Zusammenfassung

Die Absicherung von Intranets wird aufgrund steigender Teilnehmerzahlen im Internet, neuen Anwendungen und Diensten heutzutage immer wichtiger. Die Notwendigkeit sich mit dem Internet zu befassen und seine jeweiligen Dienste zu nutzen, ist immer mehr Institutionen bekannt. Nachdem die Anbindung an das Internet abgeschlossen wurde, beschäftigt man sich allerdings viel zu wenig mit den notwendigen Sicherheitsaspekten. Der Datenverlust bzw. die fehlende Zugriffssicherung kann dabei teuer bestraft werden und bis zum Kollaps führen. Die Lösung ist ein einheitliches und individuelles auf das eigene Intranet bezogene Sicherheitskonzept, das auf die Kommunikationsstruktur und -abläufe des jeweiligen Unternehmens zugeschnitten wird. Dabei werden zuerst Infrastruktur und Kommunikationsabläufe analysiert, bevor man detaillierte Systemlösungen integriert. Weiterhin müssen die Dienste einzeln kontrolliert und überwacht sowie Verschlüsselungsverfahren für die sichere Übermittlung von Daten implementiert werden. Es ist ein globales Sicherheitskonzept (Security Concept) in Zusammenarbeit mit dem Kunden zu entwerfen und umzusetzen, damit Attacken von außen vermieden werden können. Dabei bleibt eines zu beachten: eine absolute Sicherheit gibt es nicht! Nur die Wahrscheinlichkeit, daß solche Attacken auftreten, sollte so gering wie möglich gehalten werden. Dieser Beitrag geht kurz auf die Sicherheitslücken ein, beschreibt den Inhalt eines Sicherheitskonzepts und anschließend kurz die Anwendungsschicht Firewall. Zusätzlich wird die Möglichkeit aufgezeigt, IPsec zur Verschlüsselung zu nutzen.

1 Einleitung

Das Internet erfreut sich einer enormen Beliebtheit und damit hohen Wachstumsraten. Die Teilnehmerzahlen steigen exponential an und lassen neben Problemen bei der Adreßvergabe, Routing, Echtzeitfähigkeit auch Sicherheitslücken erkennen. Durch die wachsende Verbreitung des Internets und dem zunehmenden Einsatz von Internet-Protokollen (IP) wird dabei der Schutz vor unbefugten Zugriffen auf das Unternehmensnetzwerk immer wichtiger. Zusätzlich werden immer mehr geldliche Transaktionen über das Internet durchgeführt sowie Geschäfte abgewickelt, die eine hohe Vertraulichkeit beinhalten müssen.

Allerdings ergeben sich durch die Anbindung an Netzwerke für ein Unternehmen und dessen Mitarbeiter eine Vielzahl zusätzlicher Kommunikationsmöglichkeiten und nutzbarer Dienstleistungen. Dabei sind alle Unternehmen, die direkt an ein WAN wie das Internet angeschlossen sind, durch diese Verbindung Angriffen auf das eigene Intranet ausgesetzt. Den Systemverwaltern der firmeninternen, lokalen Netzwerke (LAN) obliegt es, betriebsspezifische, programmtechnische und persönliche Daten vor dem externen Zugriff durch Unbefugte zu schützen. Im gleichen Maße müssen Daten der verschiedenen Dienstleistungen im Netzwerk aus dem Unternehmen das lokale Netzwerk aber auch verlassen dürfen. Zusätzlich sollen sie auch nur diejenigen Adressaten erreichen, für die die Daten letztendlich bestimmt sind.

Die Nutzung der implementierten Sicherungsmechanismen der am Markt gängigen Betriebssysteme reicht selbst bei optimaler Konfiguration heutzutage bei weitem nicht aus. Optionale Hard- und Software Mechanismen zur Erweiterung des Systemschutzes des lokalen Netzwerks sind ebenfalls unzureichend. Der empfindlichste Schwachpunkt ist der Knotenpunkt der

Anbindung des lokalen Netzes an das WAN und der damit jederzeit mögliche, externe Zugriff auf jeden einzelnen Computer in dem lokalen Netzwerk. Der beste Schutz wäre demnach die Trennung der beiden Netze. Eine komplette physikalische Trennung scheidet aus, denn sie würde den notwendigen Datentransport verhindern. Ein globales Sicherheitskonzept muß also definiert werden, das die Kommunikationsstruktur berücksichtigt und Sicherheitslücken und Defizite kenntlich macht. Dabei sind die folgenden Fragestellungen bei der Analyse von Intranets einzubeziehen:

- Vorhandene Infrastruktur
- Betriebssicherheit
- Remote Access Points
- Analyse des Sicherheitsgrads des Intranets im Unternehmen
- Analyse der Sicherheitslücken
- Anforderungen an das Netzwerk
- Firewall-Konzeption für Zugangskontrolle
- Verschlüsselungssysteme und Authentifikation
- Virenscanner

2 Sicherheitslücken und Defizite

Um ein Intranet eines Unternehmens nach außen hin abzusichern, sollte ein Sicherheitskonzept erstellt werden, um die Grenzen akzeptablen Verhaltens und die Redaktion auf Übertretung genau definieren zu können. Die Anforderungen an die Sicherheit unterscheiden sich dabei von den Auftraggebern, da unterschiedliche Organisationen verschiedene Sicherheitsanforderungen besitzen. Ein Sicherheitskonzept wird dabei aber jedem Firmentyp, ob Universität oder militärischen Einrichtungen, gerecht. Die Frage, ob eine Firewall im Unternehmen zur Absicherung der Internet-Anbindung notwendig ist, stellt sich aufgrund der Gefahren nicht mehr.

Eine Verbindung zum Internet wird über das öffentliche Netz zum nächsten Point-of-Presence (POP) eines Internet Service Providers (ISP) realisiert. Über geeignete Protokolle wird dann über Wählverbindungen mittels analoger Modems, ISDN, X.25-Verbindungen oder unterschiedliche Standleitungen (DDV oder Festverbindungen) der Zugang zum Internet eröffnet. Die POPs sind wiederum untereinander und den internationalen Netzen verbunden, so daß eine transparente Kommunikation mit anderen Teilnehmern ermöglicht wird. Die ISP stellen eine eigene Infrastruktur untereinander bereit, die mit Peering Points ausgestattet sind. In einem Peering schalten Provider eigene Router in einem LAN zusammen und tauschen dort die Verfügbarkeit ihrer Netze aus. An einem Peering Point wechseln die Daten von einem Provider-Netz in das eines anderen Providers.

Computersysteme können im allgemein nicht hundertprozentig gegen Angriffe von außen geschützt werden. Es ist jedoch möglich, einzelne Gefahrenquellen deutlich zu minimieren. Das größte Gefahrenpotential geht dabei immer von den Benutzern des Computersystems aus, insbesondere von den Systemverwaltern bei starker Unachtsamkeit. Kein automatisiertes System ist in der Lage, einen versierten Systemverwalter bei der Überwachung eines Computers zu ersetzen bzw. ihn daran zu hindern, seine Machtfülle zu mißbrauchen. Ebenso bestehen oft Gefahren durch rechtmäßige Benutzer, die entweder aus Unachtsamkeit oder aus kriminellen Antrieben die Sicherheit des Systems gefährden, beispielsweise durch unbedachte Wahl von Kennworten oder Datentransfer mittels Disketten nach innen und außen. Die wichtigsten Punkte

hierbei sind sogenannte programmierte Bedrohung (Programmed Threats) und die Bedrohung durch nicht autorisierte Eindringlinge. Je nach Herkunft und Absicht können diese mit mehr oder weniger Aufwand vom System ferngehalten werden.

Bei den programmierten Gefahren kann man folgende Typen unterscheiden:

- Viren (Viruses) befallen „normale“ Programme und verbreiten sich über diese weiter, indem sie meist den ausführbaren Code des Wirtsprogrammes modifizieren. Wird das infizierte Programm ausgeführt, versucht das Virus, weitere Programme zu infizieren.
- Würmer (Worms) breiten sich in einem Netz selbständig von Knoten zu Knoten aus, ohne jedoch andere Programme zu infizieren und richten im allgemeinen keinen Schaden, außer einem erhöhten Verbrauch der Ressourcen an.
- Trojanische Pferde (Trojan Horses) sind Programme, die von Benutzern ausgeführt werden und dabei an Stelle der gewünschten Aktion andere, unbeabsichtigte Seiteneffekte hervorrufen.
- Logische Bomben (Logic Bombs) werden meist in anderen ausführbaren Programmen versteckt und werden durch bestimmte Bedingungen ausgelöst, beispielsweise an einem bestimmten Tag oder wenn ein Mitarbeiter nicht mehr auf der Gehaltsliste steht. Meistens zerstören sie dann Daten oder setzen Viren frei.
- Hintertüren (Backdoors) sind Programmteile, mit deren Hilfe ein Zugriff auf das System unter Umgehung der Authentisierungsverfahren oder mit erhöhten Privilegien ermöglicht wird.

Neben den programmierten Gefahren gibt es vor allem Probleme, die durch die direkte Beteiligung von Personen entstehen. In solchen Fällen sollte man die Einschätzung der Vorfälle nach der Motivation eines sogenannten Crackers (nicht Hacker) vornehmen. An dieser Stelle wird deutlich zwischen Crackern und Hackern unterschieden. Hacker versuchen in ein System einzudringen, da sie sich für die Umgehung der Sicherheitsmechanismen interessieren. Sie zerstören dabei keine Daten und setzen keine Viren frei. So wie sie die Hintertür eines Intranets betreten haben, so verlassen sie das Netz auch wieder. Cracker hegen hingegen von Anfang an kriminelle Absichten. Sie versuchen in ein Netzwerk einzudringen, um sich persönliche Vorteile zu beschaffen und eventuell Daten zu zerstören.

Die Unterschiede in den Motiven bestimmen im allgemeinen auch das Gefährdungspotential, das von solchen Vorfällen ausgeht. Beispielsweise wird der Hacker meistens keinen Datenverlust auslösen, es sei denn durch unbedarfte Vorgehensweise im fremden Netzwerk. Allerdings löst der Hacker bei Entdeckung durch den Netzwerkadministrator eine zeitraubende Untersuchung aus, um die Sicherheitslücken rechtzeitig stopfen zu können. Dies ist im Grunde ein relativ gewünschter Vorgang, da so die Lücken einer Firewall erkennt und beseitigt werden können. Mehr Probleme entstehen durch ambitionierte Cracker, die sich vorgenommen haben einen wirklichen Schaden im Netzwerk anzurichten und dieses Ziel auch mit einer gewissen Hartnäckigkeit verfolgen. Dabei hat der Bereich der Industriespionage bzw. der kriminellen Angriffsbemühungen statistisch deutlich zugenommen. Beispielsweise verzeichnen die Top-Level-Domäne COM (Commercial) laut Firewallsystemen in den USA einen deutlichen Anstieg von Attacken.

Neben dem tatsächlichen Schaden wie Datenverlust, Datendiebstahl usw. entsteht bei allen Vorfällen mit Personen aus dem Hackerumfeld immer das Problem, die Integrität des Systems nach einer Attacke wieder sicherzustellen. Es kann notwendig sein, den kompletten Datenbestand des Unternehmens vom Band restaurieren zu müssen, um dies zu erreichen.

Tatsache ist auch, daß sich erfahrene Hacker mit immer raffinierteren Methoden Zugang zu Systemen verschaffen. Vor solchen Attacken kann man sich nur mit extrem gut gesicherten Zugangskontrollsystemen schützen. Für die weniger erfahrenen Cracker stehen dagegen mehrere automatisierte Werkzeugkästen zum Einbruch in ein Rechnersystem zur Verfügung. Teils wurden diese Tools als Hilfsmittel für Sicherheitsanalysen, teils auch gezielt für den Einsatz bei Einbruchsversuchen entwickelt. Diese Tools sind zwar nicht so gefährlich wie ein erfahrener Cracker, sind aber vollkommen ausreichend, um in ein schlecht geschütztes bzw. ungeschütztes System einzubrechen.

2. Sicherheitskonzept

Damit eine Firewall auch eine entsprechende Wirkung hat, muß vorab ein Sicherheitskonzept erstellt werden. Erst dieses wird eine effiziente Lösung mit dem zugesicherten Sicherheitsstandard ermöglichen. Weiterhin dürfen die Teilnehmer des Intranets die Firewall kaum bemerken, da sie ungehindert weiterarbeiten sollen. Eine völlige Transparenz ist dabei natürlich nicht möglich, besonders wenn Anwendungsschicht Firewalls eingesetzt werden. Auch ist die Auswahl des Betriebssystems zu beachten. Neben Unix-Systemen, die aufgrund ihrer Komplexität Sicherheitslücken aufweisen, sind Windows-Systeme von Haus aus bereits leicht anfällig. Die Benutzbarkeit von solchen Systemen spielt ebenfalls eine bedeutende Rolle. Das heißt, einfach zu benutzende Schnittstellen für die Konfiguration, Kontrolle, Regeldefinition, Server und Alarme sind notwendig, um eine dauerhaft sichere Administration zu erreichen. Auch sollte eine Authentifikation von externen Zugängen in jedem Fall integriert sein. FTP und Telnet stellen dabei die größten Sicherheitsprobleme dar und müssen einzeln gesichert werden. Die vollständige Verdeckung von Adressen und weiteren Informationen aus dem Intranet ist ebenfalls ein wichtiger Punkt. Das Network Address Translation (NAT) ermöglicht dieses Merkmal direkt im Router, wodurch die Intranet-Adressen nicht nach draußen gelangen und für den externen Teilnehmer unsichtbar bleiben. Nur die IP-Adresse des Routers ist maßgeblich für den Zugriff von außen. Dadurch kann man in privaten Netzen nicht registrierte Adressen des Internets verwenden und spart dadurch auch noch IP-Adressen ein. Weiterhin müssen die Systeme, auf denen eine Firewall installiert ist, zur gehobenen Leistungsklasse gehören, um möglichst geringe Latenzzeiten gewährleisten zu können. Je weniger Rechenleistung die Firewall hat, um so größer ist natürlich die Verzögerung. Deshalb sollte man beim Anschaffungspreis auch keine großen Abstriche machen. Durch Logins und Alarme kann man im laufenden Betrieb das Intranet dauerhaft überwachen. Load Sharing ist für das Firewall-System ebenfalls wichtig, da die meisten Firewalls über mehrere Netzwerkadapter verfügen, die neben erhöhter Ausfallsicherheit auch eine Lastverteilung ermöglichen. Letztendlich sei noch auf den Einsatz von Verschlüsselungssystemen hingewiesen, die die Nutzung von Virtual Private Networks (VPNs) ermöglichen. Leider fehlt bislang ein einheitlicher Standard, so daß heutige Firewalls entweder leistungsschwach oder proprietär sind. Auf das Thema VPN wird aber noch in einem späteren Kapitel eingegangen.

Letztendlich ergibt sich durch die Beachtung der geschilderten Punkte ein Gesamtkonzept, welches sich nach den Bedürfnissen und Anforderungen des Kunden orientiert. Um ein solches Konzept zu planen, lassen sich folgende Thesen aufstellen:

- Der Sicherheitsbedarf muß analysiert werden: Vertraulichkeit der Daten, Datenintegrität, Dienstverfügbarkeit, Konsistenz und Transparent, Zugriffskontrollen und Überwachung
- Vertrauensverhältnis: Gegen wen will man sich schützen?

- Risikoanalyse: Was soll geschützt werden? Gegen was soll es geschützt werden? Wieviel Zeit und Arbeit soll investiert werden?
- Liste über zu schützende Güter anlegen
- Kosten-Nutzen-Analyse: Welcher finanzieller Schaden entsteht bei dem Verlust von Daten? Wie hoch ist der Aufwand zu berechnen, um die sensitiven Daten zu schützen?
- Policy und Benutzerrichtlinien erstellen
- Definition der Anforderungen an das Firewall-System
- Überprüfungsliste der Dienste anlegen
- Anforderungen an die Netzkomplexität definieren

Diese Punkte stehen für eine grobe Richtlinie, wie man bei der Konzeption eines Firewall-Systems vorgehen soll. Sie können auch an dieser Stelle nur angerissen werden, da die Parameter sich von jedem Kunden unterscheiden.

Um letztendlich offene Sicherheitslücken erkennen und abschätzen zu können, sind unabhängige Sicherheitsgremien wie das Computer Emergency Response Team (CERT) vorhanden, die kontinuierlich nach Mängeln suchen. CERT wurde 1988 von der DARPA gegründet und hat in Verbindung mit diversen Schwesterorganisationen die Aufgabe, Informationen über Sicherheitsaspekte und -vorfälle im Internet zu sammeln und zu veröffentlichen. Das CERT Koordinationszentrum studiert Sicherheitsmängel im Internet und liefert Attackenbeschreibungen. Weiterhin werden Sicherheitsalarme und Forschungsinhalte bezüglich der Sicherheit veröffentlicht. Dadurch hilft das CERT den Teilnehmern am Internet gegenüber Hackern und Crackern zu widerstehen und Risiken zu erkennen. Das CERT Koordinationszentrum ist Teil des Networked Systems Survivability Programm des Software Engineering Institute der Carnegie Mellon Universität. Unter der URL-Adresse http://www.cert.org sind mehr Informationen verfügbar.

Um eine möglichst hohe Sicherheit erreichen zu können, sind Sicherheitsaspekte wie Schutz des Netzwerks vor unbefugten Eindringen und Sicherstellen der Netzwerkverfügbarkeit grundsätzlich zu beachten. Sicherheitskonzepte für lokale Netzwerke können sich auf eine Vielzahl von unterschiedlichen Ansätzen stützen. Jede Technologie arbeitet dabei auf ihre spezielle Art und Weise und weist natürlich eigene Vor- und Nachteile auf. Der Administrator kann sie sowohl getrennt als auch gebündelt einsetzen. Neben der V.24-Schnittstelle für externe Konfigurationsmöglichkeiten (Outband Management), müssen unterschiedliche Sicherheitspunkte benannt werden:

- Schutz gegen Angriffe auf Protokollebene: Network Address Translation (NAT), IP Zugangslisten, Zugangsberechtigung, geschlossene Benutzergruppen, intelligente Filtermechanismen
- Methoden zur Authentifikation: Paßwortabfrage, PAP und CHAP, Identifizierung eingehender Rufe, Callback
- Sicherstellen der Netzwerkverfügbarkeit: Konfiguration der Backup-Leitungen, Equipment Backup
- Speicherung von Angriffsversuchen über Alarmfunktionen
- Verteilte Sicherheit: RADIUS, Dial Table, Routing Table

Zusätzlich sind Tools verfügbar, die in der Lage sind die Sicherheitsmechanismen des eigenen Netzes zu überprüfen. Teilweise ist diese Software kostenlos erhältlich. Das bekannteste Tool dieser Art ist das Security Administrator Tool for Analyzing Networks (SATAN). Dadurch wird auch der unerfahrene Administrator in die Lage versetzt, die Sicherheit seines Netzes durch

automatische Einbruchsversuche zu testen. Allerdings ist SATAN nicht weiter entwickelt worden. Sein Nachfolger heißt SAINT und ist ebenfalls frei verfügbar. Es besitzt ein komfortables HTML-Frontend, um es über einen Browser bedienen zu können. Durch den Einsatz über einen Browser, ist es praktisch für alle Plattformen einsetzbar. Andere Tools testen beispielsweise den Paßwortschutz. COPS, ein Softwarepaket zur Analyse von Schwachstellen in Unix-Systemen, beinhaltet CRACK, welches schwache Paßwörter findet. Dabei ist die Authentifikation mit biometrischen Verfahren der beste Schutz gegen das Knacken von Paßwörtern.

Wenn man einen hohen Sicherheitsstandard erzielen möchte, ist der Einsatz dieser Tools sehr hilfreich. Dabei sollte keines der Werkzeuge auf dem Gateway installiert sein, damit ein Angreifer, wenn er auf das Gateway gelangt, nicht einen fertigen Werkzeugkoffer findet, mit dem er das Netz weiter angreifen kann. Es sollte deshalb immer ein separater Rechner für diese Applikationen bereitgestellt werden.

3. Einsatz von Firewalls unter Einbeziehung der Dienste

Beim Einsatz von Firewalls gibt es verschiedene Parameter zu beachten, die die unterschiedlichen Realisierungen und Produkte betreffen. Man unterscheidet die Firewall anhand des Schichtenmodells in Paket-, Transport- und Anwendungsschicht. Die Anwendungsschicht besitzt dabei den höchsten Sicherheitsgrad, weshalb an dieser Stelle ausschließlich auf sie eingegangen wird.

Die Anwendungsschicht Firewall trennt den Datentransfer zwischen dem internen und externen Netz physikalisch und logisch komplett ab. Dies ermöglicht ein wesentlich höheres Sicherheitsniveau. Firewall auf der Anwendungsschicht arbeitet mit je einem Proxy-Server pro Dienst (Telnet, FTP, HTTP). Jede Verbindung zwischen einem Server im internen Netz und einem externen Client wird durch die Firewall in zwei Verbindungen aufgeteilt: Die Firewall stellt nach außen den Server dar und nach innen den Client - oder umgekehrt bei einer Verbindung interner Client mit externem Server. Durch die totale Prozeßkontrolle wird für die unterstützten Dienste ein sehr hoher Sicherheitsgrad erreicht. Diese doppelte Verarbeitung geht jedoch zu Lasten der Performance, so daß diese Lösung wesentlich langsamer arbeitet als Paket- oder Transportschicht Firewalls.

Die Anwendungsschicht Firewall besitzt zwei Netzwerkanschlüsse, da in der Vergangenheit Firewalls mit einem einzelnen Adapter zu leicht angreifbar waren. Dabei existiert ein unsicherer bzw. ungeschützter Bereich und eine Schutzzone, die das eigene Intranet darstellt. In diesem Fall müssen sog. Proxy fähige Programme eingesetzt werden. Bei dieser Art der Firewall können nur Daten mit Diensten transportiert werden, für die auf der Firewall ein Programm vorhanden ist. Dabei können die transportierten Daten kontrolliert werden.

Die meisten kommerziellen Firewalls sind eine Mischung aus Transport- und Applikationsschicht Firewalls. Die ausgehenden Dienste werden häufig über Transportschicht Firewalls geleitet, während die hereinkommenden Daten durch Anwendungsschicht Firewalls gefiltert werden. Ein häufig anzutreffende Kombination ist die Installation eines Paketfilters auf dem Router für die hereinkommenden Daten, der nur einen Zugriff auf die Rechner zwischen den beiden Routern und der Firewall ermöglicht. Es wird jedoch nicht der Zugriff auf den Router am internen sicheren Netz gestattet. Weiterhin wird der interne Router so konfiguriert, daß er nur einen Datenverkehr mit der Firewall zuläßt. Diese Konfiguration ist sehr effizient sowie wirksam und wird als Zwinge bezeichnet.

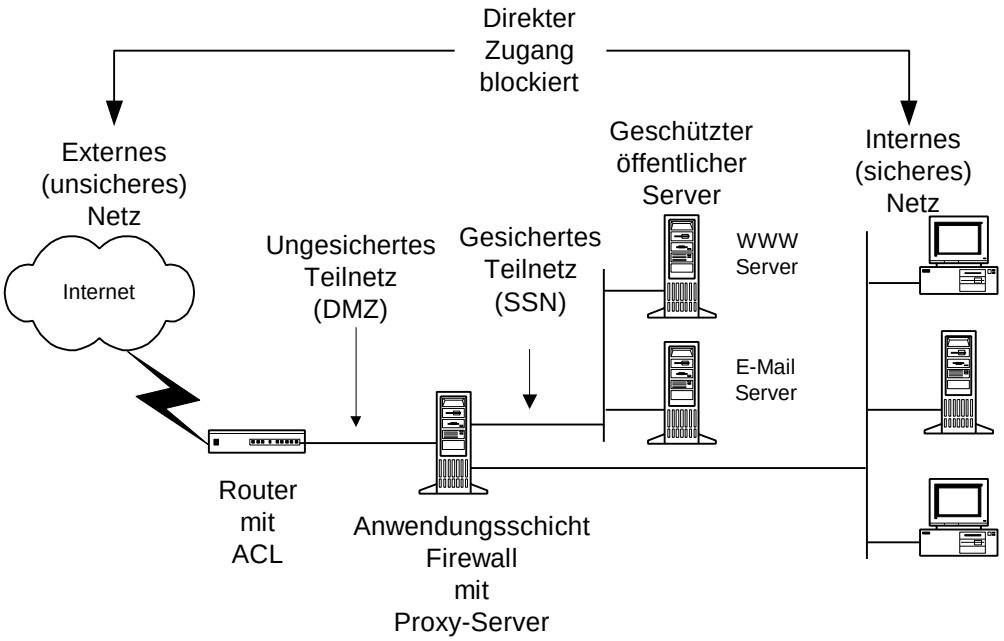

Abbildung 1: Anwendungsschicht Firewall

Der Bereich zwischen dem Router im Eingangsbereich und der Firewall wird häufig als DMZ bezeichnet. In diesem Bereich werden die externen Dienste verfügbar gemacht, auf die von außen zugegriffen wird. Wenn von außerhalb einer der Rechner im Bereich DMZ übernommen wird, so ist von dort kein Zugriff auf die Rechner des internen Netzes möglich. Es besteht jedoch die Gefahr, das die Firewall Flooding Angriffen nicht standhält. Dabei wird die Firewall zum Beispiel mit Protokollbefehlen überschwemmt und zum Zusammenbruch gebracht. Darüber hinaus kann es Probleme bei der Unterstützung neuer Applikationen im Internet geben. Eine hundertprozentige Sicherheit gibt es also auch hier nicht. Trotzdem ist dieses Firewall-System die sicherste Methode seine Daten und Informationen des eigenen Intranets vor Angriffen zu schützen. Das interne Netz wird nach der Absicherung durch die Firewall als Secure Server Network (SSN) bezeichnet.

Die Arbeitsweise dieser Firewall unterscheidet sich von denen der anderen Firewalls. Für die Teilnehmer, die über eine Anwendungsschicht Firewall kommunizieren möchten, ist zuerst eine Identifizierung und Authentifikation notwendig. Zusätzlich werden unterschiedliche Verfahren für die Authentifikation unterstützt. Deshalb wird zuerst eine Verbindung zum Anwendungsschicht Firewall aufgebaut und nicht zum Zielrechner im Intranet. Eine direkte Kommunikation findet demnach zur Gateway statt und nicht zwischen den jeweiligen Endsystemen. Nachdem sichergestellt wurde, daß eine Kommunikation zwischen bekannten Endsystemen vorliegt, wird der Datenverkehr von der Gateway transparent weitergeleitet. Die Teilnehmer merken nichts von dem dazwischen geschalteten System.

Grundsätzlich empfängt die Anwendungsschicht Firewall Datenpakete an den jeweiligen Ports. Pro Port werden bestimmte Dienste freigegeben. Dies geschieht über entsprechende Software auf der Firewall, die die Datenpakete empfängt und an die sichere Netzwerkseite weiterleitet und umgekehrt. Diese Software kann man auch als Proxy bezeichnen und wurde bereits beschrieben. Der Unterschied liegt darin, daß jeder Proxy auf einer Firewall Gateway einem bestimmten Dienst zugeordnet werden kann. Somit ist er in der Lage zusätzliche Sicherheitsdienste den Anwendungen zu vergeben. Dadurch ergeben sich mannigfaltige Möglichkeiten für Absicherung

und Protokollierung. Zu beachten ist, daß auf der Anwendungsschicht Firewall nur die minimal notwendige Software installiert ist, damit Angreifer von außen so wenig Chancen wie möglich haben auf die Proxies einzuwirken, um sie für andere Dienste nutzbar zu machen. Auch sollte das Sicherheitsmanagement nicht auf dem selben Rechner laufen, wie die Firewall. Routing-Funktionen sind auszuschließen, da ansonsten die Proxies umgangen werden können.

Aufgrund der Verbindung zum ungesicherten als auch gesicherten Bereich, muß die Anwendungsschicht Firewall natürlich Network Address Translation (NAT) kennen und anbieten. Bei der Realisierung besitzt die Firewall eine IP-Adresse im ungesicherten Netz, die als öffentliche Adresse im Internet bekannt ist, und eine IP-Adresse im geschützten Intranet. Bei der Kommunikation mit den beiden Bereichen werden auf jeder Seite nur jeweils eine IP-Adresse sichtbar, so daß keine direkte Verbindung durch die Firewall möglich ist.

4. Verschlüsselung

Um Daten außerhalb des Intranets sicher austauschen zu können, müssen Verschlüsselungssysteme eingesetzt werden. Hier ist bislang keine durchgreifende Spezifikation erfolgt, wodurch viele proprietäre Lösungen existieren. Eine Ausnahme ist IPsec, welches durch die Arbeitsgruppe der IETF 1998 vorgelegt wurde, um eine sichere IP-Architektur zukünftig bereitstellen zu können. Grundlage dieser Spezifikation bildet ein vor ein paar Jahren erarbeiteter Standard (RFC-1825). Der Vorschlag legt fest, auf welche Weise Authentifikation und Verschlüsselung auf der IP-Schicht einzurichten sind. Firewalls, die sich an diese Spezifikation halten, können untereinander chiffrierte Daten austauschen, auch wenn sie von unterschiedlichen Herstellern stammen und verschiedene Verschlüsselungsverfahren verwenden. Dies war bislang nicht möglich, da es sich immer um proprietäre Lösungen handelte.

Zu der Spezifikation RFC-1825, kommen RFC-1826 und RFC-1827 noch hinzu. Sie bauen alle aufeinander auf. Zusätzlich sind eine Menge Drafts entstanden, die unterschiedliche Themen behandeln. Beispielsweise wurde das Zusammenwirken von Authentification Header (AH), Encapsulated Security Payload (ESP) und Key Management festgelegt. Weiterhin sind spezielle Drafts für die Nutzung konkreter Verschlüsselungs- und Authentifikationsalgorithmen entstanden. Key Management Protokolle sind ebenfalls angegeben.

IPsec unterscheidet sich von den bisherigen Ansätzen. Zwar gibt es bereits Sicherheitsmechanismen auf der Anwendungsschicht, wie SSL oder PGP für E-Mails. Um aber das Intranet effizienter abzusichern, unabhängig von den Anwendungen und deren Verschlüsselungsverfahren, müßte man auf der Netzwerkschicht ansetzten. Da IP bislang keine solchen Mechanismen vorsah, entstanden proprietäre Implementierungen, die sich auch auf VPN-Produkte auswirkten. So ist kein Hersteller eines VPN-Produktes momentan in der Lage mit einem anderen zu kommunizieren. IPsec stellt hingegen eine Sicherheitserweiterung auf der IP-Schicht dar, wodurch es jedes Datenpaket vor Verfälschung (Authentizität und Integrität) schützt und zusätzlich noch verschlüsselt (Vertraulichkeit). Im Grunde würden Sicherheitsmechanismen auf der Anwendungsschicht dadurch überflüssig, wenn IPsec die Daten auch nach dem Empfang weiter schützen würde. IPsec hat dafür aber keine Möglichkeiten vorgesehen – es schützt die Daten nur zwischen zwei Instanzen. Andere Ansätze, wie z.B. die digitale Signatur, werden weiter benötigt.

IPsec ermöglicht den Datenschutz hauptsächlich durch zwei Paketerweiterungen. Hinzugekommen sind der AH und die Nutzdaten ESP. Der AH beinhaltet eine kryptographische Prüfsumme über

die Nutzdaten und Teile des Paket-Headers. Bekannte Hash-Funktionen, wie Message Digest 5 (MD5) und Secure Hash Algorithm (SHA), bilden die Prüfsumme mit einem symmetrischen Schlüssel. MD5 weist allerdings heute einige Schwächen auf, so daß man bereits SHA einsetzen sollte. Durch die Bildung der Prüfsumme entsteht ein Message Authentification Code, der die Nutzdaten vor Verfälschugn schützen soll. Zusätzlich werden wichtige Daten des IP-Headers gesichert. Das betrifft beispielsweise die Sende- und Empfangsadresse, wodurch das IP-Spoofing abgewehrt werden kann. Es werden nicht alle Felder des Headers in die Prüfsumme eingeschlossen, da sich ändernde Felder, wie z.B. TTL, die Prüfsumme ungültig machen würden. ESP wird hauptsächlich zum Verschlüsseln der Nutzdaten verwendet. Das wird mit symmetrischen Verschlüsselungsverfahren, wie DES, Triple-DES oder IDEA realisiert. Asymmetrische Verfahren könne aufgrund der Performance nicht eingesetzt werden. So kann die Datenrate von 100 MBit/s auf 1 MBit/s sinken, wenn man Public Key Verfahren einsetzen würde.

Um VPNs mittels IPsec aufbauen zu können, damit ganze Netze über virtuelle Verbindungen getunnelt werden können, wird unterschieden zwischen dem Transport Mode und dem Tunnel Mode. Der Tunnel Mode ermöglicht die sichere Datenübertragung von IP-Paketen in IPsec-Paketen. Für viele Situationen wird die Anwendung von nur einer IPsec-Funktion nicht ausreichend sein, wenn beispielsweise nur Teilstrecken im Tunnelmodus betrieben werden können, falls nicht alle Knotenpunkte IPsec erkennen. Dann müssen Kombinationsformen aus Transport und Tunnel Mode spezifiziert werden, die jede Implementierung unterstützen muß. Ansonsten besteht aber der große Vorteil, daß Datensicherheit den Anwendungen transparent zur Verfügung gestellt wird, wodurch proprietäre VPNs der Vergangenheit angehören werden.

5. Fazit

Sicherheitsmechanismen sind absolut notwendig, um die Zugriffssicheit eines Intranets garantieren zu können. Zusätzlich wenden Sie aber die Gefahren aus dem Internet nicht effektiv ab, wenn sich die Anwender nicht nach einem definiertem Regelwerk verhalten bzw. regelmäßige Kontrolle der Nachbesserung der Sicherheitslösung erfolgt. Bei der Implementierung eines globalen Sicherheitskonzepts muß deshalb neben der Kommunikationsanalyse auch eine Analyse der passiven und aktiven Infrastruktur erfolgen. Weiterhin spielt hier die Betriebssicherheit eine entscheidene Rolle, da man sich gerade hier vor Datenverlust schützen muß. Auch die verwendeten Applikationen oder die zukünftig geplanten Dienste sind für dieses Konzept entscheidend. Beispielsweise lassen Videokonferenzen die Anforderung an die Performance drastisch steigen. Aber gerade hier wird man immer einen Kompromiß zwischen der Leistung einer Systemlösung und der zur Verfügung stehenden Sicherheit machen müssen. Letztendlich beinhaltet die Erstellung eines solchen Sicherheitskonzeptes viele Bereiche eines Intranets, die alle angesprochen und eingebracht werden müssen. Erst dann wird man einen hohen Sicherheitsgrad gewährleisten können. Eine Firewall-Lösung stellt dabei nur ein Teilbereich dieser Gesamtlösung dar.

Glossar

AH	Authentification Header
CERT	Computer Emergency Response Team
COM	Commercial
DDV	Datendirektverbindung
DES	Data Encryption Standard

DMZ	De-Military Zone; entmilitarisierte Zone bei Firewall-Systemen
ESP	Encapsulated Security Payload
FTP	File Transfer Protocol
HTTP	Hypertext Transport Protocol
IDEA	International Data Encryption Algorithm; 128-Bit-Verschlüsselung
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISDN	Integrated Service Digital Network
IPsec	Standard RFC-1825, der IP-Pakete schützt und Sicherheit transparent für Anwendungen gewährleistet
ISP	Internet Service Providers
LAN	Local Area Network
MD5	Message Digest 5
NAT	Network Address Translation
PGP	Pretty Good Privacy
POP	Point-of-Presence
RADIUS	Remote Authentication Dial-In User Service
SATAN	Security Administrator Tool for Analyzing Networks
SHA	Secure Hash Algorithm
SSL	Secure Socket Layer
SSN	Secure Server Network
TTL	Time-to-Live; Feld im IPv4-Header
V.24	Definitionen der Schnittstellenleitungen zwischen Datenendeinrichtungen und Datenübertragungseinrichtungen
VPN	Virtual Private Network
WAN	Wide Area Network
X.25	Paketvermittelndes Netz

Literatur

[Weihrich97] Weihrich, Thomas: Wasserdichtes Netz - Internet-Sicherheit, Teil 1. In: Gateway 07/97; Heinz Heise Verlag; Hannover, 1997, S. 106.

[Atkinson95] Atkinson, R.: Security Architecture for the Internet Protocol; Network Working Group; Request for Comments: 1825; Category: Standards Track; IETF 1995

[Atkinson95] Atkinson, R: IP Authentication Header; Network Working Group; Request for Comments: 1826; Category: Standards Track; IETF 1995

[Atkinson95] Atkinson, R: IP Encapsulating Security Payload (ESP); Network Working Group; Request for Comments: 1827; Category: Standards Track; IETF 1995