IT-Security

9.1.1 Einleitung

Sicherheit im IT-Bereich – **IT** steht übrigens für **I**nformation **T**echnologie. Warum ist das ein so wichtiges Thema in den Firmen und in den Medien? Der Grund liegt darin, dass beim IT Bereich der Sicherheitsgegner sehr mannigfaltig sein kann. D.h. es gibt immer ein Leck das erst im Schadensfall überhaupt auffällt, es fällt erst dann auf, dass es überhaupt existiert! Sicherheit ist überall ein Thema, auch jede Gemeinde hat ein “Amt für Sicherheit“ nur sind da die Möglichkeiten eines Angreifers sehr viel besser kalkulierbar.
Bei diesem Wort liegt auch der Schlüssel **Kalkulierbares Risiko**. Für jeden von uns ist Sicherheit etwas anderes, es gibt auch verschiedene Sicherheitsbedürfnisse.

Eine Unternehmensführung muss das bestehende Risiko, den möglichen Schaden und die Kosten für die Sicherheit gegeneinander abwägen können.

Nur für die obige Forderung muss das bestehende Risiko bekannt sein oder die Lecks müssen gesucht werden um die Risiken abschätzen zu können.

Es ist auch zu beachten, dass laut einer Amerikanischen Studie über **75%** aller Schadensfälle im IT-Sicherheitsbereich **von intern** her rühren!!

Alleine aus dieser Tatsache ist bereits ersichtlich, dass das Schwergewicht in den meisten Unternehmen zur Zeit falsch gelegt wurde! Meistens werden enorme Summen zur Sicherung durch Angriffe von aussen getätigt, aber die internen Sicherheitsanstrengungen werden schlicht und einfach weggelassen.

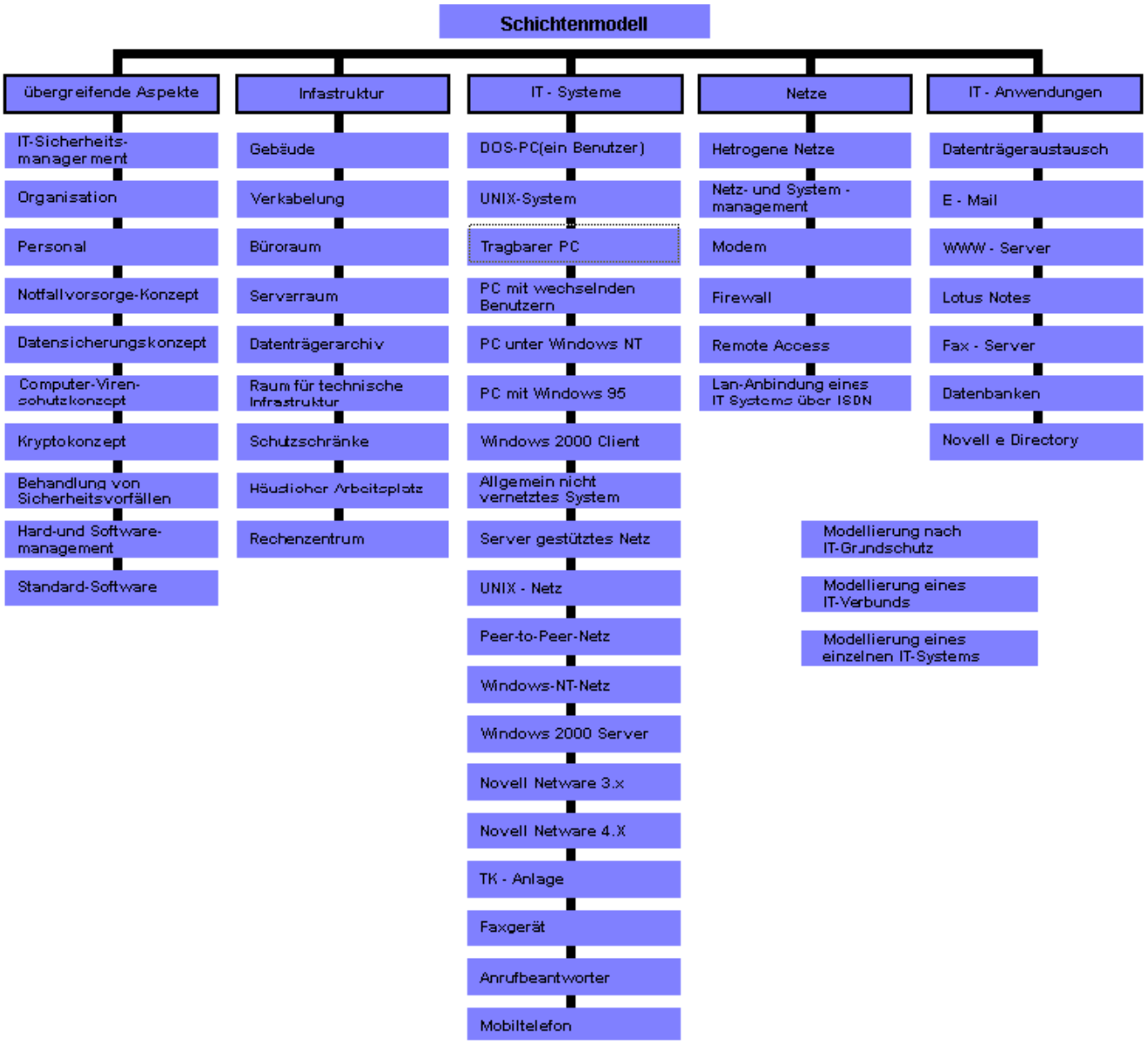
9.1.1.1 Gesetz und Strafen für Sicherheitsverletzungen:

Grundsätzlich ist zu sagen, dass jeglicher Zugang zu Daten die nicht für einem bestimmt sind illegal ist. Das gilt auch wenn die Daten schlecht- oder ungesichert sind!
Das heisst wenn Sie ein Grundstück oder eine Wohnung betreten die nicht verschlossen ist so ist dies Hausfriedensbruch. Jedoch haben sie die Möglichkeit sich Zugang zu Daten zu verschaffen weil sie herausgefunden haben, dass es ein Sicherheitsleck gibt bei dem Sie ohne Passwort Zugang erlangen können, so ist das bereits strafbar.

9.1.1.2 Cyber War’s

Worum handelt es sich denn da? Ganz einfach Computer gestützter Krieg. Wie denn dass? So ganz ohne Panzer? Ja – In den heutigen Kriegen will man dem Feind einfach nur wertvolles zerstören und möglichst grossen finanziellen Schaden zufügen. Das heisst alle zentralen Infrastruckturpunkte sind von Interesse: Strassen-, Bahn-, Schiffsverbindungen, Strom-, Gas-, Wasserversorgung und natürlich Telefon- und Datenverbindungen. Die Mitarbeiter der Staatssicherheit werden so ausgebildet, dass sie nicht nur nach Schwachstellen im eigenen Land suchen können sondern auch durch Schwachstellen von Systemen anderer Länder eindringen können.
Man stelle sich vor, wenn durch einen Servicezugriff ein Kraftwerk ausgeschaltet werden kann, so ist der Schaden um ein etliches grösser als dies bei einem Raketen Angriff möglich währe. Sie denken das sei so abwegig? Nein, die Erbauer eines Kernkraftwerks haben im Normalfall Zugriff auf den Zentralrechner zu Wartung und Service Zwecken. Die Möglichkeiten kann sich jeder selber vorstellen.
So als Beispiel: Der Ausfall des Hauptrechners einer Schweizer Kantonalbank würde nach 24 Stunden einen Konkurs zur Folge haben!

9.1.2 IT-Sicherheit nach Bereichen:



Quelle: www.bsi.de

Nur wenn in allen Bereichen die Notwendigen Anstrengungen gemacht werden, kann von effektivem Schutz gesprochen werden!

9.1.2.1 Die Gefährdungslage eines PCs als Beispiel:

Für den IT-Grundschutz eines PC's (ein Benutzer) werden folgende Gefährdungen angenommen:

Höhere Gewalt:
- Personalausfall
- Ausfall des IT-Systems
- Feuer
- Wasser
- Staub, Verschmutzung

Menschliche Fehlhandlungen:
- Fahrlässige Zerstörung von Gerät oder Daten

- Nichtbeachtung von IT-Sicherheitsmassnahmen
- Gefährdung durch Reinigungs- oder Fremdpersonal
- Fehlerhafte Nutzung des IT-Systems

Technisches Versagen:
- Ausfall der Stromversorgung
- Defekte Datenträger

Vorsätzliche Handlungen:
- Manipulation/Zerstörung von IT-Geräten oder Zubehör
- Manipulation an Daten oder Software
- Diebstahl
- Unberechtigte IT-Nutzung
- Computer-Viren
- Makro-Viren

Massnahmenempfehlungen

Nachfolgend wird das Massnahmenbündel für den Bereich PCs (ein Benutzer)" vorgestellt: Zur Realisierung des IT-Grundschutzes wird empfohlen:

Infrastruktur:
- Geeignete Aufstellung eines IT-Systems

Organisation:
- Datenträgerverwaltung
- Regelungen für Wartungs- und Reparaturarbeiten
- Nutzungsverbot nicht freigegebener Software
- Überprüfung des Software-Bestandes
- Ordnungsgemässe Entsorgung von schützenswerten Betriebsmitteln
- Hinterlegen des Passwortes
- Herausgabe einer PC-Richtlinie (optional)
- Einführung eines PC-Checkheftes (optional)

Personal:
- Schulung vor Programmnutzung
- Schulung zu IT-Sicherheitsmassnahmen

Hardware/Software:
- Passwortschutz für IT-Systeme
- Bildschirmsperre
- Regelmässiger Einsatz eines Viren-Suchprogramms
- Geeigneter Umgang mit Laufwerken für Wechselmedien (optional)
- Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen (optional)
- Prüfung eingehender Dateien auf Makro-Viren
- Test neuer Hard- und Software
- Nutzung der BIOS-Sicherheitsmechanismen

Notfallvorsorge:
- Geeignete Aufbewahrung der Backup-Datenträger
- Sicherungskopie der eingesetzten Software
- Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen
- Verhaltensregeln bei Auftreten eines Computer-Virus
- Erstellen einer PC-Notfalldiskette
- Sicheres Update des BIOS
- Regelmässige Datensicherung

9.1.3 Einige Beispiele für Sicherheit in Ihrem Unternehmen

Telefonie Sperren: Bei Ihrem Telefonanschluss sind Auslandsgespräche und 0900er Nummern blockiert, dies damit die Kosten nicht ins Uferlose wachsen können. Nun Sie als findiger IT-Security Verantwortlicher überlegen sich was da wohl wie gemacht wurde. Sie kommen zum Schluss, dass in der Telefonanlage die ersten Ziffern in einer Sperrliste sind so z.B. 00*, 0900*, 156* und 157*. Nun stellen sie sich die Frage, was ist zu unternehmen, damit nicht mehr diese Ziffern am Anfang sind? Na klar die Carrier-Vorwahl die löst das Problem! In der Schweiz sind zur Zeit alle Festnetzanschlüsse zur SwissCom Zentrale gelegt und die entscheiden dann SwissCom oder PreSelect zu einem anderen Carrier. D.h. bei SwissCom ist vorerst mal jeder! Jetzt versuche ich das mal mit Deutschland: 0 für das AMT und dann 10741 für SwissCom und jetzt noch die Nummer 0049..... und siehe da es klappt. Wenn ich bei SwissCom bin so merkt das keiner da so oder so alles auf die selbe Rechnung geht, bin ich irgendwo PreSelected, so wird nun neu dieses Gespräch auf der SwissCom Abrechnung mit drauf sein und nicht mehr beim PreSelect Carrier!

Telefonie via Relay: Sie wohnen in der nähe ihrer Firma und wollen via ihrem Büro zu Ihrer Cousine nach Amerika telefonieren. Kein Problem Sie können ja ihren Festnetzanschluss im Büro auf Ihr Handy umleiten. Ja klar. Also netterweise lassen es die meisten Telefonzentralen zu, dass die Weiterleitung auch von remote aus Ein- und Ausgeschaltet werden kann. In den meisten Fällen kann auch die Zielnummer der Umleitung von remote aus konfiguriert werden. Also man nehme eine freie Durchwahlnummer und leite diese zum Kollegen in die USA um und das war's. Ein Anruf ins Büro auf diese DDI geht jetzt nach Amerika, ausschalten nicht vergessen! B.t.w. Eingehende und abgehende Nummern werden in der TK-Anlage aufgezeichnet! (Geht natürlich nur mittels Passwort das von intern her hinterlegt werden muss)

Zugang: Wenn sich ein Elektriker im Overall am Empfang meldet und sagt, es sei eine Störung auf einer Datenleitung gemeldet worden, wo denn die Telefon-Anlage und der Server sei? Wird ihm da geholfen?
Oder wie sieht's mit dem Zugang der Putzequipe aus? Haben die Zugang zum Server? Für Geld lässt sich jeder kaufen, es ist nur eine Frage der Summe! D.h. Wenn Sie jemanden dazu überreden oder bezahlen können auf dem Server oder einem PC der gerade läuft ein Programm ab dem Internet zu starten - dann war's das. Es gibt da so kleine Programme auf dem Netz, wenn die laufen hat man Vollzugriff aus das gesamte Dateisystem!

Feuer & Wasser: Steht der Server im Keller auf dem Boden? Sie glauben, da könne nirgends Wasser eintreten. Oder etwa Rückstoss über die Kanalisation oder ein Rohrleitungsbruch? Daraus folgt! Jeder Server der im Keller steht muss auf ein Podest von mindestens 60cm oder auf einen Tisch stehen!
Jeder Rechner ist durch Feuer und Überspannung gefährdet! Deshalb ist auf folgendes zu achten:

- RAID ist nur Redundanz, ein Schutz gegen defekte Komponenten
- Bänder müssen physikalisch an einem anderen Ort aufbewahrt sein
- Überspannungsspitzen und Unterbrüche lassen sich mit USV (UPS) verhindern
- Eigenständige Rauchmelder kosten nur ca. 80 Euro!

Die Passworte: Zu einfache Passwörter lassen sich durch systematisches Ausprobieren herausfinden. Das systematische Ausprobieren nennt sich Brute Force. Genauere Erklärung weiter unten im Text. Gute Passworte bestehen aus mindestens 12 Zeichen, mindestens 2 Zahlen und mindestens 2 Sonderzeichen! Dann ist mit Bruteforce nichts zu wollen!

Beispiel: Eine Untersuchung von Klein (Klein, Daniel V. 1990, USENIX Security Workshop Proceedings, Portland August 1990) an 15000 Accounts ergab eine Erfolgsquote von 24,2%, wobei Wortlisten mit Std. Worten, Namen, Tastaturfolgen, Geburtsdaten und Orten ver-

wendet wurden. (Nochmals zur Erläuterung das sind ¼ aller Passworte die gefunden wurden!)

9.1.4 Begriffe für den Angriff via Ethernet / TCP/IP

DoS: Ein solcher Angriff, auch "Denial of Service" genannt, zielt darauf ab, die IT-Benutzer daran zu hindern, Funktionen oder Geräte zu benutzen, die ihnen normalerweise zur Verfügung stehen. Dieser Angriff steht häufig im Zusammenhang mit verteilten Ressourcen, indem ein Angreifer diese Ressourcen so stark in Anspruch nimmt, dass andere Benutzer an der Arbeit gehindert werden. Es können z. B. die folgenden Ressourcen künstlich verknappt werden: Prozesse, CPU-Zeit, Plattenplatz, Inodes, Verzeichnisse, E-Mail.

Dies kann z. B. geschehen durch
- das Starten von beliebig vielen Programmen gleichzeitig
- das mehrfache Starten von Programmen, die viel CPU-Zeit verbrauchen
- das Belegen aller freien Inodes in einem Unix-System
- das Anlegen sehr vieler kleiner Dateien in einem Verzeichnis auf einem DOS-PC
- die gezielte Überlastung des Netzes
- das Kappen von Netzverbindungen

Modem: Eine Kommunikationskarte (z.B. eine ISDN-Karte oder ein Modem) kann eingehende Anrufe automatisch entgegennehmen. Abhängig von der eingesetzten Kommunikationssoftware und deren Konfiguration besteht dann die Möglichkeit, dass ein Anrufer unbemerkt Zugriff auf das angeschlossene IT-System nehmen kann.

Über eine Kommunikationskarte kann ein externer Rechner als Terminal an einen Server angeschlossen werden. Falls der Benutzer sich nach einer Terminalsitzung abmeldet, aber die Leitung ansonsten bestehen bleibt, ist vom externen Rechner ein Zugang wie über ein lokales Terminal möglich. Damit haben Dritte, die Zugang zu diesem Rechner haben, die Möglichkeit, Benutzerkennungen und Passwörter zu testen. Wesentlich gefährlicher ist der Fall, dass die Verbindung unterbrochen wird, aber der Benutzer nicht automatisch am entfernten System ausgeloggt wird. Dann kann der nächste Anrufer unter dieser Benutzerkennung weiterarbeiten, ohne sich anmelden zu müssen. Er hat somit vollen Zugriff auf das IT-System, ohne sich identifiziert und authentisiert zu haben.

SYN Flood: Überfluten des Sockets mittels synchronisations verbindungs Aufbauten. SYN flood ist keine intrusion attack, macht keinen Datenzugriff und ändert keine Daten.
Wenn Daten via TCP/IP gesendet werden, wird ein simples handshaking verfahren verwendet. Das geschieht in dem ein Client eine SYN (synchronised data packet) Anforderung an den Server gesendet. Der Server antwortet mit einem SYN/ACK (acknowledge receipt of the packet). Die Verbindung zwischen dem Client und dem Server ist nun hergestellt und die Kommunikation steht.
Ein SYN flood attacker sendet dauernd Verbindungsanforderungen an den Server. Als Resultat ist der Server nicht mehr in der Lage auf die Requests zu antworten. Nun sind alle möglichen Connections verbraucht und es können keine neuen mehr aufgebaut werden. Nach einer gewissen Zeit haben die Connections die nicht mehr bedient werden einen Time-Out und werden gelöscht. Wenn nun noch genügend Verbindungsanforderungen in der Warteschlange stehen so werden diese neuen leeren Verbindungen sofort wieder verwendet.
Jetzt ist das System für die wirklichen Kunden nicht mehr zugänglich.
Firewalls erkennen solche Datenfluten und können diese blockieren, jedoch das ankommende Datenaufkommen bleibt bestehen.

IP-Spoofing: IP-Spoofing ist eine Angriffsmethode, bei der falsche IP-Nummern vorgetäuscht werden, um dem angegriffenen Gerät eine falsche Identität vorzutäuschen.

Bei vielen Protokollen der TCP/IP-Familie erfolgt die Authentisierung der kommunizierenden IT-Systeme nur über die IP-Adresse, die aber leicht gefälscht werden kann. Nutzt man darüber hinaus noch aus, dass die von den Rechnern zur Synchronisation beim Aufbau einer TCP/IP-Verbindung benutzten Sequenznummern leicht zu erraten sind, ist es möglich, Pakete mit jeder beliebigen Absenderadresse zu verschicken. Damit können entsprechend konfigurierte Dienste wie rlogin benutzt werden. Allerdings muss ein Angreifer dabei u. U. in Kauf nehmen, dass er kein Antwortpaket von dem missbräuchlich benutzten Rechner erhält.

Weitere Dienste, die durch IP-Spoofing bedroht werden, sind smtp, rsh, rexec, X-Windows , RPC-basierende Dienste wie NFS und der TCP-Wrapper, der ansonsten ein sehr sinnvoller Dienst zur Einrichtung einer Zugangskontrolle für TCP/IP-vernetzte Systeme ist. Leider sind auch die in Schicht 2 des OSI-Modells eingesetzten Adressen wie Ethernet- oder Hardware-Adressen leicht zu fälschen und bieten somit für eine Authentisierung keine zuverlässige Grundlage.

In LANs, in denen das Address Resolution Protocol (ARP) eingesetzt wird, sind sehr viel wirkungsvollere Spoofing-Angriffe möglich. ARP dient dazu, zu einer 32-Bit grossen IP-Adresse die zugehörige 48-Bit grosse Hardware- oder Ethernet-Adresse zu finden. Falls in einer internen Tabelle des Rechners kein entsprechender Eintrag gefunden wird, wird ein ARP-Broadcast-Paket mit der unbekannten IP-Nummer ausgesandt. Der Rechner mit dieser IP-Nummer sendet dann ein ARP-Antwort-Paket mit seiner Hardware-Adresse zurück. Da die ARP-Antwort-Pakete nicht manipulationssicher sind, reicht es dann meist schon, die Kontrolle über einen der Rechner im LAN zu bekommen, um das gesamte Netz zu kompromittieren.

Missbrauch des ICMP-Protokolls: Das Internet Control Message Protocol (ICMP) hat als Protokoll der Transportschicht die Aufgabe, Fehler- und Diagnoseinformationen zu transportieren. Es lässt sich in mehrfacher Weise missbrauchen. Zum einem können über Redirect Pakete die Routingtabellen eines Rechners geändert und z. B. unerwünschte Routen konfiguriert werden. Zum anderen kann ein Angreifer gefälschte Destination Unreachable Pakete in die Verbindung einschleusen, so dass die bestehende Verbindung unterbrochen wird und somit die Verfügbarkeit der Netzverbindung nicht mehr gewährleistet ist.
Achtung das ICMP Protokoll (dem auch Ping angehört) sollte nicht einfach gefiltert werden! Denn über dieses Protokoll werden die Korrekturanforderungen der Packetgrösse geregelt! Dies ist mit dem Fachbegriff die MTU (Maximum Transmission Unit) die MTU von Ethernet ist 1500 Byte. Wenn jetzt z.B. ein FireWall das df-Bit (Dont Fragment) setzt und ICMP unterdrückt ist, dann laufen keine Encapsulierten Verbindungen mehr. Z.B. Ihr FireWall Filtert ICMP, Sie haben ADSL mit MTU=1435, Microsoft.com hat ICMP unterdrückt und df gesetzt. Jetzt empfangen Sie nur noch Pakete bis max. 1435Bytes alle grösseren können nicht mehr zusammengesetzt werden!

Source-Routing: Der Missbrauch des Routing-Mechanismus und -Protokolls ist eine sehr einfache protokollbasierte Angriffsmöglichkeit. In einem IP-Paket lässt sich der Weg, auf dem das Paket sein Ziel erreichen soll oder den die Antwortpakete nehmen sollen, vorschreiben. Die Wegbeschreibung kann aber während der Übertragung manipuliert werden, so dass nicht die durch die Routing Einträge vorgesehenen sicheren Wege benutzt werden (z. B. über die Firewall), sondern andere unkontrollierte Wege.

Missbrauch der Routingprotokolle: Routing Protokolle wie RIP (Routing Information Protocol) oder OSPF (Open Shortest Path First) dienen dazu, Veränderungen der Routen

zwischen zwei vernetzten Systemen an die beteiligten Systeme weiterzuleiten und so eine dynamische Änderung des Weges ermöglicht. Es ist leicht möglich, falsche RIP-Pakete zu erzeugen und somit unerwünschte Routen zu konfigurieren (auch von Extern).

Der Einsatz von dynamischem Routing ermöglicht es, Routing-Informationen an einen Rechner zu schicken, die dieser in der Regel ungeprüft zum Aufbau seiner Routingtabellen benutzt. Dies kann ein Angreifer ausnutzen, um gezielt den Übertragungsweg zu verändern. Bei Cisco hilft der Befehl: No Ip Directed Broadcast Abhilfe, dann werden nur noch Broadcast von benachbarten Geräten entgegengenommen.

DNS Spoofing: Dies ist eine etwas komplexere Methode. Immer wenn ein Domänen Name angefragt wird, so muss dieser zuerst in eine IP-Adresse umgewandelt werden. Dies übernimmt der DNS-Server. Da die DNS-Anfragen verbindungslos sind, kann jeder andere PC (des Hackers) auch eine Antwort liefern, ohne dass das auffällt. Dies geht insbesondere gut, da der DNS-Server eine gewisse Zeit zum Suchen benötigt. Die Antwort des effektiven DNS-Server kommt zuspät und wird nicht mehr beachtet. Wenn jetzt für eine Domäne die IP des Hackers verwendet wird so laufen alle Anfragen an diese Maschine, die die Daten aufzeichnet und dann an die effektive IP weiterleitet. Dies ohne, dass jemand davon was merken kann.

Intrusion Detection und Intrusion Response Systeme: Intrusion Detection Systeme lassen sich im wesentlichen in zwei Klassen einteilen: Signaturanalyse und Anomalie-Erkennung.
Die Signaturanalyse beruht auf der Annahme, dass sich viele Angriffe anhand einer bestimmten Abfolge von Protokolldaten erkennen lassen. Ein Beispiel ist das sogenannte Portscanning. Als Vorarbeit für einen Angriff wird zunächst festgestellt, welche Dienste auf dem angegriffenen Rechner ansprechbar sind, d. h. zu welchen TCP-Ports eine Verbindung aufgebaut werden kann. Hierzu wird mit Hilfe eines Programms ein Verbindungsaufbaupaket nacheinander an alle TCP-Ports geschickt. Erfolgt ein Verbindungsaufbau, ist dort ein Dienst installiert und kann angegriffen werden. Die entsprechende Signatur, also Erkennungsmerkmal, dieses Angriffs ist einfach: Verbindungsaufbaupakete, die nacheinander an alle TCP-Ports geschickt werden.
Es zeigen sich aber auch sofort die Probleme bei dieser Art der Angriffserkennung: In welcher Reihenfolge müssen die Ports angesprochen werden und in welchen zeitlichen Abständen, damit ein Angriff von einem normalen Betrieb unterschieden werden kann? Aktuelle Portscanning-Programme arbeiten so, dass nicht nacheinander Port 1, Port 2 bis Port n angesprochen werden, sondern dies in zufälliger Reihenfolge erfolgt. Auch können die Pakete nicht direkt nacheinander verschickt werden, sondern in zufälligen Zeitabständen (z. B. 1 s, 100 ms, 333 ms, 5 s ...). Dies macht die Erstellung einer Signatur schwierig.

Eine subtile Variante des Portscanning besteht darin, einzelne Pakete von verschiedenen Quell-Adressen zu senden. In Verbindung mit der oben aufgezeigten zeitlich versetzten Initiierung der Pakete ist die Wahrscheinlichkeit gegenwärtig sehr hoch, dass ein solcher Angriff unerkannt bleibt.

Bei der Anomalie-Erkennung geht man andererseits davon aus, dass sich das normale Verhalten der Nutzer oder Rechner statistisch erfassen lässt und wertet Abweichungen hiervon als Angriff. Ein Beispiel hierfür ist der Zeitraum, in dem eine Benutzerin normalerweise an ihrem Rechner angemeldet ist. Arbeitet sie z. B. fast immer Montags bis Freitags in der Zeit von 8.00 Uhr bis 17.00 Uhr mit Abweichungen von maximal 2 Stunden, so kann eine Aktivität am Samstag oder um 24.00 Uhr als Angriff gewertet werden. Das Problem bei der Anomalie-Erkennung ist die Festlegung des normalen Verhaltens. Hierfür lassen sich zwar mit Hilfe von Schwellwerten oder Wahrscheinlichkeitsbetrachtungen einige Aussagen machen. Ob es sinnvoll ist, eine Aktivität des Benutzers A am Montag um 19.10 Uhr sofort

als Angriff zu bewerten, erscheint fraglich. Auch ändert sich das normale Verhalten eines Benutzers in der Regel, so dass eine Anpassung vorgenommen werden muss. Wer aber sagt dem ID-System, dass diese Verhaltensänderung regulär ist und kein Angriff?

Des weiteren ist eine Unterteilung der ID-Systeme nach der Art der Datenaufnahme sinnvoll. Diese kann entweder mit Hilfe eines dedizierten Sniffers irgendwo im Netz erfolgen (Netzbasiertes ID-System), oder Teil der normalen Protokollierungsfunktionalität auf einem der angeschlossenen Rechner (Hostbasierte ID- Systeme) sein. Beides hat Vor- und Nachteile. Die netzbasierten Systeme haben zwar die Möglichkeit, einen umfassenden Angriff, der gleichzeitig verschiedene Rechner betrifft, leichter zu erkennen. Es ist aber erheblich schwieriger, komplexe Angriffe (z. B. über weitere Zwischenstationen) auf einen Rechner zu erkennen. Darüber hinaus können netzbasierte Systeme keine verschlüsselten Daten analysieren. Für die hostbasierten ID-Systeme gilt andererseits, dass für ihren Einsatz u. U. umfangreiche Änderungen an den Protokollierungsfunktionen der Rechner notwendig sind.

Da auch bei der automatischen Auswertung von Protokollinformationen die Datenschutzbestimmungen oder Personalvereinbarungen beachtet werden müssen, kann es u. U. notwendig werden, diese Daten pseudonymisiert abzulegen.

Vor der Kopplung von ID-, IR-System und Firewall sollten folgende Aspekte beachtet werden:

Ist es möglich, gezielt einen Angriff auf die Firewall zu initiieren, der vom ID-System irrtümlich als echter Angriff gewertet wird? Eine daraufhin vom IR-System ausgelöste Sperrung bestimmter Dienste über die Firewall kann erhebliche Konsequenzen auf die Verfügbarkeit haben.
Die Interaktion zwischen ID-, IR-System und Firewall sollte hinreichend transparent dokumentiert sein. Nur so ist es möglich, zu jedem Zeitpunkt abzuschätzen, von wem die Firewall administriert wird: vom IR-System oder vom Administrationspersonal. Im Zweifelsfall sollten Entscheidungen des Administrationspersonals Vorrang haben.
Um Angriffe gegen ein ID-System selbst auszuschliessen, sollten diese vom Netz her weitestgehend unsichtbar sein. Einfachste Massnahme ist die Zuweisung einer IP-Adresse, die im Internet nicht geroutet wird. Empfohlen sei weiterhin die Deaktivierung des ARP-Protokolls für das entsprechende Interface, so dass weder auf ARP- noch auf IP-Pakete reagiert wird.

9.1.5 Die Beweggründe für Datenklau oder Zerstörung

Der zur Zeit am steilsten ansteigende Wirtschaftszweig ist wohl die Wirtschaftskriminalität. D.h. ich verschaffe mir mit illegalen Mitteln Wettbewerbsvorteile und da brauche ich Hilfe eines Spezialisten für illegale Angriffe oder kurz ein Hacker.

Allgemein ist zu sagen, dass es folgende Beweggründe gibt:
- Einer Firma (Mitbewerber) Finanziellen / Wirtschaftlichen schaden zufügen
- Freude am Schaden anderer
- Seine Fähigkeiten unter beweis stellen
- Freude an illegale Aktionen
- Daten Klau im Auftrag eines Mitbewerbers
- Frust über die eigene Firma
- Absehbarer Job-Wechsel mit Daten- und Kundenstamm
- Fahrlässigkeit
- Ahnungslosigkeit beim ausprobieren von Programmen

9.1.6 Vorgehen eines Hacker‘s

Ein Hacker ist auf der Suche nach Sicherheitslücken! Der erste Gedanke wird sein, da gibt es Leute die können von remote (extern) auf interessante Daten aus dem Büro zugreifen. Wie kann ich es also hinkriegen, dass ich das selbe auch machen kann. Geht das via Internet, brauche ich Namen und Passwort, wie sind die Sicherheiten aufgebaut, usw...
Jetzt werden **INFORMATIONEN GESAMMELT** alles was es da so gibt! Alle Email Adressen, alle Telefonnummern, Versionen aller Server (SMTP, WEB, FTP), Betriebssystem des Server / der Clients, Namen der Benutzer auf den Server (Vorname, Name oder Kurzzeichen ...)
Nun fehlt es nur noch an den Passworten. Als erstes werden Wortlisten in der Sprache des Unternehmens verwendet. Damit sollten bereits 1 bis 3% der Passworte gefunden werden. Der zweite Schritt nennt sich BruteForce das bedeutet, es werden alle Zeichen- und Zahlenkombinationen durchprobiert. Beginnend a, b, c, .. z, aa, ab, ac, .. usw.
Mit dieser Methode lassen sich Passworte bis 10 Zeichen Länge bestehend aus Zahlen und Buchstaben binnen 30 Tagen finden. Als Beispiel wird oft versucht, via IIS (**I**nternet **I**nformation **S**erver) mit Port 80 (Web) die Kopie vom SAM (**S**ecurity **A**ccess **M**anager) herunter zu laden. Wenn auf dem Webserver vom Microsoft nicht alle notwendige Patches geladen sind so gelingt dies auch. In der SAM sind alle Benutzernamen und die Schlüssel zu den Passworten abgelegt. D.h. wenn die SAM ins ASCII Format konvertiert wurde so stehen die Benutzernamen im Klartext zur Verfügung. Bei Microsoft wird ein Hash verwendet der nur eine Verschlüsselung jedoch keine Entschlüsselung zulässt. Das ist der Trick und darum ist bis heute ein dechiffrieren gar nicht möglich, nur ein BruteForce! Das heisst es wird jede Kombination verschlüsselt und dann mit dem Hash aus der SAM verglichen bis die beiden übereinstimmen.

9.1.7 Der Benefit für ein Unternehmen einen Hackauftrag zu vergeben

Wie wir gesehen haben ist Wissen gleich Erfolg und Macht. D.h. das vertiefte Wissen über die Kunden um Bezug auf die Konkurrenz ist zwar nur ein kleiner Stein des Puzzles aber alle Steine des Puzzles ergeben ein klares Bild!
So als Beispiel: Ich bin der Chef der Firma ProfilRad AG, wir stellen Auto Pneus her und vertreiben diese an die Firmen die Pneus wechseln.
Jetzt wissen die Aussendienstmitarbeiter welchen Umsatz welcher Händler macht, jedoch ist nicht bekannt welcher Händler auch noch bei der Konkurrenz einkaufen geht.
Ein findiger Hacker ist auf die Idee gekommen auf der Webseite www.ProfilRad.ch im Händlerbereich für Bestellungen ein kleines JavaApplet zu Programmieren, das mit der Datenbank auf dem Server verbunden ist. Wenn sich jetzt ein Händler für Bestellungen anmeldet wird auch das Applet gestartet und erkennt den Anmeldenamen des Händler. Jetzt wird ausspioniert, ob dieser Händler auch bei der Konkurrenz einkaufen geht? Wie wird das gemacht? Die Konkurrenz heisst z.B. www.Michelin.ch. Auf der Homepage von Michelin ist z.B. ein Bild mit folgender URL zu finden www.Michelin.ch\Pneu.gif. Das JavaApplet macht jetzt zwei HTTP Anfragen für die obige URL und misst die jeweilige Zeit, bis die Antwort da ist. Und was nützt das jetzt? Das bringt Information! Denn der Internet Browser hat einen Cache für Files und der ist im Normalfall auf 20 Tage eingestellt. Das bedeutet, wenn ich in den letzten 20 Tagen nicht bei Michelin auf der Homepage war, dann würde die erste Abfrage bedeutend länger dauern, da diese Abfrage übers Internet läuft. Die zweite Anfrage würde direkt aus dem Cache des Internet Browsers abgerufen werden.
Jetzt kann ich die Datenbank bei ProfilRad mit den gewonnen Daten füllen:

- Datum des Konkurrenz Tests
- War bei der Konkurrenz Ja / Nein
- Cookie für PC Identifikation (Falls der Kunde mehrere hat)

Das ganze gibt aber erst mit der Fülle aller Kundendaten ein Bild!
Bei einem vorgeschalteten Proxy ginge das aber nicht, aber auch das liesse sich prüfen!

In der Datenbank müsste sich zyklisch alle 20 Tage (je nach Einstellung beim Kunden) einen Eintrag mit Konkurrenz Michelin Nein finden lassen.
Jetzt mache ich das für die ganze Konkurrenz und alle Kunden und prüfe auch gleich noch wie viele PC's sich pro Händler für Einlagen jeweils melden.
Jetzt kann der Aussendienst aus dem vollen schöpfen, denn er weiss von jedem Händler von welchem Konkurrenten auch Ware bezogen wird und in welchem Rahmen!
Ist das nun strafbar? Ja, denn es ist eine Verletzung der Persönlichkeitssphäre und persönliche Daten dürfen nicht ohne Einwilligung weiterverarbeitet und genutzt werden!
Dieses Sicherheitsleck wurde übrigens im Internet Explorer 6.x behoben.

9.1.8 Die etwas komplexeren Hack-Methoden

Wie gesagt, das Abhören von Daten die nicht für einem bestimmt sind ist strafbar. Dies gilt jedoch nicht für die Geheimdienste! D.h. Jeder Geheimdienst darf im Land und im Ausland Daten sammeln und Verarbeiten und zum eigenen Erfolg nutzen! Es geht sogar so weit, dass es auch keine richterlichen Bescheide geben muss für eine Aktion (inkl. Hausdurchsuchungen und Festnahmen). Dies hatte auch zur Folge, dass das Amerikanische DoD (**D**epartment **o**f **D**effensive) zur gefürchtetsten Abteilung des Amerikanischen Staatssystems gehört.

Noch kurz was zur Entstehung des ganzen:

1957 Die UDSSR startet den ersten Satelliten SPUTNIK in eine Weltumlaufbahn. Die USA müssen militärisch reagieren und gründen die ARPA (**A**dvanced **R**esearch **P**rojects **A**gency), die in das Verteidigungsministerium integriert ist. Die Aufgabe der ARPA ist, neue Technologien im Bereich Kommunikation und Datenübertragung zu entwickeln, um der USA einen technischen Vorsprung gegenüber der UDSSR zu verschaffen. (:amk:)

1969 Das ARPANET unter Einfluss des DoD entsteht.
Die ersten 4 Knoten entstehen mit Hilfe eines Computer IMPs von BBN. Als Haupt-Knoten-Computer wurde jeweils ein Honeywell DDP-516 mini computer mit 12KB Speicher eingesetzt. AT&T stellte 50kbps-Leitungen zur Verfügung.

1973 Die ersten internationalen Anschlüsse an das ARPANET erfolgen: Das "University College of London" in England und das "Royal Radar Establishment" in Norwegen.
Bob Kahn prophezeite Internetprobleme und startete das Programm für Internet-Überwachung bei der ARPA. (:vgc:)
Cerf und Kahn präsentieren im September bei der INWG an der Universität von Sussex in Brighton, England die Basis-Ideen für das INTERNET.

1989 Die Anzahl der Hosts im Netz bricht die Schallmauer von 100'000.
Von europäischen Service-Providern wird die RIPE (Reseaux IP Europeens) geformt um die Notwendigkeit für administrative und technische Koordination aufzuzeigen, um ein Pan-Europäisches IP-Netzwerk betreiben zu können. (:glg:)

1994 Das ARPANET (jetzt INTERNET) feiert seinen 25. Geburtstag.
Kommunen, wie Lexington und Cambridge, Mass., USA, gehen direkt mir eigener Verbindung ans Internet.
Der US Senat und das weisse Haus bieten Informationsserver an.
Die ersten Online-Geschäfte tauchen im Internet auf.

1996 US-Telefongesellschaften nehmen Notiz von Internet-Telefonen und bitten den US-Kongress diese Technologie zu verbannen obwohl es diese Technologie schon Jahre gab.

Das bedeutet das Militär hat das Internet erfunden und mit den Universitäten entwickelt und den Universitäten und der Öffentlichkeit übergeben, da das System für Militärische Mehrfach Datenpfade zu ungeeignet schien. Jedoch hat das Militär weiterhin die Finger fest darin wenn auch nicht die Oberhand!

In den USA und in England ist das Projekt ECELON dazu da nicht Amerikanische und (Amerikanische) Daten für den Geheimdienst zu sammeln. (In der Schweiz ist das Satos-3)

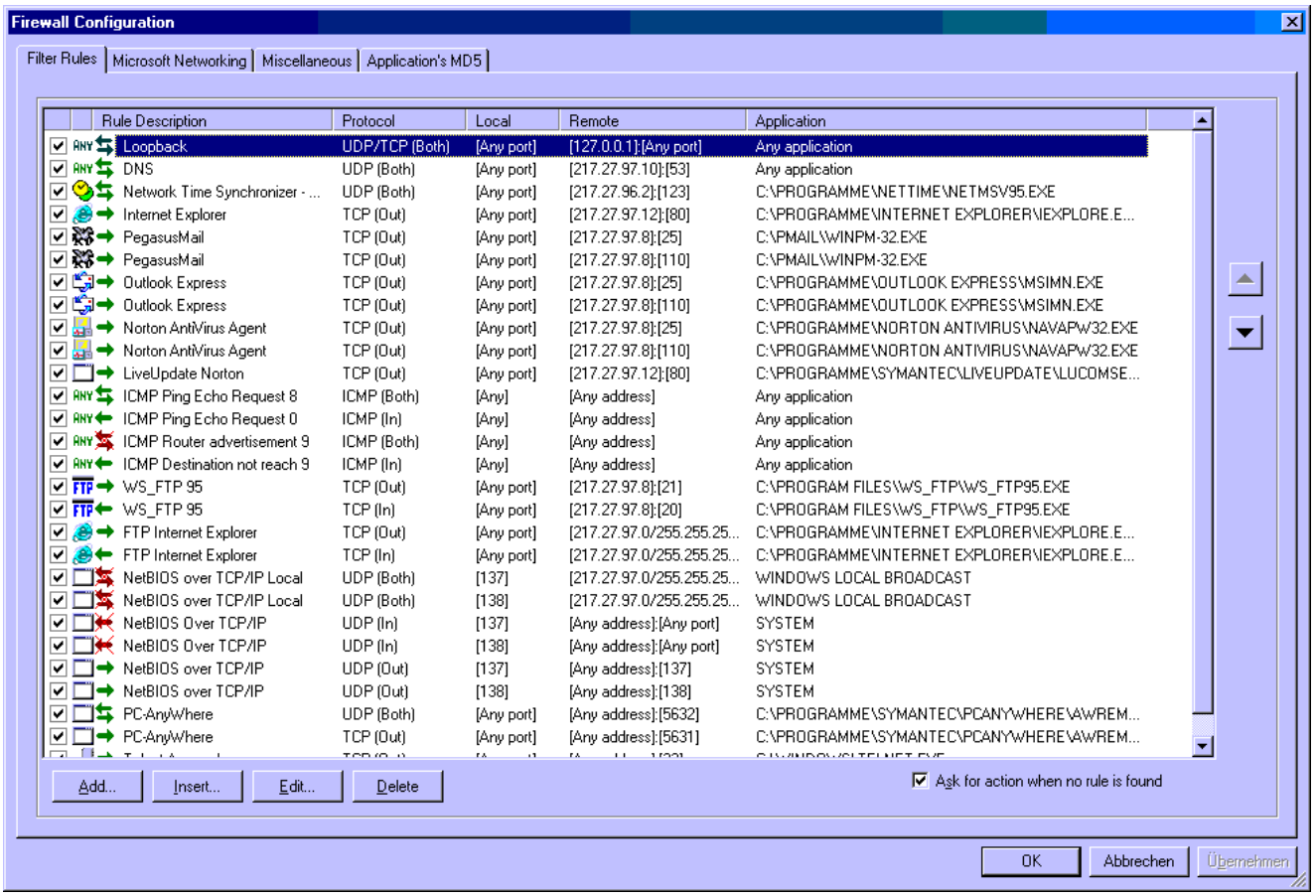
9.1.9. Schutz vor Hackerattacken

Bsp. Windows:
- Administrator kopieren zu Admin! Und Administrator mit Gastrecht versehen
- Alle Patches von Microsoft auf dem neusten Stand
- Ports die nicht verwendet werden schliessen (z.B. auf dem Router, geht bei jedem)
- Antivirus installieren mit automatischem Update
- Firewall Hardware-Box (keine PC-Basierenden, braucht Unterhalt durch Profi.)
- Bei jeder Telefon-Einwahl nur mit authentifizierter Absender Telefon id.
- Remote Connection nur die notwendige ISP freigeben inkl. deren Netze
- E-Mail IP-NameLookUp, Absender Check, SPAM Filter (junk Mailers)
- Alle Dienste müssen Logfiles erstellen!
- Keine Modems auf den Client PC's erlauben!
- Passworte die von aussen her zugänglich sind mind. 12 Zeichen lang.
  Das Passwort muss mindestens 2 Zahlen und mindestens 2 Sonderzeichen!
- Windows Verzeichnis bei der Installation neu wählen
  z.B. C:\WinSys anstatt C:\WinNT (Hacker holen alles aus dem Std. Verzeichnis)

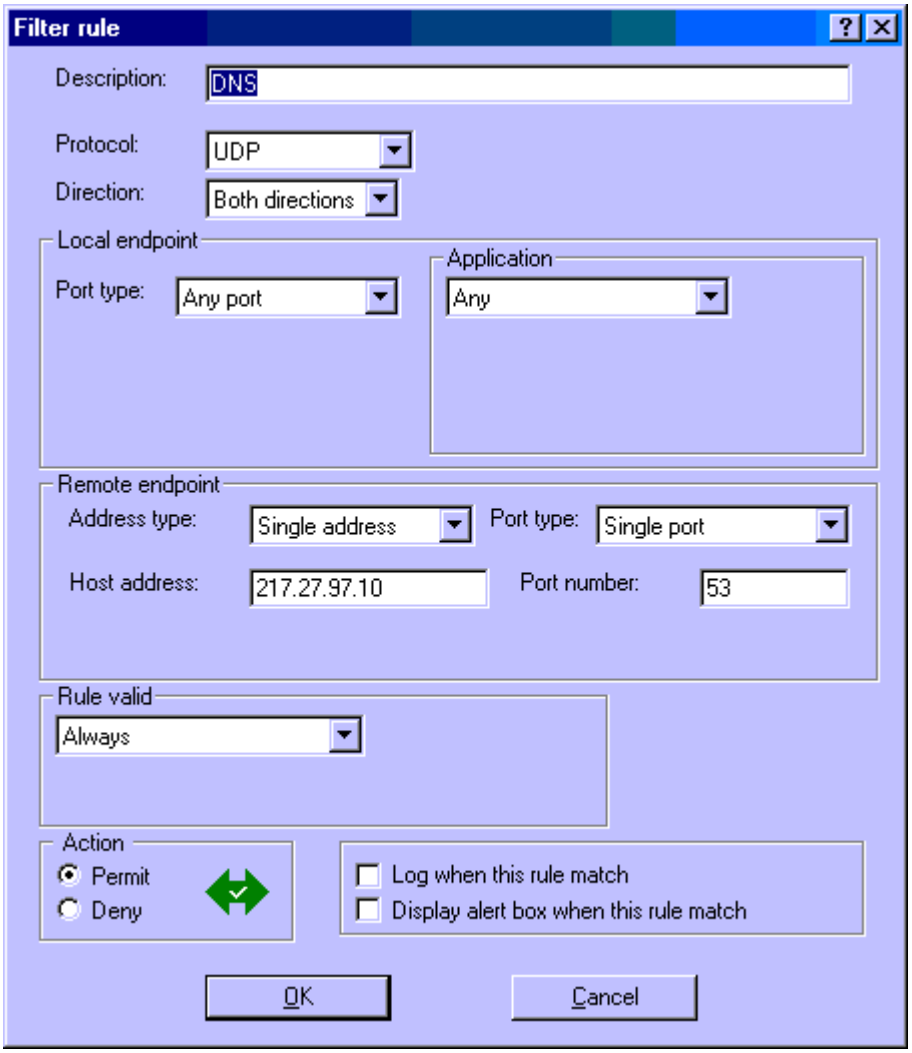
Schutz via Firewall (nur standalone sind wirklich sicher):
- NAT (Maskrading) genügt nicht, denn alle Dienste sind von innen nach aussen offen
- DNS Dienste intern bereit stellen (falls nötig, für Proxy und Mail nicht notwendig)
- DNS UpDates nur via UpStream Provider (2 Host zulassen)
- Alle PC’s verwenden einen Proxy Server für alle externen Anfragen.
- Alle internen PC’s haben keinen Gate nach aussen (nur Intranet)
- Nur der Proxy, hat Internet Zugang (ev. DNS, Mail Server)
- Alle Connections werden aufgezeichnet, und ev. gefiltert

Beispiel mit einer PC Arbeitsstations FireWall:
Also wie schon erwähnt eine Software Firewall ist nie so sicher wie eine eigenständige Box. Da sich auf dem PC Windows befindet und das eben auch so seine Eigenheiten hat. Zudem kann jeder Benutzer den Task oder Service des Firewalls beenden wenn er denkt, dass zu viele Fehlermeldungen auftreten mit denen nichts angefangen werden können.
Unter folgender URL ist eine FreeWare Firewall für Windows zu finden. Diese Firewall ist sehr primitiv und unterstützt nur Layer III also nichts mit MAC Adressen und auch kein NAT oder so. Auch Intrusion detection ist nicht vorhanden. Das ist das erkennen von Scans und folgen die nicht von standard Programmen stammen können, DoS , usw...
ftp://www.clinch.ch/NetzWerk/PC_Firewall/pf2.exe

Unten ist eine Liste von Regeln als Beispiel für Regeln bei einem PC Firewall. Interessant ist, dass die Software die Layer III Dienste mit den Programmen verbindet. So wird z.B. unterschieden ob FTP vom Web-Browser oder aus dem WS_FTP Programm her kommen. So kann z.B. der WebBrowse nur via Proxy betrieben werden und das WS_FTP nur via eigene Home-Page IP Adresse um eine erhöte Sicherheit zu erlangen.

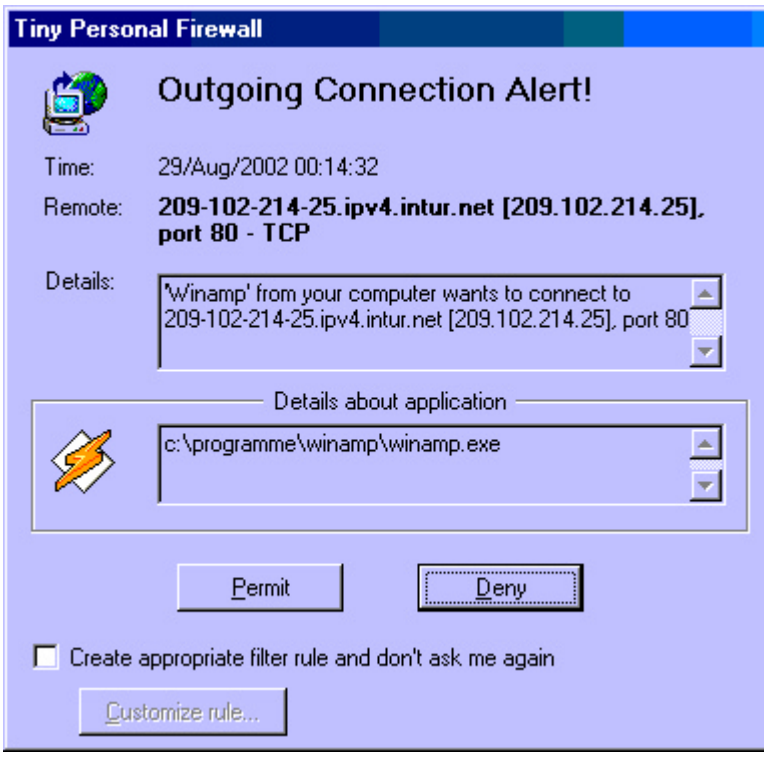


In der obigen Grafik ist zu ersehen, dass jede Regel noch oben oder unten verschoben werden kann. Jedoch werden bei diesem Firewall immer alle Regeln durchlaufen bis zum Ende.


Filter rule
Description:
DNS
Protocol:
UDP
Direction:
Both directions
Local endpoint
Port type:
Any port
Application
Any
Remote endpoint
Address type:
Single address
Port type:
Single port
Host address:
217.27.97.10
Port number:
53
Rule valid
Always
Action
Permit
Deny
Log when this rule match
Display alert box when this rule match
OK
Cancel

Ein unbekannter Dienst wird aktiviert:

Und was passiert jetzt wenn ein neuer nicht bekannter Dienst eine Verbindung aufbauen will? Unten das Fenster das erscheint. Jetzt kann sofort Erlaubnis erteilt werden oder nicht. Mit dem Create Filter kann das direkt in die Filterliste aufgenommen werden. Hier ist natürlich auch ein Schwachpunkt des ganzen, denn wenn Meldungen kommen wird mal mit dem einem Knopf versucht zum Ziel zu kommen, dann mit dem anderen bis die störenden Meldungen nicht mehr erscheinen. Somit zerstören unerfahrene Benutzer das gesamte Sicherheitskonzept.



Im obigen Fall hat das Programm WinAmp (ein FreeWare Medien Player) versucht eine Verbindung zu 209.102.214.25 herzustellen mit dem Dienst http via Port 80. Es wurde auch gleich noch ein Remote Lookup gemacht mit der Antwort 209-102-214-25.ipv4.intur.net. Mit Permit oder Deny kann jetzt die Aktion für dieses Paket gemacht werden Permit heisst durchlassen Deny heisst verwerfen.