dafür betreibt, muss auch der Zugriff von außen auf den DNS-Server erlaubt werden.

Bei der Planung einer DMZ ist es eine Überlegung wert, den primären DNS-Server für den externen Zugriff in die DMZ zu stellen. Ein sekundärer DNS-Server für den internen Rechnerzugriff wäre dann in das interne Netz zu stellen. Die beiden DNS-Server sind dann die einzigen Rechner, die den DNS-Dienst durch die Firewall nutzen dürfen. Dieses Verfahren wird auch als Split DNS bezeichnet. Der interne DNS-Server beantwortet auch die Anfragen der internen Rechner nach internen Adressen. Der externe DNS-Server beantwortet nur Fragen nach den von extern sichtbaren Rechneradressen.

Ping, Traceroute und Co

Die Dienste, die das Protokoll ICMP benutzen, dienen im Wesentlichen der Nerzwerkanalyse und Fehlerdiagnose. Sinnvollerweise werden sie nur von den Mitarbeitern der EDV-Abteilung benutzt. Deshalb können sie für alle anderen Beschäftigten gesperrt werden. Auch für Zugriffe von außen sollten diese Dienste gesperrt werden, damit niemand von außen diese Dienste zur Analyse des internen Netzes verwenden kann.

Gute Firewalls erlauben die automatische (dynamische) Freischaltung von ICMP-Antwortpaketen für kurze Zeit, nachdem eine entsprechende Anfrage abgeschickt wurde.

Bei den meisten Firewalls gibt es die beiden Möglichkeiten „reject“ und „drop“ als Reaktion auf eine nicht zu-

[1] R.W. Gerling, Zugriff auf E-Mail von unterwegs, KES, Heft 4/2000, Seite 16 - 21

[2] http://www.pgpinternational.com

gelassene Verbindung. Bei Verbindungen von außen sollte „drop“ der Standard sein: Das Paket wird ohne Rückmeldung an den Eindringling verworfen. Damit weiß ein potentieller Angreifer nicht, ob der Zielrechner nicht existiert oder ob eine Firewall die Verbindung nicht zulässt. Ein „reject“ liefert jedoch eine Fehlermeldung und gibt damit einen Hinweis auf die Existenz der Firewall. Von Innen kann man für zur Diagnose benötigte Befehle ein „reject“ einrichten. Damit haben die EDVler etwas weniger Probleme bei der Fehlersuche.

WWW (http, https)

Zugriffe auf da WWW geschehen im Allgemeinen über http (Port 80) oder https (mit SSL verschlüsseltes http über Port 443). Diese beiden Ports machen keine Probleme. Problematisch ist die dagegen die Unsitte vieler Betreiber von Web-Seiten, für bestimmte Anwendungen weitere Ports zu verwenden. Dies merkt man an der Angabe eines besonderen Ports an der URL: z.B. http://www.demo.de:1600. In diesem Beispiel wird für das http Protokoll der abweichende Port 1600 verwendet. Es macht wenig Sinn, alle diese Sonderfälle durch spezielle Regeln in der Firewall zu berücksichtigen. Hier muss eine gut überlegte Sicherheitspolicy her, die die gewollten Regeln der Web-Nutzung festlegt. Es kann ja durchaus beabsichtigt sein, alle dies Web-Seiten, die spezielle Ports verwenden, zu sperren.

Erlauben die Regeln die Nutzung eines Proxy-Caches außerhalb der Firewall, so werden alle diese Sonderports automatisch mit freigeschaltet. Der Web-Browser baut eine Verbindung zum Proxy-Server auf (häufig über den Port 8080), und erst der Proxy-Server stellt die Verbindung zu dem speziellen Port her.

Eine Paketfilter-Firewall kann keine aktiven Inhalte (ActiveX Controlls, Javascript etc.) filtern. Moderne Paketfilter bieten allerdings Schnittstellen zu entsprechender Filtersoftware. Hier sind die Vorteile (einfaches Management an einer Stelle) und die Nachteile (Durchsatzprobleme) gut gegeneinander abzuwägen. Eine gute dezentrale Antivirensoftware mit zentralem Policymanagement ist unter Umständen vorzuziehen.

Die rasende Verbreitung des „I Love you“-Virus war möglich, weil alle Virenscanner (auch die zentralen) diesen Virus nicht sofort erkannten. Es muss im Allgemeinen mit einer Zeitspanne von mindesten drei Stunden gerechnet werden, bevor die Virensignaturen aktualisiert sind. Viel besser wäre es, die Ausführung aktiver Inhalte aus Mailprogrammen und Web-Browsern komplett zu unterbinden.

URL- und andere Inhalts-Filter (die nicht nach Viren suchen) werden in der Regel dazu eingesetzt, Anwender zu reglementieren, also eine Form der Zensur vorzunehmen. Diese Reglementierung kann abhängig von den beabsichtigten Zielen, unterschiedlich scharf realisiert werden. Häufig soll die Filterung eine private Nutzung des Internets durch die Beschäftigten oder aber den Zugriff auf gesetzwidrige Inhalte unterbinden. Es ist unumstritten, dass diese Form der Zensur zum einen nie aktuell (jeden Tag gibt es neue Inhalte im Internet) und zum anderen immer fehlerhaft ist. Dann kann man die Filterung aber auch ganz weglassen und die Beschäftigten auf Nutzungsverbote in Benutzerordnung, Dienstanweisungen und Betriebsvereinbarungen verweisen.

E-Mail (pop3, imap, smtp)

Für das Handling der E-Mail sind die Dienste SMTP zum Versand und Pop3 bzw. IMAP zum Abholen der E-Mail vom Mail-Server zuständig. Die Firewall muss immer ein- und ausgehende SMTP-Verbindungen zum Mail-Server zulassen, da sonst kein E-Mail Austausch mit dem Rest der Welt möglich ist. SMTP-Verbindungen zu anderen Rechnern im Firmennetz sollten unterbunden werden. Da SMTP auf Grund der Komplexität der Software ein hohes Risiko für Sicherheitslücken bietet, sollte nur der zentrale Mailserver, der von kompetenten Fachleuten sicherheitsmäßig auf dem aktuellen Stand gehalten wird, von außen ansprechbar sein.

Das unter WWW zum Thema zentrales Viren-Scannen Gesagte gilt auch für E-Mail. Hinzu kommt, dass ein zentraler Virenscanner verschlüsselte E-Mail zum Scannen nicht entschlüsseln kann. Nur wenn ein Recovery-Verfahren[3] implementiert würde, wäre das zentrale Entschlüsseln der E-Mail zum Scannen möglich. Da auf dem zentralen Scanner-Rechner jedoch der firmeninterne „Nachschlüssel“ vorgehalten werden muss, entsteht eine große Sicherheitslücke. Ist der zentrale „Nachschlüssel“ kompromittiert, liegt die komplette verschlüsselte Firmenkommunikation offen. Diese Sicherheitslücke ist den fadenscheinigen Vorteil des zentralen Scannens der verschlüsselten E-Mail nicht wert.

Pop3 und IMAP stellen ein hohes Sicherheitsrisiko dar, da beide Protokolle Passworte im Klartext übertragen. Deshalb sollten beide im Firewall ein- und ausgehend gesperrt werden. Wenn ein Zugriff auf die Postfächer von außen erforderlich ist, sollten geeignete Tunnelmechanismen verwendet werden. Hier gibt es je nach Anwendungsumgebung und eingesetzten Betriebssystemen verschiedene Möglichkeiten: SSL-Proxies[4], Secure Shell[5] oder gar IPsec[6] bieten unterschiedlichste Möglichkeiten (eine Übersicht bei Gerling[7]).

ftp

FTP steht für File Transfer Protocol und dient dem Übertragen von Dateien zwischen Rechnern. Auch

[3] R.W. Gerling, Company Message Recovery, Datenschutz und Datensicherheit, 22 38 (1998)

[4] Z.B. http://www.stunnel.org. Zur Installation und Anwendung siehe R.W. Gerling, Verschlüsselung im betrieblichen Einsatz, datakontext 2000.

[5] http://www.ssh.fi

[6] http://www.ipsec.org.

[7] R.W. Gerling, Zugriff auf E-Mail von unterwegs, KES, Heft 4/2000, Seite 16 - 21

wenn der normale Anwender es häufig nicht merkt, werden viele Datei-Downloads von Web-Seiten mittels ftp durchgeführt. FTP ist für Firewalls ein kompliziertes Protokoll, da für den so genannten Kommandokanal eine Verbindung vom Klient zum Server aufgebaut wird, für die Übertragung der Daten aber eine Verbindung vom Server zum Klient. Diese von innen quasi angeforderte, aber von außen aufgebaute Verbindung überfordert häufig statische Paketfilter. Mit dynamischen Paketfiltern oder Statefull Inspection Firewalls (z.B. Checkpoints Firewall 1) gelingt jedoch meist die Zuordnung der beiden Verbindungen.

Es muss überlegt werden, ob ausgehende FTP-Verbindungen zulässig sein sollen. FTP-Verbindungen in das Unternehmen werden nur für (Fern-)Wartungszwecke auf die entsprechenden Server und, falls erforderlich, für Wartungsarbeiten von EDV-Mitarbeitern von daheim auf spezielle Rechner zugelassen. Der Zugriff von außen auf Rechner für Wartungszwecke muss auf das notwendige Maß beschränkt werden. Da auch FTP das Anmeldepasswort im Klartext überträgt, muss FTP so weit wie möglich durch sichere kryptographische Verfahren (z.B. sftp oder scp aus dem Secure Shell Paket oder Tunneln der FTP Verbindung) ersetzt werden. Ein genereller Zugriff von außen nach innen sollte nicht vorgesehen werden. Ein eventueller FTP-Server (z.B. zum Kundensupport mit anonymous Zugang) sollte in der DMZ stehen.

news (nntp)

Öffentliche Nachrichten werden im Internet in thematisch gegliederten Diskussionsforen (Newsgroups) ausgetauscht. Dieser News-Dienst wird auch als Usenet (Kurzform von Users´ Network) bezeichnet. Er gleicht einer riesigen Zeitung mit Fachartikeln, Leserbriefen und Kleinanzeigen. Die Artikel werden auf zentralen Rechnern (Newsservern) in Datenbanken gehalten; der Zugriff erfolgt über Newsreader-Programme.

Soweit bestimmte Newsgroups für betriebliche/dienstliche Zwecke benötigt werden, sollte ein interner Newsserver eingerichtet werden. Auf diesem werden alle notwendigen Newsgroups vorgehalten. Damit stellt sich auch das Problem des Zugriffs auf rechtlich fragwürdige Newsgroups nicht, da diese im Unternehmen nicht vorhanden sind.

SAP

Der Zugriff auf den SAP-Server (oder einen anderen vergleichbaren) im Unternehmen sollte gesperrt werden. Ein Fernwartungszugriff von außen auf den SAP-Server kann/muss im erforderlichen Umfang freigeschaltet werden. Hierbei gilt, dass nur genau benötigten, die anwendungsspezifischen Ports, für die IP-Adressen freigeschaltete werden, die der Dienstleister benennt. Die Regeln für den Fernwartungszugriff sollten üblicherweise eingegeben aber inaktiv sein. Nur wenn der Dienstleister den Zugriff anfordert, wird er für das erforderliche Zeitfenster freigeschaltet. Damit ist der Zugriff auf das SAP von außen nur auf kleine Zeitfenster beschränkt. Darüber hinaus sollte geprüft werden, ob nicht Programme wie SECUDE[8] zur weiteren Sicherung des Fernzugriffs eingesetzt werden können.

telnet

Mit Hilfe von Telnet ist es möglich, auf einem entfernten Rechner eine Terminalsitzung aufzubauen (Remote Login) und textorientierte Anwendungen zu nutzen. Dazu benötigt man eine individulle Zugangsberechtigung oder einen öffentlichen Zugang auf dem entfernten Rechner. Über Telnet sind zum Beispiel Informationssysteme wie Datenbanken (z.B. Juris) oder Bibliotheken zu nutzen. Telnet wird ebenfalls häufig für die Fernwartung von Rechnern eingesetzt. Das große Risiko bei telnet ist die Übertragung der Anmeldepasswort im Klartext.

[8] http://www.secude.de/products-deutschhtml/secudefuerr3deutsch.htm

Der Zugriff von außen auf Server für Wartungszwecke wird auf das notwendige Maß beschränkt und soll so weit wie möglich durch sichere kryptographische Verfahren (z.B. Secure Shell) ersetzt werden. Auch hier sind Zeitfenster zu nutzen.

Jeder, der einmal Secure Shell genutzt hat, weiß, dass es genauso komfortabel wie telnet zu nutzen ist. Trotzdem muss viel Überzeugungsarbeit geleistet werden, bis der Umstieg erfolgt.

Netzwerklaufwerke

Auf interne Netzwerklaufwerke (egal ob über NETbios, NFS oder andere Protokolle) sollte von außen nur zugreifbar sein, wenn dieses erforderlich ist. Viele dieser Protokolle enthalten Sicherheitslücken, die den freien Zugriff zu einem großen Risiko werden lassen. Gerade die Microsoft Protokolle (Dateifreigaben) gelten hier als besonders kritisch.

X

Das X-Protokoll, dass zur entfernten Anzeige eines Grafikbildschirms genutzt wird, hat bekannte Sicherheitslücken. Zur Absicherung kann Secure Shell benutzt werden. In diese Software ist ein Mechanismus integriert (Port Forwarding), der es dem X-Protokoll erlaubt, die verschlüsselte Verbindung mit zu nutzen. Die Daten des X-Protokolls werden über den verschlüsselten Tunnel umgeleitet und sind deshalb vor dem Abhören geschützt. Deshalb sollte das X-Protokoll in der Firewall gesperrt werden, um den Umstieg aus das Tunneln über Secure Shell zu erzwingen.

Der Rest

Es gibt sicherlich noch etliche Spezialprotokolle, die nur für einige Unternehmen wichtig sind. Netzwerkdruck und Datenbankanwendungen sind nur zwei typische Vertreter. Auch bei diesen Protokollen ist zu prüfen, ob sie von außen zugänglich sein müssen. Wenn nein, sind sie in der Firewall zu sperren. Wenn ja, müssen die Sicherheitslücken untersucht werden. So sind z.B. Printserver häu-

fig über telnet zugänglich und stellen deshalb eine nicht unerhebliche Sicherheitslücke dar.

10 Firewall und Recht

Eine Firewall stellt eine Telekommunikationsanlage gemäß § 3 Nr. 17 des Telekommunikationsgesetzes (TKG)[9] dar, da sie „als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren“ kann. Damit gelten die Vorschriften des TKG.

Protokollierung

Das *„geschäftsmäßige Erbringen von Telekommunikationsdiensten“* ist *„das nachhaltige Angebot von Telekommunikation einschließlich des Angebots von Übertragungswegen für Dritte mit oder ohne Gewinnerzielungsabsicht“*. Sobald die eigene Tätigkeit als *„geschäftsmäßiges Erbringen von Telekommunikationsdiensten“* eingestuft werden kann, gelten die Vorschriften des § 87 „Technische Schutzvorschriften“ und des § 89 „Datenschutz“. Außerdem ist die Teledienstunternehmen-Datenschutzverordnung[10] zu beachten. Selbstverständlich gilt für alle auf der Firewall erhobenen personenbezogenen Daten die Zweckbindung des § 31 Bundesdatenschutzgesetz.

Mitbestimmung

Eine Firewall ist auf Grund der Protokolldaten zur Verhaltens- und Leistungskontrolle im Sinne des § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz geeignet. Damit unterliegt die Einführung einer Firewall der erzwingbaren Mitbestimmung. Es ist deshalb dringend erforderlich, eine entsprechende Betriebsvereinbarung abzuschließen. In dieser Betriebsvereinbarung sind die Details der Protokollierung und der Auswertung der Protokolle zu regeln. Die Festlegung der Filterregeln, d.h., die Frage, welche Dienste zugelassen werden, unterliegt nicht der Mitbestimmung.

Zwei Dienste sind aus Sicht der Mitarbeitervertretungen im Allgemeinen kritisch zu sehen: das Surfen (http. https) und der E-Mail Versand (smtp). Beim Surfen sollte die Frage diskutiert werden, inwieweit durch eine Teilanonymisierung (z.B. Unterdrücken der letzten 8 Bit der IP-Adressen des Internen Netzes bei den Protokollen http und https) das Schutzziel erreicht und die Privatsphäre der Mitarbeiter gewahrt werden kann. Das Versenden der E-Mail zeigt sich bei genauer Analyse als unkritisch, da von der Firewall nur Verbindungen zwischen Mailservern protokolliert werden. Der E-Mail Versand nach außen geschieht nämlich nicht von den Arbeitsplatzrechnern, sondern vom Mailserver.

Schlussbemerkung

Es gibt sie nicht, die universell verwendbare sichere Firewall-Lösung. Jedes Unternehmen muss für sich entscheiden, wie viel Sicherheit es will, und welche Dienste es zulassen oder nicht zulassen will. Diese Arbeit muss individuell geleistet werden. Der vorliegende Artikel, hilft die richtigen Fragen zu stellen.

Wenn das Firewallkonzept des Unternehmens steht, muss die Geschäftsleitung es in Kraft setzen. Sicherheit kann nur von oben nach unten durchgesetzt werden und nicht umgekehrt.

Wenn die Firewall kneift, werden Mitarbeiter nach Auswegen suchen. Die Erfahrung zeigt, dass eine restriktive Firewall zu einer Zunahme der betrieblichen Modem- oder ISDN-Karten führen kann. Es versteht sich eigentlich von selbst, dass es hinter der Firewall keine (unkontrollierten) Internet-Zugänge geben darf. Notfalls müssen geeignete Kontrollen die Modems zurückdrängen.

Eine Firewall lebt. Regeln müssen an geänderte Kommunikationsbedürfnisse und neue Sicherheitslöcher angepasst werden.

Firewalls garantieren keine Sicherheit, sie reduzieren lediglich das Risiko. Insbesondere stellt jede Regel, die einen Zugriff von außen nach innen erlaubt, eine Sicherheitslücke dar. Die Zahl und Größe der Löcher sollte minimiert werden. Ein ständiges Beobachten und Überwachen des Firewall-Betriebes ist also unerlässlich. □

Dienst	*Port*	*Port mit TLS/SSL*
FTP-data	*20*	*989*
ftp	*21*	*990*
Secure Shell	*22*	*–*
Telnet	*23*	*992*
SMTP	*25*	*465*
DNS	*53*	*–*
HTTP	*80*	*443*
POP3	*110*	*995*
nntp	*119*	*563*
IMAP	*143*	*993*
irc	*194*	*994*
ldap	*389*	*636*
socks	*1080*	*–*
Http Proxy	*8080*	*–*

Tabelle: Übersicht über einige ausgewählte wichtige Portnummern. Alle Portnummern finden sich in RFC 1700[11].

[9] Telekommunikationsgesetz (TKG) vom 31. Juli 1996 (BGBl. I S. 1120); wesentliche Auszüge siehe z.B. http://www.lrz-muenchen.de/~rgerling/gesetze/tkg_aus.html

[10] http://www.bmwi.de/Homepage/download/telekommunikation_post/TDSV_kab_221100.pdf, vom Bundeskabinett beschlossen am 22.11.2000; die Zustimmung des Bundesrates war bereits erfolgt; damit tritt die neue TDVS am Tag nach der Veröffentlichung im Bundesgesetzblatt in Kraft.

[11] siehe auch zum Beispiel: A. Badach, E. Hoffmann, Technik der IP-Netze, Hanser Verlag München, 2001.