Connection

Ausgabe 17 **Februar 1999**

Firewall & Intrusion Detection

Was erreicht optimale IT-Sicherheit?

von Joachim Koch und Lars Schonert

Die Schriftenreihe von

Connector®
Gesellschaft für Kommunikation und Beratung mbH

Hertzstraße 2
D-69126 Heidelberg
Telefon: +49 (0) 6221 - 13801 0
Telefax: +49 (0) 6221 - 13801 10
E-Mail: info@connector.de
http://www.connector.de

Management Summary

In den letzten Ausgaben des Connection Newsflash‘ wurde das Thema Intrusion Detection unter verschiedenen Gesichtspunkten behandelt. Ziel dieser Connection ist es, Verbindungen zwischen Intrusion Detection Strategien und dem Einsatz von Firewallsystemen aufzuzeigen.

In sehr vielen Unternehmen werden bereits Firewall-Lösungen eingesetzt, um das interne Netz vor dem potentiell unsicheren Internet zu schützen. Dem Schutz durch Firewalls sind jedoch Grenzen gesetzt, die nur durch weitergehende Intrusion Detection Systeme erweitert werden können.

Diese Connection gibt Ihnen einen Überblick über vorhandene Firewall-Lösungen und beschreibt die einzelnen Architekturvarianten. Im zweiten Teil werden Ihnen die grundlegenden Methoden des Intrusion Detection mit ihren Stärken und Schwächen vorgestellt.

Optimale IT-Sicherheit kann durch heute erhältliche Produkte nicht erreicht werden. Und auch in Zukunft wird es nie möglich sein, IT gegen alle nur denkbaren Sicherheitsrisiken zu schützen: Es wird immer Menschen geben, die erfindungsreicher als dann erhältliche Intrusion Detection Systeme sind. Nur: Zur Zeit gibt es noch keine Produkte, die alle Methoden des Intrusion Detection integrieren. Es existieren bereits Implementationen einzelner Intrusion Detection Methoden, die sich jedoch nicht sinnvoll gemeinsam anwenden lassen. Bis dieser Stand erreicht ist, werden noch mindestens 2-3 Jahre vergehen. Bis dahin werden Sie auf Ihre Firewall – als Teil eines zukünftigen Intrusion Detection Systems – angewiesen bleiben, die immerhin einen gewissen Schutz vor unliebsamen Eindringlingen bietet.

Die Autoren

Diese Ausgabe der Connection verfaßten für Sie Joachim Koch und Lars Schonert.

Joachim Koch ist als IT-Consultant im Bereich IT Risk Management unter besonderer Berücksichtigung technischer Fragestellungen tätig.

Lars Schonert ist IT-Consultant im Bereich IT Risk Management mit technischen Referenzen. Dabei hilft die Arbeit als Systemadministrator und Verantwortlicher für die Sicherheit der Inhousetechnik.

Sollten Sie Fragen zu dieser Ausgabe der Connection haben, wenden Sie sich bitte an feedback@connector.de.

Joachim Koch

Lars Schonert

Inhaltsverzeichnis

1 Einleitung

Es gibt mittlerweile kaum eine größere Institution, die über einen Internetzugang verfügt, ohne gleichzeitig einen Schutzmechanismus in Form einer Firewall einzusetzen. Allerdings hören genau an dieser Stelle auch meist die Bemühungen auf: Ist eine Firewall erst einmal aufgebaut und installiert, ist die lokale Informationstechnik (IT) ja sicher, und weitere Bemühungen sind unnötig – ein Trugschluß, der erhebliche Risiken in sich bergen kann.

Wie beinahe jedes Softwareprodukt, kann auch die Firewall-Software mehr oder weniger gravierende Fehler enthalten. Handelt es sich hierbei um sicherheitsrelevante Schwachstellen und werden diese bekannt, reagieren i.a. zuerst Hacker und versuchen über diese Schwachstellen in das betreffende System einzudringen. Genau an dieser Stelle setzt ein Intrusion Detection System an: Selbst wenn ein Eindringling in der Lage ist, sich Zugang zu einem bestehenden System zu verschaffen, wird dieses Eindringen (hoffentlich) durch das Intrusion Detection System entdeckt, und es können unmittelbar Abwehrmechanismen greifen. Damit es jedoch erst gar nicht zu einem solchen Einbruch kommt, ist es wichtig, daß die IT-Systemadministratoren kontinuierlich über den aktuellen Entwicklungsstand bestehender IT-Sicherheitsmechanismen informiert und gleichzeitig fortlaufend über potentielle Risiken in den eingesetzten IT-Sicherheitsprodukten orientiert sind.

2 Firewall

2.1 Einführung

In vielen Firmen, Organisationen und Institutionen bilden Firewalls den zentralen Schutzmechanismus. Dabei schützen sie interne Daten und Dienste gegen unbefugte Zugriffe und Angriffe von außen. Häufig geschehen diese Zugriffe über das Internet und die damit verbundenen Dienste und Protokolle. Durch diese unbefugten Zugriffe auf Firmendaten und bereitgestellte Dienste entstehen jährlich Schäden in Millionenhöhe. Diesen Schäden gilt es durch den Einsatz eines Sicherheitskonzepts vorzubeugen.

Die folgenden Ausführungen beschäftigen sich mit einer Möglichkeit der Sicherung von Netzwerken und Ressourcen mittels einer Firewall. Beschrieben werden dabei die Funktionsweise, ihre Einsatzgebiete und anschließend die Grenzen einer solchen Sicherheitsarchitektur. Wie Sie eventuell bereits gelesen oder gehört haben, bieten aktuelle Firewalls nur einen begrenzten Schutz vor unlauteren Aktivitäten. Erst das aktive Zusammenspiel zwischen dem zugrunde liegenden Sicherheitskonzept, welches sich an den Anforderungen Ihrer Informationstechnologie orientiert, und dem Schutz durch die Firewall kann dem Sicherheitsanspruch der heutigen Zeit gerecht werden.

2.2 Grundlagen

Der Begriff der Firewall umspannt eine Vielzahl von Technologien und Lösungen. Primär versteht man unter einer Firewall das Konzept der Sicherung von schutzwürdiger Kommunikation innerhalb eines geschlossenen Netzwerkes. Dabei werden die Übergänge zwischen Netzwerken, im speziellen der Übergang zwischen dem Firmennetzwerk und dem Internet, durch den Einsatz einer Firewall geschützt.

Visualisierend kann man sich eine Firewall als eine Wand zwischen zwei Netzwerken vorstellen, die durch Regeln und Aktivitäten bestimmte „Türen“ öffnen und schließen kann. Die folgenden Ausführungen geben einen Überblick über die bestehenden Konzepte und deren Ausprägungen, die Einsatzgebiete und Grenzen von Firewallsystemen.

2.3 Typen und Funktionsweisen

Existierende Firewallprodukte kann man anhand zweier grundlegender Technologien kategorisieren. Die erste Kategorie wird durch die Paketfilter vertreten, in der zweiten Kategorie findet man das Application Level Gateway, umgangssprachlich auch als Proxy bezeichnet.

Heutige Firewallsysteme bilden in aller Regel eine Symbiose aus den beiden aufgeführten Technologien, werden jedoch durch Eigenentwicklungen erweitert.

2.3.1 Paketfilter

Die Grundlage der meisten Firewallsysteme bilden sogenannte *Paketfilter*.

Paketfilter arbeiten auf den unteren Schichten des OSI-Referenzmodells, im speziellen auf Schicht zwei (Sicherungsschicht) und drei (Vermittlungsschicht). Dabei regeln diese Paketfilter den Netzwerkverkehr anhand eines fest definierten Regelwerkes. Die zum Einsatz kommenden Regeln basieren auf einfachen Informationen der zu übertragenden Pakete. Diese Informationen befinden sich im Header (Kopf) eines jeden Paketes und enthalten unter anderem Informationen über die Quelle und das Ziel eines jeden Paketes. So kann zum Beispiel eine Verbindung eines Kundenrechners, welcher sich auf Ihrer Homepage umsehen möchte, erlaubt sein. Anhand der Quelladresse wird der Kundenrechner erkannt und die Verbindung zum Webserver freigegeben. Stellt sich jedoch heraus, das die IP-Adresse eine nicht erwünschte Quelladresse darstellt, kann der Zugang zum Webserver gesperrt werden.

Anhand dieser Informationen und den definierten Regeln ist es dem Paketfilter möglich, folgende Aktivitäten durchzuführen:

- Steuerung der Kommunikation zwischen Computer, Teilnetzen oder Netzwerken (erlaubt oder verbietet diese) aufgrund der Quell- und Zieladressen. Dabei kann der Paketfilter Kommunikationsanforderungen für definierte Computer, Netzwerke oder Teilnetze zulassen oder abweisen.

- Festlegung, welche Verbindung oder Applikation welchen Port nutzen darf (Öffnen und Schließen des Ports). Somit können die Zugriffe auf die einzelnen Dienste gesteuert und kontrolliert werden.

Die hierfür notwendigen Regeln sind starr und oft sehr komplex. Zum einen sind bei großen Netzwerken relativ viele Regeln für die Ausgestaltung eines differenzierten Sicherheitskonzeptes notwendig, und zum zweiten sind diese Regeln passiv, müssen also vom Administrator exakt festgelegt und angepaßt werden. Ein wichtiger Nachteil reiner Paketfilter ist die fehlende Möglichkeit, den Inhalt einzelner Pakete und die zugrunde liegende Applikation zu erkennen und bewerten zu können. Um diese Funktionalität zu erfüllen, müssen die Pakete auf einer höheren Schicht des OSI-Referenzmodells, auf der Ebene der Applikationen (Schicht 7), untersucht werden.

Aktuelle Firewallkonzepte sehen den Einsatz von reinen Paketfilter als alleinigen Schutz nicht mehr vor. Vielmehr kommt eine Abstufung und Kombination der verschiedenen Funktionalitäten der verschiedenen Firewallkonzepte zum Einsatz.

2.3.2 Application Level Gateway - Proxyserver

Die zweite Form einer Firewall stellt das Application Level Gateway (ALG) dar.

Dieses Firewallkonzept hat die Problematik der Paketfilter behoben, den Inhalt der zu übermittelnden nicht einsehen zu können. Application Level Gateways besitzen die spezielle Fähigkeit, den Netzwerkverkehr auf der Ebene der Applikationen, also Schicht sieben des OSI-Referenzmodells, zu untersuchen. Diese Funktionalität erlaubt die Untersuchung der einzelnen Pakete und deren Inhalt. Somit kann das Regelwerk den speziellen Bedürfnissen Ihrer Sicherheitsstrategie exakter angepaßt werden.

Application Level Gateways arbeiten nach folgendem Prinzip:

- Annahme einer Verbindungsanforderung
- Prüfung dieser Verbindungsanforderung anhand des Regelwerkes auf Zulässigkeit
- Bei Zulässigkeit baut das Application Level Gateway die Verbindung zum gewünschten Ziel auf und vermittelt die Verbindung zwischen Quelle und Ziel

Das besondere des Application Level Gateway ist die permanente Überwachung des Netzwerkverkehrs. Dies wird durch die Zwischenschaltung des Gateways erreicht. Direkte Punkt-zu-Punkt Verbindungen sind nicht mehr möglich, da sich zwischen den Kommunikationspartnern immer das ALG befindet.

Die gesamte Verbindung, also sämtliche empfangene Pakete, werden auf Schicht sieben des OSI-Referenzmodells „angehoben“ und bewertet. Dabei kann der Inhalt der einzelnen Pakete und die zugrundeliegende Applikation ermittelt werden. Das Application Level Gateway kann somit ganze Sessions überwachen und bei Auftreten von unlauteren Aktivitäten gezielt reagieren.

Der Hauptunterschied zu reinen Paketfilter ist in folgenden Punkten begründet: Eine Untersuchung des Netzwerkverkehrs auf der Ebene der Applikationen (Schicht 7) ist möglich. Inhalte und Operationen des Netzwerkverkehrs können untersucht und gesteuert werden.

2.3.3 Hybridfirewall

Die beiden Firewallkonzepte, Paketfilter und Application Level Gateway, besitzen Vor- und Nachteile.

Paketfilter sind sehr effizient und ermöglichen einen hohen Netzwerkdurchsatz. Die Möglichkeiten der Steuerung und Kontrolle des Netzwerkverkehrs aufgrund des Inhalts sind begrenzt.

Application Level Gateways besitzen die Fähigkeit der exakten Analyse des Netzwerkverkehrs auf Anwendungsschicht. Ihr vordringlichster Nachteil ist der Performanceverlust innerhalb des Netzwerkverkehrs. Die dafür benötigten Maschinen müssen eine relativ hohe Rechenleistung aufweisen können, um die Untersuchung des Netzwerkverkehrs mit akzeptabler Verzögerung durchführen zu können.

Um dennoch ein performantes und sicheres System bereitstellen zu können, wurden die beiden Firewallkonzepte gemischt. Diese Mischung, oder besser Symbiose, bezeichnet man als Hybridfirewalls. Sie stellen einen akzeptablen Kompromiß zwischen den einzelnen Anforderungen an ein Firewallsystem, besonders hinsichtlich Performance und Sicherheit dar.

Bei Hybridfirewalls kommt eine Weiterentwicklung der einfachen Paketfilter zum Einsatz, die sogenannte Stateful Inspection. Diese ermöglicht die Erkennung der Kommunikation zugrunde liegenden Applikationstypen.

2.3.4 Stealth Gateway

Einen spezieller Typ Firewall wird durch die Stealthtechnologie bereitgestellt.

Das Stealth Gateway arbeitet auf Schicht zwei des OSI-Referenzmodells (Sicherungsschicht). Das Besondere dieses Konzeptes liegt in dem virtuellen „Nichtvorhandensein“ dieser Firewall begründet. Eine Stealthfirewall arbeitet auf dem zu untersuchenden Netzwerk ohne eigene, erkennbare IP-Adresse und kann somit von Angreifern erst einmal nicht wahrgenommen und somit nicht angegriffen oder umgangen werden.

Die Stealthtechnologie kommt häufig als sogenannte „vorgeschaltete Firewall“ zum Einsatz. Sie unterstützt dahinter liegende Firewallsysteme durch eine vorherige Selektion des Netzwerkverkehrs.

2.4 Funktionalitäten

Verschiedene Anbieter von Firewallsystemen bieten unterschiedliche Funktionalitäten an. Wichtige Funktionalitäten werden an dieser Stelle aufgeführt und kurz erläutert:

2.4.1 Eigenständiges Betriebssystem

Einige Hersteller liefern für ihre Firewallsysteme spezielle Betriebssysteme aus. Der Vorteil dieser Systeme liegt im verminderten administrativen Aufwand, da das System nicht separat gepflegt werden muß. Angreifer haben in der Regel geringe Kenntnisse über den Aufbau und die Schwachstellen solcher Systeme und somit wenige Angriffspunkte.

2.4.2 Integrierte Benutzerverwaltung

Heutige Firewallsysteme (mit Ausnahme der Stealthtechnologie) ermöglichen eine eigene Benutzerführung. Der Vorteil liegt in der strikten Trennung von allgemeiner und sicherheitsrelevanter Benutzerführung. Spezielle Bedeutung hat diese Funktionalität in Bezug auf Virtual Private Networks. Für den Remote-Zugriff auf das System können speziellere Regeln und Restriktionen aufgebaut werden und erhöhen somit die Sicherheit des Gesamtsystems.

2.4.3 Paketfilter

Paketfilter ermöglichen die Untersuchung des Netzwerkverkehrs aufgrund von einfachen Informationen der einzelnen Pakete, wie Quelladresse und Zieladresse sowie bestimmten TCP/IP-Ports. Dabei kann der Weg der Pakete beeinflußt werden. Paketfilter haben auf den Inhalt der zu übermittelnden Daten keinen Zugriff, da sie die Pakete nicht logisch verbinden können.

2.4.4 Application Level Gateway

Application Level Gateways untersuchen den Netzwerkverkehr auf der Applikationsebene. Somit haben sie Zugriff auf den Inhalt der einzelnen Pakete und können gezielt Angriffe durch Begrenzung der erlaubten Operationen und schädliche Inhalte abwehren.

2.4.5 Stateful Inspection

Stateful Inspection ist eine Weiterentwicklung der Paketfilter.

Der Nachteil reiner Paketfilter ist die Beschränkung auf die Untersuchung der einzelnen Pakete des Netzwerkverkehres. Dem Paketfilter war es nicht möglich, die zugrunde liegende Applikation zu erkennen.

Stateful Inspection ermöglicht dies durch das Anlegen einer Geschichte (History) der einzelnen Pakete in einer Tabelle. Die Methode der Stateful Inspection schließt aus dieser History der einzelnen Pakete (auf der Basis logischer Verknüpfungen) auf den zugrunde liegenden Anwendungstyp der Verbindung. Durch die Ermittlung des Anwendungstyps kann das Regelwerk spezieller angepaßt werden.

2.4.6 Virtual Private Networks

Virtuelle Netzwerke verbinden zwei Lokationen miteinander, wobei eine sichere Verbindung im Vordergrund steht. Die dabei zum Einsatz kommende Verbindung wird verschlüsselt. Werden VPN's über das Internet aufgebaut, so nutzt man vornehmlich die Technik des IP-Tunnelings. Dabei wird zwischen den beiden Kommunikationspartner ein sicherer Tunnel, mittels Tunnelingprotokollen, aufgebaut. Dieser Tunnel ist durch einen festgeschriebenen Weg definiert.

2.4.7 Network Address Translation (NAT)

Hinter Address-Translation verbirgt sich die Möglichkeit der Nutzung eines definierten Bereichs von IP-Adressen, welcher nicht über das öffentliche Netzwerk geroutet, also weitergeleitet, werden kann. Die Technologie des NAT ermöglicht die Umsetzung von Internet IP-Adressen in nicht routingfähige, interne IP-Adressen. So kann zum Beispiel die gesamte interne Struktur hinter einer IP-Adresse verborgen werden. Dies erschwert Angreifern die Ermittlung der internen Strukturen und somit die Ausnutzung von Schwachstellen.

Address-Translation bietet bereits einen geringen Schutz vor Zugriffen, da die einzelnen Rechner nicht mehr direkt mit dem Internet verbunden sind.

2.4.8 Regelwerke

Die Funktionen einer Firewall, welche das Auditverhalten und die Aktionen steuert, müssen definiert werden. Hierzu gehört die Definition der folgenden Komponenten:

- zu überwachende Objekte
- zu überwachende Protokolle
- zu überwachende Dienste
- Alarmfunktionen
- Aktivitäten der Firewall bei Verstoß gegen das Regelwerk.

Das Regelwerk ist eine Zusammenfassung von Definitionen erlaubter und nicht erlaubter Aktivitäten von Verbindungen über die Firewall. Die Erstellung eines solchen Regelwerkes setzt ein ausgereiftes Sicherheitskonzept voraus.

Wichtige Anforderungen an ein solches Regelwerk sind:

- Alles ist verboten, was nicht ausdrücklich erlaubt wird. Alle nicht erwünschten Dienste und Protokolle sind zu deaktivieren.
- Wenige, aber dafür sehr effiziente Regeln, an der Häufigkeit von Zugriffen orientiert.
- Keine Inkonsistenzen innerhalb des Regelwerkes.

2.5 Grenzen der Sicherheit

Die Firewall ist kein Garant für ein sicheres System. Verschiedene Umgebungsvariablen der Firewall können das Sicherheitskonzept schwächen oder gar unterlaufen. Das schwächste Glied in der Sicherheitskette spiegelt das Sicherheitsniveau der Gesamtkonzeption wider.

2.5.1 Betriebssystem

Für viele Firewallsysteme stellt das zugrundeliegende Betriebssystem die größte Schwäche dar. Ein Angreifer macht sich in diesem Fall die Schwachstellen des Betriebssystems zunutze, um die Firewall zu umgehen oder gar auszuschalten.

Um diese Lücke zu schließen, sind folgende Punkte zu beachten:

- Deaktivierung aller nicht benötigten Dienste und Server
- Keine Installation fremder Applikationen (Eine Firewall sollte immer auf einem dedizierten System laufen.)
- Jedes System hat Schwächen. Aus diesem Grund müssen alle Lücken des Systems, welche durch den Hersteller oder externe Quellen bekannt werden, geschlossen werden.
- Das System muß gezielt kontrolliert werden.

2.5.2 Installierte Komponenten, Dienste und Server

Auf einem Firewallsystem sollte immer nur die Firewall an sich zum Einsatz kommen. Zusätzliche Software, Dienste und Server setzten die Sicherheit des Gesamtsystems durch eventuelle Inkonsistenzen des Systems herab.

Aus diesem Grund sollte das Firewallsystem als dediziertes System betrieben werden.

2.5.3 Das Produkt Firewall

Nicht nur Betriebssysteme und Applikationen weisen Schwächen auf. Auch die Software des Firewallsystems kann mitunter Fehler haben.

Diese Schwächen werden, so zeigen es Untersuchungen, sofort und sehr intensiv ausgenutzt. Aus diesem Grund ist ein Änderungsmanagement für die Firewall unbedingt notwendig. Dieses kontrolliert und überwacht die Aktualität des Firewallsystems und paßt es bei gegebenen Umständen an. Um die Sicherheit nicht zu gefährden, müssen alle bekannten Schwächen innerhalb kürzester Zeit behoben sein.

2.5.4 Die Systemumgebung

Häufig betreiben Unternehmen und Institutionen, neben dem offiziellen Zugang über das Internet, Remote-Zugänge. Über diese Zugänge bekommen Außendienstmitarbeiter Zugriff auf die internen Ressourcen.

Sobald diese Zugänge nicht in das Konzept der Firewall mit eingebunden sind, stellen sie eine Herabsetzung der gesamten Sicherheit Ihrer Informationssysteme dar.

Mittels dieser Zugänge ist es möglich, sämtliche Sicherheitsmechanismen der Firewall und des dahinter verborgenen Sicherheitskonzepts zu unterlaufen. Die Sicherheit der Firewall wird durch das schwächste Glied in der Kette (in diesem Fall der Remote-Zugriff) ad absurdum geführt. Aus diesem Grund sind auch diese Zugänge in das Sicherheitskonzept und in die Firewall zu integrieren. Eine Möglichkeit bilden Virtual Private Networks mittels Verschlüsselung und definierter Vertrauensstellung.

2.6 Die Schwäche „Mensch“

Die größte Schwäche und der wahrscheinlichste Angriffspunkt eines Firewallsystems ist der Mensch. Ob Fehler oder Absicht, die meisten Systeme werden durch den Menschen, der sie bedient und nutzt, unsicher und geschädigt.

2.6.1 Der Administrator

Auf den Administratoren von Firewallsystemen ruht eine große Verantwortung. Sie sind in aller Regel für die technische Umsetzung des Sicherheitskonzeptes zuständig. Dabei können folgende Schwachstellen produziert werden:

- Das Regelwerk ist zu komplex. Dadurch bilden sich Inkonsistenzen im Regelwerk, welche nicht mehr erkannt werden können, und setzten die Gesamtsicherheit herab. Scheinbare Verbote überlappen sich und erlauben dadurch unerwünschte Aktivitäten.
- Das Betriebssystem ist nicht ausreichend abgesichert worden. Dabei wird die Annahme, eine Firewall alleine schaffe Sicherheit, fehlinterpretiert.
- Der Verantwortliche für das Firewallsystem mißbraucht seine Stellung, konfiguriert Fehler und Schlupflöcher in die Firewall. Um diese Gefahr zu minimieren ist der Einsatz von mehreren Verantwortlichen notwendig. Zudem kann man das Konzept der Firewall und die reale Umsetzung dieses Konzepts von externen Stellen überprüfen lassen.

2.6.2 Der Benutzer

Der Benutzer stellt in zweifacher Hinsicht eine Gefahr für die Sicherheit der IT dar.

2.6.2.1 Fehler des Benutzers

An dieser Stelle sind allgemeine Fehler des Benutzers gemeint, welche die Sicherheit aufweichen. Durch Fehler in der Handhabung, gepaart mit Fehlern in der Konfigurationen der Firewall, können Sicherheitslöcher entstehen.

Das Zusammenspiel von inkonsistenten Regeln, einem ungenügenden Sicherheitskonzept und einem unbedarften Benutzer kann das Sicherheitskonzept einer Firewall zunichte machen. In vielen Konzepten wird neben einem Regelwerk für die Firewall auch ein

Regelwerk für den Benutzer aufgestellt. Paradebeispiel ist das Verbot des Öffnens von aktiven Inhalten in einer E-Mail. Hält sich der Benutzer nicht an diese Regel können z.B. Trojanische Pferde, welche das Ausspionieren des Netzwerkverkehrs ermöglichen, im Netzwerk ihr Unwesen treiben.

2.6.2.2 Angriffe des Benutzers

In den häufigsten Fällen von Angriffen stammen diese von internen Benutzern.

Folgende Beispielaktivitäten von internen Benutzern können Schaden verursachen:

- Installation eines Modems oder einer ISDN-Karte für den externen Zugriff. Damit werden die aufgestellten Regeln der Firewall, welche auch die Aktivitäten der Benutzer einschränken können, außer Kraft gesetzt
- Installation von Snifferprogrammen oder Trojanischen Pferden

Der interne Benutzer umgeht damit Auflagen und Regeln, welche für einen sicheren Zugang zum Internet sorgen und die internen Ressourcen schützen sollen.

Viele Administratoren und IT-Verantwortliche unterschätzen diese Gefahr und planen sie aus diesem Grund nicht in das Sicherheitskonzept ein. In diesen Fällen stellt die Firewall nach außen eine undurchdringliche Mauer dar, von innen kann die Firewall jedoch ungehindert unterlaufen werden.

Die Entdeckung dieser internen Angriffe und Schwachstellen gestaltet sich relativ schwierig, da eine Unterscheidung zwischen Erlaubtem und Verbotenem aufgrund des hohen Netzwerkverkehrs fast unmöglich ist.

2.6.3 Der Angreifer

Der Angreifer versucht das Firewall-System durch intelligente Angriffe zu unterlaufen oder zu zerstören. Somit verschafft er sich Zugriff auf interne Ressourcen und kann diese für seine Zwecke mißbrauchen. Um dies zu erreichen, erkundigt er sich nach bekannten Schwachstellen des Firewallsystems, des Betriebssystems oder versucht Schwachstellen innerhalb des Sicherheitskonzepts zu erkennen. Diese Schwachstellen nutzt der Angreifer, um das System zu umgehen und Daten auszuspionieren oder zu schädigen.

Nicht alle Angreifer haben die Zerstörung eines Systems zum Ziel. Im wesentlichen kann man zwischen folgenden Angreifern unterscheiden:

- Der allgemeine Hacker versucht ein bestehendes Sicherheitssystem zu umgehen. Dabei sind Datendiebstahl oder Zerstörung nicht der Hauptantrieb.
- Professionelle Auftragshacker zielen hingegen direkt auf den Datendiebstahl oder die Zerstörung der Systeme ab.

2.7 Adaptive Sicherheit

Beschäftigt man sich mit dem Thema der Netzwerksicherheit und dem Einsatz von Firewalls wird schnell klar, daß diese Sicherheit nicht ausreichend ist.

Gerade Angriffe von innen sind relativ schwer zu erkennen. Das System, das Konzept und die Benutzer können unter Umständen gravierende Schwachstellen darstellen. Die Entwicklung seitens der Angreifer wird zunehmend schneller und effizienter.

Da die Informationstechnologie mit ihren Diensten und Ressourcen in vielen Fällen das Rückrat von Firmen, Organisationen und Institutionen darstellt, muß über eine weitergehende Sicherheit nachgedacht werden.

Aus diesem Grund gewinnt das Thema „Sicherheit jenseits der Firewall“ immer mehr Bedeutung. Die Methodik des Erkennens von Schwachstellen und Angriffen bezeichnet man als Intrusion Detection.

3 Intrusion Detection

3.1 Grundlagen

Es existieren vielfältige Definitionsansätze des Begriffs *Intrusion Detection* (ID). Sicherlich ist jedem Leser und jeder Leserin bewußt, was mit ID gemeint ist. Dennoch sollen an dieser Stelle die Begriffe *Intrusion* und *Intrusion Detection* definiert und abgegrenzt werden, um Mißverständnisse auszuschließen.

Intrusion ist eine Abfolge verwandter, mutwilliger Aktionen eines Angreifers mit dem Ziel, unberechtigt sicherheitsrelevante Zugriffe auf einen Computer oder ein Netzwerk zu erhalten.

Intrusion Detection ist der *Prozeß*, diese böswilligen Aktionen zu *identifizieren* und entsprechend der Aktionen zu *reagieren* und zusätzlich potentiellen Angriffen *vorzubeugen*.

Intrusion Detection beinhaltet somit folgende Aspekte:

1. **Prävention**
   Potentielle Angriffsversuche werden *proaktiv* abgewehrt.
2. **Entdeckung**
   Angriffe, die nicht abgewehrt werden können, werden erkannt.
3. **Reaktion**
   Nach einem Angriff bzw. bei verdächtigen Vorgängen werden angemessene Handlungen ausgeführt.

Im folgenden wird von diesem weit gefaßten Begriff von Intrusion Detection ausgegangen, der nicht nur Entdeckung und Reaktion beinhaltet, sondern zudem die proaktive Präventi-

on einschließt. Eine Firewall kann gemäß dieser Definition als Teilbereich des Intrusion Detection aufgefaßt werden.

3.2 Methoden

In den folgenden Abschnitten werden die Methoden, die in einem Intrusion Detection System (IDS) Anwendung finden, näher erläutert. Um es bereits an dieser Stelle vorwegzunehmen: Es gibt zur Zeit kein kommerzielles IDS, das alle im folgenden beschriebene ID-Methoden bietet. Auch bereits bestehende Ansätze lassen sich nicht sinntragend kombinieren, so daß auf diese Weise ein umfassendes IDS erreicht werden kann.

3.2.1 Audit Trail Processing

Jedes Betriebssystem bietet die Möglichkeit, z.B. System- und Benutzeraktionen in Log-Files abzulegen. Meist beinhalten diese Log-Files sicherheitsrelevante Sachverhalte wie z.B. Anmelde- bzw. Abmeldezeiten, Änderungen an der Berechtigungsstruktur usw. Beim Audit Trail Processing werden genau diese Logging-Informationen durch ein IDS untersucht. In der Sicherheitskonzeption kann anschließend spezifiziert werden, über welche Logging-Informationen und in welcher Tiefe das Audit Trail Processing durchgeführt wird. Das wird anhand des zu überwachenden Systems geschehen: Je wichtiger das betreffende System ist und je sensibler die dort gespeicherten Daten sind, desto mehr Aktionen werden auch überwacht werden und mittels Audit Trail Processing einer regelmäßigen Überprüfung unterzogen.

Es gilt allgemein, daß die Performance eines Systems um so mehr sinkt, je mehr Daten in Logfiles gespeichert werden müssen. Durch das Audit Trail Processing wird dieser Performance-Verlust zusätzlich erhöht.

Es sollte also sehr genau abgewogen werden, welche Daten in Logfiles gespeichert werden, und im zweiten Schritt, welche Logfile-Informationen zusätzlich überwacht werden sollen, um ein performantes System sicherzustellen.

3.2.2 On-the-Fly Processing

Beim on-the-fly Processing werden im Gegensatz zu dem oben beschriebenen Audit Trail Processing die Daten aus dem direkten Netzwerkverkehr gesammelt und in Echtzeit untersucht. Es wird deutlich, daß sich auch diese Methode negativ auf die Gesamtperformance des zu schützenden Systems auswirken kann. Das gilt insbesondere, wenn zu viele Daten aus dem laufenden Netzwerkstrom extrahiert und untersucht werden müssen. Diese ID-Methode sollte folglich nur für gezielte Systeme auf einer genau zu spezifizierenden – nicht zu breiten – Datenbasis Einsatz finden.

Verglichen mit dem Audit Trail Processing, das ja **bestehende** Logfiles untersucht, wird das on-the-fly Processing verwendet, um erste Anzeichen eines bevorstehenden Schadens nach Möglichkeit **vorauszusehen**. Betrachtet man die oben angegebenen Aspekte des Intrusion Detection, nimmt on-the-fly Processing einen Sonderfall ein zwischen Prä-

vention, die vor einem Angriff erfolgt und diesen idealerweise verhindert, und Entdeckung, die erst nach einem erfolgten Angriff möglich ist.

3.2.3 Profile of Normal Behavior

Die dritte Methode des Intrusion Detection besteht darin, festzulegen, welche Aktionen – von Benutzern und System – „normales“ Verhalten widerspiegeln. Diese zulässigen Aktionen werden in einer Knowledge Base abgelegt und definieren das entsprechende Profil. Ein systembezogenes Profile of Normal Behavior könnte beispielsweise die durchschnittliche Prozessorlast oder die durchschnittliche Anzahl der Benutzer enthalten. Weicht das tatsächliche Systemverhalten von diesem definierten Profil ab, könnte ein Angriff vorliegen, und die Administratoren haben die Möglichkeit einzuschreiten.

Diese Methode hat den Vorteil, daß im Vergleich zu der folgenden Methode der Signature of Abnormal Behavior keine Informationen zu bereits erfolgten Angriffen nötig sind. Ein IDS, das ein Profile of Normal Behavior einschließt, kann auch auf neue, bisher unbekannte Angriffe reagieren. Allerdings soll an dieser Stelle nicht verschwiegen werden, daß ein solches Profile of Normal Behavior schwer zu ermitteln ist. Meist müssen statistische Auswertungen über ein repräsentativen Zeitraum herangezogen werden.

3.2.4 Signature of Abnormal Behavior

Nach geglückten Systemangriffen werden die Vorgehensweise und Methodik des Angreifers oftmals dokumentiert. Hacker sind auf sich stolz und beschränken sich nicht nur darauf, aufzuzeigen, welches System sie „geknackt“ haben, sondern geben gelegentlich auch preis, wie ihnen der Angriff möglich wurde. Diese Vorgehensweise bietet einen Ansatz für die Signature of Abnormal Behavior. Aber nicht nur für Angriffe von außen eignet sich diese Methode: Es ist mehr als verdächtig, wenn ein Mitarbeiter der Marketingabteilung immer wieder versucht, Zugriff auf die Gehaltsdatenbank der Personalabteilung zu erlangen.

Wie bereits im vorigen Abschnitt beschrieben, sind jedoch für diese Methode Kenntnisse unautorisierten Verhaltens nötig. Alles, was nicht in der Knowledge Base als abnormal behavior definiert wurde, ist zunächst einmal unverdächtig und zugelassen.

Ein IDS, das sich nur auf diese Methode der Erkennung beschränkt, müßte ständig aktualisiert werden, und stünde dennoch hilflos neuen Angriffstaktiken gegenüber.

3.2.5 Parameter Pattern Matching

Eng verwandt mit der Methode des Abnormal Behavior ist das Parameter Pattern Matching. Meist setzt dieses Verfahren direkt auf den Netzwerkpaketen auf und durchsucht diese nach verdächtigen Inhalten, wie beispielsweise „del *.*“, „/etc/passwd“ oder bekannten Virensignaturen, wie sie auch bei Virenscannern eingesetzt werden. Sobald diese Zeichenketten bemerkt werden, kann ein Administrator alarmiert werden, oder der Port, über den diese Zeichenkette übertragen wurde, kann geschlossen werden.

3.2.6 Zusammenfassung

Jede der vorgestellten Methoden besitzt ihre Vor- und Nachteile. Ein ideales Intrusion Detection System würde alle fünf Methoden integrieren. Jedoch gibt es dieses ideale IDS nicht – noch nicht. Tatsächlich wird intensiv daran gearbeitet, ein solches System zu schaffen. Es wird jedoch noch einige Zeit dauern, bis alle Methoden gleichzeitig angewendet werden können. Erste Ansätze sind in den derzeit erhältlichen Firewall-Lösungen sichtbar. Zusätzlich zur der eigentlichen Firewall gibt es Zusatzmodule, die beispielsweise E-Mails auf verdächtige Inhalte untersuchen. Bei diesen Untersuchungen finden Parameter Pattern Matching-Methoden Anwendung.

Es bleibt abzuwarten, wann ein marktreifes IDS erscheinen wird. Wir gehen davon aus, daß das frühestens in zwei bis drei Jahren der Fall sein wird.

4 Fazit

4.1 Firewall-Anwendung

Firewallsysteme und ihre Möglichkeiten werden immer noch zu hoch bewertet. Die Installation einer Firewall stellt in keinster Weise die Sicherheit her, die heute von Sicherheitssystemen gefordert werden müssen. Dazu gehören Vorbeugung, Erkennung und das Handeln in der Gesamtheit des Sicherheitskonzepts. Firewalls stellen eine vorbeugende Maßnahme gegenüber unautorisierten Zugriffen und Angriffen dar. Da sich die Techniken der Hacker ebenso wie die Techniken der Firewall in einer stetigen Entwicklung befinden, muß über die Implementation von zusätzlichen Mechanismen der Erkennung und des proaktiven Handelns nachgedacht werden. Dieser Weg wird durch die Entwicklung von Intrusion Detection Systemen beschritten. Das Zusammenspiel von vorbeugendem Schutz (Firewall) und proaktiver Schwachstellenanalyse (Intrusion Detection System) ermöglicht eine höhere Qualität der Sicherheitsmechanismen innerhalb eines Informationssystems.

4.2 Intrusion Detection

Intrusion Detection Systeme sind zur Zeit Gegenstand der Forschung. Zwar werden einige ID-Methoden durch heute erhältliche Softwareprodukte bereits verwendet. Es ist jedoch nicht möglich, diese Produkte gegenseitig zu integrieren und so ein umfassendes IDS zu erhalten.

4.3 Ergebnis

Um es vorweg zu nehmen: Optimale IT-Sicherheit gibt es nicht und wird es auch niemals geben. Es wird immer ausgesprochen kreative Menschen geben, deren Berufung es zu sein scheint, in scheinbar sichere Systeme einzudringen, wohlgemerkt ohne dabei Scha-

den anrichten zu wollen. Und das ist gut so: Viele Sicherheitslöcher sind durch diese Hacker aufgedeckt worden. Die Problematik besteht jedoch in den beabsichtigten Schäden, der Spionage und den „Nachahmungstätern“, die sehr wohl kriminelle Hintergedanken besitzen.

Wenn Sie ihre IT sicher machen wollen, führt zur Zeit nichts an einer guten Firewall mit entsprechenden Zusätzen wie E-Mail-Überwachung vorbei, die jedoch auch kontinuierlich gewartet werden muß.

Die Arbeit eines echten IDS muß zur Zeit noch weitestgehend durch Systemadministratoren erfolgen, die über entsprechende Erfahrungen und Skills verfügen.

5 Anhang

5.1 Literatur

Amoroso, Edward: *Intrusion Detection, an introduction to Internet surveillance, correction, traps, trace-back, and response.* New Jersey 1999.

Escamilla, Terry: *Intrusion Detection, Network Security Beyond the Firewall*. Wiley Computer Publishing, 1998.

Hoffmann, Jens: *Intrusion Detection (II): Angriffe systematisch verhindern, entdecken und verfolgen.* Connector Newsflash, Dezember 1998, siehe: http://www.connector.de/medien/newsflash/dez98/flashdez98h.html

Krause, Micki u. Harold F. Tipton (Hrsg.): *Handbook of Information Security Management 1999*. Auerbach 1999.

Ulrich, Jörg: *Intrusion Detection – Gesteigerte Sicherheit des Netzes durch systematische Kontrolle.* Vortrag Computas Fachkonferenz NetSiKom 1999.

Ulrich, Jörg: *Intrusion Detection (I): Sind Sie sicher?* Connector Newsflash, November 1998, siehe: http://www.connector.de/medien/newsflash/nov98/flash1198.html

5.2 Links

5.2.1 Intrusion Detection

- http://www.att.com/isc/team/amoroso.html
- http://www.intrusion.net
- http://www.cert.org/nav/recovering.html

5.2.2 Firewall

- http://pathit.com/wars/war_sec1.htm
- http://www.checkpoint.de
- http://www.sun.com/security/

Anmerkungen : Für Verweise auf URLs im Internet, die nicht in der Domain connector.de liegen, kann die dauerhafte Verfügbarkeit nicht gewährleistet werden. Dokumentnamen der Internet Drafts werden bei Neufassung mit neuen Versionsnummern versehen. Obsolet gewordene Drafts werden im allgemeinen nicht mehr verfügbar gemacht.

5.3 Urheberrecht