(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
1. April 2004 (01.04.2004)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2004/028107 A2

(51) Internationale Patentklassifikation[7]: H04L 29/06

(21) Internationales Aktenzeichen: PCT/EP2003/010120

(22) Internationales Anmeldedatum:
11. September 2003 (11.09.2003)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
102 41 974.4 11. September 2002 (11.09.2002) DE

(71) Anmelder und
(72) Erfinder: **KÄMPER, Peter** [DE/DE]; Ludwig-Thoma-Str. 9, 83229 Aschau in Chiemgau (DE).

(74) Anwalt: **DTS München**; St.-Anna-Str. 15, 80538 München (DE).

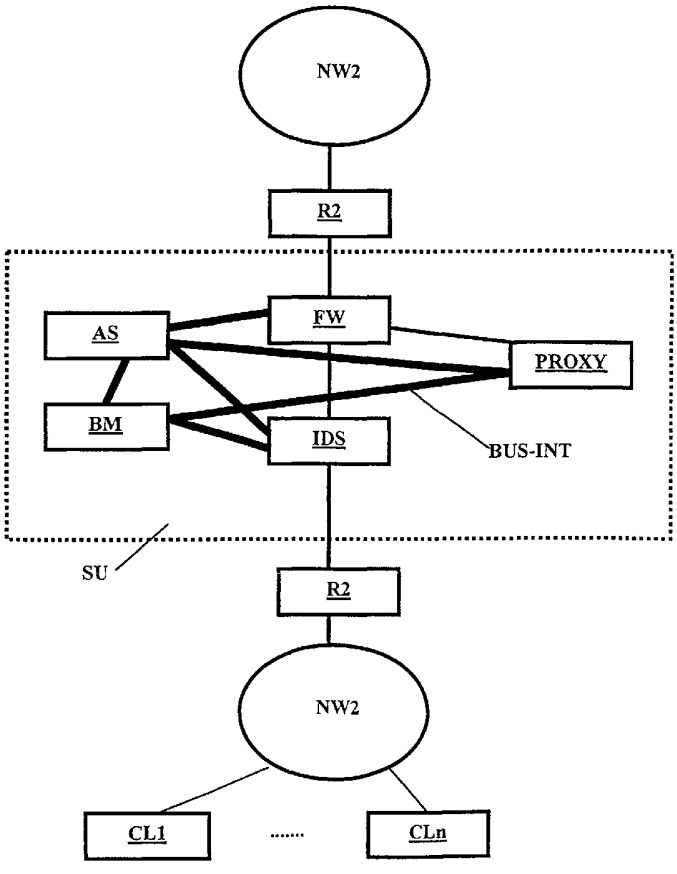
(81) Bestimmungsstaaten *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(regional)*: ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL,

[Fortsetzung auf der nächsten Seite]

(54) **Title:** MONITORING OF DATA TRANSMISSIONS

(54) **Bezeichnung:** ÜBERWACHUNG VON DATENÜBERTRAGUNGEN



(57) **Abstract:** The invention relates to a monitoring system for monitoring the security of network-based data transmissions, comprising a computer system (AS-RS) for determining on the basis of first data, which are obtained from at least one system (FW, PROXY, IDS) for monitoring first data transmissions between a first network (NW1) and a second network (NW2) and which respectively characterize some of the first data transmissions, whether the data transmissions fulfill specified first security requirements.

(57) **Zusammenfassung:** Überwachungssystem zur Überwachung der Sicherheit netzwerkbasierter Datenübertragungen, mit einem Rechnersystem (AS-RS) zum Ermitteln aus von wenigstens einem System (FW, PROXY, ISS) zur Kontrolle von ersten Datenübertragungen zwischen einem ersten NETZWERK (NW) und einem zweiten NETZWERK (NW) erhaltenen ersten Daten, die jeweils einzelne der ersten Datenübertragungen charakterisieren, ob die Datenübertragungen vorgegebene erste Sicherheitsanforderungen erfüllen.

WO 2004/028107 A2

PT, RO, SE, SI, SK, TR), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— *ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

ÜBERWACHUNG VON DATENÜBERTRAGUNGEN

Gebiet der Erfindung

Die vorliegende Erfindung betrifft die Sicherheit bei netzwerkbasierten Datenübertragungen und insbesondere Sicherheitsaspekte bei Datenübertragungen zwischen wenigstens zwei Netzwerken, auch unter Berücksichtigung von Datenübertragungen innerhalb eines Netzwerks, die zur Übertragung in ein anderes Netzwerk vorgesehen sind.

Hintergrund der Erfindung

Um die Sicherheit bei Datenübertragungen zwischen zwei Netzwerken zu gewährleisten, werden üblicherweise als sogenannte "Firewalls" bezeichnete Systeme verwendet. Der Begriff "Netzwerk", wie er hier verwendet wird, umfasst einzelne oder mehrere Einheiten umfassende Anordnungen, beispielsweise in Form von Rechnersystemen, von und zu denen Daten übertragen werden können. Beispiele hierfür sind das Internet, Intranets, einzelne, beispielsweise als Personal-Computer ausgeführte Rechnereinheiten umfassende Anordnungen mit Einrichtungen oder damit verbundenen Vorrichtungen für Datenübertragungen zu und von anderen Systemen und dergleichen.

Eine Firewall dient im Wesentlichen dazu, nicht erwünschte, unzulässige Datenübertragungen von einem Netzwerk zu einem anderen Netzwerk zu verhindern. Im Allgemeinen schützt eine Firewall ein Netzwerk auch vor unerlaubten Zugriffen aus einem anderen Netzwerk, wobei hierfür üblicherweise für einen Zugriff erforderliche und/oder einen Zugriff einleitende Datenübertragungen aus einem anderen Netzwerk verhindert werden, wenn sie zu einem unerlaubten Zugriff führen würden.

Um unerwünschte, unerlaubte Datenübertragungen und Zugriffe zu verhindern und erwünschte, erlaubte Datenübertragungen und Zugriffe zuzulassen, verwendet eine Firewall im Allgemeinen eine sogenannte Paketfilterung. Bei netzwerkbasierten Datenübertagungen werden Daten im Allgemeinen paketweise übertragen, wobei die Pakete Informationen umfassen, die beispielsweise die Quelle der zu übertragenden Daten, das Ziel, zu dem die Daten übertragen werden sollen, zur Erstellung der zu übertragenden Daten verwendete Protokolle (z.B. Protokolle zur Erstellung von Textdokumenten, Grafikdokumenten, Video/Audio-Dokumente, ausführbaren Softwarecodes, beispielsweise in Form von Softwareprogrammen, und dergleichen) etc. Bei

einer Paketfilterung werden Regeln definiert, die beispielsweise Datenübertragungen von bestimmten Quellen und/oder zu bestimmten Zielen verhindern sollen. Gemäß solcher Regeln verhindert eine Firewall Datenübertragungen von einem Netzwerk zu einem anderen Netzwerk oder lässt solche zu. Da bei einer Paketfilterung zu übertragende Daten zumeist nicht selbst überprüft werden, ist es üblich, Filterregeln zu definieren, die eine Klassifizierung von Dateninhalten beispielsweise auf der Grundlage von bei der Erstellung zu übertragender Daten verwendeter Protokolle, zulassen. Auf diese Weise ist es beispielsweise möglich, mittels einer Firewall Datenübertragungen von Textdaten zuzulassen, während Daten, die einen ausführbaren Code oder Bilddaten umfassen, nicht übertragen werden.

Für Datenübertragungen zwischen zwei Netzwerken ist es oftmals erforderlich, in einem Netzwerk einen sogenannten Proxy zu verwenden, der Datenübertragungen von diesem Netzwerk zu einem anderen Netzwerk überhaupt erst ermöglicht. Folglich werden Proxy's oftmals auch als Sicherheitssysteme für Datenübertragungen verwendet. Da ein Proxy eines Rechnersystems, das den Proxy zur Kommunikation mit anderen Netzwerken oder Systemen benötigt, eine Voraussetzung für Datenübertragung von und zu diesem Netzwerk darstellt, kann der Proxy auch dazu verwendet werden, nur bestimmte Datenübertragungen zuzulassen bzw. zu verhindern. Beispielsweise ist es möglich, mittels eines Proxy's den Benutzer eines Netzwerks Zugriffe auf bestimmte von einem anderen Netzwerk bereitgestellte Dienste und/oder Daten zu ermöglichen. Hierfür können zum Beispiel im Zusammenhang mit den Diensten und/oder Daten des Netzwerks, auf das zugegriffen werden soll, verwendete Protokolle zugrundegelegt werden. Beispiele hierfür sind sogenannte HTTP-Proxy's und FTP-Proxy's, die lediglich Datenübertragungen gemäß HTTP bzw. FTP zulassen. Des Weiteren ist es bekannt, mittels eines Proxy's für einen Virenschutz bei Datenübertragungen zu sorgen.

Eine Firewall oder ein Proxy gewährleisten nicht, dass unerwünschte, nicht zulässige Datenübertragungen stattfinden. Um einen solchen, im Folgenden als Angriff bezeichneten Vorgang zu erkennen, ist es bekannt sogenannte "Intrusion Detection" Systeme (IDS) zu verwenden. Die Aufgabe eines IDS's besteht im Wesentlichen darin, die Verletzung von Sicherheitsbestimmung bzw. -anforderungen zu erkennen und entsprechende Gegenmaßnahmen einzuleiten. Um einen Angriff erkennen zu können, ist es erforderlich, dass ein IDS mit Informationen zu versehen ist, die angeben, woran ein Angriff zu erkennen ist. Üblicherweise setzen unberechtigte Dritte bestimmte, sich oftmals wiederholende Techniken ein, um einen Angriff durchzuführen. Das heißt, Angriffe auf ein Netzwerk erfolgen nach Mustern, die auf diesem Gebiet als Signaturen bezeichnet werden. Derartige Signaturen umfassen TCP-Port Scans, UDP-Port Scans, IP-Pakete mit falschen Parametern, tunneln, einkapseln, überfluten und dergleichen. Da diese Signaturen auf dem Gebiet bekannt sind, wird an dieser Stelle auf eine nähere Beschreibung verzichtet.

Auch wenn die zuvor genannten Systeme für eine gewisse Sicherheit bei Datenübertragungen sorgen, gibt es grundlegende Probleme, die die Sicherheit wesentlich beeinträchtigen. So werden beispielsweise sogenannte Log-Dateien erstellt, die einzelne Datenübertragungsvorgänge protokollieren. Im Allgemeinen wären in solchen Log-Dateien alle Datenübertragungsvorgänge aufgezeichnet, was es für einen Systemadministrator nahe zu unmöglich macht, bei einer Vielzahl von Datenübertragungsvorgängen diejenigen zu identifizieren, die einen Angriff auf ein Netzwerk darstellen. Des Weiteren ist es für einen Angreifer möglich, eine Log-Datei zu verändern, um einen Angriff zu verschleiern.

Des Weiteren ist es bei den zuvor genannten, bekannten Sicherheitssystemen nicht gewährleistet, dass die jeweiligen definierten Sicherheitsbestimmungen bzw. -regeln ab wann eine Datenübertragung zu verhindern ist und wann nicht, nicht abschließend vorab definiert werden können. Es ist zwar möglich, Charakteristika bekannter Angriffsverfahren zu definieren und dementsprechende Sicherheitsüberwachungsregeln aufzustellen. Diese Vorgehensweise greift aber nicht, wenn ein Angreifer eine einem den Sicherheitssystemen nicht bekannten Angriffsvorgang durchführt.

Die genannten Beispiele von Nachteilen bekannter Sicherheitssysteme bei Datenübertragungen zwischen Netzwerken sind lediglich als beispielhaft zu verstehen. Da die Probleme und Nachteile bekannter Sicherheitssysteme, zur Kontrolle von Datenübertragungen zwischen Netzwerken, auf dem Gebiet gut bekannt sind, wird an dieser Stelle auf eine nähere Diskussion verzichtet.

Aufgabe der Erfindung

Die Aufgabe der vorliegenden Erfindung besteht im Allgemeinen darin, Nachteile bekannter Sicherheitsmaßnahmen und -verfahren bei Datenübertragungen, insbesondere zwischen Netzwerken, zu beseitigen. Im Speziellen soll es die vorliegende Erfindung ermöglichen, die bei bekannten, als Firewall, Proxy und IDS bezeichneten Sicherheitssystemen existierende Nachteile vermeiden, um die Sicherheit bei Datenübertragungen zwischen Netzwerken zu erhöhen und darüber hinaus für anwendungsspezifische, individuelle und benutzerfreundliche Sicherheitslösungen zu sorgen.

Kurzbeschreibung der Erfindung

Der der zur Lösung der genannten Aufgabe zugrundeliegende Ansatz der vorliegenden Erfindung besteht im Allgemeinen darin, Systeme zur Überwachung, Kontrolle und Analyse von Datenübertragungen zwischen Netzwerken in einer Weise gemeinsam zu verwenden, die es erlaubt, die einzelnen Sicherheitsmaßnahmen unterschiedlicher Systeme sowie deren eigene Sy-

stemsicherheit zu erhöhen und andererseits Sicherheitsmaßnahmen unterschiedlicher Systeme so zu kombinieren und Synergieeffekte zu nutzen, dass die Sicherheit insgesamt erhöht wird und auch, vorzugsweise laufend, angepasst werden kann. Insbesondere erlaubt es die vorliegende Erfindung, einzelne Sicherheitssysteme in Abhängigkeit von einander und unter Berücksichtigung von Sicherheitsmaßnahmen, Datenüberwachungsergebnissen (z.B. in Form von entsprechenden Protokollen) und dergleichen einzelner Sicherheitssysteme an die aktuell gewünschten und erforderlichen Sicherheitsanforderungen anzupassen.

Hinsichtlich der Sicherheit von Sicherheitssystemen an sich verfolgt die vorliegende Erfindung den Ansatz, einzelne Sicherheitssysteme so auszuführen, dass sie im Wesentlichen nur die Mittel (z.B. Hardware und Software) aufweisen, die für ihren vorgesehenen Betrieb unmittelbar erforderlich sind. So ist es beispielsweise gemäß der vorliegenden Erfindung vorgesehen, dass zur Inbetriebnahme ("Booten") und zum eigentlichen Betrieb erforderliche Daten nicht in einzelnen Sicherheitsvorrichtungen lokal gespeichert, sondern zentral bereitgestellt werden. Des Weiteren ist es erfindungsgemäß vorgesehen, dass zum Betrieb erforderliche Softwareprogramme, beispielsweise in Form von Betriebssystemen, auf ein zum eigentlichen Betrieb erforderliches Mindestmaß reduziert sind. Darüber hinaus lehrt die folgende Erfindung, Daten und Informationen, die von einzelnen Sicherheitssystemen hinsichtlich von Datenübertragungen durch Netzwerke ermittelt/erzeugt werden, nicht in den entsprechenden Sicherheitssystemen lokal vorzuhalten, sondern zentral zu protokollieren. Hierbei kann eine mit einer Datenbank vergleichbare Einheit verwendet werden.

Zur Umsetzung des der vorliegenden Erfindung zugrundeliegenden Ansatzes, werden, wie in den Ansprüchen definiert, einzelne Sicherheitssysteme bereitgestellt, die, in Abhängigkeit ihrer Aufgabe, hinsichtlich der Sicherheit von Datenübertragungen zwischen Netzwerken erfindungsgemäß ausgeführt sind. Zum Aufbau eines erfindungsgemäßen Gesamtsicherheitssystems können einzelne oder mehrere erfindungsgemäße Sicherheitssysteme verwendet werden. Alternativ ist es möglich, ein vorhandenes Gesamtsicherheitssystem so zu modifizieren, dass es insgesamt oder wenigstens hinsichtlich sicherheitsrelevanter Komponenten erfindungsgemäß arbeitet. Entsprechendes gilt für die in den Ansprüchen definierten, erfindungsgemäßen Verfahren.

Insbesondere stellt die vorliegende Erfindung ein Überwachungssystem gemäß Anspruch 1, ein Datentypenkontrollsystem gemäß Anspruch 17, ein Dateninhaltskontrollsystem gemäß Anspruch 26, ein Datenübertragungskontrollsystem gemäß Anspruch 34, ein Steuerungssystem gemäß Anspruch 43 und eine Sicherheitsumgebung gemäß Anspruch 51 für netzwerkbasierte Datenübertragungen bereit.

Hierbei werden von den unten aufgeführten Begriffen jeweils folgendes umfasst:

Rechnersystem:	Einzelne Rechnersysteme, Personal Computer, Rechnercluster, Rechnernetzwerk, etc.
Netzwerk:	vernetzte Datenverbindungen, Kommunikationssysteme, Rechnersysteme, Router, Knoten, etc; das Internet; Verbindungen zwischen wenigstens zwei Netzwerken; etc.
Datenübertragungen charakterisieren Daten:	Sicherheitsprotokolle, Log-Dateien, Scripts, Verbindungsdaten, Kontrollinformationen, Kommunikationsanfragen, etc.
Sicherheitsanforderungen:	Definitionen von zulässigen Datenübertragungen, Dateitypen, Übertragungszeiten, Übertragungsraten, Datenquellen, Dateninhalten, Übertragungszielen, Verbindungsbestätigungen, Kontrolle von Verbindungen, Datenziele, Datenquellen, etc.
Speichereinheit:	nicht flüchtige Speicher, Festplatten, Streamer, Datenbanken, Hautspeicher, Caches, Speichermedien, etc.
Speicheruntereinheit:	siehe Speichereinheit
unterschiedliche Sicherheitszustände charakterisierende Angaben:	Daten, die Angriffe, Angriffsversuche, Einbrüche und dergleichen angeben; Angriffsmuster, Signaturen; etc.
Eingabeeinheit:	Tastatur, Maus, Mikrophon, Datenschnittstellen, (ISDN-Karten, Modems), Scanner, Zeicheneingabegeräte, Lichtgriffel, etc.
Anweisungen zur Steuerung des Betriebs eines Systems durch einen Benutzer:	Softwarecode, Eingabe einzelner/mehrer Befehle, Interaktive Benutzung eines Steuerungsprogramms, etc.

Schnittstelleneinheit:	Modems, Netzwerkkarten, Interfacegeräte- und Einrichtungen, etc.
Betriebsdaten:	Betriebssoftware, Softwarecode(teile), Betriebssystem(teile), Parameter für Software und Hardware, Scripts, Datenbankaufbau, Datenbankinhalte, Datenbanksteuerung, Treiber, Prozessdaten, Prozesssteuerung, Protokolle, Anwender- und Anwendungsdaten, etc.
Sicherheitsanforderungen charakterisierende Sicherheitsanforderungsdaten:	Daten, die Sicherheitsanforderungen (s.o.) definieren

Des Weiteren stellt die vorliegende Erfindung Verfahren gemäß den Ansprüchen ... bereit, die vorzugsweise zum Betrieb der zuvor genannten Systeme bzw. der zuvor genannten Sicherheitsumgebung verwendet werden.

Darüber hinaus stellt die vorliegende Erfindung Softwareprodukte gemäß den Ansprüchen ... bereit, die die Durchführung einzelner oder mehrerer Schritte einzelner oder mehrer erfindungsgemäßer Verfahren ermöglichen.

Weitere Merkmale und Vorteile der vorliegenden Erfindung ergeben sich jeweils aus entsprechenden, von den oben genannten Ansprüchen abhängigen Ansprüchen.

Kurzbeschreibung der Zeichnungen

Bei der folgenden Beschreibung bevorzugter Ausführungsformen der vorliegenden Erfindung wird auf die beigefügten Figuren Bezug genommen, von denen zeigen:

Fig. 1	eine schematische Darstellung einer erfindungsgemäßen Sicherheitsumgebung,
Fig. 2	eine schematische Darstellung eines erfindungsgemäßen Datentypenkontrollsystems,
Fig. 3	eine schematische Darstellung eines erfindungsgemäßen Dateninhaltskontrollsystems,

Fig. 4 eine schematische Darstellung eines erfindungsgemäßen Datenübertragungskontrollsystems,

Fig. 5 eine schematische Darstellung eines erfindungsgemäßen Überwachungssystems,

Fig. 6 bis 15 schematische Darstellungen unterschiedlicher Ansichten erfindungsgemäßer graphischer Benutzungsschnittstellen, und

Fig. 16 eine schematische Darstellung eines erfindungsgemäßen Steuerungssystems.

Beschreibung bevorzugter Ausführungsformen

Wie in Fig. 1 schematisch dargestellt, wird eine Sicherheitsumgebung SU für Datenübertragungen zwischen einem ersten Netzwerk NW1 und einem zweiten Netzwerk NW2 verwendet. Datenübertragungen können sowohl von dem Netzwerk NW1 zu dem Netzwerk NW2 als auch in umgekehrter Richtung erfolgen. Zu beachten ist hierbei allerdings, dass dabei, wie aus dem Folgenden ersichtlich, keine unmittelbare Datenverbindung zwischen den Netzwerken NW1 und NW2 besteht.

Im Folgenden wird, ohne damit eine Einschränkung zu beabsichtigen, angenommen, dass das erste Netzwerk NW1 ein als Intranet ausgeführtes Netzwerk ist. Neben einem für das erste Netzwerk NW1 verwendeten Router R1 umfasst das erste Netzwerk NW1 mehrere als Client CL1, ... CLn bezeichnete Rechnervorrichtungen. Datenübertragungen von und zu den Client's CL1, ..., CLn erfolgen hinsichtlich des zweiten Netzwerks NW2 über den Router R1. Datenübertragungen zwischen den Client's CL1, ..., CLn erfolgt innerhalb des ersten Netzwerkes NW1 über die in dieser Figur nicht bezeichneten Erfindung zwischen den Client's CL1, ..., CLn.

Des Weiteren wird im Folgenden angenommen, dass das zweite Netzwerk NW2 das Internet ist, wobei für Datenübertragungen von und zu dem zweiten Netzwerk NW" ein Router R2 vorgesehen ist.

Abweichend von Figur 1 ist es möglich, dass der Router R1 und/oder Router R2 in die Sicherheitsumgebung SU als Komponente derselben integriert ist (sind).

Daten, die von dem zweiten Netzwerk NW2 zu dem ersten Netzwerk NW1 übertragen werden sollen, werden, von dem Router R2 zu einem Datentypenkontrollsystem FW übertragen.
Das Datentypenkontrollsystem FW dient u.a. zur Paketfilterung von für Datenübertragungen

aus dem zweiten Netzwerk NW2 verwendeten Datenpaketen. Daher kann das Datentypenkontrollsystem FW in dieser Hinsicht mit einer Firewall verglichen werden.

Ein mit dem Datenkontrollsystem FW zusammenarbeitendes Dateninhaltskontrollsystem PROXY gilt als Stellvertreter-Server für Netzwerkdienste und/oder -protokolle wie z.B. HTTP, HTTPS, DNS, SMTP, FTP und dergleichen. Daher kann das Dateninhaltskontrollsystem PROXY in dieser Hinsicht mit einem Proxy-Server verglichen werden. Des Weiteren dient das Dateninhaltskontrollsystem PROXY dazu, IP-Datenströme zu trennen, über das Datentypenkontrollsystem FW übertragene Daten inhaltlich zu kontrollieren (z.B. hinsichtlich pornografischer Inhalte), Virenschutz bereitzustellen hinsichtlich von Datenübertragungen von und zu dem zweiten Netzwerk NW2 durchgeführte Aktivitäten zu protokollieren und dergleichen. Nach außen, d.h. seitens des zweiten Netzwerks NW2 ist lediglich die IP-Adresse des außenliegenden Routers R2 erkennbar. Das Dateninhaltskontrollsystem PROXY verrichtet, aus Sicht des zweiten Netzwerks NW2, seine Dienste anonym. Dies kann auch hinsichtlich des ersten Netzwerks NW1 zutreffen.

Ein von der Sicherheitsumgebung SU umfasstes Datenübertragungsanalysesystem IDS, das mit dem Datentypenkontrollsystem FW und dem Dateninhaltskontrollsystem PROXY zusammenarbeitet, dient zur Erkennung von bei unerlaubten Zugriffen bzw. Angriffen aus dem zweiten Netzwerk NW2 auf das erste Netzwerk NW1 verwendete Angriffsmuster oder Signaturen zu erkennen. In dieser Hinsicht ist das Datenübertragungsanalysesystem IDS mit einem bekannten Intrusion Detection System vergleichbar.

Mittels eines Überwachungssystems AS werden Protokolleinträge der Datentypenkontroll-, Inhaltskontroll- und Datenübertragungsanalysesysteme FW, PROXY, IDS, beispielsweise in Form von Log-Dateien, empfangen und gespeichert. Hierfür verwendet das Überwachungssystem AS eine in dieser Figur lediglich beispielhaft als baueinheitlich integriert dargestellte Datenbank, in der eine Protokollierung von Daten und/oder Informationen hinsichtlich von Datenübertragung protokolliert werden. Eine solche, unter anderem auch vom Gesetzgeber geforderte Protokollierung umfasst Angriffe/Einbrüche und Einbruchs/Angriffs-Versuche, Datenübertragungen zu dem ersten Netzwerk NW1 sowie von diesem über die Sicherheitsumgebung SU in ein anderes Netzwerk, beispielsweise das zweite Netzwerk NW2 und dergleichen.

Aufgrund seiner Aufgabe kann das Überwachungssystem AS auch als Audi-Server bezeichnet werden. Das Überwachungssystem AS kommuniziert mit den zuvor genannten System FW, PROXY und IDS über ein internes Bussystem BUS-INT oder eine damit vergleichbare Kommunikationsverbindung, das z.B. als Kommunikationsnetzwerk ausgeführt sein kann. Das interne Bussystem BUS-INT ist physikalisch von Kommunikationsverbindungen, beispielsweise in Form von Bussen, Kabeln und dergleichen, die für Datenübertragungen zwischen den Netz-

werken NW1 und NW2 bzw. den Routern R1 und R2 verwendet werden, physikalisch getrennt.

Die zentrale Verwaltung und Steuerung der zuvor genannten Systeme der Sicherheitsumgebung SU erfolgt mittels eines Steuerungssystems BM. Dementsprechend kann das Steuerungssystem BM auch als Boot- und Managementserver für die Sicherheitsumgebung SU bezeichnet werden. Auch das Steuerungssystem BM kommuniziert innerhalb der Sicherheitsumgebung SU über das interne Bussystem BUS-INT mit den anderen Komponenten.

Zur Erhöhung der Sicherheit kann, wie in Figur 1 veranschaulicht die Sicherheitsumgebung SU wenigstens teilweise redundant ausgeführt sein. Beispielsweise können zwei Datentypenkontrollsysteme, zwei Dateninhaltskontrollsysteme, zwei verwendet werden. Auch die für interne Kommunikationszwecke verwendeten Kommunikationsverbindungen innerhalb der Sicherheitsumgebung SU können mittels zweier interner Bussysteme redundant ausgeführt sein. Mittels der jeweils zweier Router für anstelle der Router R1 und R2 kann die Sicherheitsumgebung SU auch in dieser Hinsicht redundant ausgeführt werden.

Im Folgenden werden die einzelnen Komponenten einer Sicherheitsumgebung SU hinsichtlich ihres Aufbaus, ihres Betriebs und Ihres Zusammenwirkens detaillierter beschrieben. Dabei wird auf die nicht redundant ausgeführte Sicherheitsumgebung SU gemäß Figur 1 Bezug genommen, wobei die folgenden Ausführungen entsprechend für zwei- oder mehrfach ausgeführten Sicherheitsumgebungen entsprechend gelten.

DATENTYPENKONTROLLSYSTEM ("Firewall")

Das Datentypenkontrollsystem FW kontrolliert Datenströme zwischen dem zweiten Netzwerk NW2 und dem ersten Netzwerk NW1. Hierbei werden Datenpakete mit bestimmten Datentypen (z.B. Realaudio) und Datenpakete, die nicht identifiziert werden können standardmäßig nicht weitergeleitet. Diese sind dann auch nicht zu kontrollieren. Allerdings werden die Datenpakte protokolliert und zur Analyse, insbesondere hinsichtlich einer Angriffserkennung, verwendet. Ein vollständiges Blockieren von Daten ist ebenfalls möglich. Das Datentypenkontrollsystem FW lässt nur solche Datenpakete durch, deren Herkunft, deren Inhalt und deren Ziel vorgegebenen Regeln entsprechend.

Das Datentypenkontrollsystem FW ist mit einer Verkehrsampel vergleichbar. Die Ampel steuert lediglich den Verkehrsfluss, kontrolliert aber nicht den Inhalt der Wagen (hier Daten). Das bewerkstelligt das Datentypenkontrollsystem FW ebenfalls nicht, da dann der Verkehrsfluss (Datenübertragungen) nicht mehr möglich wäre. Eine Inhaltskontrolle bei Datenübertragungen erfolgt hier mittels des Dateninhaltskontrollsystems PROXY und des

Datenübertragungsanalysesystems IDS.

Wie in Fig. 2 dargestellt, umfasst das Datentypenkontrollsystem FW ein Rechnersystem FW-RS (z.B. mit einer einzenlen CPU (800 MHz, 512 MB), zwei externen NIC´s, einem internen "Boot"- NIC, einem internen "Proxy"- NIC). Hierbei sind Datenübertragungsgeschwindigkeiten von 2 Mbit bis 2 Gbit (Glasfaserverkabelung) vorgesehen.

Als Betriebssystem wird für das Datentypenkontrollsystem FW ein spezieller, sehr kleiner Unixkernel verwendet, bei dem nahezu alle nicht unbedingt erforderlichen Services entfernt sind. In erste Line wird nur ein Netzwerkartentreiber unterstützt. Wie unten ausgeführt, ist im Allgemeinen auch keine Unterstützung für Wiedergabe- und Eingabeeinheiten (z.B. Monitor, Maus, Tastatur etc.) vorgesehen. Dadurch wird der Kernel sehr schnell und sehr stabil und kann schnell aktualisiert werden ("Update"). Des weiteren kann der Kernel auch keinen fremden Code (z.B. bei einem Angriff) ausführen, da der Kernel hierfür keine Services vorhält. Vielmehr werden nur bekannte Soft- und Hardware unterstützt. Die daraus resultierende Inflexibilität des Datentypenkontrollsystems FW führt zu einer erhöhten Sicherheit.

Des weiteren kann das Datentypenkontrollsystem FW eine Schnittstelleneinheit FW-INT umfassen, z.B. in Form eines Modems oder einer Rechnerschnittstelle. Dies erlaubt eine Unterstützung des Datentypenkontrollsystems FW z.B. per Telefon. Um zu verhindern, dass auf das Datentypenkontrollsystem FW von einem der Netzwerke NW1 und NW2, insbesondere von dem Netzwerk NW2 als externem Netzwerk, zugegriffen werden kann, kann die Schnittstelleneinheit FW-INT so ausgeführt sein, dass nicht über eines dieser Netzwerke NW1 und NW2 erreichbar ist. Allerdings ist eine solcher "remote" Zugriff nur mit Genehmigung und Unterstützung eines Benutzers möglich, da die Schnittstelleinheit FW-INT im Normalfall ausgeschaltet. Bei Bedarf muss der Benutzer die Schnittstelleinheit FW-INT aktivieren und einen Zugriff auf das Datentypenkontrollsystem FW zu ermöglichen. Hierfür kann auch die Übermittlung eines Passworts erforderlich sein. Zur Kontrolle werden solch Vorgänge ebenfalls mittels des Überwachungssystems AS protokolliert. Nach Beendigung wird die Schnittstelleinheit FW-INT wieder deaktiviert, um weiter Zugriffe zu verhindern.

Die zentrale Steuerung und Verwaltung des Datentypenkontrollsystems FW erfolgt über das Steuerungssystem BM. Insbesondere kann die Benutzerverwaltung des Datentypenkontrollsystems FW nur lokal an dem Steuerungssystem BM selbst vorgenommen werden. Alternativ ist es auch möglich dies unmittelbar am Datentypenkontrollsystem FW vorzunehmen, wofür zusätzliche Einrichtungen, wie zum Beispiel eine Tastatur, ein Monitor und dergleichen, verwendet werden können. In beiden Fällen ist es erforderlich, unmittelabr zu dem Steuerungssystem BM bzw. dem Datentypenkontrollsystem FW zu gelangen, was schon physiklisch eine unerlaubte Modifikation das Datentypenkontrollsystems FW erschwert. Als

zusätzliche Sicherheit können weitere Maßnahmen ergriffen werden, wie z.B. eine Erfassung biometrischer Daten ("Fingerabdruck") und Eingabe von Pass- oder Codewörtern.

Das Datentypenkontrollsystem FW startet ("booted") vom Steuerungssystem BM aus. Neue Einstellungen, Betriebsmodi, Regel und dergleichen für das Datentypenkontrollsystem FW können mittels des Steuerungssystems BM zentral vorgenommen werden. Eine Besonderheit besteht darin, dass in einem Speicher des Datentypenkontrollsystems FW vorhandene Einstellungen, Betriebsparameter und dergleichen beim Booten nicht benutzt werden. Wie jedes Rechnersystem, ist es auch zum Betrieb des Datentypenkontrollsystems erforderlich, Dateien, Parameter, Daten, Informationen etc. für ein Betriebssystem des Datentypenkontrollsystems FW zu verwenden, um dieses zu betreiben. So werden beispielsweise Dateien verwendet, in denen Benutzerinformationen, Benutzernamen, Kennworte und dergleichen enthalten sind, die bei einer Kontrolle von Datenübertragungen von dem Datentypenkontrollsystem FW verwendet werden. Diese Dateien können beispielsweise eines Angriffs sein. Hierbei wird versucht, diese Dateien zu modifizieren. Sollte eine Modifikation durch einen Angriff erfolgreich durchgeführt worden sein, ist es weiterhin erforderlich, dass das Datentypenkontrollsystem FW erneut gestartet ("rebooted") wird, um die Änderungen dieser Dateien wirksam werden zu lassen. Bei herkömmlichen als Firewall dienenden Sicherheitssystemen würde dann auf die modifizierte Dateien zurückgegriffen werden, wodurch es einem Angreifer ermöglicht wird, aufgrund der geänderten Kontrollregeln, die Firewall zu überwinden.

Dies wird bei der Sicherheitsumgebung SU dadurch verhindert, dass die zum Betrieb des Datentypenkontrollsystems FW erforderlichen Informationen nicht lokal gespeichert werden, sondern von den Steuerungssystem BM zur Verfügung gestellt werden. Insbesondere werden zum Betrieb des Datentypenkontrollsystems erforderliche Informationen in einem Speicher des Steuerungssystems BM gespeichert. Beim Booten des Datentypenkontrollsystems FW wird dann auf solche Daten zurückgegriffen. Aufgrund der Verwendung des internen Bussystems BUS-INT, das von für Datenübertragungen zwischen den Netzwerken NW1 und NW2 verwendeten Kommunikationsverbindungen physikalisch getrennt ist, ist es einem Angreifer nicht möglich, auf das Steuerungssystem BM und insbesondere auf dessen Speicher zuzugreifen.

Für das Datentypenkontrollsystem werden Regeln oder Regelsätze definiert, gemäß derer Datentypenkontrollsystem FW Datenübertragungen aus dem zweiten Netzwerk NW2 zulässt oder verhindert. Solche Regelsätze definieren, wer von wo wohin welche Daten übertragen und auf welche Daten zugreifen kann. Üblicherweise werden solche Regeln in einer sogenannten flachen Datei gespeichert. Ein Nachteil dieser Vorgehensweise besteht darin, dass der mittels solcher in einer derartigen Datei gespeicherten Regeln definierte Schutz nicht in einzelne Regeln unterteilt werden kann. Dies hat im Allgemeinen zur Folge, dass eine Firewall dienende Sicherheitsvorrichtung nicht von unterschiedlichen Benutzern unterschiedlich administriert werden

kann.

Dies wird dadurch verhindert, dass zum Betrieb des Datentypenkontrollsystems FW vorgesehene Regelsätze in einer dem Steuerungssystem BM zugeordneten Datenbank vorhanden sind. In dieser Regelsatzdatenbank, die beispielsweise für mehrere Sicherheitsumgebungen SU verfügbar ist, werden einzelne Regeln oder Regelsätze definiert, gemäß derer Datentypenkontrollsysteme FW Datenübertragungen überwachen bzw. kontrollieren. Des Weiteren ist es vorgesehen, dass den einzelnen Regeln und Regelsätzen der Regelsatzdatenbank Informationen darüber zugeordnet sind, welche Sicherheitsumgebung welche Regeln und/oder Regelsätze verwenden darf. Dies betrifft auch Änderungen von Regeln und Regelsätzen der Regelsatzdatenbank, wie sie im folgenden im Zusammenhang mit Änderungen von Regeln und Regelsätzen für das Datentypenkontrollsystem FW beschrieben ist.

Regeln und Regelsätze werden anwendungsspezifisch erstellt. Mittels einer graphischen Benutzungsschnittstelle des Steuerungssystems BM können Regeln und Regelsätze eingegeben werden. Die Regeln und Regelsätze werden im Allgemeinen als sogenannte Scriptdatein von dem Steuerungssystem BM gespeichert. Eine Änderung von Regeln und Reglesätzen kann im Allgemein nicht unmittelbar an dem Datentypenkontrollsystem FW durchgeführt werden.

Von dem Datentypenkontrollsystem FW erstellte Protokollierungen werden, im Gegensatz zu bekannten Firewalls, ebenfalls nicht lokal gespeichert. Vielmehr werden über das interne Bussystem BUS-INT Protokollinformationen des Datentypenkontrollsystems FW beispielsweise in Form von Log-Dateien, zu dem Überwachungssystem AS übertragen und dort in einer Datenbank zur späteren Verwendung gespeichert. Dies macht es einem Angreifer unmöglich, auf von dem Datentypenkontrollsystem erstellte Protokollierungen zuzugreifen und diese zu verändern. D.h., dass ein Angreifer nicht in der Lage ist, seine "Spuren", d.h. seinen Angriff angebende Protokollierungen, zu verändern oder zu löschen. Es ist vorgesehen, dass die Protokollierung in Echtzeit erfolgt und die Daten verschlüsselt zum Überwachungssystem AS übertragen werden.

Wie unten näher erläutert, erlaubt es die Kombination von Protokollierungen mittels des Überwachungssystems AS sicherheitsrelvante Vorgänge besser zu erkennen, als dies herkömmlichen Firewalls möglich ist (z.B.:. Herr Müller darf HTTP-Übertragungen durch das Datentypenkontrollsystem FW durchführen. Bei einer herkömmlichen Firewall würde ein sich Herr Müller ausgebender Angreifer das Datentypenkontrollsystem FW durchdringen können, obwohl überhaupt keine Datenübertagungen von dem echten Herr Müller stammen, dieser z.B. nicht an an seinem Arbeitsplatz (PC) arbeitet. Dies wir aber von der Sicherheitsumgebung SU erkannt).

Im Fall eines Angriffs hat die Auslastung des Datentypenkontrollsystems FW eine entscheiden-

de Bedeutung, da dabei das Rechnersystem FW Rechenzeit zur Bearbeitung der Datenpakete benötigt. Je mehr Ressourcen vorhanden sind, desto besser und desto mehr Angriffe können von dem Datentypenkontrollsystem FW abgewehrt werden. Daher ist es vorgesehen, dass das Datentypenkontrollsystem FW im Normalfall in einem Bereich von 5 – 10 % und hinsichtlich seines Speichers bis zu 15 % ausgelastet ist. Dies stellt für Angriffe genügend Reserven zur Verfügung.

Bei Verwendung mehrerer Datentypenkontrollsysteme FW erfolgt eine Lastverteilung über das IP-Routing. Bei einer Lastverteilung ist insbesondere zu beachten, dass die im Falle eines Angriffs verfügbare Leistung des Datentypenkontrollsystems FW ausreicht, um einen Angriff zu erkennen und gegebenenfalls abzuwehren.

DATENINHALTSKONTROLLSYSTEM ("Proxy-Server")

Wie oben erläutert, ermöglicht das Dateninhaltskontrollsystem PROXY die Verbindungen von Außen nach Innen und umgekehrt, d.h. vom zweiten Netzwerk NW2 zum ersten Netzwerk NW1 und umgekehrt. Das Dateninhaltskontrollsystem PROXY erhält alle von dem Datentypenkontrollsystem FW durchgelassenen Daten, z.B. als HTTP-, FTP-, SMTP- und DNS-Pakete. Diese werden von dem Dateninhaltskontrollsystem PROXY hinsichtlich ihrer Inhalt untersucht und gegebenenfalls gefiltert. Hierbei können statische Filterverfahren verwendet werden. Hiefür können Worte und Begriffe, die eine besondere Bedeutung haben oder haben könnten, eingetragen (z.B. Worte mit pornographischer Bedeutunng, Wort mit geschäftlichem Bezug ("Geschäftsbericht", "Intern", "Vertraulich", etc.). Datenpakete mit solchen "unsauberen" und internen Inhalten können dann von dem Dateninhaltskontrollsystem PROXY erkannt werden. Dies gilt nicht nur für Datenübertragungen von dem zweiten Netzwerk NW2 zu dem ersten Netzwerk NW1 sondern auch in umgekehrter Richtung. Eine weitere Aufgabe des Dateninhaltskontrollsystems PROXY ist Virenschutz.

Von dem Dateninhaltskontrollsystem PROXY erstellte Protokollierungen werden ebenfalls nicht lokal gespeichert. Vielmehr werden über das interne Bussystem BUS-INT Protokollinformationen des Dateninhaltskontrollsystems PROXY beispielsweise in Form von Log-Dateien, zu dem Überwachungssystem AS übertragen und dort in einer Datenbank zur späteren Verwendung gespeichert. Dies macht es einem Angreifer unmöglich, auf von dem Datentypenkontrollsystem erstellte Protokollierungen zuzugreifen und diese zu verändern. Dies wird zusätzlich noch dadurch erschwert, indem für das Dateninhaltskontrollsystem PROXY lokale Firewalls vorgesehen sind. Es ist vorgesehen, dass die Protokollierung in Echtzeit erfolgt und die Daten verschlüsselt zum Überwachungssystem AS übertragen werden.

Wie unten näher erläutert, erlaubt es die Kombination von Protokollierungen mittels des

Überwachungssystems AS sicherheitsrelvante Vorgänge besser zu erkennen, als dies herkömmlichen Proxy-Servern möglich ist.

Wie in Fig. 3 dargestellt, umfasst das Dateninhaltskontrollsystem PROXY ein Rechnersystem Datentypenkontrollsystem PROXY-Rechnersystem. Als Betriebssystem wird für das Dateninhaltskontrollsystem PROXY ein spezieller, sehr kleiner Unixkernel verwendet, bei dem nahezu alle nicht unbedingt erforderlichen Services entfernt sind. Wie unten ausgeführt, ist im Allgemeinen auch keine Unterstützung für Wiedergabe- und Eingabeinheiten (z.B. Monitor, Maus, Tastatur etc.) vorgesehen. Dadurch wird der Kernel sehr schnell und sehr stabil und kann schnell aktualisiert werden ("Update"). Des weiteren kann der Kernel auch keinen fremden Code (z.B. bei einem Angriff) ausführen, da der Kernel hierfür keine Services vorhält. Vielmehr werden nur bekannte Soft- und Hardware unterstützt. Die daraus resultierende Inflexibilität des Dateninhaltskontrollsystems PROXY führt zur einer erhöhten Sicherheit.

Des weiteren kann das Dateninhaltskontrollsystem PROXY eine Schnittstelleneinheit PROXY-INT, z.B. in Form eines Modems oder einer Rechnerschnittstelle. Dies erlaubt eine Unterstützung des Dateninhaltskontrollsystems PROXY z.B. per Telefon. Um zu verhindern, dass auf das Dateninhaltskontrollsystem PROXY von einem der Netzwerke NW1 und NW2, insbesondere von dem Netzwerk NW2 als externem Netzwerk, zugegriffen werden kann, kann die Schnittstelleneinheit PROXY-INT so ausgeführt sein, dass nicht über eines dieser Netzwerke NW1 und NW2 erreichbar ist. Allerdings ist eine solcher "remote" Zugriff nur mit Genehmigung und Unterstützung eines Benutzers möglich, da die Schnittstelleinheit PROXY-INT im Normalfall ausgeschaltet. Bei Bedarf muss der Benutzer die Schnittstelleinheit PROXY-INT aktivieren und einen Zugriff auf das Dateninhaltskontrollsystem PROXY zu ermöglichen. Hierfür kann auch die Übermittlung eines Passworts erforderlich sein. Zur Kontrolle werden solch Vorgänge ebenfalls mittels des Überwachungssystems AS protokolliert. Nach Beendigung wird die Schnittstelleinheit PROXY-INT wieder deaktiviert, um weiter Zugriffe zu verhindern.

Die zentrale Steuerung und Verwaltung des Dateninhaltskontrollsystems PROXY erfolgt über das Steuerungssystem Steuerungssystem BM, die nur lokal an dem Steuerungssystem BM selbst vorgenommen werden. Alternative ist es auch möglich dies unmittelbar am Dateninhaltskontrollsystem PROXY vorzunehmen, wofür zusätzliche Einrichtungen, wie zum Beispiel eine Tastatur, ein Monitor und dergleichen, verwendet werden können. In beiden Fällen ist es erforderlich, unmittelabr zu dem Steuerungssystem BM bzw. dem Dateninhaltskontrollsystem PROXY zu gelangen, was schon physiklisch eine unerlaubte Modifikation das Dateninhaltskontrollsystems PROXY erschwert. Als zusätzlliche Sicherheit können weitere Maßnahmen ergriffen werden, wie z.B. eine Erfassung biometrischer Daten ("Fingerabdruck") und Eingabe von Pass- oder Codewörtern.

Das Dateninhaltskontrollsystem PROXY startet ("booted") vom Steuerungssystem BM aus. Neue Einstellungen, Betriebsmodi, Regel und dergleichen für das Dateninhaltskontrollsystem PROXY können mittels des Steuerungssystems BM zentral vorgenommen werden. Eine Besonderheit besteht darin, dass in einem Speicher des Dateninhaltskontrollsystem PROXY vorhandene Einstellungen, Betriebsparameter und dergleichen beim Booten nicht benutzt werden.

DATENÜBERTRAGUNGSKONTROLLSYSTEM ("IDS")

Das Datenübertragungskontrollsystem IDS umfasst, wie in Fig. 4 dargestellt ein Rechnersystem IDS-RE, Protokollinstanzen (nicht bezeichnet), eine Speichereinheit PROXY-MEM (z.B. in Form einer Datenbank) mit darin bereitgestellten Angriffsmustern und Signaturen.

Von dem Dateninhaltskontrollsystem PROXY erstellte Protokollierungen werden ebenfalls nicht lokal gespeichert. Vielmehr dient das Überwachungssystem AS als übergeordneter "Wächter", wofür Protokollinformationen des Dateninhaltskontrollsystems PROXY, beispielsweise in Form von Log-Dateien, über das interne Bussystem BUS-INT zu dem Überwachungssystem AS übertragen und dort in einer Datenbank zur späteren Verwendung gespeichert werden. Dies macht es einem Angreifer unmöglich, auf von dem Datentypenkontrollsystem erstellte Protokollierungen zuzugreifen und diese zu verändern. Dies wird zusätzlich noch dadurch erschwert, indem für das Dateninhaltskontrollsystem PROXY lokale Firewalls vorgesehen sind. Es ist vorgesehen, dass die Protokollierung in Echtzeit erfolgt und die Daten verschlüsselt zum Überwachungssystem AS übertragen werden. Es ist vorgesehen, dass das Datenübertragungskontrollsystem IDS Angriffsmuster anhand einer dynamischen Datenbank erkennt, die in vorbestimmten Abständen, z.B. alle vier Stunden, aktualisiert wird. Vorteilhafterweise erfolgt eine Aktualisierung automatisch.

Erkennt das Datenübertragungskontrollsystem IDS einen Angriff, kann dieser mittels das Datenübertragungskontrollsystems IDS und des Datentypenkontrollsystems FW verhindert werden. Angriffe charakterisierende Daten werden, falls erforderlich oder gewünscht, vorgefiltert an das Überwachungssystem AS übertragen, um z.B. auch für eine Information des Benutzers bzw. Betreibers der Sicherheitsumgebung SU zu sorgen.

Als Betriebssystem wird für das Datenübertragungskontrollsystem IDS ein spezieller, sehr kleiner Unixkernel verwendet, bei dem nahezu alle nicht unbedingt erforderlichen Services entfernt sind. Wie unten ausgeführt, ist im Allgemeinen auch keine Unterstützung für Wiedergabe- und Eingabeinheiten (z.B. Monitor, Maus, Tastatur etc.) vorgesehen. Dadurch wird der Kernel sehr schnell und sehr stabil und kann schnell aktualisiert werden ("Update"). Des weiteren kann der Kernel auch keinen fremden Code (z.B. bei einem Angriff) ausführen, da der Kernel hierfür keine Services vorhält. Vielmehr werden nur bekannte Soft- und

Hardware unterstützt. Die daraus resultierende Inflexibilität des Datenübertragungskontrollsystems IDS führt zur einer erhöhten Sicherheit.

Des weiteren umfasst das Datenübertragungskontrollsystem IDS eine Schnittstelleneinheit IDS-INT, z.B. in Form eines Modems oder einer Rechnerschnittstelle. Dies erlaubt eine Unterstützung des Datenübertragungskontrollsystems IDS z.B. per Telefon. Um zu verhindern, dass auf das Datenübertragungskontrollsystem IDS von einem der Netzwerk NW1 und NW2, insbesondere von dem Netzwerk NW2 als externem Netzwerk, zugegriffen werden kann, kann die Schnittstelleneinheit IDS-INT so ausgeführt sein, dass nicht über eines dieser Netzwerke NW1 und NW2 erreichbar ist. Allerdings ist eine solcher "remote" Zugriff nur mit Genehmigung und Unterstützung eines Benutzers möglich, da die Schnittstelleinheit IDS-INT im Normalfall ausgeschaltet. Bei Bedarf muss der Benutzer die Schnittstelleinheit IDS-INT aktivieren und einen Zugriff auf das Datenübertragungskontrollsystem IDS zu ermöglichen. Hierfür kann auch die Übermittlung eines Passworts erforderlich sein. Zur Kontrolle werden solch Vorgänge ebenfalls mittels des Überwachungssystems AS protokolliert. Nach Beendigung wird die Schnittstelleinheit IDS-INT wieder deaktiviert, um weiter Zugriffe zu verhindern.

ÜBERWACHUNGSYSTEM ("Audit-Server")

Die Hauptaufgabe des in Fig. 5 veranschaulichten Überwachungssystems AS ist das Speichern und Analysieren der empfangen Protokollierungen des Datentypenkontrollsystems FW, des Dateninhaltskontrollsystems PROXY und des Datenübertragungskontrollsystems IDS . Des weiteren erhält das Überwachungssystem AS Protokollierungen von dem Steuerungssystem Steuerungssystem BM, die verwendet werden können, um die von den zuvor genannten Kontrollsystemen Datentypenkontrollsystem FW, PROXY und IDS bereitgestellten Informationen zusätzlich auf Richtigkeit, Konsistenz und dergleichen überprüfen zu können.

Protokollierungen werden eine mit einer Datenbank vergleichbaren Speichereinheit AS-MEM geschrieben. Die Speichereinheit AS-MeM umfasst eine erste Speicheruntereinheit AS-MEM-RT, als "Real-Time"-Datenbank dient. Mittels dieser werden Protokollierung eines ersten Zeitraums gespeichert und analysiert. Dieser Zeitraum kann z.B. für aktuelle Protokollierungen ("inert der letzten 1, 2, 5, 10,.... Minuten") definiert sein. Mittels einer zweiten Speicheruntereinheit AS-MEM-LT können Protokollierung eines zweiten Zeitraums gespeichert werden, beispielsweise für einen Zeitraum der letzten 1, 2, 5, 10, 12 ... Monate. Zur Analyse von Protokollierungen können die ersten und zweiten Speicheruntereinheiten AS-MEM-RT und AS-MEM-LT getrennt oder in Kombination herangezogen werden.
Um unzulässige Datenbankzugriffe zu verhindern kommuniziert auch das Überwachungssystem AS über das interne Bus-System BUS-INT. Ein physikalischer Zugriff auf das Überwachungssystem AS besteht nur innerhalb an dem Überwachungssystem AS selbst ("im

EDV-Schrank")

Ferner umfasst das Überwachungssystem AS ein Rechnersystem AS-RS (z.B. mit einer Intel®-kompatiblen CPU, eventuell als Mehrfachprozessorsystem ausgeführt, mindestens einer RAID-5, einem internen NIC, mehreren externen NICs, einer VGA-Unterstützung, einer Unterstützung UNIX®-basierter Softwareanwendungen und dergleichen). Zur Bedienung des Überwachungssystems AS wird eine lokal angeordnete Eingabeeinheit AS-IN verwendet, die z.B. eine Tastatur, eine Maus, eine Mikrophon und dergleichen umfassen kann. Zur graphischen Wiedergabe von Protokllierungen selbst und/oder von Kontroll- und Analyseergebnissen hinsichtlich zu verwertender Protokllierungen weist das Überwachungssystem AS eine Wiedergabeeinheit Überwachungssystem AS-DIS (z.B. einen VGA-Monitor) und eine darüber darstellbare graphische Benutzungsschnittstelle AS-GUI auf. Beispiele unterschiedlicher Ansichten der graphischen Benutzungsschnittstelle AS-GUI sind in Fig. 6 bis 15 zu sehen.

Zur Speicherung der Protokollierungen erforderliche Speichermedien (z.B. Festplatten) können ausgetauscht werden, wobei aber, im Gegensatz zu bekannten Sicherheitssystemen, dass dies nur lokal gesteuert erfolgen kann. Des weiteren ist erfoderlich, bei einem Ausserbetriebnehmen des Überwachungssystems AS die gesamte Sicherheitsumgebung SU herunterzufahren. Datenübertragungen zu und von dem ersten Netzwerk NW1 sind dann nicht möglich. Dies gilt auch für eine Ausserbetriebnahme der anderen Komponenten der Sicherheitsumgebung SU.

Das Überwachungssystem AS kombiniert die Protokolleinträge der verschiedenen Systeme und kann somit Angriffe, Angriffsversuche und erfolgte Einbrüche aufgrund von Protokollierungen einzelner der genannten Systeme FW, PROXY, IDS und BM, aber eben auch durch Kombination von Protokollierungen mehrer der genannten Systeme FW, PROXY, IDS und BM feststellen. Protokollierungen ("Log-Dateien") unterschiedlicher herkömmlicher System sind im Allgemeinen zeitlich nicht synchronisiert, weshalb ein Zusammenhänge zwischen Protokollen getrenntes Systems bisher nicht erkannt werden konnten.
Dies wird durch das Überwachungssystem Überwachungssystem AS, und inbesondere durch deren Eigenschaft, vergleichbar mit einer in der Datenbank zu wirken. Die Kombination unterschiedlicher Protokollierung der Kontrollsysteme FW, PROXY und Datenübertragungskontrollsystem IDS, eventuell in Kombination mit Protokollen des Steuerungssystems BM kann bisher nicht erkennbare Einbruch identifizieren.

Das Regelwerk ist sehr komplex und wird erst in Zusammenarbeit mit dem Anwender entstehen. Nach der Installation der Sicherheitsumgebung SU soll das Überwachungssystem AS alle Daten protokollieren. Dies ermöglicht es alle Systeme FW, PROXY, IDS und Steuerungssystem BM, die mit dem Überwachungssystem AS zusammenarbeiten, werden des Betriebs hinsichtlich der Sicherheit bei Datenübetragungen zu optimieren. Wenn zum Beipsiel

dem ersten Netzwerk NW1 kein FTP-Datenpaket kommuniziert werden soll, darf das Datentypenkontrollsystem FW auch keine FTP-Datenpakte durchlassen. Stellt das Überwachungssystem AS danach dennoch eine Übertragung solche Daten fest, wwird draus auf einen Fehler oder einen Angriff geschlossen. Wie auf solche Zustände zu reagieren ist, wird in Richtlinien definiert, die der Sicherheitsumgebung und/oder den Anwendern und Benutzers der Sicherheitsumgebung angeben, wie zu reagieren ist.

Das Regelwerk für das Überwachungssystem AS kann nach der Installation verändert werden. Dies kann autmatisch, durch die Sicherheitsumbegung SU selbst, z.B. unter Steuerung des Steuerungssystems Steuerungssystem BM, und/oder durch von Aussen vorgenommene Änderungen an der Sicherheitsumgebung SU erfolgen. Von Aussen vorgenommene Änderungen an der Sicherheitsumgebung SU sind, wie im Folgenden beschrieben, aus Sicherheitsgründen Einschränkungen unterworfen.

Oftmals ist es das Ziel eines Angreifes die Kommunikationsmöglichkeiten der Sicherheitsumgebung SU zu unterbinden, beispielsweise deren E-Mail-Server zu deaktiveren. Um in einem solchen Fall Informationen über Angriffe, Angriffsversuche und erfolgte Einbrüche kommuizieren zu können (z.B. zu einem für die Sicherheitsumgebung SU zuständigen Administrator), kann das Überwachungssystem AS entsprechende Informationen über mehrere Kommnukationswege übermitteln. So ist beispielsweise eine Einheit AS-GSM zur Kommunikation über ein mobiles, zelluläres Telefonnetzwerk z.B. mittels SMS und/oder Sprachnachrichten vorgsehen. Weitere Übermittlungsmöglichkeiten umfassen digitale und analoge Bild-, Ton,- und Fax-Übertragungen und dergleichen. In welcher Zeit das Überwachungssystem AS auf Angriffe, Angriffsversuche und erfolgte Einbrüche reagiert wird im Allgemeinen mit Anwendern bzw. Benutzern der Sicherheitsumgebung Sicherheitsumgebung SU, auch für Einzelne derselben und/oder für unterschiedliche Angriffe, Angriffsversuche und erfolgte Einbrüche individuell, definiert.

Die gespeicherten Daten des Überwachungssystems AS charakterisieren das gesamte erste Netzwerk NW1, dessen Benutzer und deren Verhalten. Daher sind diese Daten höchst schützenswert , wofür vorteilhafterweise ein höchstmögliche Sicherheitsstufe definiert wird. Auf dem Gebiet sind Sicherheitsstufen von 0 bis 5. 5 als maximalem Wert definiert. Beipielsweise kann die Sicherheitstufe des Überwachungssystems AS mit 4 definiert werden.

Des weiteren kann das Überwachungssystem AS eine Schnittstelleneinheit AS-INT, z.B. in Form eines Modems oder einer Rechnerschnittstelle. Dies erlaubt eine Unterstützung des Überwachungssystems AS z.B. per Telefon. Um zu verhindern, dass auf das Überwachungssystem AS von einem der Netzwerke NW1 und NW2, insbesondere von dem Netzwerk NW2 als externem Netzwerk, zugegriffen werden kann, kann die Schnittstelleneinheit AS-INT so ausge-

führt sein, dass nicht über eines dieser Netzwerke NW1 und NW2 erreichbar ist.

STEUERUNGSSYSTEM ("Boot- und Management-Server")

Wie in Fig. 16 dargestellt, umfasst das Steuerungssystem BM ein Rechnersystem BM-Rechnersystem, auf das nur lokal zugegriffen werden kann. Neben oben genannten lokalen Zugriffsbeschränkungen (z.B. Erfassung biometrischer Daten, Codes, etc.) ist das Steuerungssystem BM dadurch vor Mißbrauch geschützt, dass es keine physikalische Möglichkeit des Zugriffes von Aussen gibt.

Das Steuerungssystem BM koomuniziert in der Sicherheitsumgebung SU über das interne Bus-System BUS-INT. Alle Modifikationen und zum Betrieb erfordelichen Daten werden, wie oben ausgeführt, durch das Steuerungssystem BM bereitgestellt oder zumindest unter dessen Steuerung und Kontrolle veranlasst bzw. übertragen. Erforderliche Daten werden in einer Speichereinheit BM-MEM des Steuerungssystems BM gespeichert. Zur Eingabe von beispielsweise für Systemmodifikationen erforderliche Daten und/oder Informationen kann die lokal vorgesehene Eingabeeinheit BM-IN verwendet werden.

Des weiteren kann das Steuerungssystem BM eine Schnittstelleneinheit BM-INT, z.B. in Form eines Modems oder einer Rechnerschnittstelle. Dies erlaubt eine Unterstützung des Steuerungssystems BM z.B. per Telefon. Um zu verhindern, dass auf das Steuerungssystem BM von einem der Netzwerke NW1 und NW2, insbesondere von dem Netzwerk NW2 als externem Netzwerk, zugegriffen werden kann, kann die Schnittstelleneinheit BM-INT so ausgeführt sein, dass nicht über eines dieser Netzwerke NW1 und NW2 erreichbar ist.

*****

PATENTANSPRÜCHE

1. Überwachungssystem zur Überwachung der Sicherheit netzwerkbasierter Datenübertragungen, mit
einem Rechnersystem (AS-RS) zum Ermitteln aus von wenigstens einem System (FW, PROXY, IDS) zur Kontrolle von ersten Datenübertagungen zwischen einem ersten Netzwerk (NW1) und einem zweiten Netzwerk (NW2) erhaltenen ersten Daten, die jeweils einzelne der ersten Datenübertragungen charakterisieren, ob die Datenübertragungen vorgegebene erste Sicherheitsanforderungen erfüllen.

2. Überwachungssystem nach Anspruch 1, mit
dem Rechnersystem (AS-RS) zum Ermitteln aus von wenigstens einem System (FW, PROXY, IDS) zur Kontrolle von zweiten Datenübertagungen innerhalb der ersten Netzwerks (NW1) erhaltenen zweiten Daten, die jeweils einzelne der zweiten Datenübertragungen charakterisieren, ob die zweiten Datenübertragungen vorgegebene zweite Sicherheitsanforderungen erfüllen.

3. Überwachungssystem nach Anspruch 1 oder 2, mit
dem Rechnersystem (AS-RS) zum Ermitteln, ob die vorgegebenen ersten und/oder zweiten Sicherheitsanforderungen verletzt sind, durch Kombinieren von charakterisierenden ersten und/oder zweiten Daten unterschiedlicher Kontrollsysteme (FW, PROXY, IDS).

4. Überwachungssystem nach einem der vorherigen Ansprüche, mit
dem Rechnersystem (AS-RS) zum Steuern des wenigstens einen Kontrollsystems (FW, PROXY, IDS) derart, dass bei einem fehlerhaften Betrieb und/oder einem Ausfall des Rechnersystems (AS-RS) das wenigstens eine Kontrollsystem (FW, PROXY, IDS) erste und/oder zweite Datenübertagungen verhindert.

5. Überwachungssystem nach einem der vorherigen Ansprüche, mit
einer Speichereinheit (AS-MEM) zum Speichern aller charakterisierenden ersten und/oder zweiten Daten oder zum Speichern von Daten der charakterisierenden ersten und/oder zweiten Daten, die eine Verletzung der vorgegebenen Sicherheitsanforderungen angeben.

6. Überwachungssystem nach Anspruch 5, bei dem
die Speichereinheit (AS-MEM) eine erste Speicheruntereinheit (AS-MEM-RT) zum Speichern von innerhalb eines ersten Zeitraums (RT) erhaltenen charakterisierenden ersten und/oder zweiten Daten und eine zweite Speicheruntereinheit (AS-MEM-LT) zum Speichern von innerhalb eines zweiten Zeitraums (LT) erhaltenen charakterisierenden ersten

und/oder zweiten Daten.

7. Überwachungssystem nach Anspruch 5 oder 6, mit
dem Rechnersystem (AS-RS) zum Steuern von Zugriffen auf die Speichereinheit (AS-MEM).

8. Überwachungssystem nach einem der vorherigen Ansprüche, mit
einer Wiedergabeeinheit (AS-DIS) zum Wiedergeben von Daten der charakterisierenden ersten und/oder zweiten Daten, die eine Verletzung der vorgegebenen ersten und/oder zweiten Sicherheitsanforderungen angeben.

9. Überwachungssystem nach Anspruch 8, mit
der Wiedergabeeinheit (AS-DIS) zum Wiedergeben von Angaben, die unterschiedliche Sicherheitszustände der ersten und/oder zweiten Datenübertagungen charakterisieren.

10. Überwachungssystem nach einem der vorherigen Ansprüche, bei dem
die Wiedergabeeinheit (AS-DIS) eine graphische Benutzerschnittstelle (AS-GUI) umfasst.

11. Überwachungssystem nach einem der vorherigen Ansprüche, mit
einer Eingabeeinheit (AS-IN) zur Eingabe von Anweisungen zur Steuerung des Betriebs des Überwachungssystems durch einen Benutzer, die unmittelbar in der Nähe des Rechnersystems (AS-RS) angeordnet ist, wobei nur Steuerungsanweisungen über die Eingabeeinheit (AS-IN) von dem Überwachungssystem verwendet werden.

12. Überwachungssystem nach einem der vorherigen Ansprüche, mit
einer Schnittstelleneinheit (AS-INT) für Zugriffe auf das Überwachungssystem.

13. Überwachungssystem nach einem der vorherigen Ansprüche, bei dem
das Rechnersystem (AS-RS) zum Betrieb erforderliche erste Betriebsdaten von einem externen Rechnersystem (BM) zum wenigstens teilweise Steuern des Überwachungssystem erhält.

14. Überwachungssystem nach einem der vorherigen Ansprüche, bei dem
das Rechnersystem (AS-RS) erste und/oder zweite Sicherheitsanforderungsdaten, die die ersten und/oder zweiten Sicherheitsanforderungen charakterisieren, von einem externen Rechnersystem (BM) zur Bereitstellung der ersten und/oder zweiten Sicherheitsanforderungsdaten erhält.

15. Überwachungssystem nach einem der vorherigen Ansprüche, mit
von für Datenübertagungen verwendeten Kommunikationsverbindungen (NW1, NW2) physikalisch getrennten Kommunikationsverbindungen (BUS-INT) für Datenübertragungen von und zu dem Überwachungssystem.

16. Überwachungssystem nach einem der vorherigen Ansprüche, das
als Audit-Server ausgeführt ist.

17. Datentypenkontrollsystem zur Kontrolle netzwerkbasierter Datenübertragungen in Abhängigkeit von Datentypen, mit
einem Rechnersystem (FW-RS) zum Überprüfen von ersten Datenübertragungen zwischen einem ersten Netzwerk (NW1) und einem zweiten Netzwerk (NW2) gemäß für das Datentypenkontrollsystem vorgegebenen ersten Sicherheitsanforderungen, zum Erstellen von einzelne der ersten Datenübertragungen charakterisierenden ersten Daten und zum Übertragen der charakterisierenden ersten Daten an ein Überwachungssystem (AS) zur Überwachung der Sicherheit der ersten Datenübertragungen.

18. Datentypenkontrollsystem nach Anspruch 17, mit
dem Rechnersystem (FW-RS) zum Überprüfen von zweiten Datenübertragungen innerhalb des ersten Netzwerks (NW1) gemäß für das Datentypenkontrollsystem vorgegebenen zweiten Sicherheitsanforderungen, zum Erstellen von einzelne der zweiten Datenübertragungen charakterisierenden zweiten Daten und zum Übertragen der charakterisierenden zweiten Daten an das Überwachungssystem (AS) zur Überwachung der Sicherheit der zweiten Datenübertragungen.

19. Datentypenkontrollsystem nach Anspruch 17 oder 18, mit
dem Rechnersystem (FW-RS) zur Erstellung der charakterisierenden ersten und/oder zweiten Daten in Echtzeit.

20. Datentypenkontrollsystem nach einem der Ansprüche 17 bis 19, bei dem
das Rechnersystem (FW-RS) zum Betrieb erforderliche erste Betriebsdaten von einem externen Rechnersystem (BM) zum wenigstens teilweise Steuern des Datentypenkontrollsystems erhält.

21. Datentypenkontrollsystem nach einem der Ansprüche 17 bis 20, mit
einem Betriebssystem für das Rechnersystem (FW-RS), das nur einen Betrieb des Rechnersystem (FW-RS) in unmittelbarem Zusammenhang mit netzwerkbasierten Datenübertragungen ermöglicht.

22. Datentypenkontrollsystem nach einem der Ansprüche 17 bis 21, bei dem das Rechnersystem (FW-RS) erste und/oder zweite Sicherheitsanforderungsdaten, die die ersten und/oder zweiten Sicherheitsanforderungen charakterisieren, von einem externen Rechnersystem (BM) zur Bereitstellung der ersten und/oder zweiten Sicherheitsanforderungsdaten erhält.

23. Datentypenkontrollsystem nach einem der Ansprüche 17 bis 22, mit einer Eingabeeinheit (FW-IN) zur Eingabe von Anweisungen zur Steuerung des Betriebs des Datentypenkontrollsystems durch einen Benutzer, die unmittelbar in der Nähe des Rechnersystems (FW-RS) angeordnet ist, wobei nur Steuerungsanweisungen über die Eingabeeinheit (FW-IN) von dem Datentypenkontrollsystem verwendet werden.

24. Datentypenkontrollsystem nach einem der Ansprüche 17 bis 23, mit von für Datenübertagungen verwendeten Kommunikationsverbindungen (NW1, NW2) physikalisch getrennten Kommunikationsverbindungen (BUS-INT) für Datenübertragungen von und zu dem Datentypenkontrollsystem.

25. Datentypenkontrollsystem nach einem der Ansprüche 17 bis 23, das als Firewall ausgeführt ist.

26. Dateninhaltskontrollsystem zur Kontrolle von Inhalten netzwerkbasierter Datenübertragungen, mit
einem Rechnersystem (PROXY-RS) zum Überprüfen von ersten Datenübertragungen zwischen einem ersten Netzwerk (NW1) und einem zweiten Netzwerk (NW2) gemäß für das Dateninhaltskontrollsystem vorgegebenen ersten Sicherheitsanforderungen, zum Erstellen von einzelne der ersten Datenübertragungen charakterisierenden ersten Daten und zum Übertragen der charakterisierenden ersten Daten an ein Überwachungssystem (AS) zur Überwachung der Sicherheit der ersten Datenübertragungen.

27. Dateninhaltskontrollsystem nach Anspruch 26, mit
dem Rechnersystem (PROXY-RS) zum Überprüfen von zweiten Datenübertragungen innerhalb des ersten Netzwerks (NW1) gemäß für das Dateninhaltskontrollsystem vorgegebenen zweiten Sicherheitsanforderungen, zum Erstellen von Einzelne der zweiten Datenübertragungen charakterisierenden zweiten Daten und zum Übertragen der charakterisierenden zweiten Daten an das Überwachungssystem (AS) zur Überwachung der Sicherheit der zweiten Datenübertragungen.

28. Dateninhaltskontrollsystem nach Anspruch 25 oder 26, mit
dem Rechnersystem (PROXY-RS) zur Erstellung der charakterisierenden ersten und/oder

zweiten Daten in Echtzeit.

29. Dateninhaltskontrollsystem nach einem der Ansprüche 25 bis 28, bei dem
das Rechnersystem (PROXY-RS) zum Betrieb erforderliche erste Betriebsdaten von einem externen Rechnersystem (BM) zum wenigstens teilweise Steuern des Dateninhaltskontrollsystems erhält.

30. Dateninhaltskontrollsystem nach einem der Ansprüche 25 bis 29, bei dem
das Rechnersystem (PROXY-RS) erste und/oder zweite Sicherheitsanforderungsdaten, die die ersten und/oder zweiten Sicherheitsanforderungen charakterisieren, von einem externen Rechnersystem (BM) zum Bereitstellen der ersten und/oder zweiten Sicherheitsanforderungsdaten erhält.

31. Dateninhaltskontrollsystem nach einem der Ansprüche 25 bis 30, mit
einer Eingabeeinheit (PROXY-IN) zur Eingabe von Anweisungen zur Steuerung des Betriebs des Dateninhaltskontrollsystems durch einen Benutzer, die unmittelbar in der Nähe des Rechnersystems (PROXY-RS) angeordnet ist, wobei nur Steuerungsanweisungen über die Eingabeeinheit (PROXY-IN) von dem Dateninhaltskontrollsystem verwendet werden.

32. Dateninhaltskontrollsystem nach einem der Ansprüche 25 bis 31, mit
von für Datenübertagungen verwendeten Kommunikationsverbindungen (NW1, NW2) physikalisch getrennten Kommunikationsverbindungen (BUS-INT) für Datenübertragungen von und zu dem Dateninhaltskontrollsystem.

33. Dateninhaltskontrollsystem nach einem der Ansprüche 25 bis 32, das
als Proxy-Server ausgeführt ist.

34. Datenübertragungskontrollsystem zur Analyse netzwerkbasierter Datenübertragungen, mit:
einem Rechnersystem (IDS-RS) zur Analyse von ersten Datenübertragungen zwischen einem ersten Netzwerk (NW1) und einem zweiten Netzwerk (NW2) gemäß für das Datenübertragungskontrollsystem vorgegebenen ersten Sicherheitsanforderungen, zum Erstellen von einzelne der ersten Datenübertragungen charakterisierenden ersten Daten und zum Übertragen der charakterisierenden ersten Daten an ein Überwachungssystem (AS) zur Überwachung der Sicherheit der ersten Datenübertragungen.

35. Datenübertragungskontrollsystem nach Anspruch 34, mit
dem Rechnersystem (IDS-RS) zur Analyse von zweiten Datenübertragungen innerhalb

des ersten Netzwerks (NW1) gemäß für das Datenübertragungskontrollsystem vorgegebenen zweiten Sicherheitsanforderungen, zum Erstellen von einzelne der zweiten Datenübertragungen charakterisierenden zweiten Daten und zum Übertragen der charakterisierenden zweiten Daten an das Überwachungssystem (AS) zur Überwachung der Sicherheit der zweiten Datenübertragungen.

36. Datenübertragungskontrollsystem nach Anspruch 34 oder 35, mit dem Rechnersystem (IDS-RS) zur Erstellung der charakterisierenden ersten und/oder zweiten Daten in Echtzeit.

37. Datenübertragungskontrollsystem nach einem der Ansprüche 34 bis 36, bei dem das Rechnersystem (IDS-RS) zum Betrieb erforderliche erste Betriebsdaten von einem externen Rechnersystem (BM) zum wenigstens teilweise Steuern des Datenübertragungskontrollsystems erhält.

38. Datenübertragungskontrollsystem nach einem der Ansprüche 34 bis 37, mit einem Betriebssystem für das Rechnersystem (IDS-RS), das nur einen Betrieb des Rechnersystem (IDS-RS) in unmittelbarem Zusammenhang mit netzwerkbasierten Datenübertragungen ermöglicht.

39. Datenübertragungskontrollsystem nach einem der Ansprüche 34 bis 38, bei dem das Rechnersystem (IDS-RS) erste und/oder zweite Sicherheitsanforderungsdaten, die die ersten und/oder zweiten Sicherheitsanforderungen charakterisieren, von einem externen Rechnersystem (BM) zur Bereitstellung der ersten und/oder zweiten Sicherheitsanforderungsdaten erhält.

40. Datenübertragungskontrollsystem nach einem der Ansprüche 34 bis 39, mit einer Eingabeeinheit (IDS-IN) zur Eingabe von Anweisungen zur Steuerung des Betriebs des Datenübertragungskontrollsystems durch einen Benutzer, die unmittelbar in der Nähe des Rechnersystems (IDS-RS) angeordnet ist, wobei nur Steuerungsanweisungen über die Eingabeeinheit (IDS-IN) von dem Datenübertragungskontrollsystem verwendet werden.

41. Datenübertragungskontrollsystem nach einem der Ansprüche 34 bis 40, mit von für Datenübertagungen verwendeten Kommunikationsverbindungen (NW1, NW2) physikalisch getrennten Kommunikationsverbindungen (BUS-INT) für Datenübertragungen von und zu dem Datenübertragungskontrollsystem.

42. Datenübertragungskontrollsystem nach einem der Ansprüche 34 bis 41, das als IDS-Server ausgeführt ist.

43. Steuerungssystem zur Steuerung von wenigstens einem Überwachungs-, Datentypenkontroll-, Inhaltskontroll- und/oder Datenübertragungskontrollsystem für netzwerkbasierte Datenübertragungen, mit:
    - einem Rechnersystem (BM-RS) zur Steuerung einer Übertragung von zur Steuerung des wenigstens einen Überwachungs-, Datentypenkontroll- und/oder Dateninhaltskontrollsystems gewünschten Steuerungsdaten, und
    - einem Bus-System (BUS-INT) zur Übertragung der Steuerungsdaten, der physikalisch von einem für die netzwerkbasierten Datenübertragungen verwendeten Netzwerk (NW1, NW2) getrennt ist.

44. Steuerungssystem nach Anspruch 43, mit
einer Speichereinheit (BM-MEM) zur Speicherung der Steuerungsdaten.

45. Steuerungssystem nach Anspruch 43 oder 44, mit
der Speichereinheit (BM-MEM) zur Speicherung von zum Betrieb des wenigstens einen Überwachungs-, Datentypenkontroll- und/oder Dateninhaltskontrollsystems gewünschten Sicherheitsanforderungen für dasselbe charakterisierenden Daten.

46. Steuerungssystem nach einem der Ansprüche 43 bis 45, mit
dem Rechnersystem (BM-RS) zur Steuerung einer Inbetriebnahme des wenigstens einen Überwachungs-, Datentypenkontroll- und/oder Dateninhaltskontrollsystems gemäß gewünschte Bedingungen für eine zulässige Inbetriebnahme charakterisierender Daten.

47. Steuerungssystem nach einem der Ansprüche 43 bis 46, mit
dem Rechnersystem (BM-RS) zur Steuerung einer Inbetriebnahme des wenigstens einen Überwachungs-, Datentypenkontroll- und/oder Dateninhaltskontrollsystems derart, dass während einer Inbetriebnahme nur ein Überwachungs-, Datentypenkontroll- und/oder Dateninhaltskontrollsystem in Betrieb genommen wird.

48. Steuerungssystem nach einem der Ansprüche 43 bis 47, mit
der Speichereinheit (BM-MEM) zur Speicherung der die gewünschten Bedingungen für eine zulässige Inbetriebnahme charakterisierenden Daten.

49. Steuerungssystem nach einem der Ansprüche 43 bis 48, mit
einer Eingabeeinheit (BW-IN) zur Eingabe von Anweisungen zur Steuerung des Betriebs des Steuerungssystem durch einen Benutzer, die unmittelbar in der Nähe des Rechnersy-

stems (BM-RS) angeordnet ist, wobei nur Steuerungsanweisungen über die Eingabeeinheit (BM-IN) von dem Steuerungssystem verwendet werden.

50. Steuerungssystem nach einem der Ansprüche 43 bis 49, das als Boot-Management-Server ausgeführt ist.

51. Sicherheitsumgebung für netzwerkbasierte Datenübertragungen, mit
- dem Überwachungssystem nach einem der Ansprüche 1 bis 16, und
- wenigstens einem der Kontrollsysteme nach einem der Ansprüche 17 bis 25, nach einem der Ansprüche 26 bis 33 und nach einem der Ansprüche 34 bis 42.

52. Sicherheitsumgebung nach Anspruch 51, mit
dem Steuerungssystem (BM) nach einem der Ansprüche 43 bis 50.

53. Sicherheitsumgebung nach Anspruch 51 oder 52, mit
von zur Datenübertagungen verwendeten Kommunikationsverbindungen (NW1, NW2) physikalisch getrennten Kommunikationsverbindungen (BUS-INT) für Datenübertragungen zwischen dem Überwachungssystem (AS) und/oder dem wenigstens einen Kontrollsystem (FW, PROXY, IDS) und/oder dem Steuerungssystem (BM).

54. Verfahren zur Überwachung der Sicherheit netzwerkbasierter Datenübertragungen, mit:
Ermitteln aus von wenigstens einem System (FW, PROXY, IDS) zur Kontrolle von ersten Datenübertagungen zwischen einem ersten Netzwerk (NW1) und einem zweiten Netzwerk (NW2) erhaltenen ersten Daten, die jeweils einzelne der ersten Datenübertragungen charakterisieren, ob die Datenübertragungen vorgegebene erste Sicherheitsanforderungen erfüllen, mittels eines Überwachungssystems (AS).

55. Verfahren nach Anspruch 55, mit
Ermitteln aus von wenigstens einem System (FW, PROXY, IDS) zur Kontrolle von zweiten Datenübertagungen innerhalb der ersten Netzwerks (NW1) erhaltenen zweiten Daten, die jeweils einzelne der zweiten Datenübertragungen charakterisieren, ob die zweiten Datenübertragungen vorgegebene zweite Sicherheitsanforderungen erfüllen, mittels des Überwachungssystems (AS).

56. Verfahren nach Anspruch 54 oder 55, mit
Ermitteln, ob die vorgegebenen ersten und/oder zweiten Sicherheitsanforderungen verletzt sind, durch Kombinieren von charakterisierenden ersten und/oder zweiten Daten unterschiedlicher Kontrollsysteme (FW, PROXY, IDS).

57. Verfahren nach einem der Ansprüche 54 bis 56, mit
Steuern des wenigstens einen Kontrollsystems (FW, PROXY, IDS) derart, dass bei einem fehlerhaften Betrieb und/oder einem Ausfall des Überwachungssystems (AS) das wenigstens eine Kontrollsystem (FW, PROXY, IDS) erste und/oder zweite Datenübertagungen verhindert.

58. Verfahren nach einem der Ansprüche 54 bis 57, mit
Speichern aller charakterisierenden ersten und/oder zweiten Daten oder zum Speichern von Daten der charakterisierenden ersten und/oder zweiten Daten, die eine Verletzung der vorgegebenen Sicherheitsanforderungen angeben.

59. Verfahren nach Anspruch 58, mit
Speichern von innerhalb eines ersten Zeitraums (RT) erhaltenen charakterisierenden ersten und/oder zweiten Daten in einer ersten Speicheruntereinheit (AS-MEM-RT), und
Speichern von innerhalb eines zweiten Zeitraums (RT) erhaltenen charakterisierenden ersten und/oder zweiten Daten in einer zweiten Speicheruntereinheit (AS-MEM-LT).

60. Verfahren nach einem der Ansprüche 54 bis 59, mit
Wiedergeben von Daten der charakterisierenden ersten und/oder zweiten Daten, die eine Verletzung der vorgegebenen ersten und/oder zweiten Sicherheitsanforderungen angeben, mittels einer Wiedergabeeinheit (AS-DIS)

61. Verfahren nach Anspruch 54 bis 60, mit
Wiedergeben von Angaben, die unterschiedliche Sicherheitszustände der ersten und/oder zweiten Datenübertagungen charakterisieren, mittels einer Wiedergabeeinheit (AS-DIS).

62. Verfahren nach einem der Ansprüche 54 bis 61, mit
Eingeben von Anweisungen zur Steuerung des Betriebs des Überwachungssystems durch einen Benutzer mittels einer Eingabeeinheit (AS-IN), die unmittelbar in der Nähe eines Rechnersystems (AS-RS) des Überwachungssystems (AS) angeordnet ist, wobei nur Steuerungsanweisungen über die Eingabeeinheit (AS-IN) von dem Überwachungssystem (Überwachungssystem AS) verwendet werden.

63. Verfahren nach einem der Ansprüche 54 bis 62, mit
Übertragen von zum Betrieb erforderlicher erster Betriebsdaten von einem externen Rechnersystem (BM) zum wenigstens teilweise Steuern des Überwachungssystem an das Überwachungssystem (AS).

64. Verfahren nach einem der Ansprüche 54 bis 63, mit
Durchführen von Datenübertragungen von und zu dem Überwachungssystem (AS) physikalisch getrennt von für Datenübertagungen verwendeten Kommunikationsverbindungen (NW1, NW2).

65. Verfahren zur Kontrolle von netzwerkbasierten Datenübertragungen in Abhängigkeit von Datentypen, mit
Überprüfen von ersten Datenübertragungen zwischen einem ersten Netzwerk (NW1) und einem zweiten Netzwerk (NW2) gemäß für das Datentypenkontrollsystem vorgegebenen ersten Sicherheitsanforderungen, zum Erstellen von einzelne der ersten Datenübertragungen charakterisierenden ersten Daten und zum Übertragen der charakterisierenden ersten Daten an ein Überwachungssystem (AS) zur Überwachung der Sicherheit der ersten Datenübertragungen, mittels eines Datentypenkontrollsystems (FW) .

66. Verfahren nach Anspruch 65, mit
Überprüfen von zweiten Datenübertragungen innerhalb des ersten Netzwerks (NW1) gemäß für das Datentypenkontrollsystem vorgegebenen zweiten Sicherheitsanforderungen, zum Erstellen von einzelne der zweiten Datenübertragungen charakterisierenden zweiten Daten und zum Übertragen der charakterisierenden zweiten Daten an das Überwachungssystem (AS) zur Überwachung der Sicherheit der zweiten Datenübertragungen, mittels des Datentypenkontrollsystems (FW) .

67. Verfahren nach Anspruch 65 oder 66, mit
Erstellen der charakterisierenden ersten und/oder zweiten Daten in Echtzeit.

68. Verfahren nach einem der Ansprüche 65 bis 67, mit
Erhalten mittels des Datentypenkontrollsystems(FW) von ersten und/oder zweiten Sicherheitsanforderungsdaten, die die ersten und/oder zweiten Sicherheitsanforderungen charakterisieren, von einem externen Rechnersystem (BM) zur Bereitstellung der ersten und/oder zweiten Sicherheitsanforderungsdaten.

69. Verfahren nach einem der Ansprüche 65 bis 68, mit
Eingabe von Anweisungen zur Steuerung des Betriebs des Datentypenkontrollsystems durch einen Benutzer mittels einer Eingabeeinheit (FW-IN), die unmittelbar in der Nähe eines Rechnersystems (FW-RS) das Datentypenkontrollsystems (FW) angeordnet ist, wobei nur Steuerungsanweisungen über die Eingabeeinheit (FW-IN) von dem Datentypenkontrollsystem (FW) verwendet werden.

70. Verfahren nach einem der Ansprüche 65 bis 69, mit
Übertragen von Datenübertagungen von und zu dem Datentypenkontrollsystem (FW) physikalisch getrennt von für Datenübertagungen verwendeten Kommunikationsverbindungen (NW1, NW2).

71. Verfahren zur Kontrolle von Inhalten netzwerkbasierter Datenübertragungen, mit
Überprüfen von ersten Datenübertragungen zwischen einem ersten Netzwerk (NW1) und einem zweiten Netzwerk (NW2) gemäß für das Dateninhaltskontrollsystem vorgegebenen ersten Sicherheitsanforderungen, zum Erstellen von einzelne der ersten Datenübertragungen charakterisierenden ersten Daten und zum Übertragen der charakterisierenden ersten Daten an ein Überwachungssystem (AS) zur Überwachung der Sicherheit der ersten Datenübertragungen, mittels eines Dateninhaltskontrollsystems (PROXY) .

72. Verfahren nach Anspruch 71, mit
Überprüfen von zweiten Datenübertragungen innerhalb des ersten Netzwerks (NW1) gemäß für das Dateninhaltskontrollsystem vorgegebenen zweiten Sicherheitsanforderungen, zum Erstellen von Einzelne der zweiten Datenübertragungen charakterisierenden zweiten Daten und zum Übertragen der charakterisierenden zweiten Daten an das Überwachungssystem (AS) zur Überwachung der Sicherheit der zweiten Datenübertragungen, mittels das Dateninhaltskontrollsystems (PROXY) .

73. Verfahren nach Anspruch 71 oder 72, mit
Erstellen der charakterisierenden ersten und/oder zweiten Daten in Echtzeit.

74. Verfahren nach einem der Ansprüche 71 bis 73, mit
Erhalten mittels das Dateninhaltskontrollsystems (PROXY) von zum Betrieb erforderlichen ersten Betriebsdaten von einem externen Rechnersystem (BM) zum wenigstens teilweise Steuern des Dateninhaltskontrollsystems.

75. Verfahren nach einem der Ansprüche 71 bis 74, mit
Erhalten mittels das Dateninhaltskontrollsystems (PROXY) von ersten und/oder zweiten Sicherheitsanforderungsdaten, die die ersten und/oder zweiten Sicherheitsanforderungen charakterisieren, von einem externen Rechnersystem (BM) zum Bereitstellen der ersten und/oder zweiten Sicherheitsanforderungsdaten erhält.

76. Verfahren nach einem der Ansprüche 71 bis 75, mit
Eingabe von Anweisungen zur Steuerung des Betriebs des Dateninhaltskontrollsystems durch einen Benutzer mittels einer Eingabeeinheit (PROXY-IN), die unmittelbar in der Nähe einem Rechnersystems (PROXY-RS) des Dateninhaltskontrollsystems (PROXY)

angeordnet ist, wobei nur Steuerungsanweisungen über die Eingabeeinheit (PROXY-IN) von dem Dateninhaltskontrollsystem (PROXY) verwendet werden.

77. Verfahren nach einem der Ansprüche 71 bis 76, mit
Übertragen von Datenübertagungen von und zu dem Dateninhaltskontrollsystem physikalisch getrennt von für Datenübertagungen verwendeten Kommunikationsverbindungen (NW1, NW2).

78. Verfahren zur Analyse netzwerkbasierter Datenübertragungen, mit:
Analysieren von ersten Datenübertragungen zwischen einem ersten Netzwerk (NW1) und einem zweiten Netzwerk (NW2) gemäß für das Datenübertragungskontrollsystem vorgegebenen ersten Sicherheitsanforderungen, zum Erstellen von einzelne der ersten Datenübertragungen charakterisierenden ersten Daten und zum Übertragen der charakterisierenden ersten Daten an ein Überwachungssystem (AS) zur Überwachung der Sicherheit der ersten Datenübertragungen, mittels eines Datenübertragungskontrollsystems (IDS).

79. Verfahren nach Anspruch 78, mit
Analysieren von zweiten Datenübertragungen innerhalb des ersten Netzwerks (NW1) gemäß für das Datenübertragungskontrollsystem vorgegebenen zweiten Sicherheitsanforderungen, zum Erstellen von einzelne der zweiten Datenübertragungen charakterisierenden zweiten Daten und zum Übertragen der charakterisierenden zweiten Daten an das Überwachungssystem (AS) zur Überwachung der Sicherheit der zweiten Datenübertragungen, mittels des Datenübertragungskontrollsystems (IDS).

80. Verfahren nach Anspruch 77 oder 78, mit
Erstellen der charakterisierenden ersten und/oder zweiten Daten in Echtzeit.

81. Verfahren nach einem der Ansprüche 77 bis 80, bei dem
Erhalten mittels des Datenübertragungskontrollsystems (IDS) zum Betrieb erforderliche erste Betriebsdaten von einem externen Rechnersystem (BM) zum wenigstens teilweise Steuern des Datenübertragungskontrollsystems.

82. Verfahren nach einem der Ansprüche 77 bis 81, mit
Erhalten mittels des Datenübertragungskontrollsystems (IDS) von ersten und/oder zweiten Sicherheitsanforderungsdaten, die die ersten und/oder zweiten Sicherheitsanforderungen charakterisieren, von einem externen Rechnersystem (BM) zur Bereitstellung der ersten und/oder zweiten Sicherheitsanforderungsdaten.

83. Verfahren nach einem der Ansprüche 77 bis 82, mit
Eingabe von Anweisungen zur Steuerung des Betriebs des Datenübertragungskontrollsystems durch einen Benutzer mittels einer Eingabeeinheit (IDS-IN), die unmittelbar in der Nähe eines Rechnersystems (IDS-RS) des Datenübertragungskontrollsystems (IDS) angeordnet ist, wobei nur Steuerungsanweisungen über die Eingabeeinheit (IDS-IN) von dem Datenübertragungskontrollsystem (IDS) verwendet werden.

84. Verfahren nach einem der Ansprüche 77 bis 83, mit
Übertragen von Datenübertragungen von und zu dem Datenübertragungskontrollsystem (IDS) physikalisch getrennt von für Datenübertagungen verwendeten Kommunikationsverbindungen (NW1, NW2).

85. Verfahren zur Steuerung von wenigstens einem Überwachungs-, Datentypenkontroll-, Inhaltskontroll- und/oder Datenübertragungskontrollsystem für netzwerkbasierte Datenübertragungen, unter Verwendung
- des Überwachungssystems nach einem der Ansprüche 1 bis 16, und
- wenigstens eines der Kontrollsysteme nach einem der Ansprüche 17 bis 25, nach einem der Ansprüche 26 bis 33 und nach einem der Ansprüche 34 bis 42.

86. Verfahren nach Anspruch 85, mit
Verwendung des Steuerungssystems (BM) nach einem der Ansprüche 43 bis 50.

87. Softwareprodukt, mit
Programmcodeteilen zum Ausführen der Schritte nach einem der Ansprüche 54 bis 86.

88. Softwareprodukt nach Anspruch 87, das
auf einem computerlesbaren Speichermedium oder in einer computerlesbaren Speichervorrichtung gespeichert ist.

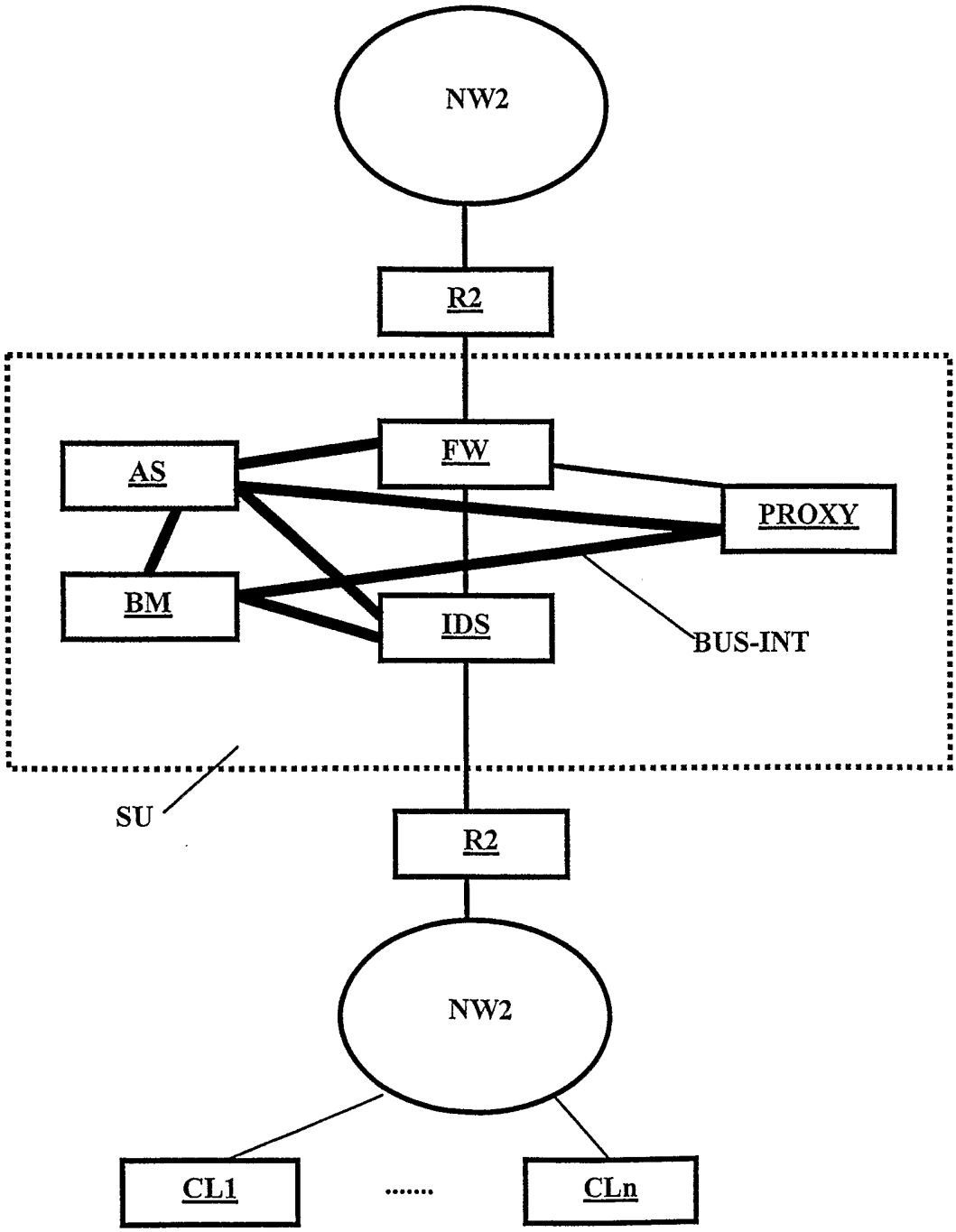


Fig. 1

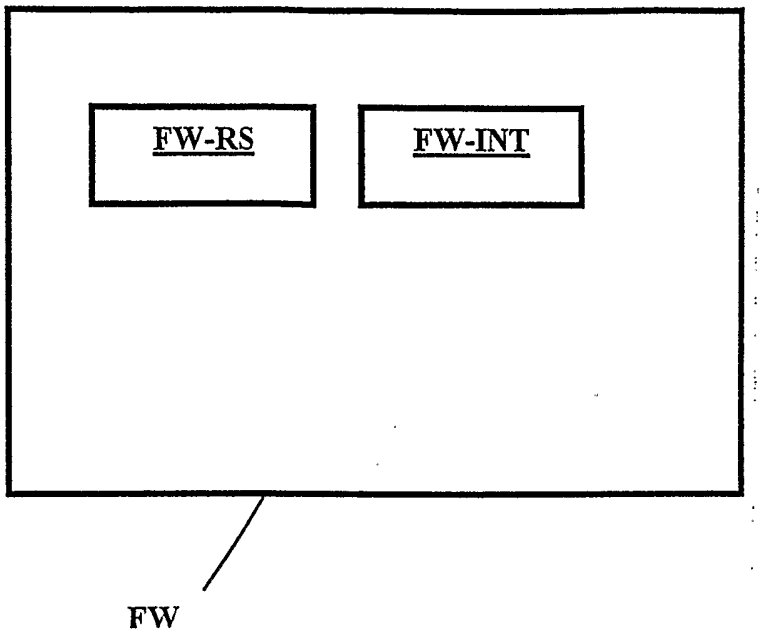


Fig. 2

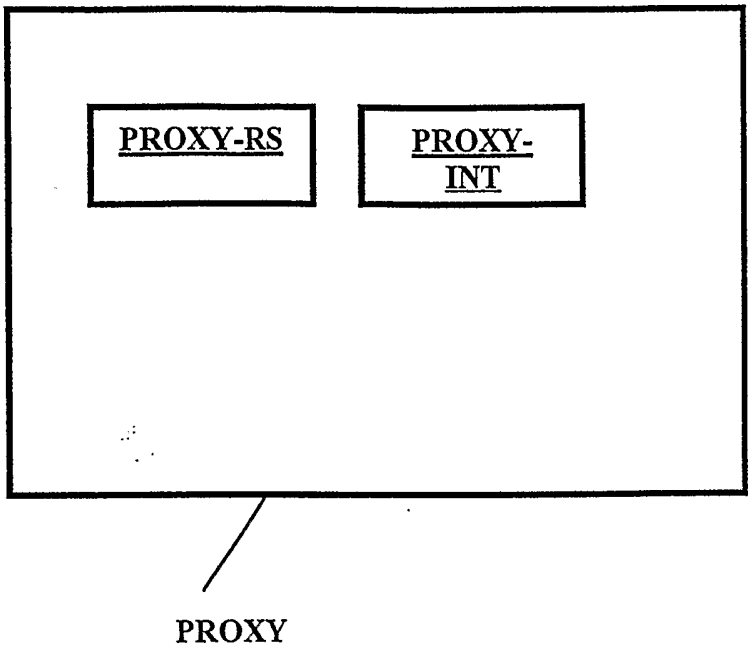


Fig. 3

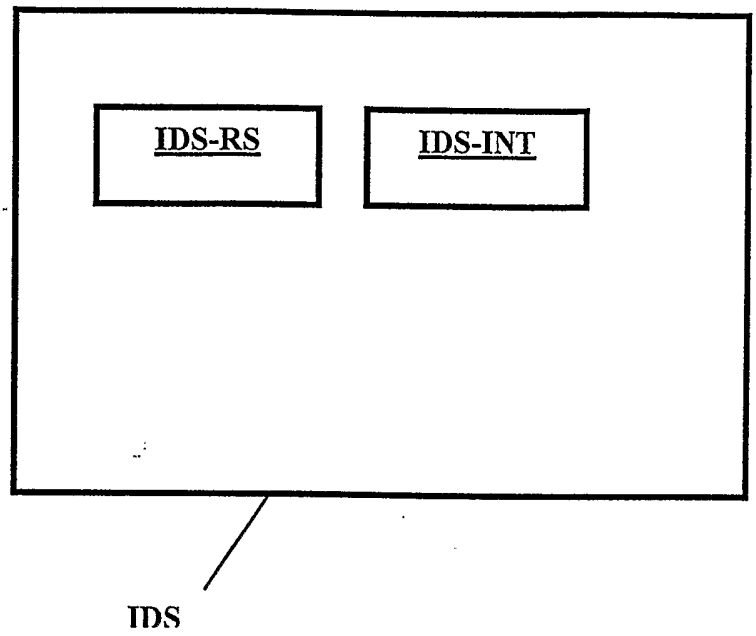


Fig. 4

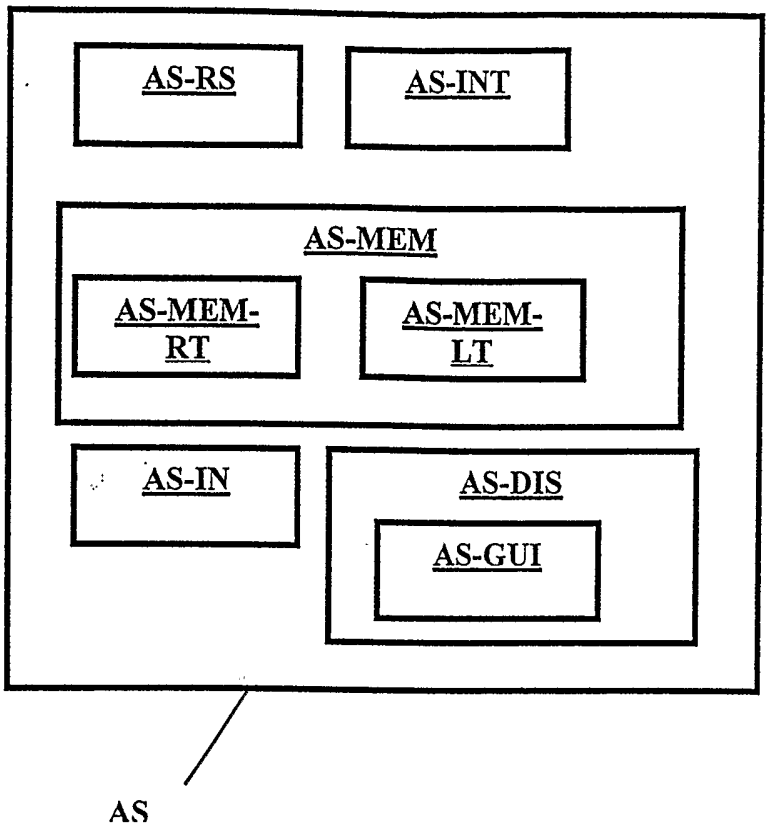


Fig. 5

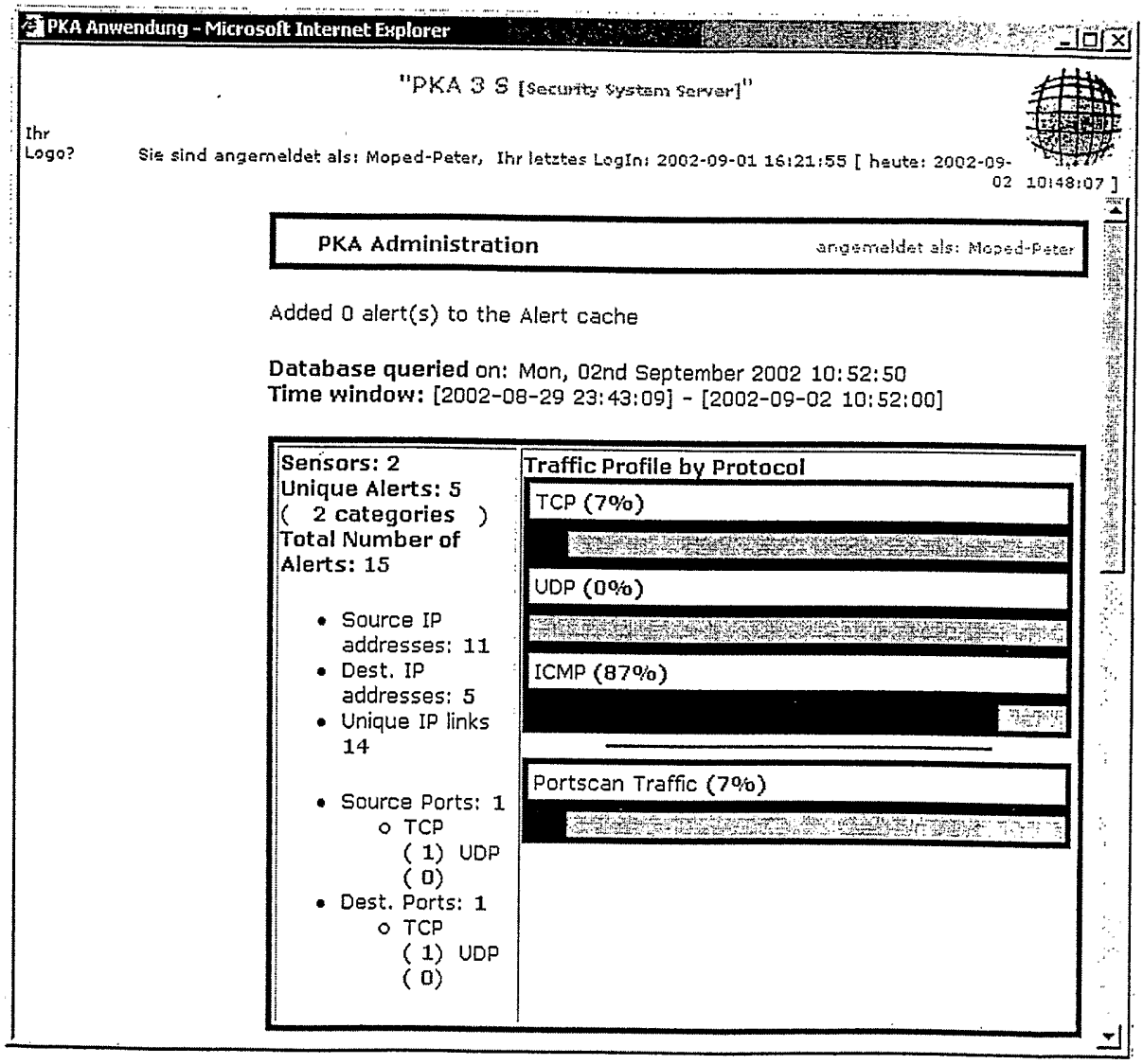

PKA Anwendung - Microsoft Internet Explorer
"PKA 3 S [Security System Server]"
Ihr Logo?
Sie sind angemeldet als: Moped-Peter, Ihr letztes LogIn: 2002-09-01 16:21:55 [heute: 2002-09-02 10:48:07]
PKA Administration
angemeldet als: Moped-Peter
Added 0 alert(s) to the Alert cache
Database queried on: Mon, 02nd September 2002 10:52:50
Time window: [2002-08-29 23:43:09] - [2002-09-02 10:52:00]
Sensors: 2
Unique Alerts: 5
(2 categories)
Total Number of Alerts: 15
Source IP addresses: 11
Dest. IP addresses: 5
Unique IP links 14
Source Ports: 1
TCP (1) UDP (0)
Dest. Ports: 1
TCP (1) UDP (0)
Traffic Profile by Protocol
TCP (7%)
UDP (0%)
ICMP (87%)
Portscan Traffic (7%)

Fig. 6

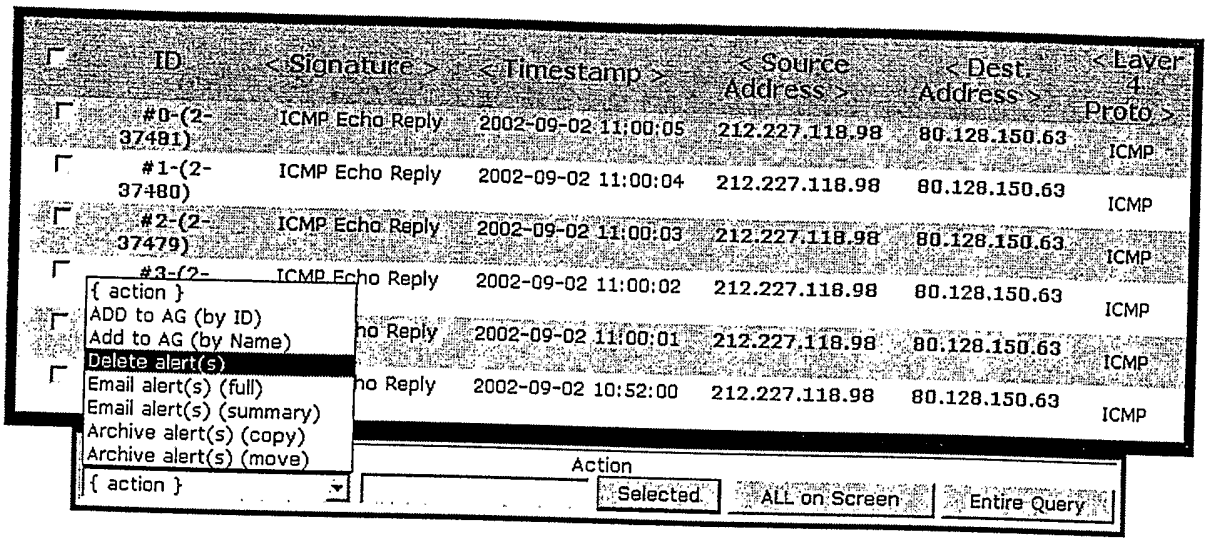

ID
< Signature >
< Timestamp >
< Source Address >
< Dest. Address >
< Layer 4 Proto >
#0-(2-37481) ICMP Echo Reply 2002-09-02 11:00:05 212.227.118.98 80.128.150.63 ICMP
#1-(2-37480) ICMP Echo Reply 2002-09-02 11:00:04 212.227.118.98 80.128.150.63 ICMP
#2-(2-37479) ICMP Echo Reply 2002-09-02 11:00:03 212.227.118.98 80.128.150.63 ICMP
ICMP Echo Reply 2002-09-02 11:00:02 212.227.118.98 80.128.150.63 ICMP
2002-09-02 11:00:01 212.227.118.98 80.128.150.63 ICMP
2002-09-02 10:52:00 212.227.118.98 80.128.150.63 ICMP
{ action }
ADD to AG (by ID)
Add to AG (by Name)
Delete alert(s)
Email alert(s) (full)
Email alert(s) (summary)
Archive alert(s) (copy)
Archive alert(s) (move)
Action
{ action }
Selected
ALL on Screen
Entire Query

Fig. 7

Source FQDN	< Source IP >	Direction	< Destination IP >	Destination FQDN	Protocol
leg-66-247-124-227-STK.sprinthome.com	66.247.124.227	-->	80.128.147.173	p508093AD.dip.t-dialin.net	TCP
Unable to resolve address	217.5.98.11	-->	80.128.156.111	p50809C6F.dip.t-dialin.net	ICMP
Unable to resolve address	217.237.152.94	-->	80.128.156.111	p50809C6F.dip.t-dialin.net	ICMP
F-gw12.F.net.DTAG.DE	62.154.17.194	-->	80.128.156.111	p50809C6F.dip.t-dialin.net	ICMP
Unable to resolve address	62.156.128.106	-->	80.128.156.111	p50809C6F.dip.t-dialin.net	ICMP
so-1100.gw-backbone-a.ka.schlund.net	212.227.112.85	-->	80.128.156.111	p50809C6F.dip.t-dialin.net	ICMP
c1.gw-schlund-a.core.kfs.ka.schlund.net	195.20.224.19	-->	80.128.156.111	p50809C6F.dip.t-dialin.net	ICMP
Unable to resolve address	217.5.98.11	-->	80.128.150.175	p508096AF.dip.t-dialin.net	ICMP
Unable to resolve address	217.237.152.94	-->	80.128.150.175	p508096AF.dip.t-dialin.net	ICMP

Fig. 8

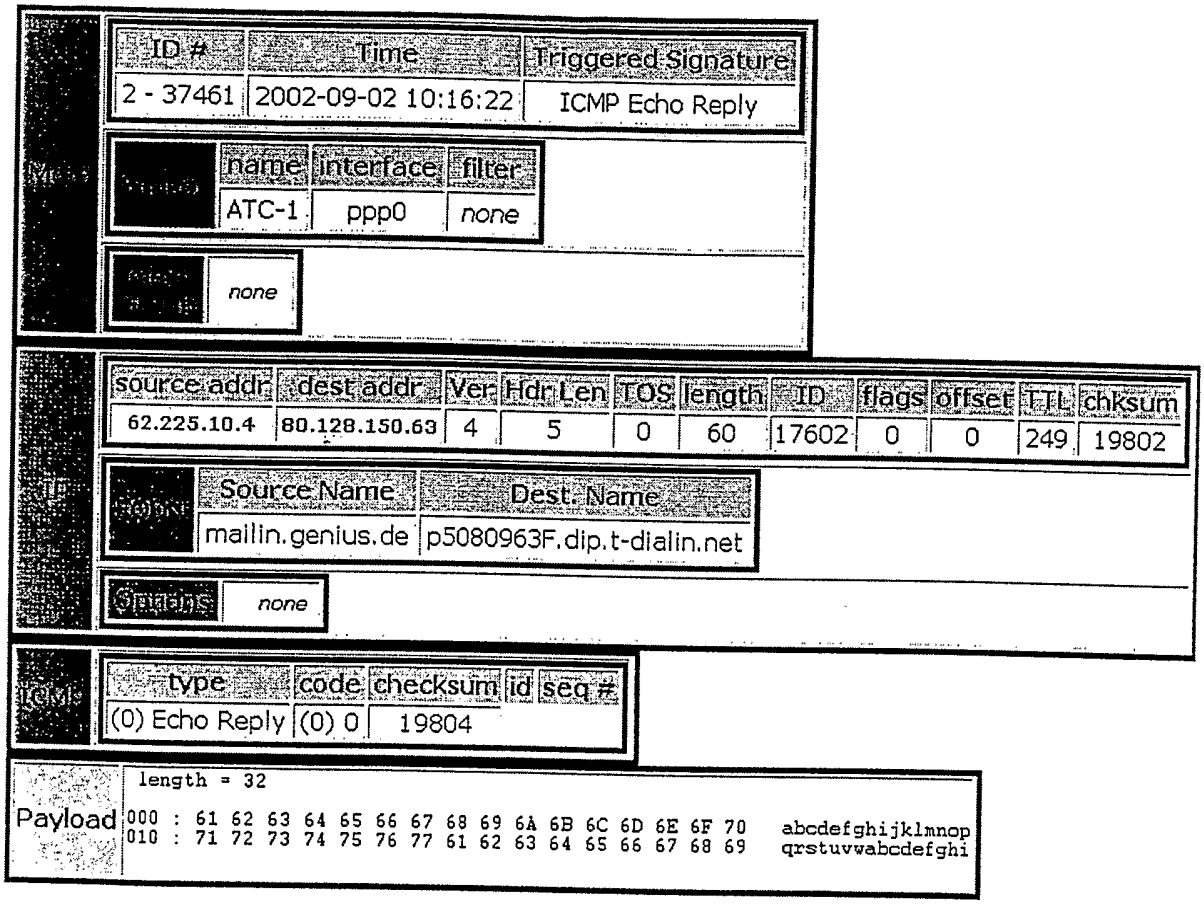

ID #
Time
Triggered Signature
2 - 37461
2002-09-02 10:16:22
ICMP Echo Reply
name
interface
filter
ATC-1
ppp0
none
none
source addr
dest addr
Ver
Hdr Len
TOS
length
ID
flags
offset
TTL
chksum
62.225.10.4
80.128.150.63
4
5
0
60
17602
0
0
249
19802
Source Name
Dest. Name
mailin.genius.de
p5080963F.dip.t-dialin.net
none
type
code
checksum
id
seq #
(0) Echo Reply
(0) 0
19804
Payload
length = 32
000 : 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 abcdefghijklmnop
010 : 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 qrstuvwabcdefghi

Fig. 9

action	submit	ip	netmask
whois		62.225.10.4	32

62.225.10.4

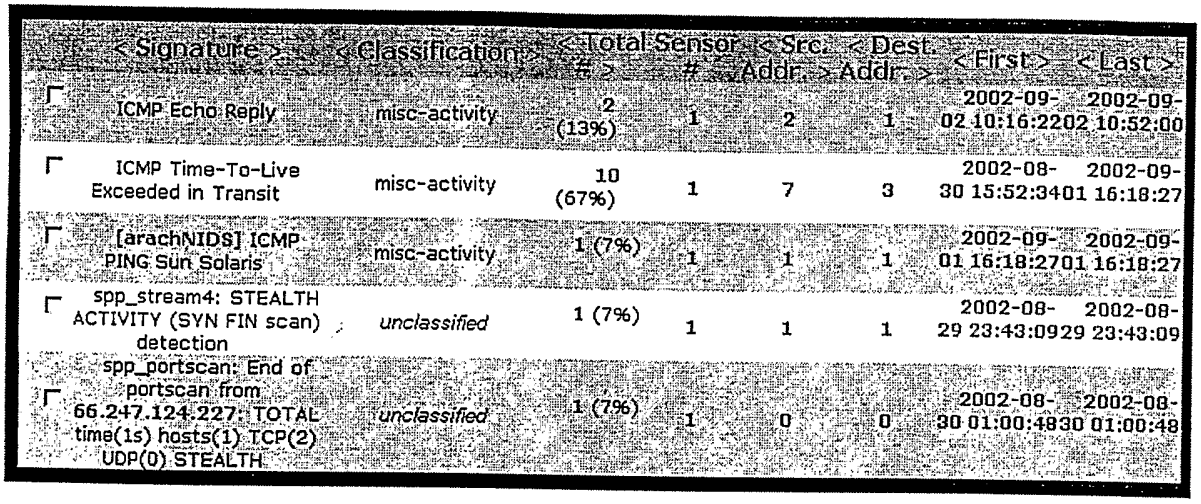
FQDN: mailin.genius.de (local whois)

Num of Sensors	Occurances as Src.	Occurances as Dest.	First Occurance	Last Occurance
1	1	0	2002-09-02 10:16:22	2002-09-02 10:16:22

Whois Information

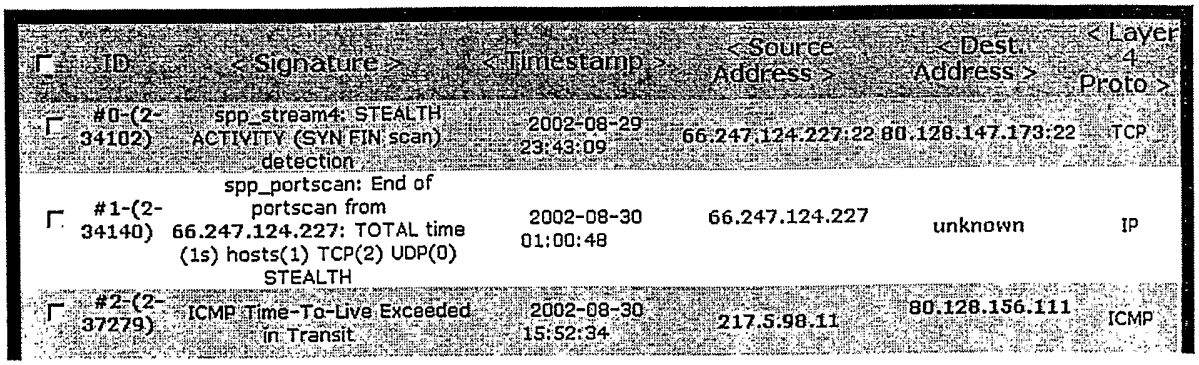
```
% This is the RIPE Whois server.
% The objects are in RPSL format.
% Please visit http://www.ripe.net/rpsl for more information.
% Rights restricted by copyright.
% See http://www.ripe.net/ripencc/pub-services/db/copyright.html

inetnum:        62.225.10.0 - 62.225.10.255
```

Fig. 10



<Signature>	<Classification>	<Total # >	Sensor #	<Src. Addr.>	<Dest. Addr.>	<First>	<Last>
ICMP Echo Reply	misc-activity	2 (13%)	1	2	1	2002-09-02 10:16:22	2002-09-02 10:52:00
ICMP Time-To-Live Exceeded in Transit	misc-activity	10 (67%)	1	7	3	2002-08-30 15:52:34	2002-09-01 16:18:27
[arachNIDS] ICMP PING Sun Solaris	misc-activity	1 (7%)	1	1	1	2002-09-01 16:18:27	2002-09-01 16:18:27
spp_stream4: STEALTH ACTIVITY (SYN FIN scan) detection	*unclassified*	1 (7%)	1	1	1	2002-08-29 23:43:09	2002-08-29 23:43:09
spp_portscan: End of portscan from 66.247.124.227: TOTAL time(1s) hosts(1) TCP(2) UDP(0) STEALTH	*unclassified*	1 (7%)	1	0	0	2002-08-30 01:00:48	2002-08-30 01:00:48

Fig. 11



ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(2-34102)	spp_stream4: STEALTH ACTIVITY (SYN FIN scan) detection	2002-08-29 23:43:09	66.247.124.227:22	80.128.147.173:22	TCP
#1-(2-34140)	spp_portscan: End of portscan from 66.247.124.227: TOTAL time (1s) hosts(1) TCP(2) UDP(0) STEALTH	2002-08-30 01:00:48	66.247.124.227	unknown	IP
#2-(2-37279)	ICMP Time-To-Live Exceeded in Transit	2002-08-30 15:52:34	217.5.98.11	80.128.156.111	ICMP

Fig. 12

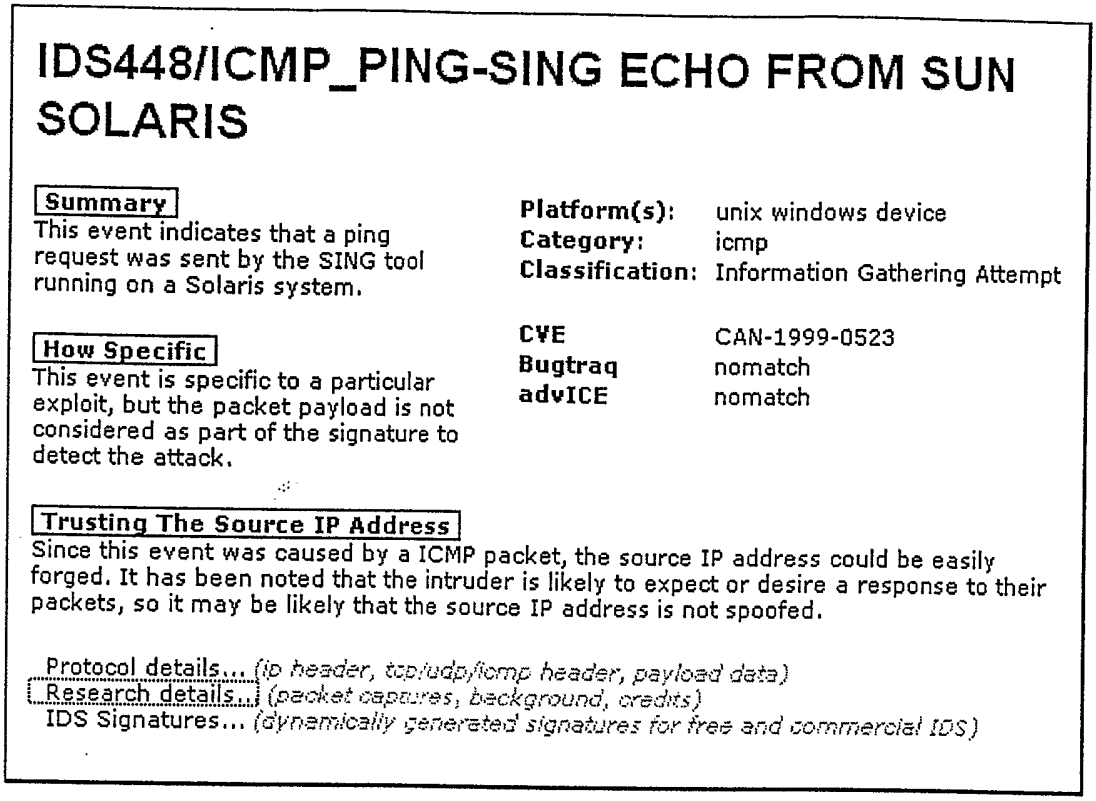

IDS448/ICMP_PING-SING ECHO FROM SUN SOLARIS
Summary
This event indicates that a ping request was sent by the SING tool running on a Solaris system.
How Specific
This event is specific to a particular exploit, but the packet payload is not considered as part of the signature to detect the attack.
Platform(s): unix windows device
Category: icmp
Classification: Information Gathering Attempt
CVE CAN-1999-0523
Bugtraq nomatch
advICE nomatch
Trusting The Source IP Address
Since this event was caused by a ICMP packet, the source IP address could be easily forged. It has been noted that the intruder is likely to expect or desire a response to their packets, so it may be likely that the source IP address is not spoofed.
Protocol details... (ip header, tcp/udp/icmp header, payload data)
Research details... (packet captures, background, credits)
IDS Signatures... (dynamically generated signatures for free and commercial IDS)

Fig. 13

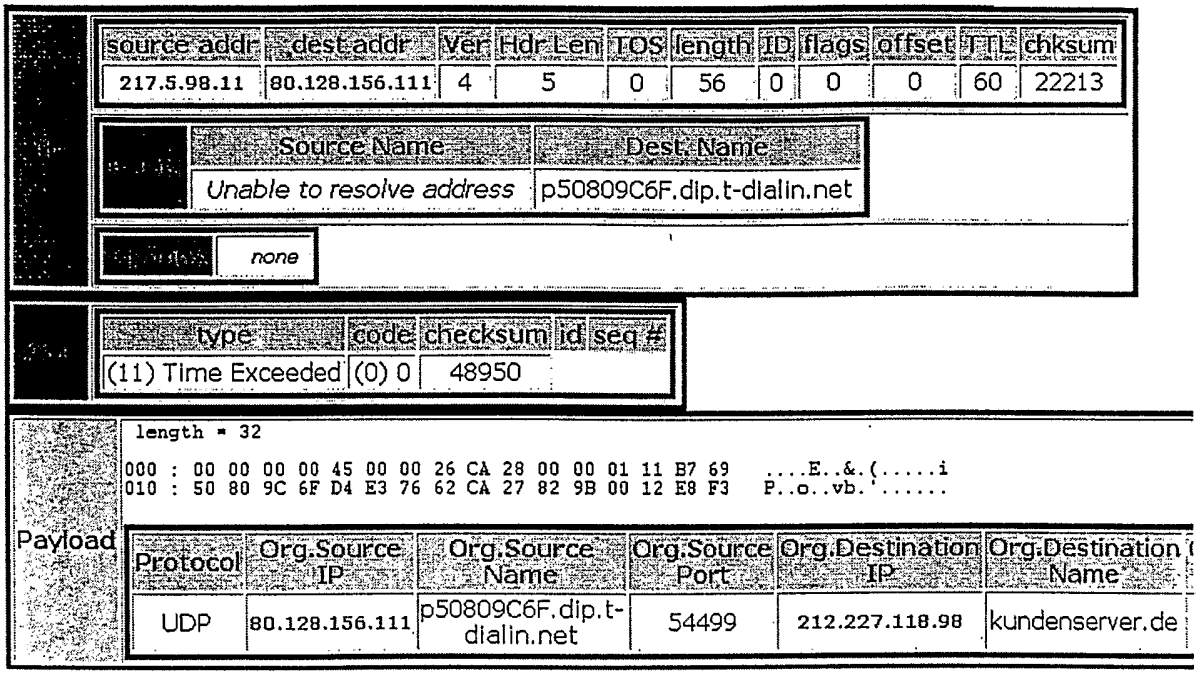

source addr
dest addr
ver
Hdr Len
TOS
length
ID
flags
offset
T TL
chksum
217.5.98.11
80.128.156.111
4
5
0
56
0
0
0
60
22213
Source Name
Dest. Name
Unable to resolve address
p50809C6F.dip.t-dialin.net
none
type
code
checksum
id
seq #
(11) Time Exceeded
(0) 0
48950
length = 32
000 : 00 00 00 00 45 00 00 26 CA 28 00 00 01 11 B7 69 ....E..&.(.....i
010 : 50 80 9C 6F D4 E3 76 62 CA 27 82 9B 00 12 E8 F3 P..o..vb.'.....
Payload
Protocol
Org.Source IP
Org.Source Name
Org.Source Port
Org.Destination IP
Org.Destination Name
UDP
80.128.156.111
p50809C6F.dip.t-dialin.net
54499
212.227.118.98
kundenserver.de

Fig. 14

Eingeloggt von Rechner 10.210.64.1 (10.210.64.1) am 02.09.2002 um 11:16:08 Uhr.

>>Seite: bisher eingeloggte Benutzer, Startseite

Session_ID	Date	Username	Name	PHP_Session_ID
117	2002-08-24 22:45:10	thesesites	ultimativer Meister	d8d5508c8b716b7bf8071ab6276d29ac
139	2002-08-27 10:46:21	fag-herbig	Herr Michael Herbig	e39cda613cb2f245619d1e2892f2d094
142	2002-08-27 12:28:54	fag-herbig	Herr Michael Herbig	9b8c532de06bbe44508b90dc799b40d8
144	2002-08-27 15:46:53	jab-brinkmann	Herr Klaus Brinkmann	d28448ec3cb902a1a72ec23a14644306
180	2002-09-02 09:55:44	pichler	Herr Dr. Cletus von Pichler	574b9211b35911643e74d6d646f4628b
182	2002-09-02 10:29:48	peter@pka	Moped-Peter	de47a7729695c88f4028e2d34ce459d5
auswählen	alle	alle	alle	alle

bisher eingelogte Benutzer | besuchte

Fig. 15

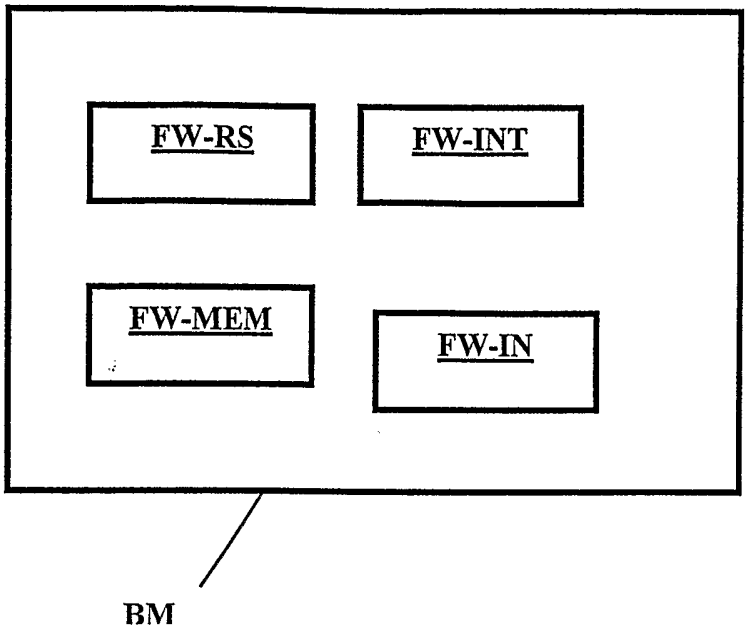


Fig. 16