Fachhochschule Landshut

Fachbereich Elektrotechnik und Informatik

Konzeption und Einrichtung einer Firewall in einem mittelständischen Unternehmen

Diplomarbeit
vorgelegt von:

Albin Selmeier

Eingereicht am: 15.03.2000

Betreuer: Prof. Dr. Peter Hartmann

Inhaltsverzeichnis

Vorwort

Diese Arbeit soll eine Hilfe sein für alle, die im Begriff sind, ein lokales Netzwerk mit dem Internet zu Verbinden und die sich Sorgen über die Sicherheit der eigenen Daten und Rechner machen.

Zur Nachvollziehbarkeit vieler Schritte ist ein Grundlegendes Verständnis des TCP/IP Protokolls (IP-Nummern, Ports, Ablauf des Verbindungsaufbaus) notwendig.

Die Planung, allen voran der Entwurf der IT- Sicherheitspolitik ist aber all denen zu Empfehlen, die weniger an der Implementation als an der Organisation beteiligt sind.

In den folgenden Kapiteln sollen schrittweise Planung, Implementation und Test eines Firewall - Systems und der zugehörigen organisatorischen Aufgaben beschrieben werden.

Einleitung

Das Internet bietet einem mittelständischen Unternehmen ungeahnte Möglichkeiten der Kommunikation und des Datenaustausches zwischen verschiedenen Firmenstandorten, Teleworkern, externen Dienstleistern und sonstigen Quellen wie WWW oder FTP. Angestellte können von zu Hause aus im Firmennetz arbeiten, Aussenstellen haben die Möglichkeit auf interne Datenbanken zurück zu Greifen, Server unter externer Wartung sind online ohne der Anreise eines Technikers konfigurierbar, und aktuelle Programme und Treiber liegen auf öffentlichen FTP-Servern zum herunterladen bereit.

In all der Euphorie vergisst man schnell die entstehenden Gefahren dadurch, dass das eigene Netzwerk dem Internet offen gegenüberliegt. Vor allem im Management, wo die finanziellen Entscheidungen für Sicherheitspolitische Aktivitäten gefällt werden, unterschätzt man oft und gerne die Möglichkeiten, die sich aussenstehenden Personen bieten. Das grösste Problem eines IT - Sicherheitsverantwortlichen ist meist die zu leistende Überzeugungsarbeit, um die nötigen Mittel bereitgestellt zu bekommen. So wurde in Deutschland in mehr als 50% aller Firmen weniger als 100.000 Euro pro Jahr für IT - Sicherheit[1] ausgegeben (Umfrage bei 291 deutschen Unternehmen aller Grössenordnungen).

Es wird oft auch die eigentliche Gefahrenquelle falsch eingeschätzt. Entgegen der landläufigen Meinung liegt das Hauptinteresse eines Angreifers aus dem Internet nur in den seltensten Fällen darin, sich Informationen zu beschaffen, oder diese zu manipulieren. Vielmehr zielen die meisten Einbrecher darauf ab, sich fremde Rechnerresourcen zugänglich zu machen. Gekaperte Rechner dienen meist als Ausgangspunkt für weitere illegale Aktionen, wie das Einrichten von (z.B. Warez-FTP-) Servern, das Starten von verteilten DOS - Angriffen, oder das Ausführen von Handlungen unter dem Namen des Opfers (dient i.a. nur dem Verstecken der wahren Identität des Hackers, nicht der Verleumdung des Opfers).

Einige Attacken werden auch mit destruktiver Absicht geführt. Kann auf einem System kein Administrator - Zugang ergattert werden, oder ist es für den Angreifer nicht von strategischer Bedeutung, so werden oft „nur” Daten vernichtet oder das System betriebsunfähig gemacht.

Um jedoch die Vorteile des Internet geniessen zu können, ohne all den Gefahren ausgeliefert zu sein, kann und sollte man sich schützen. Für jeden einzelnen Einsatzzweck gibt es unterschiedliche Schutzmechanismen, die verwendet werden können. Ein tieferes Verständnis hierfür ist nötig, um die entstehenden Vorteile und Einschränkungen einschätzen zu können. Hilfreich kann Fachliteratur sein, wie z.B. „Building Internet Firewalls”[2] von D. Brent Chapman und Elizabeth D. Zwicky oder „Practical UNIX & Internet Security”[3] von Simson Garfinkel und Gene Spafford. In diesen Büchern sind bereits in den ersten Kapiteln Prinzipien und Methoden der Netzwerksicherung erläutert.

Aktuelle Netztopologie

Bisher eingesetzte Komponenten

Die EDV-Umgebung bei der Firma Mycompany besteht seit einigen Jahren. In dieser Zeit wurde auch das Computer-Netzwerk stark ausgebaut, welches inzwischen das gesamte Firmengelände umfasst. Zusätzlich bestehen auch Verbindungen nach aussen zu verschiedenen Dienstanbietern. Für den Betrieb dieser Topologie werden die im folgenden beschriebenen Protokolle bzw. Soft- und Hardwareelemente eingesetzt.

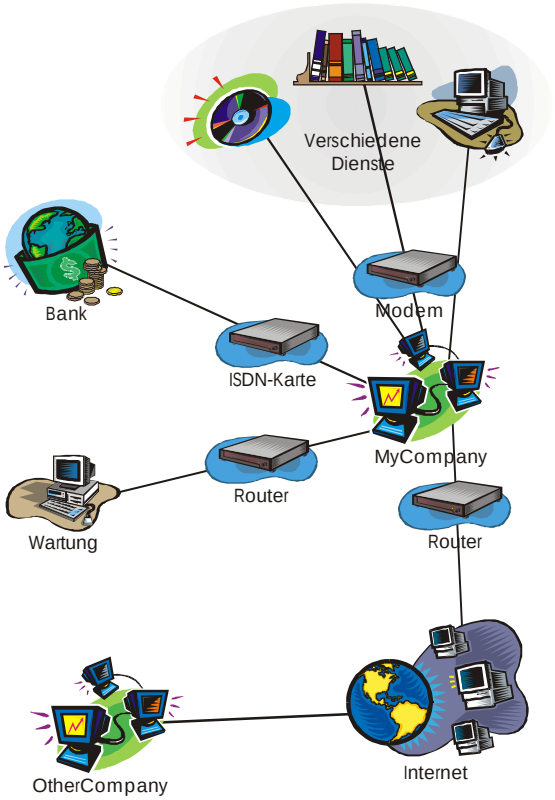


Abb.1

- **Novell IPX Netzwerk für Novell Fileserver, Netzwerk - Drucker, etc.**
  Die Benutzerverwaltung erfolgt mit Hilfe des Serverbetriebssystems Novell Netware 4.11. Es ermöglicht eine einfache und effiziente Administration der Benutzerkonten, der darauf aufbauenden Netzwerk - Sicherheit und Dateizugriffsrechte. Des weiteren werden die Drucker im Netzwerk mit diesem Protokoll vom Server adressiert.

- **TCP/IP für Anbindung der Clients an Unix-Server (DB), Class C-Net (192.12.144.0, 255.255.255.0)**
  Der ursprünglich einzige Einsatzzweck von TCP/IP lag in der Anbindung der Arbeitsplatz - Rechner an den Zentralen Datenbankserver mittels Terminalemulation. Dieser Server arbeitet unter UNIX mit einer Informix - Datenbank. Vor der Umstellung auf Windows - Clientprogramme erfolgte die Abfrage in Terminalfenstern, die mittels TCP/IP einen direkten Connect zum Zentralrechner benutzten.
  Mittlerweile werden einzelnen Benutzern auch Internetdienste (WWW, EMail, FTP, etc.) zur Verfügung gestellt. Diese Dienste erfordern ebenfalls das Internet Protocol, welches inzwischen von allen Rechnern verwendet wird.

- **Verwendete Arbeitsplatz-Rechner**
  An den Arbeitsplätzen kommen ausschliesslich INTEL-Rechner zum Einsatz. Als Betriebssystem wird Windows95 und Windows NT Workstation 4.0 eingesetzt.

- **Mailserver an Novell-Netzwerk gekoppelt**
  Als interner Mailserver wird das Programm 'Mercury/32' von David Harris wegen der einfachen Integration in das bestehende Novell-Netzwerk (IPX) mit Übernahme aller Benutzer eingesetzt. Dies erleichtert die Administration des Systems, da das Einrichten der EMail-Konten entfällt. Mails von Ausserhalb werden von einem POP3-Mailserver geholt und intern an die Benutzer verteilt. Dieser Zugriff erfolgt wiederum über TCP/IP.

- **1 Rechner mit ISDN-Karte (Internet)**
  Es besteht ein Reserverechner, mit welchem eine Verbindung ins Internet hergestellt werden kann. Dieser kommt i.a. zum Einsatz wenn Probleme mit dem regulären Zugang auftreten. Es besteht eine Verbindung vom Rechner zum Firmennetz, jedoch stellt er keine internen Server- oder Routerdienste zur Verfügung.

- **Intranetserver mit Datenbankzugriff**
  Für das Intranet besteht ein WWW-Server (Windows NT Server), der nicht nur statische Daten zur Verfügung stellt, sondern auch dynamische Datenbankabfragen. Zu diesem Zweck besteht eine ODBC-Verbindung zum Datenbankserver, deren Daten von einem Serverprogramm ausgewertet und als HTML-Datei an den Client weitergeleitet werden.

- **1 Router für dial up Internetzugang**
  Alle Verbindungen ins Internet werden von einem ISDN-Router erstellt. Auf den Windows-Clients wird lediglich dieser Router als Standard-Gateway eingerichtet, womit alle nicht-lokalen Netzwerkzugriffe ins Internet geleitet werden.

- **1 Router (Wartung), dial back zu Administrator**
  Netzwerkverbindungen zu Wartungszwecken werden mit einem extra Router erstellt. Der Verbindungsaufbau erfolgt nach einem Anruf von einer Aussenstelle durch einen Rückruf zu der jeweiligen Telefonnummer. Dadurch wird sichergestellt, daß nur autorisierte und vorher bevollmächtigte Personen (besser: Telefonanschlüsse) Zugriff erhalten.

- **3 Modems an User PCs für spezielle Anwendungen**
  Einzelne Benutzer haben noch Modems lokal an ihren PCs um spezielle Anwendungen zu ermöglichen. Diese umfassen SMS-Versand zu Mobiltelefonen, Abfrage von kommerziellen Datenbankservern, usw.

- **3 Rechner mit ISDN-Karte für Bankzugang**
  Für verschiedene Anwendungen in der Abteilung Buchhaltung wird ein spezielles Programm einer Bank verwendet, um direkten Zugriff auf Firmenkonten zu erhalten.

Geforderte Ziele

Vorüberlegungen

Vor dem Beginn der Arbeit wurden verschiedene Ziele definiert. Sie basieren auf den Gegebenheiten der vorhandenen IT-Umgebung, deren Vorteilen und Mängeln. Es handelt sich dabei um Wünsche, die schon länger bestanden, genauso wie Überlegungen, die erst in Zusammenhang mit dieser Arbeit getroffen wurden. Diese Ziele sind keine exakte Definition des geforderten, sondern mehr ein Ergebnis eines Brainstorming - Vorgangs. An der Entstehung dieser Zusammenstellung sind alle Abteilungen des Betriebs beteiligt, damit das gewünschte Bild möglichst alle Anforderungen enthält. Die genauen Anforderungen werden später in der IT-Sicherheitspolitik und den Richtlinien zur IT-Sicherheit niedergelegt.

Ziele

- Internet- Zugang für bestimmte Benutzer
  Personen, denen das Internet die Erledigung Ihrer täglichen Arbeit erleichtert, sollen ungehindert ins Netz gelangen können. Diese Personen werden von der Geschäftsleitung bestimmt und sollen zentral verwaltet werden. Bisher lag die "Zugangskontrolle" im „Standard - Gateway - Eintrag” beim Betriebssystem. Internet- Mail soll (wie bisher) ohne Restriktionen für alle Benutzer verfügbar sein
- Erlauben des Einwählens bestimmter Personen
  Um das System von Aussenstellen aus zu Warten muss es möglich sein, sich per Telefonverbindung einzuwählen. Dies kann ein Fremdanbieter für Software als auch ein Administrator der eigenen Firma am privaten PC sein.
- Sicherung des Firmennetzes vor unerlaubten externen Zugriffen
  Wenn das lokale Netzwerk fest an das Internet angeschlossen wird, müssen auch Massnahmen zur Absicherung getroffen werden Es sollen sich nur vorher festgelegte Personen (Rechner) in das LAN einwählen können. Andere Verbindungsversuche abgelehnt und evtl. an den Sicherheitsbeauftragten gemeldet werden.
- Einhalten eines gegebenen Kosten- Nutzen- Verhältnisses
  Das Projekt Firewall ist ein Werkzeug um den Arbeitsablauf in der Firma zu vereinfachen, erfordert aber einen nicht unerheblichen Aufwand zur Installation und Wartung. Das bedeutet, daß der Aufwand und der laufende Betrieb nicht das Kosten - Nutzen - Verhältnis verschlechtern darf.
- Praktikable Anpassungen an der fertiggestellten Installation sollen nicht nur von Firewall-Spezialisten, sondern auch von anderen Administratoren durchgeführt werden können. Das bedeutet, daß einfache Wartung den Vorrang vor Hochsicherheit erhalten kann.
- Dokumentation zur Nachvollziehbarkeit administrativer Arbeiten
  Alle durchgeführten Arbeitsschritte sollen dokumentiert werden, damit Neuerstellung, Wartung und Modifikation auch ohne den Autor realisiert werden kann.

- Erreichbarkeit des Firmennetzes durch externe Firmenstandpunkte mittels VPN
  Es bestehen Aussenstellen der Firma in grossem Abstand zur Hauptniederlassung (auch Ausland). Es soll die Möglichkeit geschaffen werden, eine Verbindung zu diesen Netzen/Rechnern zu schaffen. Hierbei soll es vor allem auf die Punkte Sicherheit und Kosten geachtet werden.
- Kein zusätzlicher Aufwand für Endnutzer
  Der gesamte Vorgang soll für die Benutzer völlig transparent, d.h. unbemerkt vonstatten gehen. Auch sollen möglichst wenig Konfigurationen an den Client-Rechnern vorgenommen werden, um den Administrationsaufwand gering zu halten.
- Dienste für das Internet zur Verfügung stellen
  Internet - Server sollen eingerichtet werden können, wenn diese benötigt werden sollten. Anzudenken ist hier ein Firmeneigener WWW- oder auch Mail- Server.

IT Sicherheitsprozess

Der Sicherheitsprozess als Grundlage aller Aktivitäten

Die Erstellung einer Firewall wird von vielen auf das Aufstellen eines Routers und Einrichten von Filterregeln beschränkt. Sie ist jedoch nur ein Werkzeug von vielen, die verwendet werden können. Grundlage eines effektiven Einsatzes beliebiger Sicherheitsmechanismen ist eine sauber ausgearbeitete (Informations-) Sicherheitspolitik. Sie ist der Ursprung jeglicher Standards, Verfahren und Richtlinien, die im Unternehmen zum Einsatz kommen.

Die Sicherheitspolitik einer Institution umfasst alle Aspekte der Sicherheit. In dieser Arbeit wird eine eingeschränkte Form, die IT-Sicherheitspolitik, behandelt. Diese adressiert nur jenen Aspekt der Sicherheit, die maschinell verarbeitete Informationen betrifft. Sie umfasst sowohl physikalische Aspekte wie Katastropenschutz oder Zugangskontrolle als auch Datentechnische wie Verschlüsselung, Authentizität, etc. In ihr wird festgelegt wo die Verantwortlichkeiten und Rechte für Daten liegen und in welcher Weise diese Anforderungen umgesetzt werden.

Wie weit eine Security Policy ins Detail geht hängt i.a. von den Sicherheitsanforderungen der jeweiligen Institution ab. Ihr Umfang variiert von einer Seite mit kurzen Statements bis zu mehrseitigen, sehr detaillierten Abhandlungen. Das Ausarbeiten einer Security Policy umfasst mehrere Schritte[4], die auch in verschiedenen Organisationsebenen der Institution ablaufen:

1. Bestimmung des IT-Sicherheitsniveaus
2. Etablierung des IT-Sicherheitsmanagement- Teams
3. Definieren der IT-Sicherheitspolitik

Diese Schritte werden im folgenden etwas genauer beleuchtet.

Sicherheitsniveau

Das Sicherheitsniveau einer Institution hängt von verschiedenen Faktoren ab. Die wichtigsten Kriterien sind der Grad der Vertraulichkeit der eigenen Daten und deren Integritätsanforderungen.

Als Erstes muss festgestellt werden, welche Art von Daten erfasst und bearbeitet werden. Hierbei gibt es Daten, deren Verlust allenfalls ärgerlich ist. Dies sind z.B. temporäre oder redundante Dateien. Andere aber kosten Zeit, Arbeit, oder auch Geld wenn sie verloren gehen bzw. verändert werden. Zu ihnen gehören u.a. Produktdatenbanken, Personalinformationen und Daten aus der Zeitverwaltung. Ein ebenfalls wichtiger Punkt ist die Geheimhaltung, damit weder Konkurrenten neue Entwicklungen noch eigene Mitarbeiter z.B. Lohndaten ohne Autorisierung einsehen.

Um die Daten angemessen schützen zu können, muss man sich ihrer Wichtigkeit im Ablauf der täglichen Arbeit und Entscheidungen bewusst sein. Werden sie bei strategisch wichtigen Beschlüssen zu Grunde gelegt, ist ein sehr hohes Mass an

Sicherheit dafür zu fordern. Haben fehlende bzw. fehlerhafte Daten einen wesentlichen Zeitlichen Verzug für die Institution zur Folge, jedoch keinen fatalen Einfluss auf den Betrieb, so wird man ein mittleres Sicherheitsniveau veranschlagen. Sind die Fehler jedoch zu tolerieren oder mit minimalem Aufwand zu beseitigen, so genügt ein niedriges Niveau.

Beim festlegen auf das letztendlich geforderte Sicherheitsniveau sollte man unbedingt beachten, dass der Aufwand, der mit dem Erreichen eines entsprechend hohen Niveaus verbunden ist, exponentiell ansteigt, und absolute Sicherheit nur mit gezogenem Netzstecker realisiert werden kann.

Sicherheitsteam Etablieren

Das weitere Vorgehen beim Erstellen der Sicherheitsarchitektur wird von dem zu bestimmenden Sicherheitsteam ausgeführt. Der Umfang des Teams richtet sich nach der Phase der Einführung. Während der Planung und Realisierung werden je nach Netzwerk- und Firmengröße eine oder mehrere Personen durchgehend abgestellt. Nach erfolgreichem Start können sich in der Regel nur sehr große Firmen einen Vollzeit Sicherheits-Manager leisten, jedoch ist es nicht anzuraten, eine Firewall ohne spätere Kontrolle zu betreiben.

Das Sicherheits Management - Team hat die gesamte Planung, Durchführung und den Betrieb der Sicherheitseinrichtungen zu Überwachen, wobei die Gesamt-Sicherheitsverantwortung in der oberen Führungsebene bleibt. Zu seinen Aufgaben gehört das ständige Überdenken der Sicherheitspolitik, deren Änderung und das Anpassen der technischen Umgebung. Regelmäßige Kontrollen der Integrität des LANs und Berichte und Logs darüber sind zu erstellen, um Sicherheitslöcher frühzeitig zu erkennen.

Mycompany IT Sicherheitspolitik

Die folgenden neun Punkte geben die Sicherheitspolitik in genau der Form dar, in der sie in der Firma im Einsatz ist.

Detailliertere Informationen und Anweisungen zur Sicherheitspolitik finden sich in den Richtlinien zur IT-Sicherheit (s.u.).

1 Zweck

Beschreibung des geforderten Sicherheitsniveaus maschinell verarbeiteter Informationen

Festlegung von Rechten und Pflichten der Ersteller und Benutzer von Informationen

2 Geltungsbereich

2.1 funktionell / personell

Diese TI gilt für alle Abteilungen unseres Hauses, d.h. für alle Mitarbeiter, die mit maschinell verarbeiteten Informationen arbeiten

2.2 sachlich

alle maschinell verarbeiteten Informationen bei MyCompany

2.3 Ausnahmen

keine

3 Begriffsdefinition

IT-Sicherheitsmanagement - Team

> Die anfallenden Aufgaben, um das angestrebte IT-Sicherheitsniveau zu erreichen und zu erhalten, müssen von einer Instanz oder Person innerhalb der Firma koordiniert und verantwortlich geregelt werden. Diese Instanz oder Person wird als "IT-Sicherheitsmanagement - Team" der Firma bezeichnet.

4 Verantwortungen und Zuständigkeiten

Sicherheitsniveau realisieren
jeder Mitarbeiter

Schulung zur IT-Sicherheit
Abteilung IT

technische Grundlagen schaffen, prüfen, abändern
Abteilung IT

5 Beschreibung

5.1 Ermitteltes IT-Sicherheitsniveau (hoch / mittel / niedrig):
mittel, das heißt:

- Der Schutz von Informationen, die nur für den internen Gebrauch bestimmt sind, muss gewährleistet sein.
- Kleinere Fehler können toleriert werden, Fehler, die die Aufgabenerfüllung deutlich beeinträchtigen, müssen jedoch erkenn- oder vermeidbar sein.
- Längere Ausfallzeiten, die zu Terminüberschreitungen führen, sind nicht zu tolerieren.

Insgesamt ist zu beachten:
Schäden haben Beeinträchtigungen der Firma zur Folge.

5.2 Etablierung des IT-Sicherheitsmanagement - Teams

Die Teammitglieder bei Mycompany werden von der Abteilung IT bestimmt und sind in den Richtlinien zur IT-Sicherheit festgelegt.

5.3 Sicherheitsbewusstsein

Die IT-Sicherheitspolitik ist ein wichtiger Faktor für den zuverlässigen Ablauf bei den täglichen Aufgaben der gesamten Firma. Daraus folgt, dass auch das Sicherheitsbewusstsein ein entscheidender Erfolgsfaktor ist.

Sicherheitsbewusstsein wird durch folgendes Verhalten gekennzeichnet:

- Erkennen, dass effektive Sicherheit ein kritisches und wesentliches Element der Unternehmensphilosophie ist.
- Stets vorhandenes Sicherheitsbewusstsein bei allen täglich anfallenden Aktivitäten.
- Persönliche Verantwortlichkeit für proaktive Maßnahmen in Bezug auf sämtliche Risiken für Mitarbeiter, Informationen, Vermögenswerte und die Fortführung der Geschäftstätigkeit im Notfall.
- Ausrichten des Sicherheits- und Kontrollumfangs an das jeweilige Geschäftsrisiko.
- Verantwortung des einzelnen Benutzers für IT-Sicherheit in seinem jeweiligen Arbeitsbereich.

5.4 Aus dem Sicherheitsniveau abgeleitete Ziele

- Integrität der IT (Richtigkeit der gespeicherten und verarbeiteten Daten muss sichergestellt sein)
- Manipulationen ausschliessen und Benutzerfehler verhindern
- Unfälle (sowohl technische Defekte als auch grobe Software und Bedienerfehler) vermeiden und erkennen
- Verbindlichkeit der Daten (letzte Änderungen an z.B. CAD-Zeichnungen)

- Erstellen, Ändern, Löschen von Daten nachvollziehbar und auf Benutzer abbildbar machen. Dies umfasst auch Nichtabstreitbarkeit, Beweissicherheit, Nachweisbarkeit, Verantwortlichkeit.
- Sicherung der Daten gegen unautorisierten Zugriff sowohl von Aussen als auch von Innen
- Die Definition des Sicherheitsniveaus und die daraus resultierenden Zugriffsbeschränkungen unterliegen dem Ersteller/Eigentümer der Information bzw. Daten
- Zugriffsschutz besonders wichtig bei bestehenden Verbindungen z.B. ins Internet als auch bei direktem Zugriff bei lokalen Flottweg-Rechnern
- Keine Abschottung von der Aussenwelt (z.B. Internet) um den Informationsfluss zwischen Mitarbeitern und externen Quellen zu erleichtern und zu beschleunigen.
- Zugriff auf interne Daten durch Aussenstellen ermöglichen
- Kritische Daten sollen auch von anderen Firmenstandorten online eingesehen werden können, ohne von Unbefugten gelesen werden zu können
- Öffentlichen Zugriff auf dedizierte interne Daten von aussen erlauben
- Es sollen verschiedene Dienste (z.B. im Internet) zur Verfügung gestellt werden können

6 Anmerkungen

6.1 mitgeltende Unterlagen

keine

6.2 Literaturhinweise

IT - Grundschutzhandbuch des Bundesamt für Sicherheit in der Informationstechnik

6.3 Anmerkungen

keine

7 Dokumentation und Änderungsdienst

Diese TI und sämtliche Änderungen unterliegen zusammen mit den dazugehörigen Nachweisdokumenten vollständig der Dokumentationspflicht.

Zuständig für Änderungen ist der Leiter des IT-Sicherheitsmanagement - Teams

8 Verteiler

gemäß dem in TI-ORG-0001 definierten Verteiler für diese TI-Klasse.

9 Anlagen

- Richtlinien zur IT-Sicherheit
- Mitglieder IT-Sicherheitsmanagement Team

Richtlinien zur IT- Sicherheitspolitik

- Koordination und technische Durchführung von IT-Sicherheitsmaßnahmen liegen im Aufgabenbereich des IT-Sicherheits - Team
- Nur speziell geschultes Personal für sicherheitsrelevante Aufgaben
- Interne Email steht allen Benutzern zur Verfügung
- Internet- Zugang ist von Geschäftsleitung zu genehmigen, den Benutzern stehen folgende Dienste zur Verfügung:
  - HTTP
  - FTP (Client)
  - Email (SMTP, POP3)
  - Time
  - Telnet (Client)
- Zwingende Verwendung von sicheren Passwörtern bei allen Benutzern
- Physikalische Zugangskontrolle zu sicherheitsrelevanter Hardware (z.B. Rechnerraum)
- Sichere Aufbewahrung von Offlinedaten (z.B. Datensicherung) und von Software
- Benutzer, die mit Fremddaten arbeiten, haben einen Virenscanner zu benutzen
- Zugangskontrolle von Netzwerkzugriffen sowohl im lokalen Netzwerk als auch von aussen
- Speicherung von Daten auf zentralem Server, da nur hier effektive Zugangskontrolle und regelmäßige Datensicherung realisiert werden kann
- Sicherung des lokalen Netzwerks durch eine Firewall
- Errichten eines virtuellen privaten Netzwerks (VPN) zu Aussenstellen zur sicheren Kommunikation
- Binden verschiedener Internetdienste (FTP, HTTP) an Proxies zur besseren Kontrolle und Leistungssteigerung
- Errichten einer Demilitarisierten Zone (DMZ) zum Anbieten verschiedener Services sowohl intern als auch extern
- Zugriff auf Firmendaten soll durch noch zu bestimmende Methoden für Aussenstellen ermöglicht werden
- Bisher vorhandene Modems an User-PCs werden abgeschafft und durch die Routerverbindung ersetzt

Planung der Topologie

Logische Komponenten der Netztopologie

Um ein definiertes Sicherheitsniveau zu erreichen, muss der genaue Aufbau der Firewall bestimmt werden. Zusätzlich zur Hardware-Verdrahtung und Anordnung der Firewall - Bestandteile ist auch die Verwendung verschiedener Software - Komponenten zu evaluieren. Zum Schutz des LANs kann man die Clients "verstecken", damit sie vom externen Netzwerk aus nur unter (möglichst hohem) Aufwand erkannt werden. Ausserdem kann man den Verkehr zwischen zwei Netzen kontrollieren und einschränken.

Die wichtigsten dieser Methoden sollen im folgenden erläutert werden:

Network Address Translation (NAT)

NAT ist eigentlich eine Routerfunktion, die eingesetzt wird um kleine Netze mit nur einer (offiziellen) IP-Adresse an das Internet anzubinden. Anfragen an das Internet von einem Rechner des lokalen Netzwerks werden mit einer vorher bestimmten IP-Adresse weitergeroutet. Somit kann man die Zuordnung offizieller Adressen zu allen lokalen Rechnern sparen. Von einem Rechner im Internet erscheint dann das gesamte LAN als ein einziger Rechner (der Router selbst). Hierin liegt auch der Sicherheitsaspekt, da eine Verbindung nur zum Router aufgebaut werden kann. Dieser kann seinerseits wieder bestimmte Dienste (z.B. well known ports) auf andere Rechner umleiten. Wird NAT auf einem getrennten Router eingesetzt, ist zudem noch der IP-Stack vorhandener Server geschützt, da Angriffe vorher abgefangen werden.

Masquerading

Unter Maskieren eines Netzwerks versteht man das Austauschen der Quelladresse und Portnummer in jedem Paket, welches den Router nach aussen passiert. Antwortpakete in der entgegengesetzten Richtung werden symmetrisch behandelt, damit sie wieder am Ausgangspunkt ankommen. Man verwendet diese Technik, um nach aussen andere IP-Adressen vorzugaukeln, als tatsächlich verwendet werden. Auch bei dieser Lösung wird normalerweise ein eigener Router mit eigenständigem IP-Stack verwendet (siehe NAT).

Proxy

Ein Proxy Server fungiert als Mittelsmann zwischen lokalen Anwendungen und Servern im Internet. Client Applikationen, die einen Proxy verwenden, stellen eine Verbindung zum Internet nicht direkt her. Sie adressieren den Proxy und übergeben ihm die Vollmacht (engl.: proxy), ihre Anfrage durchzuführen.

Wenn direkte Verbindungen der einzelnen Rechner nicht erlaubt sind, sondern nur vom Proxy aus, kann der gesamte Datenverkehr an einer Stelle kontrolliert und protokolliert werden.

Diese Zentrale Stellung des Servers gibt die Möglichkeit, damit eine weitere Funktion (in diesem Fall ein Nebeneffekt) zu verbinden. Man kann den Rechner mit

entsprechender Speicherkapazität ausstatten und ihn als Puffer verwenden. Somit werden Anfragen an das Internet, z.B. der Abruf einer WWW-Seite, schneller beantwortet, da keine externe Verbindung aufgebaut werden muss. Stattdessen erhält der Client die temporär gespeicherten Daten einer vorangegangenen Verbindung eines anderen Users. Bei langsamen Verbindungen ins Internet kann dies zu drastischen Leistungssteigerungen führen wenn viele Benutzer die selben Dienste nutzen.

Wie bereits angedeutet, ist ein Proxy eine sogenannte "Application Level Firewall". Dies bedeutet, dass für jeden Dienst (www, ftp, etc.) eine spezielle Proxy - Software installiert werden muss. Man kann diese Eigenschaft als Nachteil (erhöhter Administrationsaufwand) aber auch als Vorteil (restriktivere Kontrolle) betrachten. Je nach Einsatzgebiet muss entschieden werden, ob sich ein Einsatz lohnt, oder ob auf andere Mechanismen zurückgegriffen werden sollte.

IP Paketfilter

Beim IP filtering wird der Datenverkehr aufgrund der Informationen in den einzelnen IP- Packet- Headern geregelt. Dabei werden Quell- und Zieladresse als Hauptkriterium für die Filterung verwendet. So werden z.B. Pakete vom äusseren Netz kommend mit einer Quelladresse aus dem inneren Netz abgelehnt, um Angriffe abzuwehren. Auch die angesprochenen Ports (source und destination) werden blockiert um einzelne Dienste zu verbieten oder zuzulassen.

Man unterscheidet zwei Arten der Filterung:

1. Statische Filterung
   Filterung aufgrund genau festgelegter Regeln bezüglich der IP-Header
2. Stateful Inspection
   Filterung kann abhängig sein von älteren Paketen, die mit dem aktuellen in Verbindung stehen. Hiermit werden Antwortpakete bei verschiedenen Diensten akzeptiert, welche bei statischer Filterung nicht erlaubt wären.

Trifft auf ein eintreffendes Paket eine Filterregel zu, so wird es entweder einfach fallengelassen, oder dem Absender signalisiert, dass es abgelehnt wurde. Die Reaktion kann bei jeder Filterregel angegeben werden.

Abgelehnte Pakete werden nach der ausgelösten Filterregel sortiert und aufgezeichnet, um später eventuelle Angriffe zu analysieren.

Das Problem bei dieser Lösung ist, dass man nicht bestimmen kann, wer erfolgreich die Netzgrenzen passiert hat.

Virtual Private Network (VPN)

Mehrere lokale Netzwerke können mit Hilfe des Internets verbunden werden. Diese Verbindung liegt jedoch offen und ist für jeden abhörbar. Mit einem sogenannten IP-Tunnel zwischen zwei LANs kann die Verbindung nach aussen geschützt werden.

Zuerst wird eine IP-Verbindung erstellt, bei der sich die Endstellen (Firewall oder Router) authentifizieren und einen session key für die Übertragung festlegen. Alle

Datenpakete, die die beiden Netzwerke danach austauschen, werden mit dem session key verschlüsselt und auf dieser Verbindung übertragen.

Diese Technik hat mehrere Vorteile:

- Die Verschlüsselte Verbindung sorgt für vertraulichen Datentransfer
- Authentifizierung stellt sicher, dass nur der entsprechende Partner die Verbindung aufbauen kann
- Die beiden Netzwerke werden völlig transparent kombiniert
- Es sind keine WAN-Direktverbindungen nötig, da die Verbindung mit jeweils einem (meist Ortsnetz-) Zugang ins Internet funktioniert

Nachteilig wirkt sich der erhöhte Administrationsaufwand (z.B. Schlüsselverwaltung) und die unsichere Übertragungskapazität des Internets aus.

Physikalische Komponenten der Netztopologie

Neben den logischen Aspekten einer Firewall muss auch der physikalische Aufbau bestimmt werden. Verschiedene Möglichkeiten, Sicherheit zu realisieren sollen im folgenden beschrieben werden.

Bastion Host

Einen Rechner, der besonders gesichert ist und als „Bollwerk" gegen Eindringlinge eingesetzt wird, nennt man Bastion Host. Er dient der Verteidigung des lokalen Netzwerkes und sollte besondere Aufmerksamkeit vom Administrator (in der Form von regelmässigen Audits und Sicherheits- Patches) erhalten.

Dual Homed Host/Gateway

Wenn ein Rechner Teil von zwei Netzen ist (mit zwei Netzwerkkarten), spricht man von einem Dual Homed Host. Oft bietet dieser Rechner auch Gateway- Funktionen an. Um hohe Sicherheit zu erlangen wird die Routing- Funktion deaktiviert. Dann können lokale und Internet- Hosts mit dem Gateway kommunizieren, aber direkter Datenfluss wird unterbunden.

Router mit Firewall-Funktionalitäten

Es gibt viele Hersteller von Routern, die in ihre Geräte Firewall-Funktionalitäten integrieren. Dies sind meistens IP-Filter, die mehr oder weniger detailliert konfiguriert werden können. Manche Geräte aus der höheren Preisklasse bieten weitergehende Funktionen wie IP-Tunneling (VPN) oder Stateful Inspection an. Solche „Screening Router" werden jedoch sehr oft als Teil einer Firewall eingesetzt.

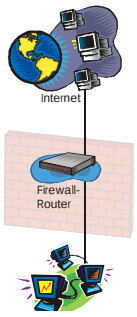


Abb.2

Der Einsatz eines solchen Routers als alleinige Firewall-Einrichtung ist jedoch nur beschränkt und nur für kleine Netze zu empfehlen. Bei hohen Sicherheitsanforderungen bietet diese Lösung nicht genügend Freiraum zum Konfigurieren und ausserdem keine Möglichkeit einer Application Level Firewall.

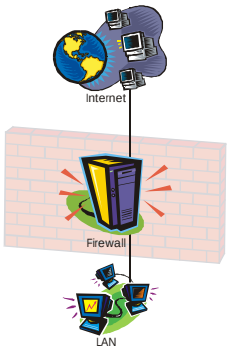


Abb.3

Firewall-Rechner mit Routerfunktion

Eine Konfiguration dieser Art bietet die gesamte Palette der Möglichkeiten, ist jedoch nicht für Hochsicherheit geeignet. Die Konzentration aller Einrichtungen auf einem Rechner bietet zu viele Möglichkeiten für Angreifer bei einer Fehlkonfiguration. Auch Fehler der verwendeten Programme führen zu Sicherheitslücken, die durch mehrstufige Firewalls geschlossen werden (können).

Firewall-Rechner hinter Router

In den häufigsten Fällen ist der Firewall- Rechner im lokalen Netz und der Router lässt nur Verkehr vom Internet zum Bastion Host zu. Dieser überprüft die Zulässigkeit der Verbindung und kann sie erlauben oder abblocken. Wenn der Router mit Packet Filtering Rules ausgestattet ist, wird die dahinter liegende Firewall zusätzlich geschützt.

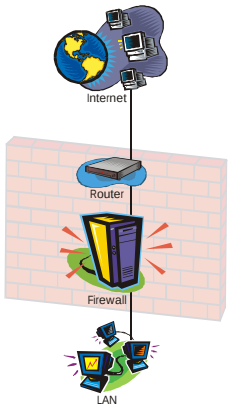


Abb.4

Der Router arbeitet mit seinem eigenen TCP/IP Stack, welcher oft wesentlich stabiler ist als der einer Softwareimplementation. DOS-Angriffe (z.B. Ping of Death, SYN-Flooding) werden somit vom Firewall-Rechner abgehalten und die Down-Zeiten verringert, da ein Router schneller wieder online ist als ein neu zu startender Rechner.

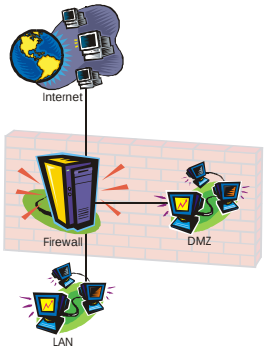


Abb.5

DMZ an Firewall

Bei vielen Anwendungen ist es von Vorteil, ein begrenzt sicheres Netz zu haben. Es entspricht nicht den hohen Sicherheitsanforderungen des LANs, erlaubt aber dennoch eine gewisse Überwachung und Abschirmung. Ein solches Netzwerk nennt man "Demilitarisierte Zone". Es wird im allgemeinen dafür benutzt, Dienste für das externe Netz zur Verfügung zu stellen.

Screened Subnet

Ein Screened Subnet ist eine Erweiterung der oben genannten Methoden, da zwischen zwei Firewall - Router ein „Abgeschirmtes Netzwerk” geschalten wird. Diesem wird nicht völlig vertraut, aber es hat auch nicht mehr einen so feindlichen Charakter wie das externe Netz.

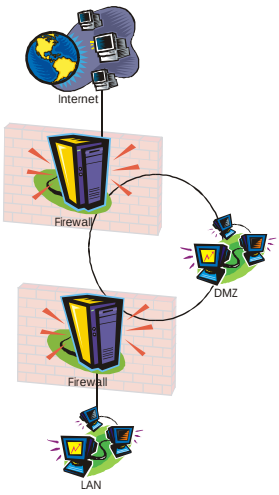


Abb.6

Im Gegensatz zu den obigen Methoden müssen hier zwei Firewall - Systeme überwunden werden, um an das LAN zu gelangen. Sind diese noch von verschiedenen Herstellern und/oder auf verschiedenen Plattformen erhöht sich der notwendige Aufwand für den potentiellen Eindringling, diese Wand zu durchbrechen.

In dieser DMZ stehen oft Dienste für das externe Netz zur Verfügung und auch das lokale Netz kann auf die DMZ zugreifen. Direkter Verkehr zwischen den beiden Netzen wird jedoch unterbunden. Eine Application Level Firewall auf einem Bastion Host kann diese Verbindung für spezielle Dienste ermöglichen.

Entscheidung für ein Gesamtsystem

Um die geforderte Sicherheit für das Firmennetz zu erreichen, soll eine Kombination verschiedener Techniken eingesetzt werden.

Der Firewall Rechner

Als Firewall wird ein Linux- Rechner mit Kernel- Filterung und Proxy für die wichtigsten Services (anfänglich nur http, kann bei Bedarf nachträglich erweitert werden) eingesetzt. Dieser sichert das interne Netz ab und bietet gleichzeitig Zugang zu der Demilitarisierten Zone. Als Grundlage für die Zugangsbeschränkungen dient die bereits definierte Sicherheitspolitik und die davon abgeleiteten Richtlinien.

Die Entscheidung zu Gunsten dieses Freeware Systems ist aus zwei Gründen gefallen. Einerseits sind die Anschaffungskosten sehr gering, da sie sich auf die Hardwarekosten beschränkt. Lediglich die Einarbeitung in ein neues und vermeintlich wenig dokumentiertes System führt zu gesteigertem Zeitaufwand. Die Dokumentation kann zwar nicht in gedruckter Form vom Software- Hersteller bezogen werden, es gibt jedoch im Internet grossartige Informationsquellen in Form von HOWTOs, FAQs und Newsgroups.

Der Zeitaufwand wird im Gegenzug durch die tiefgehenden Kenntnisse der Konfigurationsmöglichkeiten belohnt. Bei einfach zu benutzenden und vorkonfigurierten, aber komplexen Systemen herrscht oft ein Mangel an Einstellungsmöglichkeiten. Bei Linux können alle Komponenten einfach mit ASCII - Konfigurationsdateien eingestellt werden und ein Überblick über die verwendeten Einstellungen ist leicht zu erhalten.

Der zweite Grund, der für Linux spricht ist, dass es sich hierbei um ein Open Source Betriebssystem handelt. Undurchsichtige Firmenpolitik grosser Unternehmen macht es schwer, deren Sicherheitspolitik zu vertrauen. Man kann die inneren Vorgänge in Hard- bzw. Softwareelementen nur schwer bzw. überhaupt nicht nachvollziehen und überprüfen. Somit muss man glauben, was der Hersteller verspricht, oder auf den Einsatz der Anlage verzichten.

In diesem Fall trifft die Wahl somit nicht auf Standardsysteme von bekannten Herstellern, sondern Linux mit all seinen Tools und Programmen. Diese werden (auch in Zukunft) ständig von Programmierern weltweit auf Probleme und Fehler getestet und können bei bedarf auch selbst abgeändert werden.

Anbindung nach Aussen

Die Internet - Einwahl wird von einem Router mit (optimaler Weise) Standleitungsanschluss zum Provider erstellt. Über diese Leitung werden Emails versandt und empfangen und den Benutzern weitere Internet Dienste zur Verfügung gestellt. Der zuständige Router führt NAT durch, wodurch das gesamte (DMZ, Router - DMZ und interne) Netz versteckt wird. Des weiteren erledigt er eine erste Paketfilterung, um illegale Pakete, wie z.B. IP - Spoofing, abzublocken.

Eine Anbindung von Aussenstellen wird von einem VPN-Router erstellt. Er erhält einen breitbandigen Internet- Connect (dial-up), und erstellt dann einen IP - Tunnel zum Verbindungspartner. Im konkreten Fall ist dieser Partner entweder ein eigenes Netzwerk, wie im Falle Othercompany, oder ein Einzelrechner eines Teleworkers. Dieser Router erstellt auch direkte (ISDN-PPP-) Verbindungen zu Firmen, welche Fernwartung von Software- Komponenten betreiben.

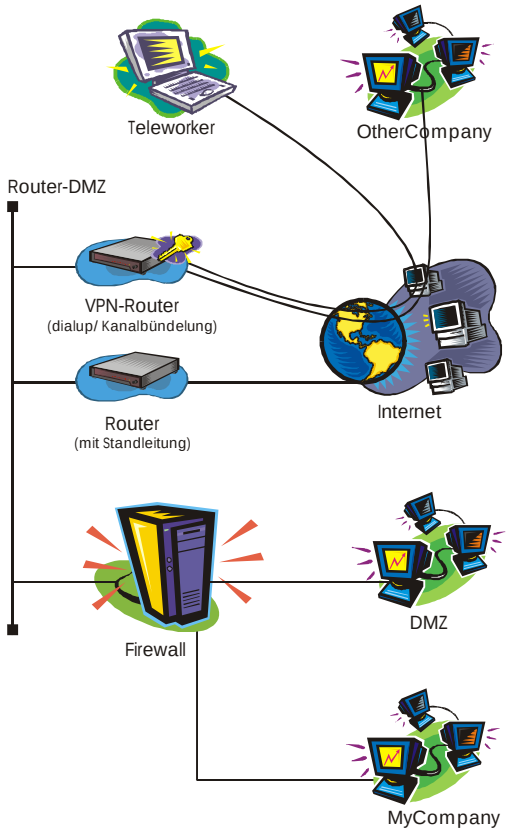


Abb.7

Router-DMZ

Die oben beschriebenen drei Komponenten (zwei Router und Firewall- Rechner) werden von einem Zwischennetz, der Router-DMZ verbunden. Da hier sonst kein Rechner angeschlossen ist, ist dieser Abschnitt leicht zu verteidigen. Es gibt keinen Host, der, im Falle eines Einbruchs, einen weiteren Ausgangspunkt für feindliche Aktivitäten liefert. Lediglich der Firewall Rechner bietet diese Eigenschaft. Ist dieser jedoch kompromittiert, liegt das lokale Netzwerk schon offen.

DMZ

Ein weiteres abgeschirmtes Netzwerk (Screened Subnet) befindet sich hinter dem Firewall - Rechner. Prinzipiell muss es als inneres Netz betrachtet werden, da es organisatorisch, also sowohl vom Routing als auch von der Zugriffskontrolle, auf der selben Ebene wie das Firmen - LAN liegt. Auf diesem werden Dienste für das Internet zur Verfügung gestellt, welche in beschränktem Maße überwacht werden sollen. Rechner in diesem Netz sind erschwert angreifbar. Einerseits werden sie bereits von der Firewall abgeschottet, damit einfache Angriffe im Vorhinein abgeblockt werden. Sie sind jedoch nicht ganz sicher. Dies liegt daran, dass eine gewisse Offenheit erlaubt werden muss, um Dienste bereit stellen zu können. Wäre dies nicht der Fall käme es schnell zu Problemen, wenn die angebotenen Services etwa um Audio, Video oder Datenbank erweitert werden sollen. Man erkauft sich hier also Flexibilität auf Kosten von Sicherheit.

Das interne Netz

Am besten gesichert ist das interne Netzwerk. Verbindungen nach innen sind zu Unterbinden und nach aussen zu Überwachen. Da den lokalen Usern möglichst viele Möglichkeiten im Internet gestattet werden sollen, dürfen nur sehr begrenzt einschränkende Methoden verwendet werden um das Netzwerk abzusichern. Es sollen http, https, ftp, mail, telnet, time, ping, nameserver, news und viele andere Dienste verwendet werden. Aus diesem Grund ist ein Dual Homed Gateway ohne Routing, aber mit Proxy- Fähigkeiten keine praktikable Lösung.

Flexibilität

Bei dieser Konstellation können die Elemente DMZ und VPN jeweils entfernt bzw. erweitert werden, ohne an dem Firewall- Rechner Änderungen vornehmen zu müssen.

Auch die Art der Verbindung ins Internet steht auf diese Weise völlig offen. Man kann nach Belieben von Wähl- auf Standleitung umstellen. Auch xDSL, Kabelanschluss oder Satelliten - Verbindungen sind einfach durch den Austausch des entsprechenden Routers implementierbar.

Das Betriebssystem

Der Linux - Rechner muss eine solide Grundlage bilden, um ein verlässliches Firewall - System aufzubauen. Es sollte stets der Grundsatz gelten, so wenig wie möglich und so viel wie unbedingt nötig. Diese Vorgehensweise wird dadurch begründet, dass jedes zusätzliche Element einen gewissen Unsicherheitsfaktor einbringt. Dieser gründet in fehlerhafter Software, schlechter Vorkonfiguration, nicht benutzter Komponenten oder unbekannten Funktionalitäten dieser Elemente. Ebenso bietet jede zugelassene Methode eines Netzwerkzugriffes auf den Rechner (auch verwendete Router sind davon betroffen) Angriffsmöglichkeiten durch Implementations- und Programmfehler.

Schon bei der Installation muss darauf geachtet werden, nur wirklich benötigte Komponenten zu Installieren. Hierzu gehört das Linux- Grundsystem, Programmiertools zum Compilieren des Kernels, einen minimalen Netzwerksupport und natürlich die Firewall- Software IP-Chains[5]. Nach der Installation muss noch der Kernel auf ein Minimum reduziert und compiliert werden. Wichtige Komponenten sind hierbei:

- Networking Support
- TCP/IP Networking
- IP Firewalling
- Network Device Support
- Ethernet (10 or 100Mbit)
- Treiber der verwendeten Netzwerkkarten

Masquerading/NAT wird abgeschaltet, da diese Funktion von den beiden ISDN-Routern durchgeführt wird. Nicht benutzte Datei- und Bussysteme sollten deaktiviert werden, da ein kleinerer Kernel auch zu mehr Performance beiträgt.

Danach ist es an der Zeit einen ersten Test mit der o.g. Einstellungen zu machen. Eine beliebte Fehlerquelle ist das Weglassen dringend benötigter Komponenten oder das Einbinden von Treiberdateien als Modul, welche schon beim Systemstart erforderlich sind. Da Module erst geladen werden, wenn sie benötigt werden, kommt es sofort zu Problemen, wenn z.B. von einer SCSI-Festplatte gestartet werden soll und der Treiber als Modul vom Kernel nachgeladen werden muss, gibt es einen Konflikt.

Im zweiten Schritt werden die Netzwerk- Dienste, welche überflüssig sind deaktiviert[6]. Bei dem verwendeten SuSE- Linux ist die Datei /etc/inetd.conf für das automatische Starten solcher Services verantwortlich. Diese muss so weit geändert werden, dass nur noch unbedingt notwendige Dienste gestartet werden.

Da in diesem Fall das Routing vom Betriebssystem- Kernel durchgeführt wird, ist dafür kein Dienst notwendig.

Ebenso wird auf remote login Möglichkeit verzichtet, und nur an der Konsole Tätigkeiten durchgeführt. Durch diese Minimalität können sämtliche in

/etc/inetd.conf genannten Services deaktiviert werden. Nach der Einschränkung des Systems sollten lediglich noch lebensnotwendige Dienste laufen.[7]

Um diese Tätigkeiten zu vereinfachen, stellt SuSE ein PERL-Script (harden_suse.pl) zur Verfügung, mit dem der zweite Schritt automatisiert wird.

Zur sofortigen Kontrolle des reduzierten Systems bieten sich die folgenden einfachen shell- Befehle an:

- netstat -an
  Dieser Befehl zeigt Netzverbindungen, offene Ports und deren Eigenschaften an.
- ps aux ww
  Listet alle Prozesse (aller User) an.

Hiermit kann schnell ein Überblick über die laufenden daemons, Hintergrundprogramme und deren Netzwerk - Aktivitäten gewonnen werden. Es gibt auch hierfür vorgefertigte Shell - Scripts von SuSE. Diese täglichen, wöchentlichen und monatlichen Einsatz ausgelegt. Offene Netzwerk - Ports und -Dienste werden genauso angezeigt wie vorhandene devices und geänderte Systemdateien.

Routing

Prinzipien

IP - Adressraum

Für den Gebrauch in privaten Netzen sind drei Adressräume reserviert[8]. Sie werden im Internet nicht vergeben und dort auch nicht weitergeleitet, d.h. von Routern blockiert. Es handelt sich hier um die Bereiche:

- 010.xxx.xxx.xxx, 255.0.0.0
- 172.016.xxx.xxx bis 172.031.xxx.xxx, 255.255.0.0
- 192.168.xxx.xxx, 255.255.255.0

Das vorhandene Netzwerk baut (aus historischen Gründen) auf dem Adressbereich 192.12.144.0, 255.255.255.0 auf. Wenn man mit diesen Adressen eine Verbindung ins Internet erstellt, wird dieser Bereich des Internets nicht geroutet und somit für lokale Anwender ausgeblendet.

Realisierung

Um diesen Zustand zu ändern, muss das gesamte LAN auf einen privaten Adressbereich umgestellt werden. Damit genügend Ressourcen für spätere Netzerweiterungen vorhanden sind, wird auf den Bereich 192.168.144.0, 255.255.255.0 umgestellt. Es wird hier nur die zweite Zahl der Adresse geändert, was die Automatisierung erleichtert. Die anderen lokalen Netzwerke (Router-DMZ, DMZ) werden auf 192.168.1.0 bzw. 192.168.112.0 festgelegt.

Mycompany	192.168.144.0
DMZ	192.168.112.0
Router DMZ	192.168.1.0
Othercompany	192.168.200.0
VPN	192.168.100.0
Internet	Dynamische IP Adresse

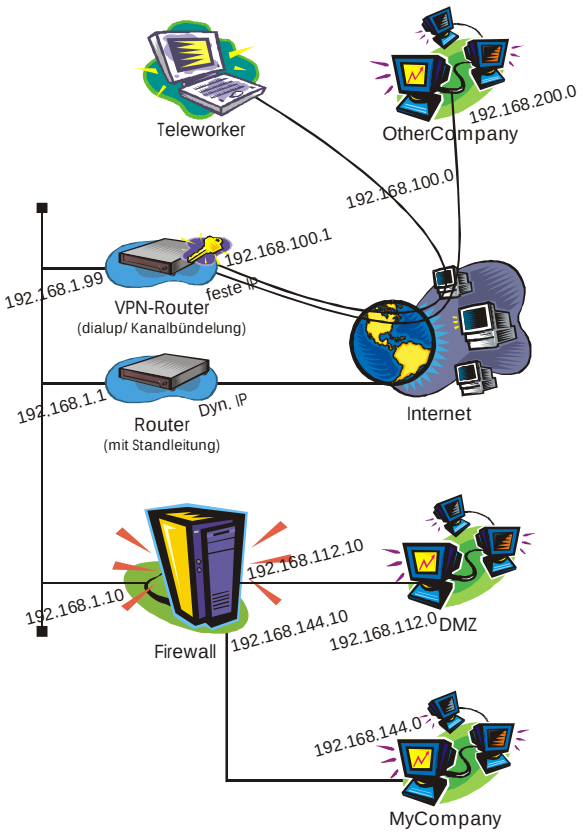


Abb.8

Konfiguration

Die folgende Tabelle zeigt die geforderten Verbindungen bzw. Einschränkungen im oben beschriebenen Firewall - Aufbau. Sie enthält einige Details, die erst in späteren Phasen Wichtigkeit erlangen, zeigt aber die nötigen Einträge für die drei verwendeten Router auf.

nach von	Mycompany	DMZ	Router- DMZ	Internet	VPN
Mycompany		mail, www, dns, ftp	alles	alles	alles
DMZ	Datenbank-Zugriff		nichts	mail, ftp, dns	nichts
Router- DMZ	nichts	nichts		Proxy-Dienste, dns	nichts*
Internet	nichts	www, ftp, mail, dns	Proxy-Dienste, dns		nichts
VPN	alles	nichts	nichts *	nichts	nichts

* für Verbindungen über das VPN werden keine Proxy-Dienste verwendet

Routing - Tabellen

Für die jeweiligen Router werden die folgenden Routing - Tabellen aus der o.g. Tabelle abgeleitet.

Firewall (192.168.144.10, 192.168.112.10, 192.168.1.10):

Ziel	**Adresse**	**Gateway**	**Maske**	**Interface**
Mycompany	192.168.144.0	0.0.0.0	255.255.255.0	eth0
DMZ	192.168.112.0	0.0.0.0	255.255.255.0	eth1
Router-DMZ	192.168.1.0	0.0.0.0	255.255.255.0	eth2
Other company	192.168.200.0	192.168.1.99	255.255.255.0	eth2
default	0.0.0.0	192.168.1.1	0.0.0.0	eth2
Dienstleister	???	192.168.1.99	255.255.255.0	eth2

VPN-Router (192.168.1.99, 192.168.100.1):

Ziel	**Adresse**	**Gateway**	**Maske**	**Interface**
Mycompany	192.168.144.0	0.0.0.0	255.255.255.0	eth
Router-DMZ	192.168.1.0	0.0.0.0	255.255.255.0	eth
Other company	192.168.200.0	0.0.0.0	255.255.255.0	isdn
Dienstleister	???	0.0.0.0	255.255.255.0	ppp-isdn

Router (192.168.1.1, dyn. IP bei ISP):

Ziel	**Adresse**	**Gateway**	**Maske**	**Interface**
Router-DMZ	192.168.1.0	0.0.0.0	255.255.255.0	eth
DMZ	192.168.112.0	192.168.1.10	255.255.255.0	eth
Mycompany	192.168.144.0	192.168.1.10	255.255.255.0	eth
default	0.0.0.0	0.0.0.0	0.0.0.0	isdn

Um das VPN (siehe Kap. VPN) abzusichern, muss das Routen von privaten Adressen zum Internet unterbunden werden.

Sollen diese Systeme sicher eingerichtet werden, dürfen sie nicht in einem Netzwerk konfiguriert werden, welches einen unbefugten Zugang zu den Geräten ermöglicht.

Testaufbau

Zum Test des Firewallsystems wird ein Netzwerk aufgebaut, welches aus einem Rechner je Subnetz besteht. Diese erhalten natürlich die entsprechenden Netzwerkadressen und Routingtabellen (i.a. Nur eine default route). Es werden sowohl Linux als auch Windows- Rechner eingesetzt, um alle Einsatzzwecke zu simulieren.

Der Physikalische Aufbau entspricht der obigen Grafik, wobei auf den Router für den standard Internetzugang verzichtet wird. Um das ISDN-Routing zu Testen, werden zwei Router (der VPN-Router und seine zukünftige Gegenstelle) an das Hausinterne Telefonnetz angeschlossen. Der VPN-Router auf der Seite des Testnetzes und seine Gegenstelle bildet die Verbindung zum momentanen Firmennetz. Somit bildet das vorhandene LAN in dieser Simulation das Internet bzw. später das externe VPN-Subnetz.

An dieser Stelle ist wieder ein Test der neu hinzugefügten Funktionen durch zu führen, um entstandene Fehler möglichst schnell zu entdecken und diese nicht anderen Arbeitsschritten zu vererben.

In diesem Stadium sollte ein ping- Befehl in allen Kombinationen von Start- und Zieladresse (d.h. Intern, DMZ, Router-DMZ und Extern) durchgeführt werden.

Packet Filtering

Um den Verkehr zwischen den jeweiligen Teilnetzen einzuschränken wird nun IP - Packet - Filtering bzw. Spoofing - protection eingebaut. Wie schon oben erwähnt wird zu diesem Zweck das Softwarepaket „IPChains"[9] verwandt. Das Programm prüft alle eingehenden IP-Pakete auf Übereinstimmung mit den definierten Regeln und führt die erste zutreffende Aktionen aus. In der IPChains - Syntax steht `ACCEPT` für Akzeptieren, `REJECT` für ablehnen und `DENY` für fallen lassen des empfangenen Pakets.

Realisierung

Beim Einrichten der Filterung kann man sich nahe an der Dokumentation des IPChains - Paketes halten.[10] Eine wichtige Richtlinie ist, wie überall bei sicherheitsrelevanten Angelegenheiten, alles zu verbieten, was nicht ausdrücklich erlaubt ist. Deshalb sollte die letzte Filterregel in der forward - Kette jeglichen Netzverkehr verbieten:

```
ipchains -A forward -j DENY
```

Somit werden alle Pakete abgelehnt, die nicht von dem angegebenen Regelwerk akzeptiert werden.

Um die Konfiguration übersichtlicher zu halten, werden danach Regelgruppen angelegt, um die verschiedenen Quell- und Zielbereiche zusammen zu fassen. Die folgenden Bezeichnungen werden für das interne LAN, die DMZ und das externe (als feindlich betrachtete) Netz verwendet:

- in (Innen, 192.168.144.0, 255.255.255.0), eth0
- dmz (192.168.112.0, 255.255.255.0), eth1
- aus (Aussen, alles ausser 192.168.0.0, 255.255.0.0), eth2

Die Regelgruppen tragen somit die Namen in-aus, in-dmz, dmz-in, dmz-aus, aus-in, aus-dmz und zeigen die Verbindungsrichtung an. So bedeutet also in-aus, dass die Verbindung von innen nach aussen aufgebaut wird. Ebenso empfiehlt die Dokumentation eine Gruppe für ICMP-ACCEPT - Packets (name: icmp-acc) und für direkte Adressierung der drei Netzwerkkarten einzurichten. Der Befehl zum Einrichten einer neuen Gruppe (hier „in-aus") lautet:

```
ipchains -N in-aus
```

Im Anschluss daran werden die Sprungregeln definiert, mit denen in die jeweilige Gruppe verzweigt wird. Hier ein Beispiel für eine Verzweigung von der Quelladresse 192.168.144.0 (intern) zu dem Ziel - Interface eth1 (DMZ):

```
ipchains -A forward -s 192.168.144.0/24 -i eth1 -j in-dmz
```

In den so erstellten Gruppen werden anschliessend die Regeln zum Akzeptieren verschiedener Protokolle (genauer: deren Ports) eingerichtet. Der Befehl zum Erlauben von z.B. WWW - Verbindungen (zu Port 80) vom Quellnetz 192.168.144.0 (innen) nach aussen lautet:

```
ipchains -A in-aus -p tcp www -j ACCEPT
```

Im Gegenzug muss die Antwort des WWW-Servers von aussen nach innen erlaubt werden. Dies wird dadurch erreicht, dass Pakete mit dem Quellport 80, ohne SYN-Flag und der Quelladresse des Webservers zugelassen sind:

```
ipchains -A aus-in -p tcp ! -y -s 192.168.112.11 www -j ACCEPPT
```

Der Befehl für DNS-Anfragen von innen an die DMZ lautet:

```
ipchains -A in-dmz -p tcp -d 192.168.112.11 domain -j ACCEPT
ipchains -A in-dmz -p udp -d 192.168.112.11 domain -j ACCEPT
```

Um die Filterregeln zu entwerfen muss darauf geachtet werden, dass Verbindungen Aus der Tabelle im Kapitel Routing können folgende geforderte Kombinationen für Port, Quell- und Zieladressraum erstellt werden:

in-aus

dns-request, ftp, nntp, ping, pop3, smtp, telnet, traceroute, www

in-dmz

dns-request, ftp, ping, pop3, smtp, www

dmz-in

dns-reply, ftp-reply, pong, smtp-reply, www-reply, Datenbank

dmz-aus

dns-request, dns-reply, pong, pop3, smtp, smtp-reply, www-reply

aus-in

dns-reply, ftp-reply, pong, smtp-reply, www-reply

aus-dmz

dns-request, dns-reply, ftp, ping, pong, pop3, smtp, smtp-reply, www

In

dns-request, ping, pong

Aus

pong

dmz

dns ,dns-reply, pong

Icmp-acc

destination-unreachable, source-quench, time-exceeded, parameter-problem

In der input chain werden Pakete behandelt, die direkt an den Firewall Rechner adressiert sind, abhängig von der angesprochenen Netzwerkkarte.

Konfiguration

Zum vereinfachten Einspielen und Auslesen der erstellten Filterregeln werden die Tools `ipchains-save` bzw. `ipchains-restore` verwendet. Das erste der beiden Programme sichert die aktuelle Konfiguration in eine Datei, wobei das zweite aus der Konfigurationsdatei die Filterregeln wieder herstellt.

Sind die Regeln komplett, wird ein Script zum Einrichten der Filterung erstellt. Am Ende der Datei wird ‘squid’ gestartet. Es handelt sich hierbei um das verwendete Proxy - Programm, auf welches später genauer eingegangen wird.

Der Aufruf des Scriptes erfolgt beim Booten des Rechners in der Datei `/etc/rc.d/boot.local` und muss manuell eingetragen werden. Um es abzusichern, müssen ihm noch entsprechende Rechte zugewiesen werden (`chmod 700`), damit es nur von root ausgeführt werden kann.

Hier der Inhalt der Datei `/etc/rc.d/rc.firewall` (Kommentare sind mit dem Zeichen "`#`" gekennzeichnet):

```
#!/bin/sh
#
# enable IP-forwarding (nedded for redirection)
echo 1 > /proc/sys/net/ipv4/ip_forward
#
# startup ipchains

# mit -P wird die Policy fuer die Kette gesetzt
ipchains -P input ACCEPT
ipchains -P forward DENY
ipchains -P output ACCEPT
# -N dient dem Anlegen von benutzerdefinierten Ketten
ipchains -N in-aus
ipchains -N in-dmz
ipchains -N dmz-in
ipchains -N dmz-aus
ipchains -N aus-in
ipchains -N aus-dmz
ipchains -N ftp-data
ipchains -N icmp-acc
ipchains -N vpn
ipchains -N in
ipchains -N aus
ipchains -N dmz

# Die input Kette dient der Kontrolle des direkten Zugriffs
# auf den Firewall - Rechner (Folgeketten: aus, in, dmz)
ipchains -A input -s 192.168.144.0/24 -d 192.168.144.10/32 -j in
ipchains -A input -s 192.168.112.0/24 -d 192.168.112.10/32 -j dmz
ipchains -A input -s 0.0.0.0/0 -d 192.168.1.10/32 -j aus

# Die forward Kette teilt den Verkehr in Unterketten, abhängig
# von Quell- und Zielnetzwerk
ipchains -A forward -s 192.168.200.0/24 -d 192.168.144.0/24 -i eth2 -j vpn
ipchains -A forward -s 192.168.144.0/24 -d 0.0.0.0/0 -i eth1 -j in-dmz
ipchains -A forward -s 192.168.144.0/24 -d 0.0.0.0/0 -i eth2 -j in-aus
ipchains -A forward -s 192.168.112.0/24 -d 0.0.0.0/0 -i eth2 -j dmz-aus
ipchains -A forward -s 192.168.112.0/24 -d 0.0.0.0/0 -i eth0 -j dmz-in
ipchains -A forward -s 0.0.0.0/0 -d 0.0.0.0/0 -i eth1 -j aus-dmz
ipchains -A forward -s 0.0.0.0/0 -d 0.0.0.0/0 -i eth0 -j aus-in
ipchains -A forward -s 0.0.0.0/0 -d 0.0.0.0/0 -j DENY -l

ipchains -A in-aus -s 0.0.0.0/0 -d 0.0.0.0/0 9037:9037 -p 6 -j ACCEPT
ipchains -A in-aus -s 0.0.0.0/0 -d 0.0.0.0/0 23:23 -p 6 -j ACCEPT
ipchains -A in-aus -s 0.0.0.0/0 8:8 -d 0.0.0.0/0 -p 1 -j ACCEPT
ipchains -A in-aus -s 0.0.0.0/0 -d 0.0.0.0/0 25:25 -p 6 -j ACCEPT
ipchains -A in-aus -s 0.0.0.0/0 -d 0.0.0.0/0 110:110 -p 6 -j ACCEPT
```

```
ipchains -A in-aus -s 0.0.0.0/0 -d 0.0.0.0/0 21:21 -p 6 -j ACCEPT
# Die Kette ftp-data legt dynamisch die Regeln für antwortende Datenverbindungen.
ipchains -A in-aus -s 0.0.0.0/0 -d 0.0.0.0/0 20:20 -p 6 -j ftp-data
ipchains -A in-aus -s 0.0.0.0/0 -d 0.0.0.0/0 443:443 -p 6 -j ACCEPT
ipchains -A in-aus -s 0.0.0.0/0 -d 0.0.0.0/0 119:119 -p 6 -j ACCEPT
ipchains -A in-aus -s 0.0.0.0/0 -d 0.0.0.0/0 37:37 -p 6 -j ACCEPT
ipchains -A in-aus -s 0.0.0.0/0 -d 0.0.0.0/0 37:37 -p 17 -j ACCEPT
ipchains -A in-aus -s 0.0.0.0/0 -d 192.12.144.10/32 53:53 -p 6 -j ACCEPT
ipchains -A in-aus -s 0.0.0.0/0 -d 192.12.144.10/32 53:53 -p 17 -j ACCEPT
ipchains -A in-aus -s 0.0.0.0/0 -d 0.0.0.0/0 33434:33500 -p 17 -j ACCEPT
ipchains -A in-aus -s 0.0.0.0/0 -d 0.0.0.0/0 -j REJECT -l

ipchains -A in-dmz -s 0.0.0.0/0 -d 192.168.112.80/32 25:25 -p 6 -j ACCEPT
ipchains -A in-dmz -s 0.0.0.0/0 -d 192.168.112.80/32 110:110 -p 6 -j ACCEPT
ipchains -A in-dmz -s 0.0.0.0/0 -d 192.168.112.80/32 21:21 -p 6 -j ACCEPT
ipchains -A in-dmz -s 0.0.0.0/0 -d 192.168.112.80/32 20:20 -p 6 -j ftp-data
ipchains -A in-dmz -s 0.0.0.0/0 -d 192.168.112.53/32 53:53 -p 6 -j ACCEPT
ipchains -A in-dmz -s 0.0.0.0/0 -d 192.168.112.53/32 53:53 -p 17 -j ACCEPT
ipchains -A in-dmz -s 0.0.0.0/0 8:8 -d 0.0.0.0/0 -p 1 -j ACCEPT
ipchains -A in-dmz -s 0.0.0.0/0 -d 0.0.0.0/0 -p 1 -j icmp-acc
ipchains -A in-dmz -s 0.0.0.0/0 -d 0.0.0.0/0 -j REJECT -l

ipchains -A dmz-in -s 192.168.112.53/32 53:53 -d 0.0.0.0/0 -p 17 -j ACCEPT
# Die Option -y bezeichnet SYN-Pakete, ! verneint eine Regel.
ipchains -A dmz-in -s 192.168.112.53/32 53:53 -d 0/0 -p 6 -j ACCEPT ! -y
ipchains -A dmz-in -s 192.168.112.80/32 20:20 -d 0/0-p 6 -j ftp-data
ipchains -A dmz-in -s 192.168.112.80/32 21:21 -d 0/0-p 6 -j ACCEPT ! -y
ipchains -A dmz-in -s 192.168.112.80/32 25:25 -d 0/0-p 6 -j ACCEPT ! -y
ipchains -A dmz-in -s 192.168.112.80/32 110:110 -d 0/0-p 6 -j ACCEPT ! -y
ipchains -A dmz-in -s 0.0.0.0/0 0:0 -d 0.0.0.0/0 -p 1 -j ACCEPT
ipchains -A dmz-in -s 0.0.0.0/0 -d 0.0.0.0/0 -p 1 -j icmp-acc
ipchains -A dmz-in -s 0.0.0.0/0 -d 0.0.0.0/0 -j REJECT -l

ipchains -A dmz-aus -s 192.168.112.80/32 25:25 -d 0/0 -p 6 -j ACCEPT ! -y
ipchains -A dmz-aus -s 192.168.112.80/32 110:110 -d 0/0 -p 6 -j ACCEPT ! -y
ipchains -A dmz-aus -s 192.168.112.80/32 80:80 -d 0/0 -p 6 -j ACCEPT ! -y
ipchains -A dmz-aus -s 192.168.112.53/32 53:53 -d 0/0 -p 6 -j ACCEPT ! -y
ipchains -A dmz-aus -s 192.168.112.53/32 53:53 -d 0/0 -p 17 -j ACCEPT
ipchains -A dmz-aus -s 192.168.112.80/32 20:20 -d 0/0 -p 6 -j ftp-data
ipchains -A dmz-aus -s 192.168.112.80/32 21:21 -d 0/0 -p 6 -j ACCEPT ! -y
ipchains -A dmz-aus -s 0.0.0.0/0 0:0 -d 0.0.0.0/0 -p 1 -j ACCEPT
ipchains -A dmz-aus -s 0.0.0.0/0 -d 0.0.0.0/0 53:53 -p 17 -j ACCEPT
ipchains -A dmz-aus -s 0.0.0.0/0 -d 0.0.0.0/0 53:53 -p 6 -j ACCEPT
ipchains -A dmz-aus -s 0.0.0.0/0 -d 0.0.0.0/0 25:25 -p 6 -j ACCEPT
ipchains -A dmz-aus -s 0.0.0.0/0 -d 0.0.0.0/0 110:110 -p 6 -j ACCEPT
ipchains -A dmz-aus -s 0.0.0.0/0 -d 0.0.0.0/0 -p 1 -j icmp-acc
ipchains -A dmz-aus -s 0.0.0.0/0 -d 0.0.0.0/0 -j REJECT -l

ipchains -A aus-in -s 0.0.0.0/0 9037:9037 -d 0.0.0.0/0 -p 6 -j ACCEPT ! -y
ipchains -A aus-in -s 0.0.0.0/0 0:0 -d 0.0.0.0/0 -p 1 -j ACCEPT
ipchains -A aus-in -s 0.0.0.0/0 23:23 -d 0.0.0.0/0 -p 6 -j ACCEPT ! -y
ipchains -A aus-in -s 0.0.0.0/0 53:53 -d 0.0.0.0/0 -p 6 -j ACCEPT ! -y
ipchains -A aus-in -s 0.0.0.0/0 53:53 -d 0.0.0.0/0 -p 17 -j ACCEPT
ipchains -A aus-in -s 0.0.0.0/0 37:37 -d 0.0.0.0/0 -p 6 -j ACCEPT ! -y
ipchains -A aus-in -s 0.0.0.0/0 443:443 -d 0.0.0.0/0 -p 6 -j ACCEPT ! -y
ipchains -A aus-in -s 0.0.0.0/0 21:21 -d 0.0.0.0/0 -p 6 -j ACCEPT ! -y
ipchains -A aus-in -s 0.0.0.0/0 20:20 -d 0.0.0.0/0 -p 6 -j ftp-data
ipchains -A aus-in -s 0.0.0.0/0 110:110 -d 0.0.0.0/0 -p 6 -j ACCEPT ! -y
ipchains -A aus-in -s 0.0.0.0/0 119:119 -d 0.0.0.0/0 -p 6 -j ACCEPT ! -y
ipchains -A aus-in -s 0.0.0.0/0 -d 0.0.0.0/0 -p 1 -j icmp-acc
ipchains -A aus-in -s 0.0.0.0/0 -d 0.0.0.0/0 -j DENY -l

ipchains -A aus-dmz -s 0.0.0.0/0 -d 192.168.112.80/32 25:25 -p 6 -j ACCEPT
ipchains -A aus-dmz -s 0/0 -d 192.168.112.80/32 110:110 -p 6 -j ACCEPT
ipchains -A aus-dmz -s 0/0 25:25 -d 192.168.112.80/32 -p 6 -j ACCEPT ! -y
ipchains -A aus-dmz -s 0/0 110:110 -d 192.168.112.80/32 -p 6 -j ACCEPT ! -y
ipchains -A aus-dmz -s 0.0.0.0/0 -d 192.168.112.0/24 80:80 -p 6 -j ACCEPT
ipchains -A aus-dmz -s 0.0.0.0/0 80:80 -d 0.0.0.0/0 -p 6 -j ACCEPT ! -y
ipchains -A aus-dmz -s 0.0.0.0/0 -d 192.168.112.80/32 21:21 -p 6 -j ACCEPT
ipchains -A aus-dmz -s 0/0 -d 192.168.112.80/32 20:20 -p 6 -j ftp-data
ipchains -A aus-dmz -s 0.0.0.0/0 -d 192.168.112.53/32 53:53 -p 6 -j ACCEPT
ipchains -A aus-dmz -s 0.0.0.0/0 -d 192.168.112.53/32 53:53 -p 17 -j ACCEPT
```

```
ipchains -A aus-dmz -s 0.0.0.0/0 53:53 -d 0.0.0.0/0 -p 17 -j ACCEPT
ipchains -A aus-dmz -s 0.0.0.0/0 53:53 -d 0.0.0.0/0 -p 6 -j ACCEPT ! -y
ipchains -A aus-dmz -s 0.0.0.0/0 8:8 -d 0.0.0.0/0 -p 1 -j ACCEPT
ipchains -A aus-dmz -s 0.0.0.0/0 -d 0.0.0.0/0 -p 1 -j icmp-acc
ipchains -A aus-dmz -s 0.0.0.0/0 -d 0.0.0.0/0 -j DENY -l

# Diese Kette dient dem flüssigeren Ablauf des Netzwerks
ipchains -A icmp-acc -s 0.0.0.0/0 3:3 -d 0.0.0.0/0 -p 1 -j ACCEPT
ipchains -A icmp-acc -s 0.0.0.0/0 4:4 -d 0.0.0.0/0 -p 1 -j ACCEPT
ipchains -A icmp-acc -s 0.0.0.0/0 11:11 -d 0.0.0.0/0 -p 1 -j ACCEPT
ipchains -A icmp-acc -s 0.0.0.0/0 12:12 -d 0.0.0.0/0 -p 1 -j ACCEPT

# Alle Pakete, die sich innerhalb des VPN bewegen sind zugelassen
# Wichtig: Der Router zum Internet darf keine privaten Adressen weiterleiten!
ipchains -A vpn -s 0.0.0.0/0 -d 0.0.0.0/0 -j ACCEPT

ipchains -A in -s 0.0.0.0/0 -d 0.0.0.0/0 -i ! eth0 -j DENY -l
ipchains -A in -s ! 192.168.144.0/24 -d 0.0.0.0/0 -j DENY -l
ipchains -A in -s 0.0.0.0/0 -d 0.0.0.0/0 53:53 -p 6 -j ACCEPT
ipchains -A in -s 0.0.0.0/0 -d 0.0.0.0/0 53:53 -p 17 -j ACCEPT
ipchains -A in -s 0.0.0.0/0 0:0 -d 0.0.0.0/0 -p 1 -j ACCEPT
ipchains -A in -s 0.0.0.0/0 -d 0.0.0.0/0 -j icmp-acc
ipchains -A in -s 0.0.0.0/0 -d 0.0.0.0/0 -j REJECT -l

ipchains -A aus -s 0.0.0.0/0 80:80 -d 0.0.0.0/0 -p 6 -j ACCEPT
ipchains -A aus -s 0.0.0.0/0 -d 0.0.0.0/0 -i ! eth2 -j DENY -l
ipchains -A aus -s 0.0.0.0/0 0:0 -d 0.0.0.0/0 -p 1 -j ACCEPT
ipchains -A aus -s 0.0.0.0/0 53:53 -d 0.0.0.0/0 -p 6 -j ACCEPT ! -y
ipchains -A aus -s 0.0.0.0/0 53:53 -d 0.0.0.0/0 -p 17 -j ACCEPT
ipchains -A aus -s 0.0.0.0/0 -d 0.0.0.0/0 61000:65096 -p 17 -j ACCEPT -l
ipchains -A aus -s 0.0.0.0/0 -d 0.0.0.0/0 61000:65096 -p 6 -j ACCEPT -l
ipchains -A aus -s 0.0.0.0/0 -d 0.0.0.0/0 -j icmp-acc -l
ipchains -A aus -s 0.0.0.0/0 -d 0.0.0.0/0 -j DENY -l

ipchains -A dmz -s 0.0.0.0/0 -d 0.0.0.0/0 -i ! eth1 -j DENY -l
ipchains -A dmz -s ! 192.168.112.0/24 -d 0.0.0.0/0 -j DENY -l
ipchains -A dmz -s 192.168.112.80/32 80:80 -d 0.0.0.0/0 -p 6 -j ACCEPT ! -y
ipchains -A dmz -s 0.0.0.0/0 0:0 -d 0.0.0.0/0 -p 1 -j ACCEPT
ipchains -A dmz -s 192.168.112.53/32 53:53 -d 0.0.0.0/0 -p 6 -j ACCEPT ! -y
ipchains -A dmz -s 0.0.0.0/0 53:53 -d 0.0.0.0/0 -p 17 -j ACCEPT
ipchains -A dmz -s 0.0.0.0/0 -d 0.0.0.0/0 -j icmp-acc
ipchains -A dmz -s 0.0.0.0/0 -d 0.0.0.0/0 -j REJECT -l
#
# running squid proxy
# using default values in /etc/squid.conf
# depending on /etc/firewall.allow
/etc/rc.d/squid start
```

Mit `-s` wird die Quelladresse und mit `-d` die Zieladresse festgelegt. Der Ausdruck `X/Y` bezeichnet die IP Adresse X mit der Netzmaske (Anzahl relevanter Bits) Y. Anschliessend gibt es noch die Möglichkeit einen Bereich von Portnummern an zu geben. Dies geschieht in der Form `von:bis`. Die Option `-p` bezeichnet das verwendete Protokoll. Hierbei steht 1 für ICMP, 6 für TCP und 17 für UDP. Verwendet man das Zeichen `!` vor einem Kriterium, so wird dieses verneint. Vor allem bei der Option -y (SYN-Packets) wird es gern verwendet, um aktiven Verbindungsaufbau zu untersagen.

Test

Der nun folgende Test ist schnell erklärt. Es muss jeder Netzverkehr simuliert werden, der durch die Filterregeln abgedeckt werden soll. Angefangen beim einfachen ping, über Zugriffe auf Web- oder Mailserver bis hin zu Domain - Registration - Anfragen.

Auch wenn dieser Teil der Arbeit einfach ist, so nimmt er doch viel Zeit in Anspruch. Vor allem die Menge der erlaubten Dienste führt zu hoher Fehleranfälligkeit bei der Konfiguration. Um diesen Schritt zu erleichtern, bietet es sich an, jeden erlaubten Netzverkehr (z.B. WWW - Verbindung von aussen in die DMZ) einzeln zu aktivieren und gleich im Anschluss das Ergebnis zu prüfen.

Proxy

Realisierung

Um die ISDN - Netzlast zu verringern, wird an der Schnittstelle des LANs zum Internet ein HTTP - Proxy eingesetzt. Dieser regelt auch den Zugriff mittels ACLs (Access control list). Als Software wird „Squid"[11] verwendet.

Damit an den Clients keine Konfiguration vorgenommen werden muss und um sicher zu gehen, dass HTTP-Verkehr zwingend über den Proxy durchgeführt wird, kommt Squid als transparent - proxy zum Einsatz. Dies bedeutet, dass das Programm automatisch alle Verbindungen über den Firewall - Rechner hinweg kontrolliert. Wird also z.B. Von Innen nach Aussen eine Verbindung erstellt, so wird sie von Squid abgefangen, ohne dass der Benutzer dies erkennt. Anschliessend verhält sich Squid wie ein regulär adressierter Proxy.

Um die Transparenz zu erreichen, muss auf Paketfilterebene angesetzt werden. Anstatt HTTP-Pakete einfach zuzulassen, werden diese an den Proxy (auf Port 3128) umgeleitet. Umleiten (`REDIRECT`) basiert auf dem Prinzip des Masquerading, weshalb diese Funktionalität unbedingt schon bei der Systeminstallation in den Kernel aufgenommen werden muss.

Dieses Vorgehen erfordert auch, dass der Firewall - Rechner HTTP - Antwortpakete (Quellport 80, Zielport >1024) vom Webserver akzeptiert (siehe Filterregeln in der Kette „`aus`).

Konfiguration

Die Konfiguration des Proxy - Servers läuft in folgenden Schritten ab:

1. Squid als Proxy einrichten
2. Redirect - Anweisungen in IPChains
3. ACL definieren

Proxy einrichten

Als erster Schritt wird Squid als normaler Proxy - Server eingerichtet. An dieser Stelle der Installation können allgemeine Einstellungen (wie z.B. Cachegrösse oder -verzeichnis) getroffen und an den verwendeten Rechner angepasst werden. Für den transparenten Dienst[12] müssen folgende Einstellungen getroffen werden:

```
http_port 8080
httpd_accel_host virtual
httpd_accel_port 80
httpd_accel_with_proxy on
httpd_accel_uses_host_header on
```

Ein kurzer Test mit einem Client - Rechner, dessen Browser auf den Squid-Cache eingerichtet wurde, zeigt die grundlegende Funktionsfähigkeit.

Redirect

Da der Verkehr des LANs kontrolliert und gepuffert werden soll, wird jeglicher Verkehr von Clients im LAN auf den Proxy umgeleitet. Dies geschieht mit den beiden Befehlen:

```
ipchains -A input -s 192.168.144.0/255.255.255.0 -d 0/0 80:80 -p 6 -j REDIRECT 3128
ipchains -A input -s 0/0 80:80 -d 192.168.144.0/255.255.255.0 -p 6 -j REDIRECT 3128
```

Somit ist es nicht nötig eine HTTP-Verbindung von innen nach aussen und in die DMZ zu erlauben. Eine solche Regel wäre sogar falsch, da sich so nur Sicherheitslücken aufgrund von Mehrfachdefinitionen ergeben.

ACL Definieren

Access Control Lists werden durch drei Teile definiert:

1. ACL Name
   ist ein logischer Name für die Verwendung innerhalb von /etc/squid.conf
2. ACL Typ
   dient zum Interpretieren des dritten Teils der ACL. Es können Schlüsselwörter wie z.B. `src` (Quelladresse), `dst` (Zieladresse) oder `time` (zum zeitlichen Beschränken des Zugangs) verwendet werden.
3. ACL String
   bezeichnet den Inhalt der Liste. Er kann z.B. aus einer Liste von IP-Adressen bestehen.
   An dieser Stelle kann auch eine Datei angegeben werden. Sie enthält dann eine grössere Anzahl an Kriterien, z.B. eine Liste von IP-Adressen.

Die folgende Zeile beschreibt z.B. den Zugriff auf das Netz 192.168.112.0 unter dem Namen „dmz”:

```
acl dmz dst 192.168.112.0/24
```

Werden mehrere Schlüssel in einer ACL Definition verwendet, werden sie mit einem logischen `ODER` verknüpft.

Mit der Anweisung `http_access` werden Zugriffe auf Basis der vorher definierten ACLs erlaubt bzw. Verboten:

```
http_access allow dmz
```

erlaubt somit den Zugriff auf die DMZ. Werden hier mehrere ACLs in einer Zeile verwendet, so werden diese mit einem logischen `und` verbunden.

Die gesamten ACLs und http_access Regeln lauten dann:

```
acl all src 0.0.0.0/0.0.0.0
acl darf src "/etc/firewall.allow"
acl fwvib src 192.168.144.0/255.255.255.0
acl dmz dst 192.168.112.0/255.255.255.0

http_access allow dmz
http_access allow darf
http_access deny
```

In der Datei Firewall.allow befinden sich die IP-Adressen der Rechner mit erlaubtem Internetzugang.

VPN

Realisierung

Um Aussenstellen dynamisch an die Hauptniederlassung zu binden wird ein VPN aufgebaut. Um dies zu erstellen wird eine feste (offizielle) IP-Adresse und ein Tunnel - Protokoll benötigt. Zur Auswahl stehen dazu verschiedene proprietäre Ansätze verschiedene Unternehmen wie 3Com, Microsoft (PPTP, Point to Point Tunneling Protocol) oder Cisco (CET, Cisco Encryption Technology) und IPSec. Hier kristallisiert sich schnell IPSec als geeignetstes Protokoll heraus.

Zum einen ist IPSec Herstellerunabhängig. Dies garantiert eine breitere Einsatzbasis auf verschiedenen Hardware - Plattformen. Wäre man z.B. mit CET auf Cisco Router angewiesen, hat man mit IPSec einen offenen Standard zur Verfügung, der von der IETF als RFC vorgelegt[13] und somit zum Standard erhoben ist.

Zum anderen behält IPSec für zukünftige Entwicklungen und andere Einsatzgebiete weitere Möglichkeiten offen. So kann z.B. nur die Authentifikation, ohne Verschlüsselung der Daten eingesetzt werden.

Zum Einrichten des VPN sind lediglich vier Schritte notwendig:

- Einrichten eines dedizierten Subnetzes im VPN-Router
  Ein spezieller Adressraum für das VPN ist nötig, um eine Kommunikation zwischen den VPN-Endgeräten zu ermöglichen. Verschlüsselter Verkehr zwischen den Routern (bzw. Endrechnern mit IPSec-Client) erfolgt auf diesem Segment.
- Routing - Tabellen mit Informationen über verwendete Schlüssel erweitern
  Jedem Endpunkt einer VPN-Verbindung (seiner IP - Adresse) muss ein Hauptschlüssel zugewiesen werden. Dieser wird als Geheimnis bei der Session - Key - Vereinbarung verwendet. Alle Verbindungen im erstellten Tunnel werden danach mit diesem Session - Key verschlüsselt. Auf Wunsch vereinbaren die beiden Kommunikationspartner in regelmässigen Abständen neue Schlüssel, um den Schaden bei einer eventuellen Kompromittierung des Session - Keys zu begrenzen.
- Festlegen des Schlüssel - Austausch - Protokolls
  Es existieren mehrere Schlüssel - Austausch - Protokolle, aber aus drei Gründen wird hier das IKE (Internet Key Exchange Protocol) verwendet.
  Zum Ersten handelt es sich um den am weitesten verbreiteten Standard und garantiert somit die grösstmögliche Interoperabilität. Ausserdem bietet IKE die Möglichkeit während einer IPSec - Verbindung den Schlüssel zu ändern und somit die Lebensdauer von Session - Keys fest zu legen.
  Der dritte Grund liegt in der Erweiterbarkeit der Infrastruktur. Im Gegensatz zu vielen anderen Protokollen unterstützt IKE Certification Authorities (CA) und erleichtert somit die Schlüsselverteilung bei einer grossen Anzahl von Schlüsseln. Diese Option wird vorerst nicht eingesetzt, kann aber in Zukunft grosse Erleichterung bringen.

- Festlegen des Verschlüsselungs - Algorithmus
  Um die Kommunikation zu ermöglichen müssen in beiden Endpunkten des VPN die zu verwendenden Algorithmen ausgewählt werden. Hierbei muss vor allem auf die Abschaltung der „nicht Verschlüsseln - Funktion geachtet werden. Die Stärke der zu verwendenden Methode hängt auch von der vorhandenen Bandbreite und von der Leistungsfähigkeit der verwendeten CPU ab. Man kann sich hier an der am wenigsten performanten Komponente (vermutlich die Telefonleitung) orientieren, um den gewünschten Datendurchsatz zu ermitteln.

Konfiguration

Als Hardware werden an den Grenzen des VPN Router der Marke Cisco vom Typ 801 eingesetzt. Diese verwenden IOS als Konfigurationssprache, die sehr komplex, aber auch sehr mächtig ist. Das folgende Listing beschränkt sich auf die, für das VPN nötigen Befehle. Kommentare werden mit einem ‘!’ Eingeleitet.

```
!
! Internet Key Exchange (IKE)
!
crypto isakmp enable
crypto isakmp identity address
!
crypto isakmp policy 1
 encryption 3des
 hash md5
 authentication pre-share
 group 2
 lifetime 3600
!
! IPSec
!
crypto ipsec transform-set cm-transformset-1 ah-md5-hmac esp-3des
crypto map cm-cryptomap local-address Dialer 1
!
crypto map cm-cryptomap 1 ipsec-isakmp
 match address 100
 set transform-set cm-transformset-1
 set security-association lifetime seconds 3600
 set security-association lifetime kilobytes 102400
!
interface Dialer 1
 description connected to Internet
 crypto map cm-cryptomap
```

Der Abschnitt „`crypto isakmp`” definiert IKE als Schlüssel - Austausch - Protokoll und die dazu zu verwendenden Methoden (Triple-DES bzw. MD5). Ausserdem wird die Authentifizierung mittels „pre-shared secret” gewählt, also durch ein, bei der Installation gewähltes Passwort. Die Lebensdauer eines Session - Key beträgt 3600 Sekunden, danach wird ein neuer Schlüssel ausgehandelt.

Der Teil `IPSec` gibt die Verbindungseigenschaften des Tunnels an. Danach wird IPSec an die Verbindung „`Dialer 1`” gebunden, die den connect zum ISP darstellt, also die Wählleitung zum Internet.

Auditing

Thematik

Um die Funktionsfähigkeit des Firewall - Systems (wie oben entworfen) auf Dauer sicher zu stellen, müssen regelmässige Überprüfungen durchgeführt werden. Es dürfen keine unauthorisierte Veränderungen vorgenommen worden sein und alle Versuche dazu festgehalten werden.

Passive (reaktive) Methoden

PortScans erkennen

Um versuchte Einbrüche in das System zu erkennen, muss als erstes ein durchgeführter port scan erkannt werden. Diese Scans dienen dem Aufstöbern von verwundbaren Stellen in einem Netzwerk oder bei einem Rechner. Bei erfolgtem Scan werden verschiedene Aktivitäten ausgelöst:

- Logeintrag
  Mit Hilfe des Programms „scanlogd"[14] (enthalten in der SuSE-Distribution) werden viele verschiedene Angriffarten automatisch erkannt und Datum, Uhrzeit, Quelladresse, Zieladresse und Zielport in einer Logdatei abgelegt.
  Diese Datei sollte regelmässig, mindestens einmal wöchentlich ausgewertet werden und auf unregelmässigkeiten überprüft werden. Treten vermehrt Scans von bestimmten Adressen ausgehend auf, bietet es sich an, den jeweiligen Eigentümer der Ausgangsdomain zu Kontaktieren. In vielen Fällen handelt es sich hierbei um kompromittierte Rechner von ISPs oder um so genannte Script-Kiddies, die sich über einen Provider in das Internet einloggen.
- Mail an root
  Um den Systemadministrator frühzeitig über Vorfälle zu informieren, sollte bei einem erkannten Port-Scan eine Mail an den Administrator gesandt werden. Scanlogd erledigt auch diese Aufgabe. Dieser hat alle daraufhin folgenden Aktivitäten durchzuführen.
- Evtl. Sperren der Route zum Ausgangspunkt der Portscans
  Einem Scan folgt oft ein Angriff. Um diesem Vorzubeugen kann der Administrator bei einem erkannten Scan einen Eintrag in der Routing - Tabelle erstellen, der weitere Angriffe vom Quellrechner aus unterbindet.
  Diese Methode sollte jedoch sparsam und wohl überlegt eingesetzt werden. Man muss bedenken, dass Quelladressen gefälscht sein können, oder aus einem Adresspool eines Internet Service Providers stammen können, den sich viele Benutzer teilen.

- Gegenmassnahmen ergreifen
  Bei einem eindeutig erkannten Einbruchversuch bietet es sich an, alle Verfügbaren Daten (z.B. von Logdateien) auszuwerten und den Ausgangspunkt des Angriffes zu lokalisieren. Handelt es sich hierbei um einen ISP, ist dieser oft dankbar für einen Hinweis, da es sich nicht selten um einen kompromittierten Host handelt. Auch Admins grösserer Netzwerke haben manchmal schwarze Schafe, die ihren Rechner nicht immer für deren eigentliche Aufgabe verwenden. Hier ist wiederum Vorsicht geboten. Man sollte immer erst freundlich anfragen und nicht sofort Beschuldigungen äussern. Es kann leicht passieren, dass sich ein Systemadministrator während eines Audit (seines eigenen Netzwerkes) bei der Eingabe der IP-Adresse vertippt und aus Versehen ein fremdes LAN prüft.

Überwachen des Systems

Zum Überwachen des Dateisystems auf Veränderungen existiert ein Programm namens tripwire[15]. Dieses erstellt einmalig eine Prüfsumme für alle wichtigen Dateien auf dem Firewall - Rechner. Diese Checksum wird dann, zusammen mit der Konfigurationsdatei, auf ein read-only Dateisystem kopiert. Dies wird entweder durch einen speziellen Server im Netzwerk oder einer schreibgeschützten Diskette erreicht. Danach überprüft ein cron-job regelmässig aufgrund der vorhandenen Hashwerte, ob Dateien oder Verzeichnisse geändert wurden. Tritt dabei eine Ungewöhnlichkeit auf, die der Administrator nicht nachvollziehen kann, tritt der Abschnitt „Reaktion auf einen möglichen Einbruch in Aktion.

Aktive Methoden

Audit

Beim aktiven Auditing wird geprüft, ob die bestehende Konfiguration einem Angriff standhalten kann. Stellen sich bei einem Test Schwachstellen heraus, wird analysiert, wo diese liegen. Im Anschluss an das Audit muss das Ergebnis dokumentiert werden und evtl. Gefundene Schwachstellen behoben werden.

Zu diesem Zweck gibt es professionelle Scanprogramme, aber auch frei verfügbare Tools. Die ersteren sind in ihren Tests sehr ausgereift und stabil. Sie bieten oft auch Hilfestellungen zur Fehlerbehebung und Absicherung penetrierbarer Rechner. Ausserdem bieten die Hersteller oft guten Support zu ihrer Software und deren Anwendung. Zum Test der Software gibt es meistens eine Demo-Version zum Download mit eingeschränkten Fähigkeiten („cripple ware”) oder mit begrenzter Nutzungsdauer („time bombs”).

Scanner, die frei im Internet zur Verfügung stehen, bieten bei Problemen keine direkte Unterstützung durch die Programmierer. Man muss sich durch Howtos, FAQs und Homepages arbeiten um ihre Funktionalität voll ausnutzen zu können.

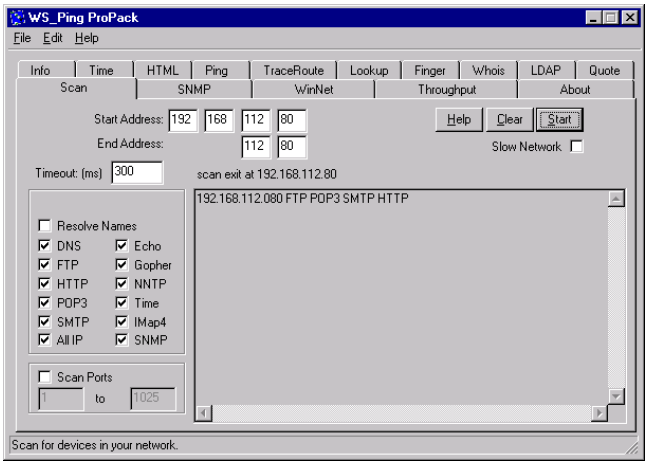
Ein guter Ansatz zum Prüfen der Firewall ist, sie einem simulierten Einbruch aus zu setzen. Gewöhnlich werden Systeme erst auf offene Ports geprüft. Auf diesen gefundenen Schwachstellen werden danach Fehler in der Stapelverwaltung (IP - Stack) oder im Protokoll gesucht. Beliebte Tools zum Brechen von Firewalls und anderen Sicherheitsvorkehrungen sind:

- SATAN[16] (System Administrator Tool for Analyzing Networks): Sicherheitstool für UNIX Rechner um vorhandene Probleme aufzuzeigen
- SAINT[17] (Security Administrator's Integrated Network Tool): Basiert auf SATAN, hat aber erweiterte Fähigkeiten
- NetCat[18]: Tool zum lesen und schreiben auf TCP/UDP Netzwerkverbindungen zu beliebigen Ports
- Sniffit, TCPdump, IPGrab: Netzwerksniffer zum mitlesen des Netzwerkverkehrs an einem Interface
- Nessusd[19]: Ein Client/Server Portscanner. Der Server wird auf einem UNIX Rechner gestartet und kann von Clients auf unterschiedlichen Plattformen kontrolliert werden.
- NetScan Tools[20]: Kommerzielles Programm für Windows zum Ausführen verschiedener Netzanalysen
- WS_Ping[21]: Kompakter, kommerzieller Netzscanner für Windows

Um den Rahmen dieser Abhandlung nicht zu sprengen, werden im folgenden beispielhaft die Ergebnisse von Angriffen und Reaktionen darauf gezeigt.

Als erstes wird der Firewall Rechner von ausserhalb des LAN gescannt. Dabei ergeben sich, wie erhofft, keine offenen Ports, die ausgebeutet werden können. Auch ein Test des internen Netzes ergibt keine Verwundbarkeit.

Führt man hingegen einen Scan auf einen Server aus der DMZ durch, ändert sich dieses Bild. Die Programme NetScan Tools sowie WS_Ping Pro liefern eine Liste von offenen Ports. Es treten jedoch (wie erwartet) nur diejenigen Dienste auf, die durch den Paketfilter erlaubt wurden. Der laufende Gopher - Server z.B. wird nicht erkannt. Um weitere Informationen über den Zielrechner zu erhalten, kann man nun NetCat starten. Dieses liefert als Ausgabe den „rohen" Netzverkehr, wie er vom angesprochenen Server als Antwort auf Benutzereingaben erzeugt wird. Um z.B. dem HTTP-Server auf den Zahn zu fühlen, führt man Netcat mit der Option 80 (der HTTP-Port) aus. Ein entsprechender Bildschirmdialog sieht folgendermassen aus:



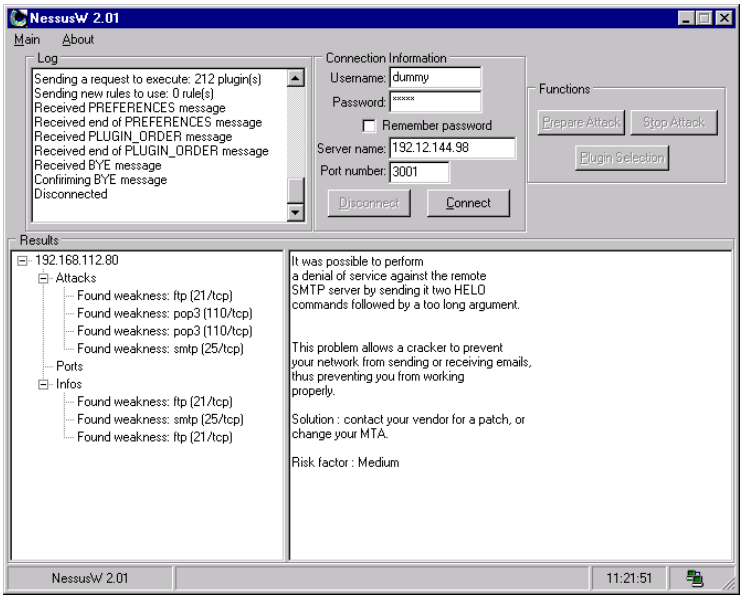

```
Localhost:~ # netcat 192.168.112.80 80

HTTP/1.0 400 Ungültige Anforderung
Content-Type: text/html

<body><h1>HTTP/1.0 400 Ungültige Anforderung
</h1></body>
Localhost:~ # _
```

Durch diese gewonnenen Informationen kann man als Hacker gezielt nach Fehlern in der verwendeten Server Software suchen und diese ausnutzen. Als Administrator muss man hingegen bemüht sein, ständig alle Sicherheitslücken durch Patches und Updates zu stopfen.

Wenn man das Programm Nessusd (hier: die Oberfläche des Windows - Client) verwendet, liefert die Software gleich mögliche Verwundbarkeiten des Zielrechners, sowie Ratschläge, diese zu beheben. Das Fenster in der unteren rechten Ecke beinhaltet die Analyse durch den Scanner. Im Falle des SMTP - Serverprogrammes rät Nessus zu einem Patch oder Update und gibt gleichzeitig eine kurze Beschreibung der Art der Verwundbarkeit an.

Reaktion auf einen möglichen Einbruch

Erstellte Verbindungen von Aussen und Innen werden protokolliert. Dieses Protokoll muss manuell (ähnlich dem von scanlogd) auf unregelmässigkeiten geprüft werden. Sind hier unerlaubte Zugriffe aufgeführt, müssen vom Operator entsprechende Massnahmen getroffen werden. Dazu gehören:



- Prüfen des Firewall - Rechners auf Kompromittierung
- Suche nach Trojanischen Pferden auf Client - Rechnern im LAN bzw. DMZ
- Kontrolle der Benutzerkonten im LAN und auf dem Firewall - Rechner

Genauer detailierte Informationen bietet das CERT Coordination Center des Carnegie Mellon Software Egineering Institute in der Abhandlung „Steps for Recovering from a UNIX Root Compromise"[22] an.

Echtbetrieb

Vorarbeit

Konfiguration der bestehenden Komponenten

Die aktuelle Infrastruktur wird (entsprechend der Anforderung) zum grössten Teil beibehalten, was den Konfigurationsaufwand in sehr kleinem Rahmen hält. Die einzige, zu tätigende Aktion ist die Umstellung des LAN - IP-Adressraums auf private Adressen (siehe Kapitel Routing).

Dokumentation für User

Benutzer des Firmennetzes werden im Rahmen des bestehenden Schulungsprogramms auf die erhöhten Sicherheitsanforderungen durch die ständige Verbindung ins Internet hingewiesen. Auch Schulung in den Bereichen Viren, Trojanische Pferde und Würmer wird verstärkt. Es muss hier mit Nachdruck darauf hingewiesen werden, dass das Ausführen von Programmen aus dem Internet stets mit einem hohen Risiko für die interne EDV - Umgebung verbunden ist.

Dokumentation für Administratoren

Für Administratoren dient diese Arbeit als Grundlage zum Verständnis des eingerichteten Firewall Systems.

Routinearbeiten und kleine Änderungen der Konfiguration (z.B. neue Filterregeln) werden in der Praxis aus Einfachheitsgründen und wegen der kürzeren Reaktionszeit innerhalb der Abteilung oft von anderen Mitarbeitern erledigt. Auch um in Abwesenheit der Sicherheitsbeauftragten und geübten Linux Systemoperatoren den Netzwerkbetrieb aufrecht zu erhalten, werden kurze, leicht verständliche Schritt - für - Schritt - Anleitungen benötigt. Diese Dokumentationen werden entweder in Zusammenarbeit mit den entsprechenden Mitarbeitern für deren jeweilige Bedürfnisse erstellt, oder sie müssen sehr ausführlich und umfangreich gehalten werden.

Wichtig hierbei ist nicht nur, dass sie verständlich und nachvollziehbar sind, sondern auch ihre Auffindbarkeit und Erreichbarkeit im Bedarfsfall.

Realisierung

Sind die bisherigen Schritte richtig durchgeführt worden, beschränkt sich der Start des Echtbetriebes auf das Austauschen des bisherigen Internetrouters gegen das eben erstellte Firewall - System.

Die neuen Router werden an ihre endgültige Position gestellt (z.B. Rechnerraum), aber noch nicht an das Firmennetz angeschlossen. Darauf folgt ein kurzer Test, ob die Verkabelung in Ordnung ist, und ob alle Netzverbindungen erstellt werden können. Danach wird der alte Router vom LAN getrennt und die Firewall angebunden. Wenn alles richtig gelaufen ist, sollte im lokalen Netz lediglich ein kurzer Aussetzer zu erkennen sein.

Aufgaben nach der Einführung

Prüfen der Integrität

Um sicherzustellen, dass kein Einbruch und keine Übernahme des Firewall - Systems erfolgt ist, müssen regelmässig die log - Dateien und die automatisch generierten Mails an den Benutzer `root` geprüft werden.

Stellt man hier Inkonsistenzen fest, muss man vorgehen wie im Kapitel „Audit/Reaktion auf einen möglichen Einbruch” vorgehen.

Wartung

Neu geforderte Protokolle und Änderungen bei den Zugriffsrechten müssen nachgetragen werden.

Besteht ein gerechtfertigter Bedarf an bisher nicht erlaubten Protokollen, muss dieser Anforderung Rechnung getragen werden. Paketfilterregeln müssen ergänzt werden, damit das neue Protokoll verwendet werden kann.

Wenn ein passender Proxy zur Verfügung steht und durch entsprechend frequente Benutzung des neuen Dienstes sein Einsatz lohnenswert scheint, bietet sich die Verwendung des Softwarepaketes an.

Erweiterung des Netzwerks

Wird das Netzwerk erweitert (neue Subnetze hinzugefügt), müssen entsprechende Einträge in allen Routern und Paketfiltern hinzugefügt werden. Dies gilt sowohl für Änderungen im LAN, als auch für Aktualisierungen im VPN.

Reaktion auf Bandbreitenengpässe

Sollte es sich herausstellen, dass sich ein Engpass im System bildet, muss die verantwortliche Komponente (z.B. Telekommunikationsleitung, Verschlüsselung, Benutzerverwaltung) identifiziert und gegebenenfalls erweitert oder ausgetauscht werden.

Bugfix, Bugfix, Bugfix

Die eingesetzte Software muss ständig auf auftauchende Sicherheitslücken überwacht werden. Dies geschieht am besten durch regelmässiges Lesen von Herstellerhinweisen (am aktuellsten auf der jeweiligen Homepage), Sicherheits - Mailinglisten (z.B. bugtraq@securityfocus.com) oder entsprechender Newsgroups.

Die meisten Systemeinbrüche basieren auf öffentlich bekannten Schwachstellen von weit verbreiteten Programmen, die leicht im Internet zu identifizieren sind. Werden Probleme mit einer eingesetzten Version eines Programms bekannt oder sogar Schwachstellen veröffentlicht, muss man unbedingt und schnellstmöglich einen Bugfix anbringen, das Programm mit einem Update auf den neuesten Stand bringen, oder durch äquivalente Software ersetzen.

Nachwort

Nach all dem Aufwand kann man sich als Administrator durchaus sicher fühlen. Dieses Gefühl darf aber nicht über eine wichtige Tatsache hinweg täuschen:

> Sicherheit ist ein Lebensstil, und keine endgültige Lösung!

Neue Techniken und Softwareentwicklungen bieten regelmässig neue Angriffspunkte, die nur durch ständiges Sicherheitsbewusstsein der Administratoren und auch der User im Griff gehalten werden kann.

Aber auch wenn ein perfektes Firewall - System (was es leider nicht gibt) installiert wäre, muss immer noch eines beachtet werden:

> Etwa 80% der unberechtigten Zugriffe auf interne Daten werden von eigenen Mitarbeitern durchgeführt.

Einige der Verletzungen entstehen aus Zufall, durch falsche Rechtevergabe, andere aus Neugier der User, welche aber nicht böswillig handeln und ein weiterer Teil handelt mit Vorsatz illegal.

Lokale Benutzer liefern ein weitaus grösseres Gefahrenpotenzial als Übergriffe aus dem Internet, da sie in fast allen Fällen Firmendaten und nicht nur Rechnerressourcen betreffen. Ob die Daten nun vorsätzlich oder zufällig manipuliert bzw. offen gelegt werden, ist nach einem Vorfall eher sekundär.

Glossar

ACL: Access control list, Positivliste zur Zugangskontrolle.

Audit: Revision, Prüfung (hier: einer fertigen Firewall- Installation) und Dokumentation der Ergebnisse.

Authentizität: Grundsatz, dass der Empfänger zweifelsfrei sicher sein kann, dass eine Nachricht tatsächlich von dem angeblichen Verfasser geschaffen und nicht gefälscht wurde oder anderweitig durch Dritte verändert worden ist.

Bastion Host: Speziell gesicherter Rechner, meist an Netzwerkgrenzen und mit -> Firewall- Funktionalität.

CAD: Computer Aided Design, Computer unterstütztes Zeichnen in 2D/3D

CERT: Computer Emergency Response Team, Gruppe von Netzwerk-Sicherheitsexperten, die technische Unterstützung und Ratschläge bei Sicherheitszwischenfällen bieten. Gegründet nach dem „Internet Wurm" Zwischenfall

CNC: Computerized Numerical Control, verwendet zur Steuerung von Maschinen

DDOS Distributed denial of service, ->DOS-Angriff mit verteilten Ausgangspunkten

Demilitarisierte Zone: Ausdruck aus dem militärischen Sprachgebrauch für eine Sicherheitszone zwischen Kampfgebieten. Gesicherter Netz-Bereich, der sowohl von externen als auch lokalen Computern erreicht werden kann. -> Firewall

Dial-up: Eine Verbindung ins Internet wird erst dann erstellt (einwählen) wenn sie benötigt wird. Gegenteil: -> Standleitung

DMZ: -> DeMilitarisierte Zone

DNS: -> Domain Name Server

Domain Name Server: Server im Internet / LAN zum Umsetzen der numerischen IP-Adressen in Internet- Namen.

DOS: Denial of service, Angriff auf einen Rechner bzw. ein Netzwerk, um das Ziel arbeitsunfähig zu machen

DSL: Digital Subscriber Line, Technologie um hohe Bandbreite über normale Telefonkabel zu erreichen

FAQ: Frequently Asked Questions, Zusammengestellte Liste oft gestellter Fragen zu einem bestimmten Thema

Firewall: Ein Konstrukt aus Soft- und Hardware, zur Sicherung eines LANs.

FTP: File Transfer Protocol, Layer 5 Protokoll im -> TCP/IP Stack zum Austausch von Dateien

Gateway: Ein „Übergang”, der zwei Netze verbindet

Howto: Anleitung zur Bedienung eines Programms (how to use this)

HTML: -> Hypertext Markup Language

Hypertext Markup Language: Beschreibungssprache für -> WWW-Seiten

ICMP: Internet Control Message Protocol**,** Ein IP Protokoll zur Kommunikation zwischen Routern.

IETF: Internet Engineering Task Force, eine offene internationale Gemeinschaft von Netzwerkspezialisten, -betreibern, -anbietern und -forschern, die sich mit der Entwicklung der Internet - Architektur und dessen reibungslosen Betriebs befassen.

Integrität: Vermeidung unberechtigter Änderungen, Erstellung oder Vervielfältigung von Informationen.

Internet Protokoll: Grundlegender Teil der TCP/IP Suite

Internet Service Provider: Dienstanbieter, der einzelnen Rechnern oder LANs einen Zugang zum Internet ermöglicht.

IP: -> Internet Protocol

IP-Chains: -> Linux - Programm zum Filtern von IP-Paketen

IP-Paket: Einzelne Übertragungseinheit bei IP

IP-Spoofing: Manipulation eines -> IP-Packets, i.a. Vorgeben einer falschen IP-Adresse

IPX: Proprietäres Netzwerk- Protokoll der Firma Novell

ISDN: Integrated Services Digital Network, digitales Wählnetz für Sprach- und Datenkommunikation

ISP: -> Internet Service Provider

LAN: Local Area Network, kleines, räumlich eng begrenztes Netzwerk. Üblicherweise ein Gebäude, Stockwerk, kleines Firmengelände. -> WAN

Linux: freies Betriebssystem (Unix-Derivat), 1991 von Linus Torvalds entwickelt

Masquerading: Umsetzen der verwendeten IP-Adressen eines -> LANs bei Anbindung an ein bestehendes Netzwerk.

NAT: Network Address Translation, Routerfunktion zum Anbinden mehrerer Rechner an ein IP-Netzwerk mit nur einer offiziellen IP-Adresse.

ODBC: Open DataBase Connectivity, Plattformunabhängige, standardisierte Methode für offene Datenbankanbindung.

ping: Ein TCP/IP Diagnoseprogramm. Es sendet -> ICMP Pakete zu einer oder mehreren IP Adressen. Diese antworten darauf mit Echopaketen (pong).

POP: Post Office Protocol, Internet-Protokoll zum Abholen von Email bei einem POP-Server. Aktuelle Version: POP3

Port Scan: Testen verschiedener IP-Ports eines Zielrechners um Verwundbarkeiten bei offenen Ports zu finden.

PPP: Point to Point Protocol, Protokoll zur Punkt- zu- Punkt- Verbindung

PPS: ProduktionsPlanungs- System, Software zur Organisation von Fertigungsabläufen

Proxy: i.a. zwischengeschalteter Server zur Pufferung, Überwachung und Zugriffskontrolle

RFC: Request for comments, Vorgeschlagener Standard, liegt zum Download im Internet bereit.

Screened Subnet: durch -> Firewall geschütztes, zugängliches Netzwerk

Script kiddie: böswilliger User, der mit vorgefertigten Programmen und standardisierten Scripten durch minimalen Aufwand bekannte Sicherheitslücken ausnutzen will

Security Policy: Sicherheitspolitik einer Institution, beschreibt das dort geforderte Sicherheitsniveau

SMS: Short Message Service, Service zum Versenden von Textnachrichten an Mobilfunkteilnehmer

SMTP: Simple Mail Transfer Protocol, Internet- Protokoll zu versenden von EMail

Standleitung: Gemieteter Netzwerkzugang (i.a. zum Internet), welcher immer zur Verfügung steht und einen ständig offenen Kanal verwendet

SuSE: Hersteller einer -> Linux - Distribution

TCP: Transmission Control Protocol, Protokoll zur Sicherstellung der Kommunikation, Aufbauend auf IP

Teleworker: Netzteilnehmer, der sich per Wählverbindung in ein -> LAN einbindet und dort wie ein lokaler Anwender behandelt wird.

UDP: Users Datagram Protocol, Alternative zu TCP, benutzt allerdings weniger gesicherte Verbindung

Vertraulichkeit: Vermeidung der Offenlegung von Informationen ohne Erlaubnis des Eigentümers

VPN: Virtual Private Network, Verbindung zwei oder mehrerer LANs mit Hilfe von Tunnelprotokollen über ein anderes Netzwerk (z.B. Internet), so dass der Eindruck eines geschlossenen Netzes entsteht. -> WAN

WAN: Wide Area Network, i.a. jedes grosse Netzwerk welches mehr als ca. 1km Ausdehnung besitzt. -> LAN

Windows: Verbreitetes Betriebssystem der Firma Microsoft

World Wide Web: Grafische Komponente des Internets, basiert auf HTTP

WWW: -> World Wide Web

Literaturverzeichnis

[1]Dr.Ing. Christian Fill
Gut gerüstet, InformationWeek, Heft 19. August 1999, Seite 15ff
[2]D. Brent Chapman und Elizabeth D. Zwicky
Building Internet Firewalls, O'Reilly, ISBN 1-56592-124-0, 1. Auflage, September 1995, Kapitel 4-7
[3]Simson Garfinkel und Gene Spafford
Practical UNIX & Internet Security, 2nd Edition, O'Reilly, ISBN 1-56592-148-8, 2. Auflage, April 1996, Kapitel 2,13,16,21
[4] Bundesamt für Sicherheit in der Informationstechnik
IT-Grundschutzhandbuch 1999,
[5]Mark Grennan
Firewalling and Proxy Server HOWTO v0.67, 26. September 1999, http://www.linuxdoc.org/HOWTO/Firewall-HOWTO.html
[6]Kevin Fenzi, Dave Wreski
Linux Security HOWTO v1.0.2, Kapitel 8: Network Security, 25. April 1999, http://www.linuxdoc.org/HOWTO/Security-HOWTO.html
[7]Lance Spitzner
Armoring Linux, 25. Oktober 1999,
http://www.enteract.com/~lspitz/linux.html
[8]Network Working Group
RFC 1918, Address Allocation for Private Internets, Februar 1996,
http://www.ietf.org/rfc/rfc1918.txt
[9]Paul Russell, RustCorp IT Consulting
IPChains, http://www.rustcorp.com/linux/ipchains/
[10]Paul Russell
Linux IPChains - HOWTO, 12. März 1999,
http://www.linuxdoc.org/HOWTO/IPCHAINS-HOWTO.html
[11]mehrere Mitglieder der Internetgemeinde
Squid, http://squid.nlanr.net/
[12]Duane Wessels
Squid FAQ, Transparent Caching/Proxying,
http://squid.nlanr.net/Doc/FAQ/FAQ-17.html
[13]Network Working Group
RFC 2411, IP Security, November 1998, http://www.ietf.org/rfc/rfc2411.txt
[14]Solar Designer
scanlogd, http://www.openwall.com/scanlogd/
[15]Dr. Eugene Spafford, Gene Kim, Tripwire, Inc.
tripwire, http://www.tripwiresecurity.com/
[16]Wietse Venema und Dan Farmer
SATAN, http://www.fish.com/~zen/satan/satan.html
[17]World Wide Digital Solutions, Inc.
SAINT, http://www.wwdsi.com/saint/
[18]hobbit@avian.org
NetCat, AvianResearch, http://www.avian.org/
[19]The "Nessus" Project
Nessusd, http://www.nessus.org/

[20]Northwest Performance Software, Inc.
NetScan Tools, http://www.nwpsw.com/
[21]Ipswitch, Inc.
WS_Ping, http://www.ipswitch.com/
[22]Carnegie Mellon University
Steps for Recovering from a UNIX Root Compromise, 1. April 1998,
http://www.cert.org/tech_tips/root_compromise.html