Firewallsysteme
Ein elementarer Teil der Sicherheit in der Informationstechnik (IT)
Wozu werden sie benötigt, was können sie und wie werden sie eingesetzt?

Verfasser: Herbert **Gruschka**
Andreas **Schneider**

Inhaltsübersicht Seite

1. Zusammenfassung

Das Thema „Firewall“ hat in den letzten Jahren durch den Anschluß lokaler Netze an externe Weitverkehrsnetze und die Nutzung von Internetdiensten durch die Kommunen und deren Verwaltungen eine zunehmende Bedeutung erlangt. Angesichts des großen Nutzens, den das Internet und die dort verfügbaren Dienste bieten, wird allzu oft vernachlässigt, daß im Internet auch viele Gefahren lauern, denen begegnet werden muß. Diese Gefahren werden aus unserer Sicht noch steigen, wenn im Rahmen der vielerorts anzutreffenden eGovernment-Initiativen eigene Internet-Dienste bereitgestellt werden oder interaktive Anwendungen rund um die Uhr erreichbar sein sollen. Dieser Beitrag wendet sich daher an alle IT-Entscheider und -Verantwortlichen, um diese für ein aus unserer Sicht sehr wichtiges Thema zu sensibilisieren, die Notwendigkeit einer Absicherung lokaler Netze durch eine Firewall deutlich zu machen und die grundlegenden Unterschiede von Firewallösungen aufzuzeigen.

Folgende Punkte sind aus unserer Sicht besonders zu beachten:

– Ein ungesicherter Anschluß des lokalen kommunalen Netzes an das Internet oder an andere unsichere Weitverkehrsnetze ist in vielfacher Hinsicht (Strafrecht, Datenschutz, Kassensicherheit, Verfügbarkeit) unzulässig.

– Die Sicherung lokaler Netze durch eine Firewall setzt eine klare Strategie (IT-Sicherheitsziele, Sicherheitskonzept) und eine gewissenhafte Umsetzung dieser Vorgaben durch organisatorische und technische Maßnahmen voraus. Dies ist kein einmaliger Vorgang, sondern eine Daueraufgabe.

– Aufbau und Betrieb einer Firewall erfordern ein entsprechendes Fachwissen, welches in der Regel erst ab einer gewissen Größenordnung wirtschaftlich vorgehalten werden kann. Wird die Größenordnung nicht erreicht, ist es zweckmäßig, die damit zusammenhängenden Aufgaben einem vertrauenswürdigen Dritten zu übertragen oder eine interkommunale Zusammenarbeit (z.B. Landkreis-Behördennetz) anzustreben.

– Eine Firewall muß nicht immer am Standort selbst stehen, sondern kann auch zentral für mehrere Standorte vorgehalten werden, wenn die Übertragungsstrecken vom Standort bis zur Firewall ausreichend sicher sind.

– Maschinen, die von außen erreichbar sein müssen, da sie Internet-Dienste anbieten, gehören stets in ein besonders abgesichertes Teilnetz und sollten nicht direkt mit dem lokalen Netz verbunden sein.

– Auch bei einem Anschluß an das Bayerische Behördennetz (BYBN) hat jede Stelle für ihren Verantwortungsbereich sicherzustellen, daß ihre Daten und Programme nicht von Unbefugten eingesehen, verändert oder gelöscht werden können. Für die Einhaltung der datenschutzrechtlichen und haushaltsrechtlichen Vorschriften zur IT-Sicherheit ist jede Stelle selbst verantwortlich.

2. Einführung

Im Rahmen unserer überörtlichen Rechnungsprüfung haben wir in den letzten Jahren neben dem sparsamen und wirtschaftlichen Betrieb der vor Ort eingesetzten Informationstechnik (IT) zunehmend auch den ordnungsgemäßen und sicheren Einsatz der Hard- und Software geprüft. Hinsichtlich der inneren und äußeren Sicherheit der IT-Systeme mußten wir dabei teilweise schwerwiegende Feststellungen treffen. Um nur einige der gravierendsten Beispiele zu nennen:

– Internetzugang des lokalen Verwaltungsnetzes ohne jegliche Schutzmaßnahmen

– keinerlei Protokollierung sicherheitsrelevanter Zugriffe

– Verwendung von Installations-Paßwörtern und/oder Trivialpaßwörtern in zentralen Netzwerkkomponenten, Serversystemen, Datenbanken und finanzwirksamen Verfahren

– keine Beschränkung und Differenzierung von Benutzerrechten in finanzwirksamen Anwendungsverfahren

– keine Sicherheitseinstellungen in den Betriebssystemen (Paßwort- und Systemrichtlinien)

– keine Kontrolle von Internetdiensten (z.B. Download aller Dateien, Zugriff auf WEB-Seiten mit pornographischen Inhalten)

– unzureichender oder fehlender Virenschutz

– fehlende oder nicht funktionsfähige Datensicherungen

Diese Vielfalt von Sicherheitsmängeln ist schon bedenklich, was die Sicherheit der IT gegenüber Ausfällen, Datenverlusten, böswilligen oder allzu neugierigen Mitarbeitern anbelangt. Besonders beunruhigend ist es aber, wenn lokale Verwaltungsnetze ungeschützt mit dem Internet und so mit der ganzen Welt verbunden sind. Angesichts der häufigen Meldungen in der Fach- und Boulevardpresse über Sicherheitslücken in IT-Systemen und über weltweite Systemausfälle durch Viren, Würmer oder Hackerangriffe ist es dringend notwendig, sich mit den Gefahren auseinanderzusetzen, die beim Anschluß lokaler Netze an das Internet entstehen, und die erforderlichen Schutzmaßnahmen zu besprechen. Angesichts der Vielzahl technischer Möglichkeiten und der daraus resultierenden Gefahrenquellen ist dies ohnehin schon ein sehr breites Thema. Um nicht zu verwirren oder abzuschrecken, wollen wir versuchen, die aus unserer Sicht wichtigsten Aspekte allgemein verständlich darzustellen. Dabei ließ es sich nicht vermeiden, zum besseren Verständnis auf bestimmte grundlegende technische Zusammenhänge hinzuweisen. Für den „technischen Laien“ wird trotzdem manches zu technisch erscheinen. Dagegen können wir für den „Experten“ in diesem Beitrag nicht alle notwendigen Details darstellen; er kann sich jedoch aus der im Anhang angegebenen Literatur weitergehend informieren.

3. Was gilt es zu schützen?

Durch die Verbindung eines lokalen, nicht öffentlichen Netzes (LAN[1]) mit einem öffentlichen und daher grundsätzlich unsicheren Netz (WAN[2]), insbesondere dem auf der ganzen Welt verfügbaren Internet, sind grundsätzlich gefährdet

- die Vertraulichkeit, Verfügbarkeit und Integrität der auf den IT-Systemen gespeicherten Daten (mögliche Schäden: Verstoß gegen rechtliche oder vertragliche Vorschriften; Beeinträchtigung des informationellen Selbstbestimmungsrechts und der Persönlichkeitsrechte),

- die Verfügbarkeit der Hard- und Software, d.h. der für den Bürger, den Verwaltungsbetrieb oder die politischen Gremien notwendigen technischen Infrastruktur (mögliche Schäden: Beeinträchtigung der Aufgabenerfüllung),

- das Ansehen der Verwaltung oder der kommunalen Gebietskörperschaft und deren Einrichtungen (mögliche Schäden: negative Außenwirkung und finanzielle Auswirkungen).

Welcher Schutzbedarf sich für die eingesetzte IT-Infrastruktur, die Anwendungen und Daten ergibt, läßt sich aus unserer Sicht am besten anhand des IT-Grundschutzhandbuches (IT-GSHB)[3] des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ermitteln. Darüber hinaus ist das IT-GSHB auch eine gute Informationsquelle und eine praxisorientierte Anleitung zum Thema IT-Sicherheit im allgemeinen. Im wesentlichen bestimmt der Schaden bzw. die Summe der Schäden mit den schwerwiegendsten Auswirkungen den Schutzbedarf eines IT-Systems (Maximum-Prinzip). Soweit wir dies überblicken können, werden nach unserer Einschätzung im kommunalen Bereich Anwendungen eingesetzt und Daten gespeichert, bei denen mindestens ein mittlerer, bisweilen ein hoher, gelegentlich ein sehr hoher Schutzbedarf[4] gegeben ist. Folgende Beispiele sollen dies verdeutlichen:

- Die in finanzwirksamen Verfahren gespeicherten Daten weisen in der Regel einen mittleren Schutzbedarf aus.

- Die in Personalinformationssystemen oder Sozialhilfeverfahren gespeicherten, personenbezogenen Daten haben regelmäßig einen hohen Schutzbedarf.

- Die in Klinik-Informationssystemen gespeicherten personenbezogenen Daten der Patienten, insbesondere deren Diagnose- und Behandlungsdaten, bedingen aus unserer Sicht einen sehr hohen Schutzbedarf.

Aufgrund dieser Einschätzung weisen wir darauf hin, daß bei einem hohen oder sehr hohen Schutzbedarf die Anwendung des IT-GSHB und die Umsetzung des dort vorgesehenen Standard-Maßnahmenkatalogs nicht ausreicht. In diesen Fällen ist eine ergänzende Sicherheitsanalyse (vgl. Kapitel 2.5 IT-GSHB) anhand des IT-Sicherheitshandbuchs notwendig, um gegebenenfalls die im IT-GSHB beschriebenen Schutzmaßnahmen sinnvoll zu ergänzen oder zu verstärken.

---

1 local area network - vgl. Begriffsdefinitionen

2 metropolitan area network, wide area network - vgl. Begriffsdefinitionen

3 vgl. www.bsi.de/gshb/index.htm

4 zur Einstufung des Schutzbedarfs vgl. Kapitel 2.2 IT-GSHB

Auch ohne nähere Risikobewertung der verwendeten Internet-Dienste ist daher schon jetzt folgendes festzustellen:

Ein ungeschützter oder unzureichend abgesicherter Zugang eines lokalen kommunalen Netzes zum Internet ist bei diesem Schutzbedarf weder mit den aktuellen technischen Sicherheitsstandards, noch mit den allgemeinen oder spezialgesetzlichen Bestimmungen zum Datenschutz (z.B. § 203 StGB, AO, SGB X, BayDSG) vereinbar. Im Schadensfall drohen den Verantwortlichen dienst- und strafrechtliche Verfahren sowie Schadensersatzforderungen.

4. Wovor muß man sich schützen?

Die Angriffsszenarien und daraus resultierenden Risiken sind vielfältig und lassen sich im Rahmen dieses Beitrags nicht erschöpfend behandeln, da immer wieder neue Angriffsmethoden und -werkzeuge, aber auch neue Unzulänglichkeiten der eingesetzten Server- und Client-Programme (sogenannte Vulnerabilities) bekannt werden.

Ausgehend von den zu schützenden Werten (vgl. vorstehende Ausführungen) möchten wir die bekannteren Angriffsmethoden kurz darstellen, um später bei der Beschreibung der Firewallfunktionalitäten einen gewissen Bezugspunkt zu schaffen. Die Darstellung der einzelnen Angriffsmethoden ist größtenteils einer vom BSI veröffentlichten Studie der debis IT Security Services[5] entnommen und wurde zum Teil mit eigenen Anmerkungen ergänzt oder entsprechend komprimiert. In der Studie finden sich außerdem zahlreiche weitere Hinweise über technische und konzeptionelle Schwachstellen in Internet-Diensten und Betriebssystemen, deren Lektüre den Sicherheitsverantwortlichen und den Systemadministratoren zu empfehlen ist:

– **Port-Scans**[6]

  Portscanner klopfen an fremde Systeme an, um in Erfahrung zu bringen, welche Dienste ein Zielrechner anbietet bzw. auf welchen TCP und UDP-Ports[7] des Zielsystems ein Server auf eintreffende Datenpakete wartet.

– **IP- und DNS-Spoofing**

  Bei Spoofing-Angriffen versucht sich der Angreifer hinter einer falschen Absender- oder Empfänger-Adresse zu verstecken. Da das derzeit verwendete Internet-Protokoll (IPv4) selbst keine wirksamen Authentifizierungsmechanismen zwischen den im Internet angeschlossenen Rechnern zur Verfügung stellt, ist es z.B. möglich, falsche Rechneradressen (IP-Spoofing) oder Rechnernamen (DNS-Spoofing) zu verwenden oder die Routing-Tabellen eines Rechners/Routers zu manipulieren.

– **Denial-of-Service-Angriffe (DoS-Attacken)**

  Gezielte Angriffe auf bekannt gewordene Sicherheitslücken oder Implementierungsfehler eines Server-Dienstes können diesen lahmlegen oder zum Absturz bringen. Auch normale Abfragen eines Serverdienstes können mit einer künstlich hohen Abfragerate den Dienst

[5] [BSI1998]

[6] vgl. Begriffserläuterungen im Anhang

[7] vgl. Kapitel 9.1 Paketfilter

außer Kraft setzen, insbesondere dann, wenn die Antwort sehr viel Rechenzeit in Anspruch nimmt. DoS-Attacken auf Schwachstellen (Vulnerabilities) des Betriebssystems können einen an das Netzwerk angeschlossenen Rechner (Host) blockieren oder diesen ebenfalls zum Absturz bringen.

– **Viren**

Unter einem Virus versteht man ein sich selbst replizierendes Programm, das sich in einem Wirtprogramm oder im Bootsektor einer Festplatte festsetzt. Es kann sich außerdem in andere Programme kopieren und diese dadurch infizieren. Ein Virus läßt sich in der Regel an einem für ihn typischen Muster (Codesequenz) identifizieren. Neuere Viren können sogar ihre Codesequenzen ändern und sind deshalb besonders schwer zu erkennen. Viren beeinträchtigen in aller Regel die Funktionsfähigkeit des befallenen Rechnersystems und können zu Datenverlusten oder Schäden an Hardware führen. In letzter Zeit treten häufig sogenannte Makro-Viren auf, die sich in elektronischen Dokumenten oder Mails verstekken.

– **Trojaner**

Ein „trojanischen Pferd“ ist ein Programm mit unerwarteter Funktionalität. Beispiel für einen Trojaner ist eine Anmelde-Prozedur, die alle verarbeiteten Paßwörter sammelt, oder ein Tastaturscanner, der alle eingegebenen Tastenanschläge aufzeichnet, und diese Informationen an einen potentiellen Angreifer weiterleitet. Von Trojanern befallene Systeme werden gelegentlich auch für DoS-Attacken auf fremde Systeme mißbraucht.

– **Würmer**

Ein Wurm verbreitet Kopien seiner selbst über ein Netz. Ein Wurm ist ein eigenständiges Programm und von keinem Wirtsprogramm abhängig. Würmer führen in der Regel aufgrund ihrer Replikationsrate zu einem erhöhten Datenverkehr, können aber auch Schadensfunktionen haben, die vergleichbar mit den Viren sind.

– **Browser-Plug-Ins, Java, JavaScript, ActiveX, Java-Applets**

Webbrowser (z.B. Microsoft Internet-Explorer oder kurz IE, Netscape-Navigator oder kurz Netscape, Mozilla) können selbst nur eine beschränkte Anzahl von Daten verarbeiten und benötigen deshalb sogenannte Viewer, um Datentypen zu verarbeiten, die die Browser selbst nicht verstehen. Die weltweit am häufigsten eingesetzten Browser (IE und Netscape) unterstützen deshalb inzwischen einen Mechanismus, der es Drittherstellern erlaubt, Plug-Ins anzubieten, die nach dem Herunterladen eine integrierte und nahtlos eingepaßte Erweiterung des eigentlichen Browsers bilden. Die meisten Browser können zusätzlich noch ein oder mehrere Erweiterungssysteme (z.B. Java, JavaScript oder ActiveX) verarbeiten, die die Leistungsfähigkeit und Flexibilität der Browser ebenfalls erweitern. Werden solche Erweiterungen aus nicht vertrauenswürdigen Quellen heruntergeladen, können diese Programme zu Schäden an den befallenen IT-Systemen oder zu anderweitigen Sicherheitsproblemen (vgl. Trojaner) führen.

– **Makrosprachen**

Makrosprachen sind in diversen Office-Paketen verbreitet und im Grunde genommen Programmiersprachen, die speziell auf die jeweiligen Anwendungen zugeschnitten sind. Sehr

bekannt und leistungsfähig sind die VBA-Sprachen der Microsoft-Office-Komponenten, die in Umfang und Mächtigkeit einer herkömmlichen Programmiersprache kaum nachstehen und auch Zugriffe auf Betriebssystemressourcen erlauben.

– **Sniffer**

  Mit Netzwerk-Sniffern wird die Datenübertragung bis hinunter zur Ebene einzelner Protokollpakete überwacht und mitprotokolliert. Da manche Protokolle das bei der Authentifizierung verwendete Paßwort im Klartext übertragen (z.B. Telnet), können hierbei ernsthafte Sicherheitsprobleme entstehen.

– **Social Engineering**

  Dies ist, rein technisch betrachtet, die einfachste Form eines Angriffs. Hier wird ganz bewußt die Gutgläubigkeit und Vertrauensseligkeit der Anwender oder Administratoren ausgenutzt, um in den Besitz von sicherheitstechnisch relevanten Informationen (z.B. Benutzerkennungen und Paßwörter) zu gelangen. Von Ausspähen (Blick über die Schulter) oder Erfragen von Paßwörtern bis hin zu modernen Köpenickiaden, wenn beispielsweise ein Angreifer als Servicetechniker getarnt Zugang zu den Rechnerräumen oder den Netzwerkverteilern erlangt, um dort einen Angriff vorzubereiten, sind vielerlei Formen dieser Methode denkbar.

Mit Ausnahme der Port-Scans, die lediglich dem Ausforschen fremder Systeme dienen, können alle weiteren Angriffsarten der Vertraulichkeit und Integrität von Daten schaden, nehmen Rechnerressourcen (z.B. Rechenzeit, Plattenplatz) in Anspruch oder blockieren Kommunikationsverbindungen und/oder die daran angeschlossenen IT-Systeme.

5. Sicherheitskonzept

Auf der Grundlage der Risikoanalyse und der Ermittlung des Schutzbedarfs gilt es, Richtlinien für die Sicherheit festzulegen (sogenannte security-policy[8]). In bezug auf die Konzeption einer Firewall empfehlen wir, sich dabei an folgenden grundlegenden Sicherheitsprinzipien zu orientieren:

– **Prinzip der minimalen Zugriffsrechte**

  Das grundlegenste Sicherheitsprinzip in der IT ist das Prinzip der minimalen Zugriffsrechte. Dieses Prinzip besagt, daß jeder Administrator oder Benutzer nur die Rechte erhält, die für die Erledigung der jeweils zugewiesenen Aufgaben benötigt werden. Unabhängig davon, wie man aus Sicht moderner Mitarbeiterführung oder aus einer liberalen Grundhaltung heraus darüber denkt, verkleinert das Prinzip der minimalen Zugriffsrechte die Angriffsfläche und verringert den Schaden, der bei eventuell auftretenden Angriffen entsteht. In gleicher Weise gilt dieser Grundsatz auch für die auf einem IT-System ablaufenden Programme oder Dienste. Auch hier sollte - soweit dies technisch realisierbar ist - darauf geachtet werden, daß diese möglichst mit eingeschränkten Rechten ausgeführt werden. In diesem Zu-

[8] vgl. Begriffsdefinition im Anhang

sammenhang verweisen wir auch auf das datenschutzrechtliche Erforderlichkeitsprinzip (vgl. Art. 16 Abs. 1 und Art. 17 Abs. 1 BayDSG), das ebenfalls eine entsprechende Beschränkung der Zugriffsrechte erfordert.

– **Mehrschichtige und vielfältige Verteidigung**

Bei Sicherheitsmaßnahmen gilt generell, daß man sich nicht nur auf einen einzigen Schutzmechanismus verlassen sollte, auch wenn er nach der Produktbeschreibung oder nach Aussagen von Fachleuten besonders stark und unüberwindbar erscheint. Es empfiehlt sich daher, grundsätzlich mehrere Mechanismen einzusetzen, die sich entweder gegenseitig sichern oder verhindern, daß bei der Durchdringung einer Sicherheitskomponente (z.B. Paketfilter) die dahinter liegende IT-Infrastruktur vollständig offenliegt. Dazu gehören unter anderem zusätzliche Paketfilter unterschiedlicher Hersteller, die Bildung überwachter Teilnetze und/oder eine Segmentierung des Netzwerks sowie der Einsatz eines Intrusion Detection Systems (IDS), um auffällige Aktivitäten schneller zu erkennen. Diese aus Sicherheitsgründen grundsätzlich wünschenswerte technische Vielfalt findet aber ihre Grenzen in einer einfachen und vom zeitlichen Aufwand her vertretbaren Administration sowie in den finanziellen Rahmenbedingungen. Einen wesentlichen Beitrag zur Sicherheit von IT-Systemen liefern daneben organisatorische Maßnahmen (z.B. Aufklärung der Benutzer über mögliche Risiken, sorgfältige Systemadministration, Auswertung von Systemprotokollen,[9] Beobachtung von Virenwarnlisten im Internet und das Lesen von Veröffentlichungen über bekannt gewordene Sicherheitslücken).

– **Eine Passierstelle**

Ein wichtiger Punkt beim Aufbau einer Verteidigungsstrategie ist die Kontrolle über den jeweiligen (Internet-)Zugang. Um es mit einem Bild aus der Literatur auszudrücken: „Durch diese hohle Gasse muß er kommen." Dies läßt sich aber grundsätzlich nur dann realisieren, wenn das lokale Netz nur **einen Übergang** in das Internet besitzt und weitere Zugänge strikt untersagt sind. Besonders gilt dies auch für alle Fernwartungs- oder Wählverbindungen, die wir im Rahmen der überörtlichen Prüfung immer wieder neben den Hauptübergängen angetroffen haben.

– **Einfachheit und Klarheit**

Sicherheitstechnische Systeme sollten grundsätzlich so einfach und überschaubar wie möglich aufgebaut und gut dokumentiert sein. Dies erfordert einerseits eine systematische Vorgehensweise bei der Planung und Installation von Firewalls. Andererseits sollten keine Produkte eingesetzt werden, deren Komplexität die Systemadministratoren nicht mehr überblicken können oder die in diesem Umfang nicht für die Lösung der sicherheitstechnischen Aufgabe nötigt sind. Wir verkennen nicht, daß der Aufbau wirksamer und sicherer Internet-Firewallsysteme ein sehr komplexes Thema ist und daß der Wunsch nach Einfachheit dabei oftmals nur schwer zu erfüllen ist. Gleichwohl sollten die zuständigen Systemadministratoren - ebenso wie sachverständige Dritte - die Firewall noch überblicken und auf ihre Wirksamkeit hin überprüfen können. Ebenso sollten Systeme vermieden werden, auf denen gleichzeitig eine Vielzahl von Diensten laufen und die daher die sicherheitstechnischen Maßnahmen unnötig komplizieren.

[9] zur datenschutzrechtlichen Zulässigkeit vgl. [DS2000]

– **Fortschreibung und Pflege**

Wegen der immer noch rasanten Entwicklung der eingesetzten Hard- und Software, neuer Kommunikationsanforderungen (z.B. im Rahmen von eGovernment) und des damit einhergehenden Einsatzes neuer Entwicklungswerkzeuge, Protokolle, Dienste und Anwendungsverfahren wandeln sich auch die Anforderungen an die IT-Sicherheitssysteme. Generell gilt: Neue Technik verursacht neue Probleme. Aus diesem Grund sind das IT-Sicherheitskonzept und die daraus resultierenden Maßnahmen als laufender Prozeß anzusehen, der eigentlich nie abgeschlossen sein wird, solange die technische Entwicklung anhält[10]. Dies bedeutet für die Verantwortlichen nicht nur, daß sie mit der technischen Entwicklung Schritt halten und die Risiken und Schwachstellen der neuen Technologien kennen und bewerten müssen, sondern erfordert auch eine ständige Anpassung der technischen und organisatorischen Sicherheitsmaßnahmen an die aktuellen Bedürfnisse.

6. Was ist eine Firewall?

Das englische Wort „Firewall“ läßt sich mit „Brandschutzmauer“ übersetzen. Dieser aus dem Hochbau stammende Begriff beschreibt die Funktionsweise einer Firewall[11] aber nur unzureichend. Im Gegensatz zur Brandschutzmauer hat eine Firewall nicht nur eine abweisende, sondern auch eine durchlassende Funktion. Um überhaupt die Dienste des Internets nutzen zu können, werden auf einer Firewall zahlreiche „Löcher“ benötigt, durch die der Datenverkehr fließt. Insoweit ist eine Firewall eher mit einem zentralen Zugangskontrollsystem eines Unternehmens vergleichbar. Auch hier achten ein oder mehrere Sicherheitsangestellte/Pförtner darauf, wer das Unternehmen betritt oder verläßt oder welchen Ansprechpartner der Besucher im Gebäude erreichen will. Gegebenenfalls werden Passanten oder deren Gepäck nach bestimmten (sicherheitsrelevanten) Kriterien durchsucht bzw. das Gepäck vom Pförtner selbst entgegengenommen, um es dann stellvertretend für den Absender an den Empfänger weiterzuleiten. Etwas abstrakter ausgedrückt, ist eine Firewall daher ein Konzept und zugleich eine technische Infrastruktur für die Verbindung zwischen einem öffentlichen und einem nichtöffentlichen Netz. Eine Firewall kann nur aus einem einzelnen Gerät oder aus mehreren Servern, Überwachungsroutern und anderen Komponenten bestehen.[12] Wir werden darauf noch ausführlicher bei den Firewallarchitekturen zu sprechen kommen. Im Grunde genommen besteht eine Firewall im wesentlichen aus der geschickten Kombination mehr oder weniger intelligenter Paketfilter[13] und Proxies[14], die mit Virenscannern[15] oder anderen Schutzprogrammen (z.B. Filter-[16], Verschlüsselungs- oder Authentifizierungsprogrammen) ergänzt werden.

---

[10] Bill Gates hat anläßlich der 20-Jahr-Feier von Microsoft Deutschland im letzten Jahr bereits die nächste digitale Dekade eingeläutet.

[11] vgl. Begriffsdefinition DFN im Anhang

[12] vgl. [Barth2001]

[13] vgl. Kapitel 9.1 Paketfilter

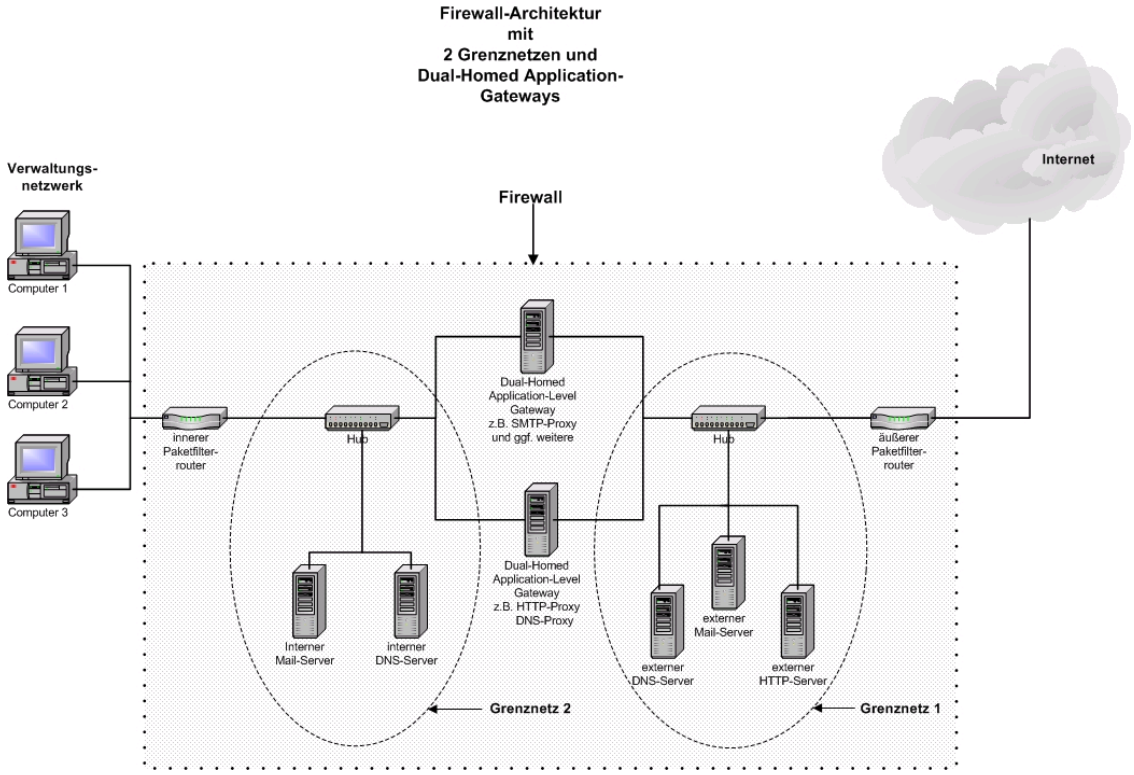
[14] vgl. Kapitel 9.2 Proxy-Systeme

[15] Virenscanner - vgl. Begriffsdefinition im Anhang

[16] z.B. URL-, Java-Script- oder ActiveX-Filter

7. Firewallarchitekturen

Wie wir bereits bei der Definition des Begriffs „Firewall“ festgestellt haben, unterscheiden sich die Firewallarchitekturen doch erheblich und können von einer Single-Box-Architektur bis hin zu Multi-Box-Architekturen mit verschiedenen Paketfilter- und Proxy-Systemen und mehreren überwachten Teilnetzen[17] reichen. Im IT-GSHB (M 2.73) sind einige dieser Firewallarchitekturen kurz schematisch dargestellt, weshalb wir an dieser Stelle darauf verweisen dürfen. Eine ausführlichere Darstellung der einzelnen Architekturen mit einer sehr detaillierten Darstellung der jeweiligen Vor- und Nachteile ist in dem Buch „Einrichten von Internet Firewalls“[18] enthalten. Die vom BSI empfohlene Architektur mit zwei überwachten Teilnetzen und einem oder mehreren Dual-homed Bastion-Hosts wollen wir nachfolgend etwas näher beleuchten, da sie alle wesentlichen Bestandteile einer wirksamen Sicherung enthält:



Bei Angriffen aus dem Internet sind naturgemäß die Maschinen am gefährdetsten, die direkt über das Internet erreichbar sind (öffentliche Adressen) und/oder Internet-Dienste anbieten oder nutzen. Es liegt also nahe, diese Maschinen in einen abgesicherten Bereich (abgesichertes Teilnetz oder Grenznetz) zu stellen, diesen besonders zu schützen und die Verbindungen am Übergang zum lokalen Netz zu trennen. Was sind nun die Vorteile einer solchen Architektur?

– Der äußere Überwachungsrouter schützt den Bastion-Host mit seinen Filterregeln und kann den Verkehr und die nutzbaren Dienste bereits erheblich einschränken. Eingehende Verbindungen lassen sich damit auf einzelne wenige Dienste (z.B. E-Mail) begrenzen.

[17] sogenanntes Grenznetz, wird gelegentlich auch als sogenannte Demilitarisierte Zone (DMZ) bezeichnet

[18] [ZCC2002]

– Zwischen dem äußeren Router und der nach außen gerichteten Netzwerkkarte des Bastion-Hosts wird ein Grenznetz gebildet, das am Bastion-Host endet. Damit wird die Struktur des zweiten (inneren) Grenznetzes und des lokalen Netzes vollständig verborgen. Maschinen, die von außen erreichbar sein müssen, wenn sie Internet-Dienste anbieten sollen (z.B. sogenannte externe Mail-, DNS- und HTTP-Server), gehören deshalb in dieses Grenznetz.

– Der Bastion-Host wickelt stellvertretend für alle im lokalen Netz befindlichen Maschinen den Internetverkehr über entsprechende Proxy-Server ab und kann darüber hinaus mit besonders wenigen Diensten sehr robust konfiguriert werden, so daß er besonders schwer angreifbar ist (sogenannte Härten).

– Zwischen der nach innen gerichteten Netzwerkkarte des Bastion-Hosts und dem inneren Router wird ein weiteres Grenznetz geschaffen, das ein weiteres Hindernis zwischen dem Angreifer und den internen Maschinen bildet, da die Struktur des lokalen Netzes auch bei einem erfolgreichen Angriff auf den Bastion-Host immer noch nicht sichtbar wäre.

– Der innere Überwachungsrouter[19] schützt das lokale Netz mit eigenen (strengeren) Filterregeln, beschränkt die zugelassenen Dienste und läßt nur Verkehr zwischen dem Bastion-Host und dem lokalen Netz zu. Der interne Verkehr im lokalen Netz wäre für einen Angreifer selbst dann nicht sichtbar, wenn er den externen Überwachungsrouter überwunden hätte und in den Bastion-Host eingebrochen wäre.

Soweit wir dies überblicken können, werden im kommunalen Bereich überwiegend Single-Box-Architekturen eingesetzt. Diese vereinen gewissermaßen die Funktionalität der Multi-Box-Architekturen in einem Gerät, da sie intern meist wie Multi-Box-Lösungen aufgebaut sind. Aus unserer Sicht ergeben sich folgende Vor- und Nachteile gegenüber Multi-Box-Lösungen:

Vorteile:

– Single-Box-Lösungen zeichnen sich in der Regel durch eine einheitliche, leicht bedienbare und verständliche Oberfläche aus, mit der sich Filter- und Access-Regeln effizienter und übersichtlicher einstellen lassen.

– Da nur ein Gerät benötigt wird, sind die Hardwarekosten bei Single-Box-Lösungen meist niedriger.

– Von den Administratoren ist nur ein Gerät zu betreuen und zu überwachen.

– Neben ausgeklügelten Paketfiltersystemen können die Single-Box-Lösungen bereits wichtige und ausgereifte Proxy-Server enthalten.

– Das sogenannte Härten des Sicherheitssystems wird bei der Installation einiger Lösungen automatisch erledigt.

Nachteile:

– Zwischen äußerem und innerem Netz befindet sich nur eine Maschine. Wenn diese überwunden wird, hat ein Angreifer vollen Zugriff auf die interne Netzstruktur.

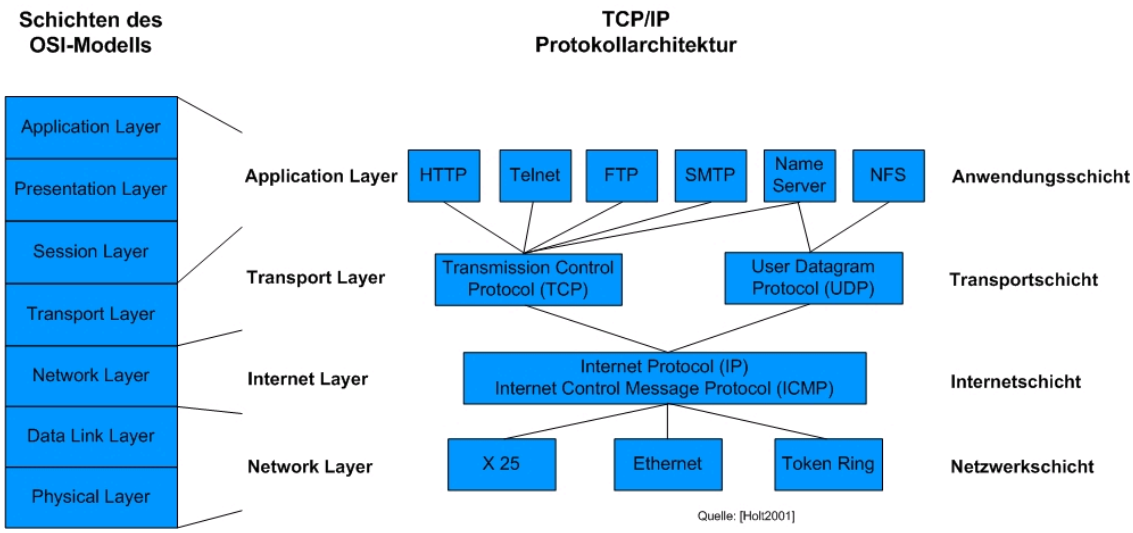
[19] manchmal als Choke-Router bezeichnet

– Die Konfiguration einer Single-Box-Lösung wird zwar durch die einheitliche Oberfläche erleichtert, teilweise werden dadurch aber auch die eigentlichen Probleme und kritischen Punkte verdeckt.

Insgesamt überwiegen aus unserer Sicht jedoch die Vorteile der Single-Box-Lösungen, zumal vielfach weder das entsprechende Wissen noch die Zeit zur Verfügung stehen, um gleichwertige Multi-Box-Lösungen aufzubauen. Allerdings wäre die zweckmäßigste und wirtschaftlichste Lösung jeweils unter Berücksichtigung der örtlichen Gegebenheiten und Sicherheitsanforderungen zu ermitteln.

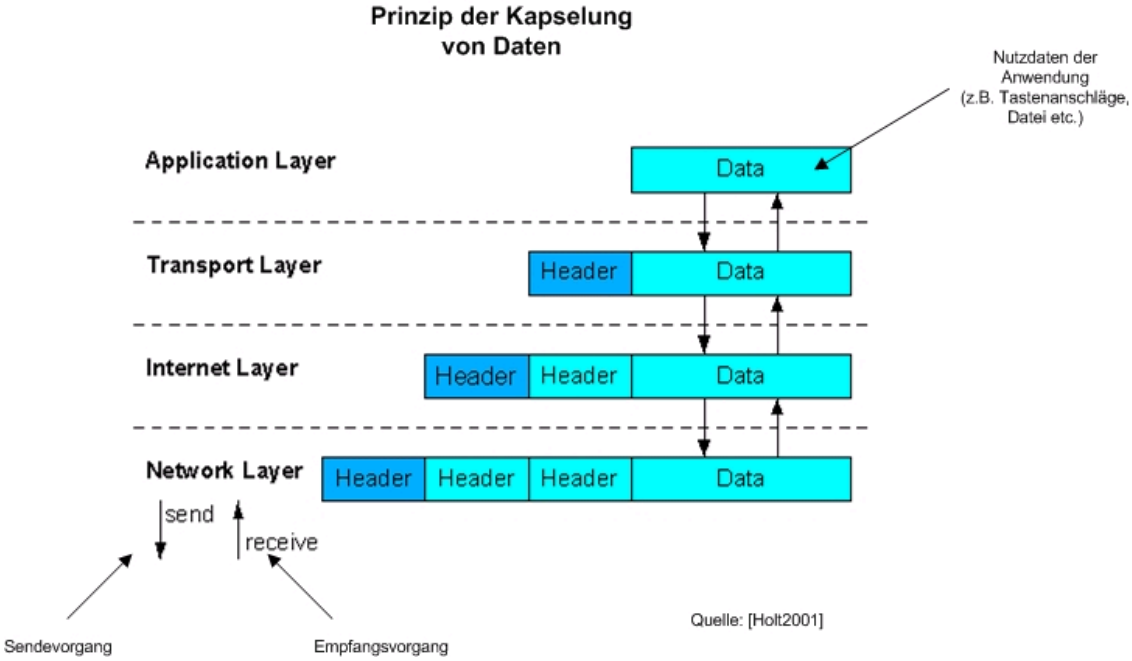
8. Protokolle und deren Pakete

Um die Vor- und Nachteile der Komponenten einer Firewall zu verstehen, müssen wir an dieser Stelle etwas näher auf das eingehen, womit Firewalls arbeiten: Protokolle und deren Pakete. Damit Informationen effizient über ein Netzwerk übertragen werden können, werden sie in kleine Teile zerlegt, die einzeln und abwechselnd gesendet werden. In IP-Netzwerken nennt man diese Teile Pakete. Da das Internet ein Netzwerk von TCP/IP-Netzen ist, wollen wir kurz den Aufbau der TCP/IP-Protokoll-Architektur in bezug auf die einzelnen Netzwerkschichten darstellen:



Für das Verständnis der weiteren Ausführungen genügt es zu wissen, daß in jeder dieser Schichten (Layer) ein Paket grundsätzlich aus zwei Teilen besteht, den relevanten Informationen für die Weiterleitung (Header) und dem Datenbereich (Data). Beim Sendevorgang behandelt jede Schicht die Informationen, die sie aus der darüberliegenden Schicht erhält, als Daten und stellt diesen Daten (Data) wiederum ihren eigenen Header voran. Dieser Vorgang wird Kapselung genannt (ähnlich wie die Häute einer Zwiebel, die darunter liegende Schichten umhüllen). Das so gebildete Gesamtpaket wird als Datagramm bezeichnet und auf der Netzwerkschicht weitergeleitet. Am anderen Ende einer Verbindung wird dieser Vorgang umgekehrt. Beim Weiterreichen der Daten von einer Schicht an die nächsthöhere Schicht wird jeder

Header (jedes Zwiebelhäutchen) von seiner entsprechenden Schicht wieder entfernt. Die nachfolgende Darstellung soll diese Abläufe verdeutlichen:



9. Firewallkomponenten

9.1 Paketfilter

Bei der Paketfilterung wird in der Regel auf den OSI-Schichten[20] drei und vier der TCP/IP-Protokollfamilie überprüft, welche Pakete an ein externes Netz oder aus einem externen Netz an die angegebene interne Zieladresse weitergereicht werden dürfen. Paketfilter stehen entweder auf Routern[21] zur Verfügung (zumeist als reine Hardwarelösungen) oder sind als reine Softwarelösungen erhältlich. Eigentlich ist die grundlegende Routing-Funktionalität schon in den meisten PC-Betriebssystemen enthalten. Während dedizierte Router ohne Paketfilter nur die optimale Verbindung für die Weiterleitung eines Pakets anhand ihrer Routing-Tabellen ermitteln, prüfen Router mit Paketfilter (gelegentlich auch als Filter- oder Überwachungsrouter bezeichnet) anhand interner Regeln, ob das Paket an das Zielsystem weitergeleitet werden darf oder nicht. Die Paketfilterung wird meistens auf sogenannten Überwachungsroutern eingesetzt, kann aber auch auf den Bastion-Hosts und dedizierten Firewallsystemen (Single-Box-Lösungen[22]) stattfinden. Die Anforderungen an einen geeigneten Paketfilter für eine Firewall hat das BSI im IT-GSHB (M 2.74) ausführlich dargestellt, weshalb wir hier nicht näher darauf eingehen wollen.

---

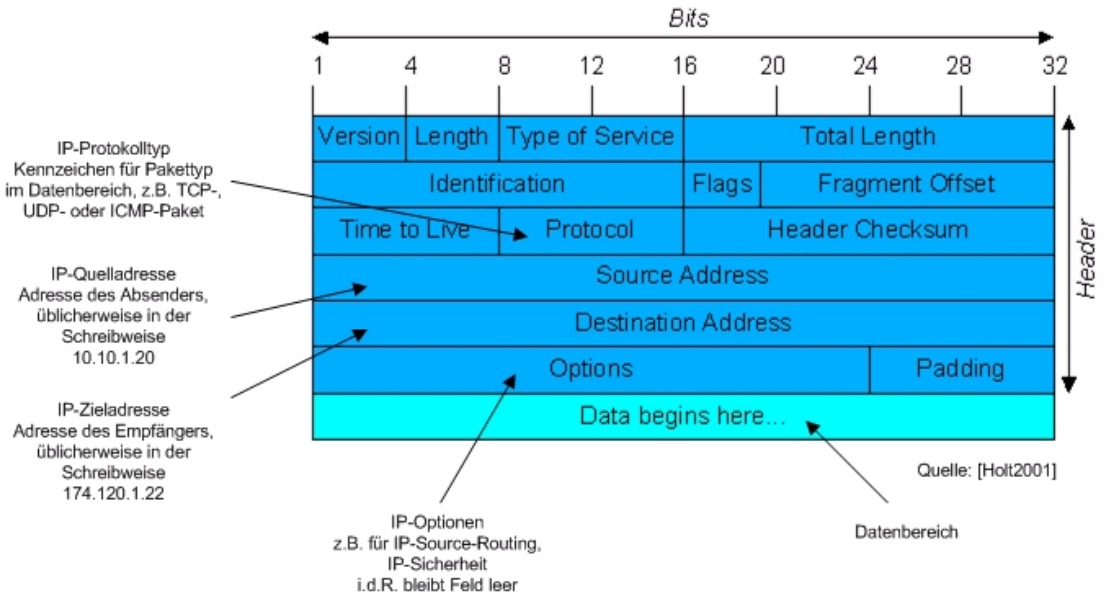
[20] Die Zusammenhänge zwischen dem OSI-Schichtenmodell, TCP/IP und anderen Protokollen sind in der Anlage dargestellt.

[21] Geräte, die IP-Netze miteinander verbinden, werden Router genannt.

[22] Gelegentlich werden diese auch als Firewall-Appliance bezeichnet.

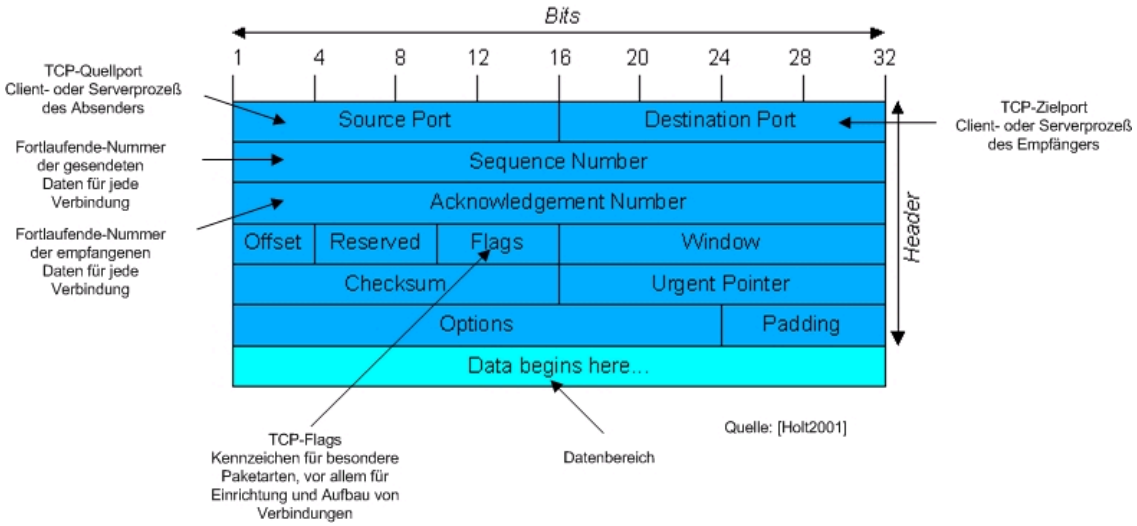
Für die Paketfilterung sind vor allem die Header der Protokolle auf der Internet- und Transportschicht von Bedeutung, die (auf Basis der am weitesten verbreiteten Protokolle IP, TCP und UDP erläutert) folgende interessante Informationen enthalten:

Internet Protocol (IP)
(Header)



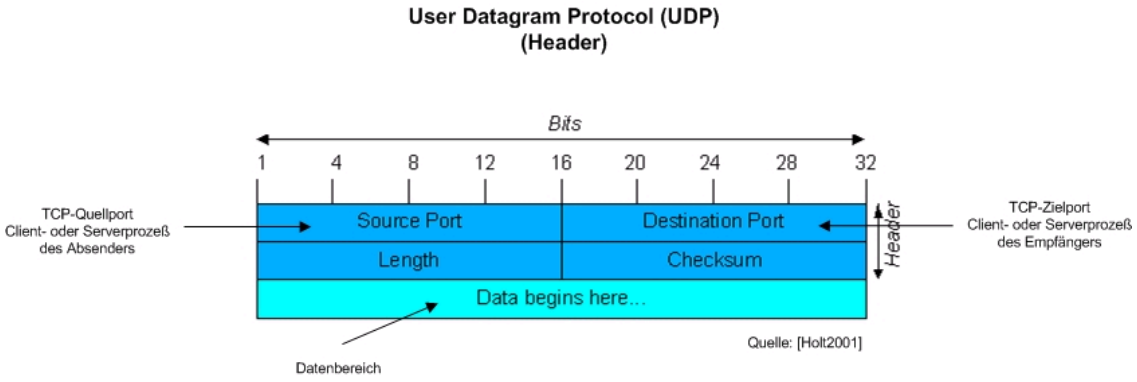
Das verbindungsorientierte[23] TCP-Protokoll trägt im sogenannten Header folgende Informationen:

Transmission Control Protocol (TCP)
(Header)



[23] vergleichbar dem Telefonieren

Das verbindungslose[24] UDP-Protokoll ist dagegen im Header auf sehr viel weniger Informationen beschränkt:



Vorteile der Paketfilterung:

- Da Router ohnehin die Paket-Header vor der Weiterleitung prüfen, ist dies eine strategisch günstige Stelle, um auch weitergehende Kontrollen (Prüfungen auf Grundlage der Ziel- und Quelladresse, Auswertung der verwendeten Sitzungs- und Anwendungsports) durchzuführen.

- Paketfilter sind sehr leistungsfähig.

- Die Paketfilterung kann mit relativ wenig Aufwand betrieben werden, zumal kommerzielle Router in der Regel bereits über eingebaute Filtersysteme verfügen.

- Die Kontrolle ein- und ausgehender TCP-Verbindungen ist auf Grundlage des Drei-Wege-Initialisierungsprozesses (three-way-handshake) sehr effizient und sicher möglich. Damit können unter anderem bestimmte Arten von Port-Scans und DoS-Attacken verhindert werden.

- Mit Hilfe dynamischer (zustandsgesteuerter) Paketfilter[25] können nicht nur laufende Verbindungen überwacht, sondern auch in Abhängigkeit von bestimmten Protokolleigenschaften neue Filterregeln generiert und Ports temporär geöffnet bzw. nach Verbindungsende wieder geschlossen werden. UDP-Pakete können ohnehin nur auf Basis der dynamischen Paketfilterung einer bestehenden UDP-Verbindung zugeordnet werden. Manche dynamischen Paketfilter erlauben, wenn auch in beschränktem Umfang, neben der Überwachung des Zustands einer Verbindung auch eine Prüfung der Paketdaten auf der Ebene einiger Kommunikationsprotokolle der Anwendungsschicht.

- Paketfilter bieten sich als Sicherheitsmechanismen für Protokolle der Anwendungsschicht an, bei denen keine dedizierten Proxies verfügbar sind, die lediglich mit einem generischen Proxy[26] arbeiten oder die überhaupt nicht proxyfähig sind.

---

[24] vergleichbar dem Versenden eines herkömmlichen Briefes

[25] häufig auch als „stateful-inspection“ bezeichnet, vgl. Begriffserläuterungen

[26] Die beiden Begriffe dedizierter Proxy und generischer Proxy werden im Kapitel 9.2 erläutert.

Nachteile der Paketfilterung:

– Paketfilter sind oft schwer zu konfigurieren, da die Filterregeln sehr schnell unübersichtlich und daher komplex werden.

– Paketfilterregeln lassen sich nur aufwendig testen.

– Die Paketfiltereigenschaften mancher Produkte sind eingeschränkt und erlauben daher nicht alle Arten von Filterregeln.

– Fehler in der Konfiguration oder Implementierung von Paketfiltern führen eher zu Sicherheitsproblemen als Fehler in Proxy-Systemen.

– Paketfilter verbergen keine Strukturen des zu schützenden Netzwerks und trennen dies nicht vom unsicheren Netz.

9.2 Proxy-Systeme

Proxies (Stellvertreter) sind in der Regel besonders geschützte Rechner (z.B. Dual-Homed Bastion-Host), über die alle Verbindungen zwischen dem lokalen Netzwerk und dem Internet geleitet werden. Im Gegensatz zu Paketfiltern trennen sie jedoch die Verbindungen am Übergang zwischen den Netzen und agieren anstelle des jeweiligen Clients. Diese Technik wird einerseits dazu benutzt, um die Leistungsfähigkeit eines Internet-Zugangs zu verbessern (sogenannte Cache-Proxies), andererseits werden damit vor allem der Verbindungsaufbau und der ein- und ausgehende Datenverkehr auf Ebene der Protokolle der Anwendungsschicht kontrolliert (sogenannte Filter-Proxies). Proxies arbeiten damit auf der siebten OSI-Schicht. Das folgende Beispiel soll anhand einer WEB-Abfrage ihre Funktionsweise verdeutlichen:

Der Client eines Benutzers (z.B. Internet-Explorer) wendet sich an den HTTP-Proxy-Server des Standorts und nicht direkt an den echten HTTP-Server im Internet. Der Proxy-Server bewertet die Anfragen des Clients und entscheidet sich dann, ob er diese weiterreicht oder verwirft. Wird die Anfrage zugelassen, leitet der Proxy-Server diese an den echten HTTP-Server weiter und nimmt auch dessen Antworten entgegen. Handelt es sich um gültige Antworten, leitet der Proxy-Server diese zum Client zurück. Für den Benutzer scheint es so, als ob er direkt mit dem echten HTTP-Server im Internet kommunizieren würde, obwohl in Wahrheit der Proxy-Server stellvertretend für den Client diese Aufgaben wahrgenommen hat.

Obwohl diese Funktionsweise allen Proxy-Servern zugrunde liegt, unterscheiden sie sich hinsichtlich ihrer Leistungsfähigkeit doch sehr stark und bieten deshalb unterschiedlich starken Schutz vor Angreifern.

Ein **dedizierter Proxy-Server** bedient nur ein einziges Protokoll der Anwendungsschicht und kennt dessen Befehle genau. Ein solcher Proxy-Server wird in der Praxis auch als **Application-Level-Proxy** oder **Application-Level-Gateway (ALG)** bezeichnet. Da dedizierte Proxies die protokollspezifischen Eigenheiten kennen, bieten sie weit mehr Funktionalitäten als einfache Paketfilter. Neben der Steuerung der Verbindungen anhand der Quell- und Zieladresse sowie des Ports erlauben sie in zunehmendem Maße eine Kontrolle der mit dem Protokoll übermittelten Inhalte. Es kann mit ihnen festgestellt werden, ob die übertragenen Befehle sicher sind oder überhaupt dem jeweiligen Protokoll entsprechen. Dies ist insbesondere deshalb wichtig, weil zwischenzeitlich bestimmte Protokolle und deren Ports von mehreren unterschied

lichen Anwendungen benutzt werden. Zum Teil wird durch eine solche Kapselung von Informationen in bekannten Diensten auch versucht, die Regeln und Einschränkungen einer Firewall zu umgehen oder einfach deren Neukonfiguration zu vermeiden. Daneben bieten dedizierte Proxies bessere Protokollmöglichkeiten an, als mit anderen Mitteln erreicht werden kann.

Generische Proxy-Server bedienen dagegen mehrere Protokolle der Anwendungsschicht, ohne das Anwendungsprotokoll selbst zu kennen und zu interpretieren. Man nennt sie in der Praxis auch **Circuit-Level-Proxies**. Sie bieten gegenüber dem reinen Paketfilter nur eine höhere Sicherheit in bezug auf Fehler in Paket-Headern und bei der Fragmentierung von Paketen. Ansonsten sind sie ebenfalls auf die Kontrolle der jeweiligen Verbindung anhand der Quell- und Zieladresse sowie des verwendeten Ports beschränkt. Nachteilig ist jedoch, daß nicht alle Protokolle problemlos durch einen generischen Proxy verarbeitet werden können, insbesondere dann, wenn Portinformationen zwischen Client und echtem Server ausgetauscht werden müssen.

Die Vorteile der Filter-Proxies sind:

- Der Proxy-Server ist der einzige Rechner, der eine gültige, im Internet sichtbare IP-Adresse benötigt.

- Es besteht keine direkte Verbindung zwischen dem internen Client und dem Internet. Die Strukturen des inneren Netzwerks (z.B. Domain-Namen, IP-Adressen, Rechnername) werden komplett verborgen.

- Ein dedizierter Proxy-Server kennt die zugelassenen Befehle des jeweiligen Protokolls und läßt deshalb nur gültige Anfragen auf dem jeweiligen Port durch oder ermöglicht deren Filterung.

- Protokollierung und Kontrolle der Zugriffe sind auf einer höheren Ebene möglich und deshalb wesentlich leistungsfähiger und variabler als auf der Ebene der niedrigeren Protokolle (IP, TCP, UDP), bei denen die auswertbaren Informationen einfach durch den Aufbau des Headers begrenzt sind.

Die Nachteile der Filter-Proxies sind:

- Der Betrieb von Filter-Proxies erfordert auf Clientseite eine Proxy-taugliche Anwendungs- oder Betriebssystemsoftware oder einen entsprechenden Router, der Pakete automatisch abfängt und zum entsprechenden Proxy-Server umleitet.

- Dedizierte Proxy-Server stehen in der Praxis nur für die wichtigsten Dienste (z.B. Telnet, FTP, SMTP, DNS, NNTP, HTTP) zur Verfügung. Alle anderen Dienste müssen - sofern dies aufgrund der Protokolleigenschaften möglich ist - entweder über generische Proxies oder Paketfilter abgewickelt werden.

- Proxies haben gegenüber Paketfiltern eine geringere Geschwindigkeit beim Datendurchsatz.

9.3 Network-Address-Translation (NAT)

Dieser Begriff beschreibt grundsätzlich die Manipulation von IP-Source- und IP-Destination-Adresse im IP-Header. Damit ist es möglich, eine bestimmte Gruppe von Netzwerk-Adressen für den internen Gebrauch und eine oder mehrere Netzwerk-Adressen für die Anbindung an externe Netzwerke zu verwenden. Manchmal wird unter dem Begriff „NAT“ auch die Änderung des Port-Eintrags subsumiert, obwohl hier eigentlich präziser von einer Port-Address-Translation (PAT) gesprochen werden müßte. In der Praxis ist in modernen Firewallsystemen meist beides möglich. Die Funktionsweise von NAT[27] läßt sich kurz wie folgt beschreiben:

Wenn ein Client ein Paket an einen Server im externen Netzwerk schickt, modifiziert das NAT-System die Quelladresse so, daß es aussieht, als käme es von einem ganz anderen Client (NAT-Address-Pool). Antwortet nun der externe Server, wird die von diesem verwendete Destination-IP-Adresse vom NAT-System wieder in die tatsächliche IP-Adresse des Clients umgewandelt, so daß der Absender dann tatsächlich auch die Antwort erhält. Voraussetzung hierfür ist jedoch, daß das NAT-System das empfangene Paket der vom Client initiierten Verbindung zuordnen kann. Die Port-Umsetzung funktioniert in gleicher Weise.

Allerdings weisen wir darauf hin, daß bei einem sauber aufgebauten Netzwerk und einer Firewallarchitektur, wie wir sie in Ziffer 7 beschrieben haben, NAT wohl nicht mehr nötig ist und auch keinen zusätzlichen Sicherheitsgewinn brächte.

Die Vorteile von NAT sind:

- NAT unterstützt die Firewall bei der Kontrolle einer nach außen gerichteten Verbindung.

- Ein NAT-System, das Adressen dynamisch anpaßt, erlaubt nur solche Pakete, die zur aktuellen, von der Innenseite initiierten Verbindung gehören. Insoweit ist damit ein weiterer (kleiner) Sicherheitsgewinn verbunden, da der betreffende Client nur für die Dauer der Verbindung direkt erreichbar ist.

- Da NAT die internen Netzwerkstrukturen verbirgt, erschwert dies einem potentiellen Angreifer die Netzwerkanalyse.

Die Nachteile von NAT sind:

- Die dynamische Adreßanpassung erfordert Zustandsinformationen, die nur bei verbindungsorientierten Protokollen (z.B. TCP) zuverlässig vorliegen. Bei UDP-Paketen können Probleme auftreten.

- Die im Datenteil eines Pakets eingebetteten IP-Adressen kann NAT nicht bei allen Protokollen umsetzen.

- NAT funktioniert nicht mit Protokollen, die eingebettete IP-Adressen mit dem Schutz der Datenintegrität kombinieren (z.B. IPSec).

- Die dynamische Anpassung von IP-Adressen oder Ports kann, abhängig davon, an welcher Stelle sie vorgenommen wird, die Protokollierung des Datenverkehrs verfälschen und die Paketfilterung beeinträchtigen.

[27] In der Linux-Welt wird anstelle von NAT meistens der Begriff „IP-Masquerading“ verwendet.

10. Lösungen

a) Auswahlkriterien für Firewallsysteme

Gute Firewallsysteme gibt es zwar nicht wie Sand am Meer, dennoch sind zwischenzeitlich einige sehr leistungsfähige Lösungen verfügbar, die anhand

- des örtlichen Schutzbedarfs,
- der von den genutzten Internet-Diensten ausgehenden Risiken und
- des Preis-/Leistungs-Verhältnisses

ausgewählt werden müssen.

Bei mittlerem bis hohem Schutzbedarf empfehlen wir grundsätzlich eine Lösung einzusetzen, die die Anforderungen des IT-GSHB an eine sichere Firewall (vgl. M 2.72, M 2.74, M 2.75) erfüllt. Bei reinen Paketfiltersystemen sollte mindestens eine dynamische Paketfilterung (statefulinspection) möglich sein. Aufgrund der höheren Schutzwirkung sind dedizierte Filter-Proxies gegenüber der reinen Paketfilterung vorzuziehen. Sind nur generische Proxies für den jeweiligen Dienst verfügbar, empfiehlt sich eine Kombination von Paketfilter und Proxy. Grundsätzlich gilt: Je weiter oben die Firewall technisch im Schichtenmodell angesiedelt ist und je detaillierter protokollspezifische Inhalte kontrolliert werden können, desto höher ist ihre Schutzwirkung. In der Praxis gibt es häufig keine Standardlösung, da die Verhältnisse zu unterschiedlich sind. Mithin ist zu berücksichtigen, daß kleinere Schwächen einer bestimmten Lösung auch durch andere Schutzmaßnahmen (z.B. durch eine höhere Rechnersicherheit im Netz, Einsatz nachgeschalteter Filterproxies oder weiterer Überwachungsrouter, Verbindung über ein zusätzlich abgesichertes Netz[28]) ausgeglichen werden können.

Die Risiken, die von den jeweils genutzten Internet-Diensten ausgehen, sind unterschiedlich. Es gibt aus technischer Sicht sichere (z.B. SSH, SSL) und unsichere Dienste (z.B. ICQ, SMTP, SNMP, TELNET), wobei es aber im Einzelfall darauf ankommt, wie und in welcher Umgebung diese Dienste genutzt werden. So ist es durchaus möglich, unsichere Dienste auf gesicherte Weise zu benutzen (z.B. SMTP über eine VPN-Verbindung). Allerdings können auch mit einem sicheren Dienst unsichere Inhalte (z.B. Viren, Trojaner) übertragen werden. Insoweit ist keine pauschale Aussage über den jeweiligen Grad der Gefährdung, der durch die Benutzung eines bestimmten Internet-Dienstes entsteht, möglich. Dieser muß individuell für jeden verwendeten Dienst im Hinblick auf die örtlichen Sicherheitsanforderungen und -richtlinien (security-policy), die technische Konfiguration der IT-Systeme des Standorts und die Art und Weise der Verwendung eines Internet-Dienstes ermittelt werden. Für die sicherheitstechnische Bewertung von Diensten und Protokollen[29] gibt es in der Fachliteratur[30] und im Internet ausreichend Hinweise, die auch den halbwegs versierten Systembetreuer in die Lage versetzen, die jeweiligen Risiken zu beurteilen.

[28] beispielsweise über kommunale Behördennetze oder das BYBN

[29] zum Unterschied zwischen Diensten und Protokollen vgl. Begriffsdefinitionen

[30] vgl. Literaturhinweise im Anhang

b) Kommerzielle Lösung oder Eigenbau?

Die Frage, ob der Eigenbau einer Firewall gegebenenfalls wirtschaftlicher und zweckmäßiger ist, kann nicht von vornherein eindeutig beantwortet werden. Wie fast immer kommt es auf die näheren Umstände an:

– Ist der Eigenbau unter Berücksichtigung aller einmaligen und laufenden Kosten (der Kalkulationszeitraum sollte ca. fünf Jahre betragen) und des damit erzielbaren Nutzens die wirtschaftlichste Lösungsvariante?

– Wird mit dem Eigenbau eine ausreichende Sicherheit erreicht?

– Ist die laufende Wartung und Pflege der Firewall über die geplante Einsatzdauer sichergestellt?

– Kann die Administration der Firewall auch von einem Vertreter bewältigt werden?

Da diese Fragen oftmals nicht oder nur eingeschränkt mit „Ja“ beantwortet werden können, dürfte sich das Thema „Eigenbau“ aus unserer Sicht meistens von selbst erledigen.

Obwohl kommerzielle Systeme aufgrund ihrer durchdachten Oberflächen regelmäßig einfacher und effizienter zu administrieren sind als „selbstgestrickte“ Lösungen, geben wir zu bedenken, daß auch deren Konfiguration komplex ist und Spezialwissen erfordert, das nur bei einem größeren IT-Betrieb und mehreren Administratoren wirtschaftlich sinnvoll vorgehalten werden kann. Soweit das notwendige Fachwissen örtlich nicht vorhanden ist, empfehlen wir, die Planung, Implementierung und Pflege von Firewallsystemen an fachkundige und vertrauenswürdige Dritte mit entsprechender Erfahrung und Zuverlässigkeit zu vergeben. Im Gegensatz zu manch anderen Bereichen in der IT muß die Firewall von Anfang an richtig funktionieren; für „learning by doing“ oder Experimente ist in diesem kritischen Umfeld kein Platz.

c) Erfahrungen mit interkommunalen Lösungen

Erfolgversprechend und auch wirtschaftlich sinnvoll scheint uns in diesem Zusammenhang ein Ansatz zu sein, der sich auf Ebene der kreisangehörigen Kommunen bei Einbindung in die sogenannten Landkreis-Behördennetze abzeichnet. Die Zusammenfassung und gemeinsame Nutzung einer Sicherheits-Infrastruktur bietet aus unserer Sicht viele Vorteile, da Personal und Technik nur an einer zentralen Stelle vorgehalten werden müssen. Die interkommunale Zusammenarbeit in diesem Bereich können wir aus diesem Grund nur begrüßen. Im Hinblick auf Art. 3 des neuen IuK-Gesetzes vom 01.01.2001 und die von den kommunalen Spitzenverbänden mit der Bayerischen Staatskanzlei im Juni 2002 abgeschlossene eGovernment-Vereinbarung[31] dürfte sich diese Entwicklung wohl auch in Zukunft verstärken. Andererseits verkennen wir nicht, daß verschiedene Kommunen aus den örtlichen Gegebenheiten heraus (z.B. spezielle Anforderungen an Bandbreite und Dienste, historisch gewachsene Strukturen, spezielle Anwendungen) möglicherweise nach wie vor auf eigene Übergänge zum Internet angewiesen sind und diese dann auch selbst schützen müssen. Selbstverständlich ist auch bei letzteren immer im Hinblick auf den Grundsatz der sparsamen und wirtschaftlichen Haushaltsführung zu hinterfragen, ob nicht zwischenzeitlich andere Lösungen in Frage kommen.

[31] sogenanntes E-Government-Pakt

d) Wahl auf Grundlage des zugrundeliegenden Betriebssystems?

Eine gute Firewall ist aus unserer Sicht keine Frage des jeweiligen Betriebssystems. Es gibt hinreichend sichere und vom BSI geprüfte Firewallsysteme für UNIX- und Windows-Betriebssysteme. Im übrigen ist es gerade im Hinblick auf die Sicherheit der sogenannten Bastion-Hosts viel wichtiger, daß sich der zuständige Administrator mit der Bedienung und den sicherheitsrelevanten Einstellungen des jeweiligen Betriebssystems gut auskennt und weiß, wie er sicherheitskritische Dienste und Programme zuverlässig deaktiviert oder entfernt, als theoretische Überlegungen in bezug auf die Sicherheit von Betriebssystemen anzustellen.

11. Trends und Entwicklungen bei Firewallsystemen

a) Trends bei Firewalltechnologien

In der Vergangenheit war bei den Firewalltechnologien ein deutlicher Trend zum Einsatz von Proxy-Systemen, insbesondere der sogenannten Application-Level-Gateways, erkennbar. Dies liegt wohl darin begründet, daß die Anforderungen komplexer werden und die verfügbaren Lösungen bereits eine Vielzahl dedizierter Filterproxies und in der Regel einen leistungsfähigen generischen Proxy enthalten. Aber auch die Paketfiltersysteme der Überwachungsrouter oder kleinere Single-Box-Lösungen werden immer leistungsfähiger. Mit Hilfe von „stateful-inspection“ und anderer Überwachungsmodule, die bis hinauf zur siebten OSI-Schicht arbeiten, bieten sie schon sehr viele Schutzmechanismen. Es hängt letztlich von den genutzten Diensten, der technischen Infrastruktur, der Konfiguration der eingesetzten IT-Systeme und dem jeweiligen Schutzbedarf ab, welche Systeme als Firewall geeignet sind. Ein Paketfiltersystem mit stateful-inspection dürfte jedoch derzeit aus technischer Sicht der Mindeststandard sein.

b) Neue Anforderungen mit eGovernment

Neue Herausforderungen für die Administratoren und Firewallsysteme in den kommunalen Gebietskörperschaften werden mit den allerorts anzutreffenden eGovernment-Aktivitäten zu erwarten sein. Dies wird insbesondere dann gelten, wenn über die reine Informationsbereitstellung und den Download von Formularen hinaus interaktive Anwendungen für den Bürger oder die sogenannten Power-User (Anwälte, Notare, Detekteien, KFZ-Händler, um nur einige zu nennen) verfügbar sind. Neben den reinen Sicherheitsaspekten werden dann auch die Anforderungen an die Verfügbarkeit und Ausfallsicherheit der Systeme (7 mal 24 Std.) erheblich höher sein als bisher. Daneben werden die sichere Authentifizierung und die Weiterleitung verschlüsselter Daten durch die Firewallsysteme hindurch zuverlässig gelöst werden müssen. Um den Anforderungen der Zukunft gewachsen zu sein, empfehlen wir eine Orientierung an den aktuellen Veröffentlichungen des BSI[32] und der Datenschutzbeauftragten des Bundes und der Länder zum Thema eGovernment[33].

[32] E-Government Handbuch, www.bsi.de/fachthem/egov/3.htm

[33] vgl. [DS2001]

c) Intrusion Detection

Wie wir an anderer Stelle schon festgestellt haben, ist eine Firewall nur ein Element der IT-Sicherheit und bietet keinen umfassenden Schutz vor Angriffen, insbesondere dann, wenn sie nicht von außen, sondern von innen (z.B. durch böswillige Benutzer oder eingeschleuste Programme) gestartet werden. In letzter Zeit wurden deshalb vermehrt Forderungen laut, die Überwachungstätigkeit der Administratoren durch automatische Überwachungssysteme zu unterstützen oder zu ergänzen. Solche Systeme werden Intrusion Detection Systeme (IDS) genannt und reichen von einfachen, passiven Programmen, die Protokolldateien lesen und nach Unregelmäßigkeiten durchsuchen, bis zu extrem komplexen Systemen, die das Verhalten des Netzwerks und des Betriebssystems nach Anomalien und den Datenstrom nach bestimmten signifikanten Signaturen untersuchen. Von der Wirksamkeit und der Komplexität solcher Systeme einmal abgesehen, stellt sich die Frage nach dem Nutzen-/Kosten-Verhältnis dieser Produkte. Des weiteren muß entsprechend geschultes Personal zur Verfügung stehen, um den Betrieb eines IDS sicherzustellen und dessen Alarmmeldungen zu verstehen. Aus unserer Sicht dürfte derzeit ein IDS erst ab einer gewissen Größenordnung zweckmäßig sein und wirtschaftlich eingesetzt werden können. Allerdings haben wir selbst noch zu wenig Erfahrungen mit IDS, um uns hierzu ein abschließendes Urteil bilden zu können.

12. Betrieb und Wartung von Firewalls

Mit der Installation einer technisch ausgereiften und gut konfigurierten Firewall ist es keineswegs getan.

Eine Firewall ist, wie wir bereits bei der Definition festgestellt haben, kein statisches, sondern ein dynamisches System, das regelmäßig überprüft, gewartet und aktualisiert werden muß. Gerade die Auswertung der Log-Dateien auf sicherheitsrelevante Vorfälle (z.B. erfolglose Anmelde- oder Verbindungsversuche, eintreffende Pakete mit internen Quelladressen, wiederholte Port-Scans etc.) ist elementarer Bestandteil eines sicheren Firewallbetriebs und sollte nicht vernachlässigt werden.

Daneben sollten die Sicherheitseinstellungen und die Protokollierung sicherheitskritischer Ereignisse sowohl nach der Installation einer Firewall wie auch im laufenden Betrieb gelegentlich mit geeigneten Programmen auf ihre Wirksamkeit hin überprüft und die lückenlose Protokollierung solcher (bewußter) Angriffe kontrolliert werden. Die Log-Dateien sind, wie andere Unterlagen über den ordnungsgemäßen Systembetrieb, bis zum Ablauf der Aufbewahrungsfristen nach § 82 KommHV in digital auswertbarer Form aufzubewahren, da sonst die Ordnungsmäßigkeit des IT-Betriebs nicht festgestellt werden kann.

Sollen neue Internet-Dienste genutzt oder angeboten werden, sind zunächst die Risiken dieser Dienste zu untersuchen. Sofern der Dienst mit den Sicherheitsrichtlinien vereinbar ist, sind die Einstellungen der Firewall entsprechend anzupassen und deren Wirksamkeit bzw. auch etwaige Seiteneffekte auf bereits vorhandene Sicherheitsmechanismen zu überprüfen. Es kommt nicht selten vor, daß Firewalleinstellungen aufgrund nachträglicher Installationen von Softwarelösungen (oft kurzerhand) verändert und ohne nähere Prüfung so belassen werden, was zu (neuen) Sicherheitslücken führen kann. Zur Betreuung einer Firewall zählt darüber hinaus auch das Studium der einschlägigen Warnmeldungen (z.B. BSI, CERT, Hersteller) und das Einspielen von Updates oder Bugfixes.

Diese Tätigkeiten erfordern nahezu das gleiche Verständnis und technische Wissen wie die Planung und Implementierung von Firewallösungen, so daß auch hier die Frage zu stellen ist, ob diese Aufgaben nicht besser an einen vertrauenswürdigen Dritten übertragen werden sollen. Diese sicher nicht einfache Entscheidung hängt im wesentlichen von den verfügbaren Personalressourcen, den haushaltsrechtlichen Vorgaben und der datenschutzrechtlichen Zulässigkeit[34] der Datenverarbeitung im Auftrag (vgl. Art. 6 BayDSG) ab. Eine gewisse Kernkompetenz, die vor allem eine Kontrolle der Aufgabenerfüllung durch den Dritten gewährleistet, muß aber nach wie vor in der Verwaltung selbst vorgehalten werden.

13. Grenzen von Firewalls

Firewalls sind primär darauf ausgerichtet, ein (internes) Netz vor Angriffen aus den daran angeschlossenen (externen) Netzen zu schützen; in der Regel ist dies das Internet. Firewalls sind aber keine umfassende und vollständige Sicherheitslösung, zumal sich manche Gefahren mit Firewalls gar nicht kontrollieren lassen. Insoweit kommt dem physischen Schutz des Netzwerks und der Server, der Rechnersicherheit, dem Virenschutz auf den Clients und Servern sowie der Schulung der Benutzer eine besondere Bedeutung zu.

Firewalls schützen insbesondere nicht vor folgenden Gefahren:

- Angriffe von böswilligen und untreuen Mitarbeitern oder Hackern im eigenen Netzwerk (z.B. mittels Netzwerk-Sniffern, Paßwort-Crackern oder auf fremden Systemen installierten Tastaturscannern)

- schlecht konfigurierte oder schlecht abgesicherte Systeme (z.B. Standardinstallationen von Betriebssystemen ohne System- und Sicherheitsrichtlinien, Benutzer mit weitreichenden Berechtigungen, Verwendung von schwachen oder leicht erratbaren Paßwörtern, Verwendung von Standard- oder Installationspaßwörtern)

- Viren, Trojaner oder Würmer, wenn sie auf Datenträgern ins Netz eingeschleust werden. Den eingehenden Datenverkehr kann eine Firewall nur bis zu einem gewissen Grad auf diese Schädlinge hin überprüfen. Der von diesen Schädlingen ausgehende Datenverkehr nach außen kann, sofern er die in der Firewall zugelassenen IP-Adressen, Ports und Protokolle verwendet, von einer Firewall leider nicht kontrolliert werden.

- Verbindungen in externe Netze, die nicht über die Firewall laufen

- Dienste, die ihre Daten in zugelassenen Protokollen und Ports verstecken

Eine Firewall ist, wenn sie richtig geplant, konfiguriert und betrieben wird, gleichwohl ein wesentlicher Bestandteil der IT-Sicherheit; beim Anschluß eines lokalen Verwaltungsnetzes an ein unsicheres öffentliches Netz (z.B. Internet) ist sie unentbehrlich. Etwas drastischer ausgedrückt: Es kommt ja auch niemand auf die Idee, ein Rathaus ohne verschließbare Eingangstüren zu bauen.

[34] vgl. 20. Tätigkeitsbericht des BayDSB, Abschnitt 17.3.3, „Outsourcing von Kommunaldaten“

14. Anhang

Literaturverzeichnis

[ZCC2002] **Einrichten von Internet Firewalls**, Elizabeth D. Zwicky, Simon Cooper & D. Brent Chapman, O'REILLY-Verlag

[BSI-GSHB] **IT-Grundschutzhandbuch 2002, Standard-Sicherheitsmaßnahmen**, Bundesamt für Sicherheit in der Informationstechnik, Bundesanzeiger-Verlag, www.bsi.de/gshb/index.htm

[Barth2001] **Das Firewall Buch**, Wolfgang Barth, SuSE PRESS

[BSI1998] **Grundlagen, Forderungen und Marktübersicht für Intrusion Detection Systeme (IDS) und Intrusion Response Systeme (IRS)**, Dr. Josef von Helden, Dr. Stefan Karsch, debis IT Security Services

[Holt2001] **Einführung in TCP/IP, Standards und Protokolle**, SS2001, Heiko Holtmann, Universität Bielefeld - Technische Fakultät

[Holt1999] **Einführung in TCP/IP**, Heiko Holtmann, Universität Bielefeld - Technische Fakultät

[Raepple1998] **Sicherheitskonzepte für das Internet**, Martin Raepple, dpunkt.verlag

[DS2000] **Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet**, Konferenz der Datenschutzbeauftragten des Bundes und der Länder, www.datenschutz-bayern.de/technik/orient/int_gesch.pdf

[DS2001] Handreichung „Datenschutzgerechtes eGovernment“, Konferenz der Datenschutzbeauftragten des Bundes und der Länder, www.lfd.niedersachsen.de/functions/downloadObject/0,,c1358174_s20,00.pdf

Begriffserläuterungen

Firewall	Eine Firewall ist eine Schwelle zwischen zwei Netzen, die überwunden werden muß, um Systeme im jeweils anderen Netz zu erreichen. Durch technische und administrative Maßnahmen wird dafür gesorgt, daß jede Kommunikation zwischen den beiden Netzen über die Firewall geführt werden muß. Auf der Firewall sorgen Zugriffskontrolle und Audit dafür, daß das Prinzip der geringsten Berechtigung durchgesetzt wird und potentielle Angriffe schnellstmöglich erkannt werden (Definition Deutsches Forschungsnetz - www.dfn-cert.de/team/ue/fw/fire/node3.html)
Stateful-inspection	Gelegentlich auch als dynamische Paketfilterung bezeichnet. Stateful-inspection ist eine Firewalltechnik, die ab der dritten Schicht des OSI-Modells (network-layer) arbeitet. Im Gegensatz zur statischen Paketfilterung wird bei stateful-inspection jede Verbindung, die zwischen den Netzwerk-Interfaces einer Firewall besteht, aufgezeichnet und es wird überwacht, ob die ein- und ausgehenden Pakete weiterhin zur bestehenden Verbindung gehören. Es wird also neben dem IP-Header der aktuelle Zustand der jeweiligen Verbindung dynamisch überwacht. Manche Systeme mit stateful-inspection sind sogar in der Lage, dynamisch Ports zu öffnen und wieder zu schließen. Im Vergleich zur statischen Filterung werden IP-Pakete bereits auf der Netzwerkschicht von einem Analysemodul entgegengenommen, das nicht nur die Überwachung der Verbindung ermöglicht, sondern die Inhalte der Pakete bis hinauf in die siebte Schicht des OSI-Modells (application-layer) untersuchen kann.
Dienst	Die Aufgabe einer Schicht innerhalb eines Protokollstapels ist die Bereitstellung eines bestimmten Dienstes (für die jeweils darüber liegende Schicht). Ein Dienst ist im Gegensatz zu einem Protokoll eine Gruppe von Operationen, die eine Schicht der über ihr liegenden Schicht zur Verfügung stellt [Holt2001].
Protokoll	Alle an einer Kommunikation beteiligten Parteien müssen sich auf Regeln einigen, die beim Austausch von Nachrichten angewendet werden sollen. Eine solche Vereinbarung wird Protokoll (protocol) genannt („Protocols are formal rules of behaviour“). Die Aufgaben eines Protokolls sind – die Adressierung der Kommunikationsendpunkte, – die Steuerung des Datenflusses, – die Bereitstellung eines sicheren Datenübertragungsdienstes. Ein Protokoll ist im Gegensatz zu einem Dienst das Regelgefüge, welches das Format und die Bedeutung der von den Partnereinheiten innerhalb einer Schicht ausgetauschten „Informationen“ festlegt [Holt2001].
Virenscanner	Programm zur Überwachung und Prüfung eines Computers auf schädliche Programme (z.B. Viren, Trojaner, Würmer)
security-policy	Oberbegriff für die Sicherheitspolitik (Festlegung von Sicherheitszielen) und das daraus abgeleitete Sicherheitskonzept (organisatorische und technische Maßnahmen zur Einhaltung der Sicherheitsziele) [Barth2001]

Online-Informationen zur IT-Sicherheit bieten unter anderem folgende Institutionen/Firmen/Mailinglisten/Newsgroups:

Bundesamt für Sicherheit in der Informationstechnik	www.bsi.de oder www.bsi.bund.de
Bundesministerium für Wirtschaft und Arbeit und Bundesministerium des Innern	www.sicherheit-im-internet.de/themes
Fa. Microsoft	www.microsoft.com/germany/ms/security
Telstra Corporation	www.telstra.com.au/infor/security.html
BugTraq	www.securityfocus.com
NTBugTraq	www.ntbugtraq.com
Cert-CC	www.cert.org
First	www.first.org
Internet Engineering Task Force	www.ietf.org
World Wide Web Consortium	www.w3c.org
USENIX Association	www.usenix.org
SysAdmin, Audit, Network, Security	www.sans.org
Diverse Hersteller von Software und Sicherheitsprodukten	