(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
27. Februar 2003 (27.02.2003)

PCT

(10) Internationale Veröffentlichungsnummer
WO 03/017613 A1

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

(21) Internationales Aktenzeichen: PCT/EP01/09328

(22) Internationales Anmeldedatum:
13. August 2001 (13.08.2001)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **IP-ONLINE GMBH** [DE/DE]; Willy-Brandt-Platz 6, 68161 Mannheim (DE). **SCOPE CONSULTING GMBH** [DE/DE]; Willy-Brandt-Platz 6, 68161 Mannheim (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **GEIS, Christoph** [DE/DE]; Friedrich-Ebert-Str. 21, 65795 Hattersheim (DE). **PAUSCH, Eberhard** [DE/DE]; An der Ziegelhütte 32, 35435 Wettenberg (DE). **SOYSAL, Thomas** [DE/DE]; In der Hydnstr. 3, 69190 Walldorf (DE). **SCHIEMANN, Ralf** [DE/DE]; Alte Bruchsaler Strasse 52, 69168 Wiesloch (DE).

(74) Anwalt: **AUE, Hans-Peter**; Tannenring 79, 65207 Wiesbaden (DE).

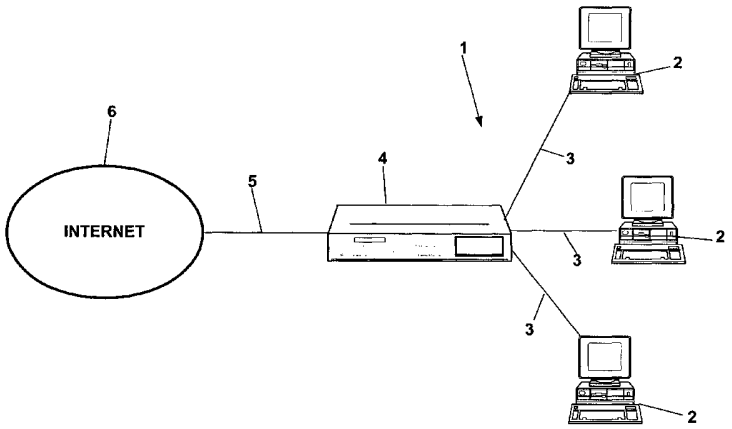
(81) Bestimmungsstaaten *(national)*: AE, AL, AU, BA, BG, CA, CN, CZ, GE, HR, HU, ID, IL, IN, JP, KP, KR, LT, LV, MK, MN, MX, NO, NZ, PL, RO, RU, SG, SI, SK, UA, US, UZ, VN, YU, ZA.

(84) Bestimmungsstaaten *(regional)*: europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD, DATA CARRIER, COMPUTER SYSTEM AND COMPUTER PROGRAMME FOR THE IDENTIFICATION AND DEFENCE OF ATTACKS ON SERVER SYSTEMS OF NETWORK SERVICE PROVIDERS AND OPERATORS

(54) Bezeichnung: VERFAHREN, DATENTRÄGER, COMPUTERSYSTEM UND COMPUTERPROGRAMMPRODUKT ZUR ERKENNUNG UND ABWEHR VON ANGRIFFEN AUF SERVERSYSTEME VON NETZWERK-DIENSTEANBIETERN UND -BETREIBERN



(57) Abstract: The invention relates to a method for the identification and defence of attacks on the server systems of network service providers and operators, using an electronic device (4) that can be integrated into a computer network and that comprises a computer programme, and relates to a data carrier, which contains a computer programme for carrying out said method. The invention also relates to a computer system, which is connected to a network, such as the Internet (6), an intranet or similar and has one or several computers that are configured as server computers (2) or client computers, and to a computer programme containing computer programme codes for the identification and defence of attacks on server systems. The invention comprises - protection against DoS and DDoS attacks (flood attacks)- link-level security,- verification of valid IP headers, - verification of IP packet characteristics, - TCP/IP fingerprint protection,- blocking of all UDP network packets,- exclusion of specific external IP addresses, - packet-level firewall function, - protection of accessible services of the target system. The invention provides the highest possible degree of security and protection against DoS and DDoS attacks.

[Fortsetzung auf der nächsten Seite]

WO 03/017613 A1

Veröffentlicht:
— *mit internationalem Recherchenbericht*
— *insgesamt in elektronischer Form (mit Ausnahme des Kopfbogens); auf Antrag vom Internationalen Büro erhältlich*

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.

(57) Zusammenfassung: Die Erfindung bezieht sich auf ein Verfahren zur Erkennung und Abwehr von Angriffen auf Serversysteme von Netzwerk-Diensteanbietern und -betreibern mittels eines in ein Computer-Netzwerk einzubindenden elektronischen Gerätes (4), dass ein Computerprogramm aufweist, sowie einen Datenträger, der ein Computerprogramm zur Durchführung dieses Verfahrens enthält. Weiterhin bezieht sich die Erfindung auf ein Computersystem, dass mit einem Netzwerk, wie Internet (6), Intranet und dergleichen, verbunden ist, aufweisend einen oder mehrere Computer, die als Server-Computer (2) oder als Client-Computer konfiguriert sind, sowie auf ein Computerprogrammprodukt, aufweisend Computerproramm-Codes zur Erkennung und Abwehr von Angriffen auf Serversysteme. Die Erfindung umfasst - Schutz vor DoS- und DDoS-Attacken (Flood-Attacken)- Link Level Sicherheit,- Untersuchung gültiger IP-Header,- Untersuchung von Merkmalen des IP-Paketes,- TCP/IP Fingerprint-Schutz,- Sperrung aller UDP-Netzwerkpakete,- Ausschließen bestimmter externer IP-Adressen,- Paket-Level-Firewall-Funktion,- Schutz von erreichbaren Diensten des Zielsystems.Durch die Erfindung wird ein möglichst hohes Maß an Sicherheit und Schutz vor DoS- und DDoS-Attacken erzielt.

Verfahren, Datenträger, Computersystem und Computerprogrammprodukt zur Erkennung und Abwehr von Angriffen auf Serversysteme von Netzwerk-Diensteanbietern und -betreibern

Die Erfindung bezieht sich auf ein Verfahren zur Erkennung und Abwehr von Angriffen auf Serversysteme von Netzwerk-Diensteanbietern und -betreibern mittels eines in ein Computer-Netzwerk einzubindenden elektronischen Gerätes, dass ein Computerprogramm aufweist, sowie einen Datenträger, der ein Computerprogramm zur Durchführung dieses Verfahrens enthält. Weiterhin bezieht sich die Erfindung auf ein Computersystem, dass mit einem Netzwerk, wie Internet, Intranet und dergleichen, verbunden ist, aufweisend einen oder mehrere Computer, die als Server-Computer oder als Client-Computer konfiguriert sind, sowie auf ein Computerprogrammprodukt, aufweisend Computerproramm-Codes zur Erkennung und Abwehr von Angriffen auf Serversysteme von Netzwerk-Diensteanbietern und -betreibern mittels eines in ein Computer-Netzwerk einzubindenden elektronischen Gerätes, dass dieses Computerprogrammprodukt enthält.

Die weltweite Vernetzung nimmt starkem Tempo zu. Eine immer größer werdende Anzahl von Unternehmen setzt verstärkt auf die scheinbar unbegrenzten Möglichkeiten im Bereich Online-Marketing und eBusiness. Mit den Möglichkeiten wachsen aber auch die Gefahren, dass die Server bekannter Firmen Institutionen durch Angriffe aus dem Internet blockiert werden.

Das Internet gewinnt als elektronischer Marktplatz im Rahmen der E-Commerce-Aktivitäten vieler Unternehmen immer mehr an Bedeutung. Gleichwohl wächst aber auch die Bedrohung der Unternehmensnetze durch DoS- und DDoS-Attacken (Denial of Service und Distributed Denial of Service = Verhindern eines Zugriffes oder Nutzens eines Computers bzw. des darauf befindlichen Serviceprozesses) überproportional an. Oft entstehen hierbei beträchtliche finanzielle Schäden, die relativ leicht, auch ohne ein tatsächliches Eindringen von Hackern in die gesicherte Systemumgebung eines Unternehmens, nur durch das erfolgreiche Verhindern der Online-Geschäfte (E-Commerce/E-Business) entstehen können. Viele Versuche dieses Problem zu bewältigen blieben, gemessen an ihren Erfolgen, weit hinter den Erwartungen zurück. Einer der ist, dass es bisher kein wirkliches Detektionssystem für diese Art von Attacken gegeben hat, welches im Prinzip die einzige Möglichkeit zur Abwehr in einer von Attacken betroffenen Systemumgebung darstellt. Ein anderes Problem liegt in der Beschaffenheit des Internets und der damit nahezu aussichtslosen Situation, die Verursachung solcher Attacken nur dann verhindern zu können, wenn uneingeschränkt alle der weltweit existierenden Netzwerkprovider einheitliche Maßnahmen zur Unterbindung solcher Hackerattacken etablieren würden. Dies ist unter anderem der Grund, dass alle auf nationaler Ebene angestrebte Versuche zur Verhinderung von DOS- bzw. DDoS-Attacken bisher leider erfolglos blieben oder nur mäßigen Erfolg hatten.

Das Internet stellt bekanntermaßen ein internationales Geflecht technischer Komponenten dar, z.B. Switches, Router und Übertragungskomponenten mit multipler Wegeführung usw.. Somit ist es für Hacker oft leicht möglich einzelne Server oder auch ganze Netze bzw. Netzwerkbereiche lahmzulegen. Lokale oder nationale Maßnahmen versprechen kaum eine wirksame Verhinderung, da es in dem internationalen Geflecht von Routern, Netz-Providern und den beliebten On-Call-Verbindungen den Hackern relativ leicht möglich ist, einen Weg bzw. eine gangbare Angriffsstrategie für ihre Vorhaben ausfindig zu machen. Selbst wenn bei solchen Angriffen nicht immer direkte Schäden durch Datenverluste oder auch Datenmanipulationen oder unbefugte Datenkopierung entstehen müssen, wirkt sich der Imageverlust entsprechend empfindlich für das betroffene Unternehmen aus.

Programme, mit deren Hilfe solche Attacken ausgeführt werden können, stehen im World Wide Web (WWW) frei zur Verfügung. Sie können von Hackern jederzeit per „Download" abgerufen werden. Die meisten dieser gefürchteten Angriffe nutzen technische Schwächen in den Datenübertragungsprotokollen aus, auf denen die Kommunikation im Internet basiert. Die betroffenen Rechner werden meist mit einer so großen Anzahl von Scheinanfragen belastet, dass ernst gemeinte Anfragen nicht mehr bearbeitet werden können. Somit ist der betroffene Rechner für einen realen Kunden scheinbar nicht mehr aktiv.

Beispielhaft werden einige bekannte Maßnahmen genannt, die DoS- und DDoS-Attacken abwehren bzw. vorbeugen können.

Im lokalen Umfeld der Netzvermittler und -provider könnten Maßnahmen ergriffen werden, die das Aufsetzen von DoS- und DDoS-Attacken mit der aktiven Verhinderung der Nutzung von gefälschten IP-Adressen erheblich erschweren würden. Viele DoS-Angriffe nutzen nämlich gefälschte IP- Absenderadressen (IP-Spoofing), um die Ermittlung des Verursachers zu verhindern bzw. erheblich zu erschweren. Durch entsprechende technische Regeln in der Netzinfrastruktur der Netzvermittler, können die Netzbetreiber diese Möglichkeit wesentlich einschränken, so dass gefälschte IP-Pakete aus dem eigenen Serviceumfeld nicht weiter ins Internet vermittelt werden. Einer Organisation, die an einen Netzbetreiber angeschlossen ist, steht dabei ein bestimmter IP-Adressbereich zur Verfügung. Jedes IP-Paket, dass aus dieser Organisation in das Internet geschickt wird, müsste eine IP-Absenderadresse aus diesem Bereich haben. Ist dies nicht der Fall, so handelt es sich sehr wahrscheinlich um eine gefälschte Adresse und das IP-Paket sollte vom Netzvermittler nicht weitergeleitet werden, d. h., es soll eine Paketfilterung auf die Absenderadressen beim Einspeisen der Pakete in das Internet durchgeführt werden. Zwar ist IP-Spoofing innerhalb des erlaubten Adressbereichs der Organisation noch immer möglich, jedoch ist der Kreis der möglichen Verursacher auf die Organisation eingeschränkt. Darüber hinaus müsste das Betreiben von so genannten „Anonymous

Hosts" weltweit überdacht und wenn möglich eingeschränkt oder auch unterbunden werden. Dies ist jedoch organisatorisch, zeitlich, rechtlich und finanziell extrem aufwändig.

Bislang ist die Widerstandsfähigkeit von Servern gegenüber der in der Praxis angewendeten DoS- und DDoS-Attacken oftmals sehr begrenzt. Einige Systeme können jedoch etwas länger andere Systeme nur sehr kurzzeitig diesen Attacken widerstehen. Länger anhaltende Attacken führen zurzeit jedoch so gut wie immer zum Erfolg.

Herkömmlich verwendete Paketfilterungslösungen helfen gegen DoS- und DDoS-Attacken leider oftmals nicht oder werden selbst so weit in Mitleidenschaft gezogen, dass sie ihre Schutzwirkung, gerade bei anhaltenden Attakken, sehr bald verlieren. Auch zahlreiche Angriffserkennungssysteme stehen weit zurück, da sie bei den DoS- und DDoS-Attacken oftmals nur das hohe Netzverkehrsaufkommen erkennen und Warnungen ausgeben, die dann meistens erst viel zu spät zu Reaktionen führen.

Im Falle eines erfolgreichen Angriffs ist es von zentraler Bedeutung, schnell reagieren zu können. Nur so ist es möglich wirksame Gegenmaßnahmen einzuleiten, eventuell den Angreifer zu identifizieren und den Normalbetrieb innerhalb kurzer Zeit wieder herzustellen. In einem Notfallplan ist daher eine geeignete Eskalationsprozedur festzuschreiben. Notwendige Angaben sind dabei u. a. Ansprechpartner, Verantwortliche, alternative Kommunikationswege, Handlungsanweisungen und La-

gerort möglicherweise benötigter Ressourcen und Sicherungsmedien.

Die Server der Serverbetreiber können als Agenten eines DoS-Angriffs missbraucht werden. Der Angreifer installiert dazu unter Ausnutzung bekannter Schwachstellen Schadsoftware. Daher müssen die Betreiber der Server diese sorgfältig und sicher konfigurieren. Nicht benötigte Netzdienste werden deaktiviert und die benötigten abgesichert. Ein hinreichender Passwort- und Zugriffsschutz sowie rechtzeitiges Ändern (insbesondere voreingestellter) Passwörter muss sichergestellt sein.

Viele WWW-Seiten im Internet sind derzeit nur nutzbar, wenn in den Browsern aus Sicherheitssicht bedenkliche Einstellungen vorgenommen werden, die von einem Angreifer missbraucht werden können.

Viele Inhalte-Anbieter stellen im Internet Programme und Dokumente zum Download bereit. Gelingt es einem Angreifer, dort ein trojanisches Pferd einzubringen, so kann er in kurzer Zeit auf eine große Verbreitung hoffen. Eine solche Vorgehensweise ist insbesondere bei DDoS-Angriffen für Angreifer verlockend, da dabei eine große Zahl von Rechnern für einen wirkungsvollen Angriff benötigt wird.

Rechner der Endanwender sind im Normalfall nicht Ziel von DoS-Angriffen. Allerdings können diese Rechner dazu benutzt werden, dass ein Angreifer in einem ersten Schritt Programme auf ihnen installiert, die dann fern-

gesteuert einen DoS-Angriff auf beliebige Rechner ermöglichen.

Rechner von Endanwendern können als Agenten für Angriffe missbraucht werden. Am leichtesten lassen sich solche Agenten über Viren, trojanische Pferde oder durch aktive Inhalte auf die einzelnen Rechner installieren. Daher ist ein zuverlässiger und aktueller Virenschutz sowie das Abschalten aktiver Inhalte im Browser dringend notwendig. Gegebenenfalls kann auch der Einsatz von Hilfsprogrammen zum Online-Schutz des Clients, beispielsweise PC-Firewalls, erwogen werden. Häufig werden aber auch insbesondere neue Computerviren nicht hinreichend erkannt und beseitigt.

Immer wieder werden neue sicherheitsrelevante Schwachstellen in den Betriebssystemen und der Serversoftware entdeckt, die wenig später durch Updates bzw. Patches der Hersteller behoben werden. Um möglichst zeitnah reagieren zu können, ist es notwendig, Software-Hersteller auf Updates zu überwachen. Die relevanten Updates sind dann schnellstmöglich einzuspielen, um die bekannt gewordenen Schwachstellen zu beheben.

Um einen Rechner vor Risiken und Gefahren zu schützen, ist z. T. erhebliches Know-how zur Erarbeitung einer effektiven IT-Sicherheitskonfiguration notwendig. Administratoren müssen daher ausreichend aus- und weitergebildet werden.

Es ist zwar nicht damit zu rechnen, dass die Maßnahmen

zur Verhinderung von IP-Spoofing wirklich zeitnah weltweit und einheitlich von den zahlreichen Netzwerk-Vermittlern und -Providern umgesetzt werden, jedoch kann man mit den zur Abwehr beschriebenen restlichen Maßnahmen bereits einen mehr oder weniger wirksamen Erfolg gegen DoS- und DDoS- Attacken erreichen. Ein befriedigendes Ergebnis lässt sich mit den bekannten Mitteln bisher jedoch nicht erreichen.

Es ist Aufgabe der Erfindung, Mittel zur Erkennung und Abwehr von Angriffen auf Serversysteme von Netzwerk-Diensteanbietern und -betreibern der eingangs genannten Art zu schaffen, mit denen DoS- und DDoS-Attacken gezielt erkannt und abgewehrt werden können, um dadurch ein möglichst hohes Maß an Sicherheit und Schutz vor DoS- und DDoS-Attacken zu erzielen und den Computer bzw. das Computersystem dauerhaft stabil und leistungsfähig zu erhalten.

Erfindungsgemäß wird die Aufgabe verfahrensmäßig gelöst durch die Bestandteile und Verfahrensschritte

- Schutz vor DoS- und DDoS-Attacken (Flood-Attacken), wobei,
  - jeder IP Syn (IP-Verbindungsaufbauwunsch) registriert und zur Bewahrung im IP-Protokoll festgelegten Zeitbeschränkung mit einem Syn Ack beantwortet wird, während das registrierte Syn-Paket auf Gültigkeit und die im Zielssystem verfügbaren Dienste geprüft wird und
  - der Verbindungsaufbau mit dem Zielsystem initialisiert und das empfangene Datenpaket an das

Zielsystem zur weiteren Bearbeitung übergeben wird, wenn die Prüfung erfolgreich abgeschlossen ist und zwischenzeitlich der wiederum von dem von außen anfragenden System auszusendende Ack sowie ein darauf folgendes gültiges Datenpaket empfangen wurde, und/oder

- Link Level Sicherheit, wobei die zu prüfenden Datenpakete direkt von der OSI-Schicht 2 (Link Level) übernommen wird, und/oder
- Untersuchung gültiger IP-Header, wobei der Aufbau jedes IP-Paketes vor dessen Weiterleitung auf das Zielsystem auf Gültigkeit überprüft und jedes ungültige IP-Paket verworfen wird, und/oder
- Untersuchung des IP-Paketes durch Überprüfung insbesondere der Länge und der Prüfsumme des IP-Paketes auf Übereinstimmung der Angaben im TCP- oder IP-Header mit dem Aufbau des IP-Paketes, und/oder
- TCP/IP Fingerprint-Schutz, wobei der als Antwort ausgehende Datenverkehr von den geschützten Systemen zu den von außen anfragenden Systemen neutralisiert wird, indem musterhafte Protokoll-Identifizierer verwendet werden, und/oder
- Sperrung aller UDP-Netzwerkpakete zur Verhinderung von Angriffen auf die geschützten Systeme über das Netzwerkprotokoll UDP (User Data Protokoll), indem über UDP erreichbare benötigte Dienste gezielt registriert und freigegeben werden, wobei Nachrichten explizit für diese UDP-Ports zugelassen werden, die übrigen Ports jedoch geschlossen bleiben, und/oder
- Längenbeschränkungen von ICMP-Paketen (Internet Control Message), wobei ICMP_Nachrichten nur in einer

vorgegebenen Maximallänge als gültige Datenpakete erkannt und hiervon abweichende ICMP-Pakete verworfen werden, und/oder

- Ausschließen bestimmter externer IP-Adressen von der Kommunikation mit dem Zielsystem, und/oder
- Paket-Level-Firewall-Funktion, wobei ein- und ausgehende IP-Pakete mittels frei definierbarer Regeln untersucht und auf Grund dieser Regeln abgelehnt oder an das Zielsystem weitergeleitet werden, und/oder
- Schutz von erreichbaren Diensten des Zielsystems durch Ausschluss bestimmter Dienste und/oder Benutzer und/oder Umlenkung von Diensteanfragen auf andere Server.

Erfindungsgemäß wird die Aufgabe auch durch einen Datenträger, enthaltend ein Computerprogramm zur Erkennung und Abwehr von Angriffen auf Serversysteme von Netzwerk-Diensteanbietern und -betreibern zum Einsatz in einem in ein Computer-Netzwerk einzubindenden elektronischen Gerät, gelöst, der die Programmschritte aufweist

- Schutz vor DoS- und DDoS-Attacken (Flood-Attacken), wobei,
  - jeder IP Syn (IP-Verbindungsaufbauwunsch) registriert und zur Bewahrung im IP-Protokoll festgelegten Zeitbeschränkung mit einem Syn Ack beantwortet wird, während das registrierte Syn-Paket auf Gültigkeit und die im Zielssystem verfügbaren Dienste geprüft wird und
  - der Verbindungsaufbau mit dem Zielsystem initia-

lisiert und das empfangene Datenpaket an das Zielsystem zur weiteren Bearbeitung übergeben wird, wenn die Prüfung erfolgreich abgeschlossen ist und zwischenzeitlich der wiederum von dem von außen anfragenden System auszusendende Ack sowie ein darauf folgendes gültiges Datenpaket empfangen wurde, und/oder

- Link Level Sicherheit, wobei die zu prüfenden Datenpakete direkt von der OSI-Schicht 2 (Link Level) übernommen wird, und/oder
- Untersuchung gültiger IP-Header, wobei der Aufbau jedes IP-Paketes vor dessen Weiterleitung auf das Zielsystem auf Gültigkeit überprüft und jedes ungültige IP-Paket verworfen wird, und/oder
- Untersuchung des IP-Paketes durch Überprüfung insbesondere der Länge und der Prüfsumme des IP-Paketes auf Übereinstimmung der Angaben im TCP- oder IP-Header mit dem Aufbau des IP-Paketes, und/oder
- TCP/IP Fingerprint-Schutz, wobei der als Antwort ausgehende Datenverkehr von den geschützten Systemen zu den von außen anfragenden Systemen neutralisiert wird, indem musterhafte Protokoll-Identifizierer verwendet werden, und/oder
- Sperrung aller UDP-Netzwerkpakete zur Verhinderung von Angriffen auf die geschützten Systeme über das Netzwerkprotokoll UDP, indem über UDP erreichbare benötigte Dienste gezielt registriert und freigegeben werden, wobei Nachrichten explizit für diese UDP-Ports zugelassen werden, die übrigen Ports jedoch geschlossen bleiben, und/oder
- Längenbeschränkungen von ICMP-Paketen, wobei

ICMP_Nachrichten nur in einer vorgegebenen Maximallänge als gültige Datenpakete erkannt und hiervon abweichende ICMP-Pakete verworfen werden, und/oder

- Ausschließen bestimmter externer IP-Adressen von der Kommunikation mit dem Zielsystem, und/oder
- Paket-Level-Firewall-Funktion, wobei ein- und ausgehende IP-Pakete mittels frei definierbarer Regeln untersucht und auf Grund dieser Regeln abgelehnt oder an das Zielsystem weitergeleitet werden, und/oder
- Schutz von erreichbaren Diensten des Zielsystems durch Ausschluss bestimmter Dienste und/oder Benutzer und/oder Umlenkung von Diensteanfragen auf andere Server.

Bevorzugt ist der Datenträger als EPROM ausgebildet und ist Bestandteil eines elektronischen Gerätes. Dieses elektronische Gerät kann ein Einschubgerät zum Einsetzen in einen Computer oder auch eine separate Gerätebox sein.

Alternativ wird die Aufgabe auch durch ein Computersystem gelöst, dass mit einem Netzwerk, wie Internet, Intranet und dergleichen, verbunden ist, aufweisend einen oder mehrere Computer, die als Server-Computer oder als Client-Computer konfiguriert sind. Dabei ist in eine zu schützende Datenleitung zwischen das Netzwerk und den Server- oder Client-Computer ein elektronisches Gerät geschaltet ist, welches mit einem Datenträger versehen ist, der ein Computerprogramm aufweist, das die Programmschritte enthält:

- Schutz vor DoS- und DDoS-Attacken (Flood-Attacken), wobei,
  - jeder IP Syn (IP-Verbindungsaufbauwunsch) registriert und zur Bewahrung im IP-Protokoll festgelegten Zeitbeschränkung mit einem Syn Ack beantwortet wird, während das registrierte Syn-Paket auf Gültigkeit und die im Zielssystem verfügbaren Dienste geprüft wird und
  - der Verbindungsaufbau mit dem Zielsystem initialisiert und das empfangene Datenpaket an das Zielsystem zur weiteren Bearbeitung übergeben wird, wenn die Prüfung erfolgreich abgeschlossen ist und zwischenzeitlich der wiederum von dem von außen anfragenden System auszusendende Ack sowie ein darauf folgendes gültiges Datenpaket empfangen wurde, und/oder
- Link Level Sicherheit, wobei die zu prüfenden Datenpakete direkt von der OSI-Schicht 2 (Link Level) übernommen wird, und/oder
- Untersuchung gültiger IP-Header, wobei der Aufbau jedes IP-Paketes vor dessen Weiterleitung auf das Zielsystem auf Gültigkeit überprüft und jedes ungültige IP-Paket verworfen wird, und/oder
- Untersuchung des IP-Paketes durch Überprüfung insbesondere der Länge und der Prüfsumme des IP-Paketes auf Übereinstimmung der Angaben im TCP- oder IP-Header mit dem Aufbau des IP-Paketes, und/oder
- TCP/IP Fingerprint-Schutz, wobei der als Antwort ausgehende Datenverkehr von den geschützten Systemen zu den von außen anfragenden Systemen neutralisiert wird, indem musterhafte Protokoll-Identifizierer

verwendet werden, und/oder

- Sperrung aller UDP-Netzwerkpakete zur Verhinderung von Angriffen auf die geschützten Systeme über das Netzwerkprotokoll UDP, indem über UDP erreichbare benötigte Dienste gezielt registriert und freigegeben werden, wobei Nachrichten explizit für diese UDP-Ports zugelassen werden, die übrigen Ports jedoch geschlossen bleiben, und/oder
- Längenbeschränkungen von ICMP-Paketen, wobei ICMP_Nachrichten nur in einer vorgegebenen Maximallänge als gültige Datenpakete erkannt und hiervon abweichende ICMP-Pakete verworfen werden, und/oder
- Ausschließen bestimmter externer IP-Adressen von der Kommunikation mit dem Zielsystem, und/oder
- Paket-Level-Firewall-Funktion, wobei ein- und ausgehende IP-Pakete mittels frei definierbarer Regeln untersucht und auf Grund dieser Regeln abgelehnt oder an das Zielsystem weitergeleitet werden, und/oder
- Schutz von erreichbaren Diensten des Zielsystems durch Ausschluss bestimmter Dienste und/oder Benutzer und/oder Umlenkung von Diensteanfragen auf andere Server.

Des Weiteren erfolgt die Lösung der Aufgabe erfindungsgemäß durch ein Computerprogrammprodukt, aufweisend Computerproramm-Codes zur Erkennung und Abwehr von Angriffen auf Serversysteme von Netzwerk-Diensteanbietern und -betreibern mittels eines in ein Computer-Netzwerk einzubindenden elektronischen Gerätes, dass dieses Computerprogrammprodukt enthält. Das Computerprogrammpro-

dukt umfasst die Programmschritte

- Schutz vor DoS- und DDoS-Attacken (Flood-Attacken), wobei,
  - jeder IP Syn (IP-Verbindungsaufbauwunsch durch zum Schein aufgebaute TCP/IP-Verbindungen) registriert und zur Bewahrung im IP-Protokoll festgelegten Zeitbeschränkung mit einem Syn Ack beantwortet wird, während das registrierte Syn-Paket auf Gültigkeit und die im Zielssystem verfügbaren Dienste geprüft wird und
  - der Verbindungsaufbau mit dem Zielsystem initialisiert und das empfangene Datenpaket an das Zielsystem zur weiteren Bearbeitung übergeben wird, wenn die Prüfung erfolgreich abgeschlossen ist und zwischenzeitlich der wiederum von dem von außen anfragenden System auszusendende Ack sowie ein darauf folgendes gültiges Datenpaket empfangen wurde, und/oder
- Link Level Sicherheit, wobei die zu prüfenden Datenpakete direkt von der OSI-Schicht 2 (Link Level) übernommen wird, und/oder
- Untersuchung gültiger IP-Header, wobei der Aufbau jedes IP-Paketes vor dessen Weiterleitung auf das Zielsystem auf Gültigkeit überprüft und jedes ungültige IP-Paket verworfen wird, und/oder
- Untersuchung des IP-Paketes durch Überprüfung insbesondere der Länge und der Prüfsumme des IP-Paketes auf Übereinstimmung der Angaben im TCP- oder IP-Header mit dem Aufbau des IP-Paketes, und/oder
- TCP/IP Fingerprint-Schutz, wobei der als Antwort ausgehende Datenverkehr von den geschützten Systemen

zu den von außen anfragenden Systemen neutralisiert wird, indem musterhafte Protokoll-Identifizierer verwendet werden, und/oder

- Sperrung aller UDP-Netzwerkpakete zur Verhinderung von Angriffen auf die geschützten Systeme über das Netzwerkprotokoll UDP, indem über UDP erreichbare benötigte Dienste gezielt registriert und freigegeben werden, wobei Nachrichten explizit für diese UDP-Ports zugelassen werden, die übrigen Ports jedoch geschlossen bleiben, und/oder
- Längenbeschränkungen von ICMP-Paketen, wobei ICMP_Nachrichten nur in einer vorgegebenen Maximallänge als gültige Datenpakete erkannt und hiervon abweichende ICMP-Pakete verworfen werden, und/oder
- Ausschließen bestimmter externer IP-Adressen von der Kommunikation mit dem Zielsystem, und/oder
- Paket-Level-Firewall-Funktion, wobei ein- und ausgehende IP-Pakete mittels frei definierbarer Regeln untersucht und auf Grund dieser Regeln abgelehnt oder an das Zielsystem weitergeleitet werden, und/oder
- Schutz von erreichbaren Diensten des Zielsystems durch Ausschluss bestimmter Dienste und/oder Benutzer und/oder Umlenkung von Diensteanfragen auf andere Server.

Ein besonderer Vorteil der erfindungsgemäßen Lösung besteht darin, dass nicht nur alle geschützten Systeme vor Angriffsversuchen mittels DoS- und DDoS-Attacken abgesichert werden, sondern auch das Computerprogramm zur Durchführung des Verfahrens zur Erkennung und Ab-

wehr von Angriffen auf Serversysteme von Netzwerk-Diensteanbietern und -betreibern selbst abgesichert ist.

Der Schutz vor DoS- und DDoS-Attacken bildet den Kern des erfindungsgemäßen Verfahrens. Diese Attacken haben zum Ziel, den oder die Zielcomputer durch eine Flut von Verbindungsaufbau-Paketen zum Erliegen, d.h. zum Abstürzen zu bringen. Die angegriffenen Systeme sind anschließend nicht mehr in der Lage, auf Kommunikationsanforderungen zu reagieren. Durch ein intelligentes Regelwerk werden nun alle geschützten Systeme vor Angriffsversuchen mittels DoS- und DDoS-Attacken abgesichert. Dabei wird eine besondere Behandlung der eingehenden Netzwerkpakete sichergestellt, indem nur die legitimen Anforderungen die geschützte Datenleitung passieren können und die Zielsysteme, wie beispielsweise WorldWideWeb- (WWW) oder Email-Server, nicht durch Massenangriffe zum Erliegen kommen.

Da im Link-Level-Sicherheits-Modul die zu prüfenden Datenpakete direkt von der OSI-Schicht 2 übernommen wird, ist eine eigene IP-Adresse nicht notwendig. Somit ist es auch nicht erforderlich, aufwändige Umkonfigurationen der bestehenden Netzwerkumgebung bezüglich der logischen Adressierung (IP-Routing) durchzuführen. Damit bildet die damit dem Verfahren betriebene Hardware keine adressierbare Netzkomponente, so dass weder ein gezielter Angriff aus dem Netzwerk noch ein Ausspähen möglich ist.

Viele TCP/IP-Implementierungen reagieren mit einem Fehlverhalten, wenn der Header eines IP-Paketes einen ungültigen Aufbau besitzt. Wenn der Aufbau jedes IP-Paketes vor dessen Weiterleitung auf das Zielsystem auf Gültigkeit überprüft wird, wird sichergestellt, dass nur IP-Pakete mit korrektem Aufbau an die Zielsysteme gelangen.

Um Angriffe auf Computersysteme erfolgreich durchführen zu können, ist das Wissen um das darauf laufende Betriebssystem wichtig, denn gezielte Angriffe auf Serversysteme basieren auf der Kenntnis um das zu Grunde liegende Betriebssystem des Zielrechners. TCP/IP FingerPrint-Routinen untersuchen das Verhalten der TCP/IP-Implementierungen des Zielsystems und können daraus das Betriebssystem ableiten. Die Erfindung stellt mit ihrer Funktionalität sicher, dass der Angreifer durch Analyse der Antwortpakete keine Rückschlüsse auf das verwendete Betriebssystem erhält. Ein IP-Fingerprint ist dadurch nicht mehr möglich.

Um Computer in einem TCP/IP-Netzwerk anzugreifen, werden unterschiedliche Methoden verwendet. Eine Möglichkeit hierzu ist das Versenden von ICMP-Nachrichten mit einer unverhältnismäßig hohen Paketlänge. Um diese Problem proaktiv zu bekämpfen, wirkt die in die Erfindung implementierte Funktion der Längenbeschränkung von ICMP-Paktene auch hierfür.

Die Möglichkeit, bestimmte externe IP-Adressen von der Kommunikation auszuschließen, erhöht die Gesamtsicher-

heit der eigenen Systeme. Wird beispielsweise erkannt, dass von einem Rechner aus dem Internet untersucht wird, welche Ports auf dem eigenen System offen und damit angreifbar sind, kann angewiesen werden, alle Pakete von diesem Computer zu verwerfen. Die Liste der ausgeschlossenen Rechner (Blacklist) kann später modifiziert werden, so dass alte Einträge wieder gelöscht werden können.

Zusätzlich zur Paket-Level-Firewall-Funktion auf IP-Paket-Ebene wird die Erfindung um Schutzmechanismen in Bezug auf die erreichbaren Dienste erweitert, die über die IP-Protokolle HTTP, FTP, NNTP, POP, IMAP, SMTP, X, LDAP, LPR, Socks oder SSL erreichbar sind. Der Ausschluss bestimmter Dienste bzw. Benutzer oder die Umlenkung von Diensteanfragen auf andere Server wird mit dieser Funktionalität gewährleistet. Eine einfache Konfiguration dieser Komponente wird über eine Administrationsoberfläche ermöglicht, über die solche Einschränkungen festgelegt werden können.

Mit dem erfindungsgemäßen Verfahren, der Software und dem das Computerprogramm enthaltenden elektronischen Gerät werden alle ein- und ausgehenden Nachrichten überwacht. Bei Erkennen einer Attacke greift die erfindungsgemäße Lösung gezielt ein und blockiert selektiv die verdächtigen Datenpakete ohne dadurch den normalen Datenverkehr zu beeinträchtigen. Alle regulären Daten werden nahezu verzögerungsfrei weitergeleitet, so dass der Einsatz der erfindungsgemäßen Lösung im Normalfall für den Anwender keinerlei Arbeits- bzw. Kommunikati-

onsbeeinträchtigung impliziert. Dies gilt auch dann, wenn die Anschlüsse an das Internetserverseitig mit hoher Geschwindigkeit (und hohem Datenaufkommen) betrieben werden (100 Mbit/s).

Weitere Maßnahmen und Ausgestaltungen des erfindungsgemäßen Verfahrens ergeben sich aus den Unteransprüchen 2 bis 6.

Nach einer Ausgestaltung des erfindungsgemäßen Verfahrens wird bei der Längenbeschränkung von ICMP-Paketen die ungültige Länge des ICMP-Paketes auf eine zulässige Länge reduziert. Dabei können neben der Längenbeschränkung von ICMP-Paketen die einzelnen ICPM-Nachrichtentypen auch vollständig gesperrt werden.

Nach einer weiteren Ausgestaltung der Paket-Level-Firewall-Funktion werden die Regeln hierfür auf der Basis bestimmter Kriterien eines IP-Paketes insbesondere in Bezug auf Ausschlüsse, Einschränkungen und Log-Ausgaben festgelegt. Das Administrationsprogramm erstellt anschließend eine Konfigurationsdatei für die Firewall.

Bei einer vorteilhaften Ausgestaltung der Erfindung erfolgen zur kontrollierten Konfiguration und Sicherstellung der uneingeschränkten Funktion des Verfahrens administrative Eingriffe nur von einer Konsole oder über gesicherte Netzwerk-Verbindungswege.

Des Weiteren kann der Zugriff auf das Zielsystem über

frei einstellbare Zeitfenster detailliert eingeschränkt werden.

Die Gesamtheit der Erfindung ist somit eine speziell konfigurierte bzw. konfektionierte Hardware auf Personal-Computer-Basis, die adaptiv mit Microchips (EPROMs) mit speziell entwickelten Microcode ausgestattet ist. Hinzu kommt ein speziell entwickeltes interdisziplinäres, jedoch system- und leitungsschichtnahes Verfahren bzw. Computerprogramm, das in Form eines Systemprogrammes auf die verscheiden ausgerichteten Probleme differenziert reagiert. Es besteht nun die Möglichkeit, den Datenstrom bereits aus dem Leitungsprotokoll (OSI Schicht 2) zu entnehmen und auf sicherheitsrelevante Inhalte der darüber liegenden Schichten (OSI Schicht 3 - OSI Schicht 7) hin zu untersuchen. Eine der wesentlichen Eigenschaften der Erfindung ist damit, die funktionelle Erweiterung der eigentlich passiven Datenleitung um die aktive Intelligenz zur Überprüfung des Datenstromes auf angriffsrelevante Inhalte. Da jedoch mit den enthaltenen Prüfroutinen, im Gegensatz zu allen anderen auf dem Markt befindlichen Sicherheitskomponenten auch nachweislich „Flood-Attacks" sowie Angriffe auf IP-Stack- und Betriebssystemebene der mit dem Verfahren geschützten Rechner erkannt und verhindert werden können, sind über den Ansatz der Einbindungsweise hinaus auch noch weitere Alleinstellungsmerkmale implementiert. Die kombinierte erfindungsgemäße Hard- und Software schützt sich und die dahinter geschalteten Systeme im internen Netzwerk aktiv. Die kombinierte Lösung wird in die jeweilige Zugangsleitung zwischen dem Screening-

Router und den zu schützenden Systemen, mitunter noch vor der eigentlichen Firewall und damit auch vor der DMZ (Demillitarisierte Zone), eingeschleift. Mittels der unterschiedlichen Methoden, die auf Grund der Modularität der Erfindung gesamtheitlich oder eingeschränkt zum Einsatz kommen, werden angriffsrelevante Inhalte einschließlich Internet Protokoll -Aufwärts erkannt und abgewehrt. Die Daten werden unabhängig von der im IP-Header eingetragenen Zieladresse aufgenommen und in einer als „neutrale Instanz" zu beschreibenden Verfahrensweise auf angriffsrelevante Inhalte hin untersucht. Als Besonderheit muss deshalb auch angesehen werden, dass das Schutzsystem selbst nicht auf IP-Ebene angegriffen werden kann, da dieses System im eigentlichen Sinne keine über das IP-Protokoll adressierbare Komponente darstellt und sich damit für aktive Netzwerkkomponenten als völlig unsichtbar darstellt.

Ein wesentliches Element der Erfindung stellt die aktive Detektion von DoS- und dDoS-Attacken dar, welche durch die erfindungsgemäße kombinierte Hard- und Software-Lösung möglich geworden ist. Allein auf der Seite der Serverbetreiber eingesetzt, kann durch die Erfindung ein aktiver Schutz der Serversysteme erreicht werden. In Verbindung mit dem Einsatz auf der Seite der Netzwerk-Provider, kann die durch DoS- und DDoS-Attacken drohende Überlastung der Leitung aktiv verhindert werden. Wichtig ist aber auch, dass das DoS-Detektionssystem nicht die herkömmlich etablierten Firewalls ersetzt, sondern lediglich um wichtige Bestandteile ergänzt.

Es versteht sich, dass die vorstehend genannten und nachstehend noch zu erläuternden Merkmale nicht nur in der jeweils angegebenen Kombination, sondern auch in anderen Kombinationen oder in Alleinstellung verwendbar sind, ohne den Rahmen der vorliegenden Erfindung zu verlassen.

Der der Erfindung zu Grunde liegende Gedanke wird in der nachfolgenden Beschreibung anhand von Ausführungsbeispielen, die in den Zeichnungen dargestellt sind, näher beschrieben. Es zeigen:

Fig. 1 eine schematische Darstellung eines erfindungsgemäßen Computersystems, das mit dem Internet verbunden ist, in einem kleinen Netzwerkumfeld;

Fig. 2 eine schematische Darstellung eines erfindungsgemäßen Computersystems, das mit dem Internet verbunden ist, in einem mittelgroßen Netzwerkumfeld;

Fig. 3 eine schematische Darstellung eines erfindungsgemäßen Computersystems, das mit dem Internet verbunden ist, in einem großen Netzwerkumfeld;

Fig. 4 eine schematische Darstellung der erfindungsgemäßen Verfahrensweise beim Verbindungsaufbau und zulässigem Protokollgebrauch;

Fig. 5 eine schematische Darstellung der erfindungsgemäßen Verfahrensweise beim Verbindungsaufbau und unzulässigem Protokollgebrauch;

Fig. 6 eine schematische Darstellung der erfindungsgemäßen Verfahrensweise beim unvollständigen Verbindungsaufbau;

Fig. 7 eine schematische Darstellung der erfindungsgemäßen Verfahrensweise nach dem Verbindungsaufbau bei zulässigem Datenverkehr;

Fig. 8 eine schematische Darstellung der erfindungsgemäßen Verfahrensweise nach dem Verbindungsaufbau bei unzulässigem Datenverkehr;

Fig. 9 eine schematische Darstellung der durch ein elektronisches Gerät geschützten Protokollebenen;

Fig. 10 eine Darstellung der Untersuchung gültiger IP-Header;

Fig. 11 eine Darstellung der Untersuchung eines IP-Pakets;

Fig. 12 eine Darstellung der Untersuchung von einstellbaren UDP-Verbindungen und

Fig. 13 eine Darstellung der Längenbeschränkung von ICMP-Paketen.

Das Computersystem 1 gemäß den Fig. 1 bis 3 besteht aus mehreren Server-Computern 2, die gegebenenfalls miteinander durch nicht weiter dargestellte Datenleitungen miteinander vernetzt sind. Die Server-Computer 2 sind jeweils über eine Datenleitung 3 mit einem elektronischen Gerät 4 verbunden. Dieses weist einen nicht näher dargestellten, als EPROM ausgebildeten Datenträger auf, der mit einem Computerprogramm zur Erkennung und Abwehr von Angriffen auf Serversysteme von Netzwerk-Diensteanbietern und -betreibern versehen ist.

Das elektronische Gerät 4 ist gemäß Fig. 1 über eine ISDN-Datenleitung 5 mit dem Internet 6 verbunden. Das elektronische Gerät 4 dient dem Schutz von DoS- und DDoS-Attacken und besitzt eine erweiterte Funktionalität als Internet-Gateway über ISDN. Ferner ist das elektronische Gerät 4 mit einem Ethernet- und einem ISDN-Adapter ausgestattet. Neben dem Schutz der im Local Area Network (LAN) liegenden Systeme vor DoS- und DDoS-Attacken wird das elektronische Gerät 4 als Router für den Zugriff auf Dienste des Internets verwendet. Der ISDN-Verbindungsaufbau erfolgt standardmäßig immer dann, wenn eine Kommunikationsanbindung an das externe Netzwerk gewünscht wird. Der Verbindungsaufbau erfolgt automatisch, wenn das im elektronischen Gerät 4 auf dem EPROM enthaltene Computerprogramm nach einer definierten Zeitspanne keine weiteren Netzwerkpakete weiterleitet. Dieses Standardverhalten kann jedoch durch ent-

sprechende Konfiguration geändert werden.

Das elektronische Gerät 4 gemäß Fig. 2 ist über eine ISDN/Ethernet-Datenleitung 7 beispielsweise mit dem Internet 6 verbunden. Ferner ist in das elektronische Gerät 4 ein nicht sichtbarer Firewall-Funktionsmodul integriert, so dass es als integrierter Firewall-Router eingesetzt wird, gegebenenfalls über einen weiteren dedizierten Router. Die Server-Computer 2 bzw. Arbeitsplatzrechner des internen Netzwerkes nutzen das elektronische Gerät 4 mit dem das Computerprogramm zur Erkennung und Abwehr von Angriffen auf Serversysteme von Netzwerk-Diensteanbietern und -betreibern enthaltenden EPROM als Übergang in das Internet über Ethernet oder ISDN. Weiterhin schützt das elektronische Gerät 4 die internen Systeme vor DoS- und DDoS-Attacken. Dabei werden ein- und ausgehende IP-Pakete mittels definierter Regeln weitergeleitet oder verworfen. Der Zugriff auf die öffentlich zugänglichen Dienste auf den lokalen Systemen wird an Hand definierter Regeln erlaubt oder abgewiesen.

Die für die einzelnen Funktionen notwendigen Regelwerke werden über ein Konfigurationsprogramm erstellt und modifiziert, das auch den vereinfachten Benutzereingaben ein vom System lesbares Konfigurationsset erstellt. Die vom elektronischen Gerät 4 mit dem Computerprogramm zur Erkennung und Abwehr von Angriffen auf Serversysteme von Netzwerk-Diensteanbietern und -betreibern angebotenen Funktionen sind weitestgehend frei konfigurierbar

und können somit für den Einsatz in das eigene Netzwerk optimal eingestellt werden.

Bei der Ausführungsform der Erfindung nach Fig. 3 ist das Firewall-Funktionsmodul 9 separat, d.h. getrennt zwischen den Server-Computern 2 und dem elektronischen Gerät 4 mit dem Computerprogramm zur Erkennung und Abwehr von Angriffen auf Serversysteme von Netzwerk-Diensteanbietern und -betreibern geschaltet. Das elektronische Gerät 4 ist über eine Ethernet-Datenleitung 8 mit dem Internet 6 verbunden und bietet den notwendigen Schutz vor DoS- und DDoS-Angriffen (Flood-Attacken). Nur Netzwerkpakete, die erkennbar nicht das betroffene Zielsystem schaden können, werden an die Firewall zur weiteren Bearbeitung geleitet. Auf der Firewall wird anschließend entscheiden, ob die Netzwerkpakete weitergeleitet oder abgewiesen werden.

Fig. 4 zeigt eine schematische Darstellung der Verfahrensweise beim Verbindungsaufbau und zulässigem Protokollgebrauch, während Fig. 5 die Verfahrensweise beim Verbindungsaufbau mit unzulässigem Protokollgebrauch darstellt.

In Fig. 6 wird das erfindungsgemäßen Verfahrensweise beim unvollständigen Verbindungsaufbau gezeigt. Fig. 7 stellt schematisch die Verfahrensweise nach dem Verbindungsaufbau bei zulässigem Datenverkehr und Fig. 8 die Verfahrensweise nach dem Verbindungsaufbau bei unzulässigem Datenverkehr dar.

Fig. 9 zeigt eine schematische Darstellung der durch ein elektronisches Gerät geschützten Protokollebenen, welches ein Computerprogramm zur Erkennung und Abwehr von Angriffen auf Serversysteme von Netzwerk-Diensteanbietern und -betreibern enthaltenden EPROM aufweist.

Die Fig. 10 zeigt eine Darstellung der Untersuchung gültiger IP-Header. In Fig. 11 ist die der Untersuchung eines IP-Pakets dargestellt. Fig. 12 zeigt eine Darstellung der Untersuchung von einstellbaren UDP-Verbindungen und Fig. 13zeigt eine Darstellung der Längenbeschränkung von ICMP-Paketen.

Liste der Bezugszeichen

1 Computersystem
2 Server-Computer
3 Datenleitung
4 elektronisches Gerät
5 ISDN-Datenleitung
6 Internet
7 ISDN/Ethernet-Datenleitung
8 Ethernet-Datenleitung

Patentansprüche

1. Verfahren zur Erkennung und Abwehr von Angriffen auf Serversysteme von Netzwerk-Diensteanbietern und -betreibern mittels eines in ein Computer-Netzwerk einzubindenden elektronischen Gerätes, dass ein Computerprogramm enthält, **gekennzeichnet durch** die Bestandteile und Verfahrensschritte
   - Schutz vor DoS- und DDoS-Attacken (Flood-Attacken), wobei,
     - jeder IP Syn (IP-Verbindungsaufbauwunsch) registriert und zur Bewahrung im IP-Protokoll festgelegten Zeitbeschränkung mit einem Syn Ack beantwortet wird, während das registrierte Syn-Paket auf Gültigkeit und die im Zielssystem verfügbaren Dienste geprüft wird und
     - der Verbindungsaufbau mit dem Zielsystem initialisiert und das empfangene Datenpaket an das Zielsystem zur weiteren Bearbeitung übergeben wird, wenn die Prüfung erfolgreich abgeschlossen ist und zwischenzeitlich der wiederum von dem von außen anfragenden System auszusendende Ack sowie ein darauf folgendes gültiges Datenpaket empfangen wurde, und/oder
   - Link Level Sicherheit, wobei die zu prüfenden Datenpakete direkt von der OSI-Schicht 2 (Link Level) übernommen wird, und/oder
   - Untersuchung gültiger IP-Header, wobei der Aufbau jedes IP-Paketes vor dessen Weiterleitung auf das Zielsystem auf Gültigkeit überprüft und

jedes ungültige IP-Paket verworfen wird, und/oder

- Untersuchung des IP-Paketes durch Überprüfung insbesondere der Länge und der Prüfsumme des IP-Paketes auf Übereinstimmung der Angaben im TCP- oder IP-Header mit dem Aufbau des IP-Paketes, und/oder
- TCP/IP Fingerprint-Schutz, wobei der als Antwort ausgehende Datenverkehr von den geschützten Systemen zu den von außen anfragenden Systemen neutralisiert wird, indem musterhafte Protokoll-Identifizierer verwendet werden, und/oder
- Sperrung aller UDP-Netzwerkpakete zur Verhinderung von Angriffen auf die geschützten Systeme über das Netzwerkprotokoll UDP, indem über UDP erreichbare benötigte Dienste gezielt registriert und freigegeben werden, wobei Nachrichten explizit für diese UDP-Ports zugelassen werden, die übrigen Ports jedoch geschlossen bleiben, und/oder
- Längenbeschränkungen von ICMP-Paketen, wobei ICMP_Nachrichten nur in einer vorgegebenen Maximallänge als gültige Datenpakete erkannt und hiervon abweichende ICMP-Pakete verworfen werden, und/oder
- Ausschließen bestimmter externer IP-Adressen von der Kommunikation mit dem Zielsystem, und/oder
- Paket-Level-Firewall-Funktion, wobei ein- und ausgehende IP-Pakete mittels frei definierbarer Regeln untersucht und auf Grund dieser Regeln abgelehnt oder an das Zielsystem weitergeleitet

werden, und/oder

- Schutz von erreichbaren Diensten des Zielsystems durch Ausschluss bestimmter Dienste und/oder Benutzer und/oder Umlenkung von Diensteanfragen auf andere Server.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet**, dass bei der Längenbeschränkung von ICMP-Paketen die ungültige Länge des ICMP-Paketes auf eine zulässige Länge reduziert wird.

3. Verfahren nach Anspruch 1, **dadurch gekennzeichnet**, dass bei der Längenbeschränkung von ICMP-Paketen die einzelnen ICPM-Nachrichtentypen vollständig gesperrt werden.

4. Verfahren nach Anspruch 1, **dadurch gekennzeichnet**, dass die Regeln für die Paket-Level-Firewall-Funktion auf der Basis bestimmter Kriterien eines IP-Paketes insbesondere in Bezug auf Ausschlüsse, Einschränkungen und Log-Ausgaben festgelegt werden.

5. Verfahren nach den Ansprüchen 1 bis 4, **dadurch gekennzeichnet**, dass zur kontrollierten Konfiguration und Sicherstellung der uneingeschränkten Funktion des Verfahrens administrative Eingriffe nur von einer Konsole oder über gesicherte Netzwerk-Verbindungswege erfolgen.

6. Verfahren nach den Ansprüchen 1 bis 5, **dadurch gekennzeichnet**, dass der Zugriff auf das Zielsystem

über frei einstellbare Zeitfenster detailliert eingeschränkt wird.

7. Datenträger, enthaltend ein Computerprogramm zur Erkennung und Abwehr von Angriffen auf Serversysteme von Netzwerk-Diensteanbietern und -betreibern zum Einsatz in einem in ein Computer-Netzwerk einzubindenden elektronischen Gerät, **gekennzeichnet durch** die Programmschritte
   - Schutz vor DoS- und DDoS-Attacken (Flood-Attacken), wobei,
     - jeder IP Syn (IP-Verbindungsaufbauwunsch) registriert und zur Bewahrung im IP-Protokoll festgelegten Zeitbeschränkung mit einem Syn Ack beantwortet wird, während das registrierte Syn-Paket auf Gültigkeit und die im Zielssystem verfügbaren Dienste geprüft wird und
     - der Verbindungsaufbau mit dem Zielsystem initialisiert und das empfangene Datenpaket an das Zielsystem zur weiteren Bearbeitung übergeben wird, wenn die Prüfung erfolgreich abgeschlossen ist und zwischenzeitlich der wiederum von dem von außen anfragenden System auszusendende Ack sowie ein darauf folgendes gültiges Datenpaket empfangen wurde, und/oder
   - Link Level Sicherheit, wobei die zu prüfenden Datenpakete direkt von der OSI-Schicht 2 (Link Level) übernommen wird, und/oder
   - Untersuchung gültiger IP-Header, wobei der Aufbau jedes IP-Paketes vor dessen Weiterleitung auf das Zielsystem auf Gültigkeit überprüft und

jedes ungültige IP-Paket verworfen wird, und/oder

- Untersuchung des IP-Paketes durch Überprüfung insbesondere der Länge und der Prüfsumme des IP-Paketes auf Übereinstimmung der Angaben im TCP- oder IP-Header mit dem Aufbau des IP-Paketes, und/oder
- TCP/IP Fingerprint-Schutz, wobei der als Antwort ausgehende Datenverkehr von den geschützten Systemen zu den von außen anfragenden Systemen neutralisiert wird, indem musterhafte Protokoll-Identifizierer verwendet werden, und/oder
- Sperrung aller UDP-Netzwerkpakete zur Verhinderung von Angriffen auf die geschützten Systeme über das Netzwerkprotokoll UDP, indem über UDP erreichbare benötigte Dienste gezielt registriert und freigegeben werden, wobei Nachrichten explizit für diese UDP-Ports zugelassen werden, die übrigen Ports jedoch geschlossen bleiben, und/oder
- Längenbeschränkungen von ICMP-Paketen, wobei ICMP_Nachrichten nur in einer vorgegebenen Maximallänge als gültige Datenpakete erkannt und hiervon abweichende ICMP-Pakete verworfen werden, und/oder
- Ausschließen bestimmter externer IP-Adressen von der Kommunikation mit dem Zielsystem, und/oder
- Paket-Level-Firewall-Funktion, wobei ein- und ausgehende IP-Pakete mittels frei definierbarer Regeln untersucht und auf Grund dieser Regeln abgelehnt oder an das Zielsystem weitergeleitet

werden, und/oder

- Schutz von erreichbaren Diensten des Zielsystems durch Ausschluss bestimmter Dienste und/oder Benutzer und/oder Umlenkung von Diensteanfragen auf andere Server.

8. Datenträger nach Anspruch 5, **dadurch gekennzeichnet**, dass dieser als EPROM ausgebildet und Bestandteil eines elektronischen Gerätes ist.

9. Computersystem, dass mit einem Netzwerk, wie Internet (6), Intranet und dergleichen, verbunden ist, aufweisend einen oder mehrere Computer, die als Server-Computer (2) oder als Client-Computer konfiguriert sind, **dadurch gekennzeichnet**, dass in eine zu schützende Datenleitung (5. 7, 8) zwischen das Netzwerk (6) und den Server- (2) oder Client-Computer ein elektronisches Gerät (4) geschaltet ist, welches mit einem Datenträger versehen ist, der ein Computerprogramm aufweist, das die Programmschritte enthält:

- Schutz vor DoS- und DDoS-Attacken (Flood-Attacken), wobei,
  - jeder IP Syn (IP-Verbindungsaufbauwunsch) registriert und zur Bewahrung im IP-Protokoll festgelegten Zeitbeschränkung mit einem Syn Ack beantwortet wird, während das registrierte Syn-Paket auf Gültigkeit und die im Zielssystem verfügbaren Dienste geprüft wird und
  - der Verbindungsaufbau mit dem Zielsystem initialisiert und das empfangene Datenpaket an

das Zielsystem zur weiteren Bearbeitung übergeben wird, wenn die Prüfung erfolgreich abgeschlossen ist und zwischenzeitlich der wiederum von dem von außen anfragenden System auszusendende Ack sowie ein darauf folgendes gültiges Datenpaket empfangen wurde, und/oder

- Link Level Sicherheit, wobei die zu prüfenden Datenpakete direkt von der OSI-Schicht 2 (Link Level) übernommen wird, und/oder
- Untersuchung gültiger IP-Header, wobei der Aufbau jedes IP-Paketes vor dessen Weiterleitung auf das Zielsystem auf Gültigkeit überprüft und jedes ungültige IP-Paket verworfen wird, und/oder
- Untersuchung des IP-Paketes durch Überprüfung insbesondere der Länge und der Prüfsumme des IP-Paketes auf Übereinstimmung der Angaben im TCP- oder IP-Header mit dem Aufbau des IP-Paketes, und/oder
- TCP/IP Fingerprint-Schutz, wobei der als Antwort ausgehende Datenverkehr von den geschützten Systemen zu den von außen anfragenden Systemen neutralisiert wird, indem musterhafte Protokoll-Identifizierer verwendet werden, und/oder
- Sperrung aller UDP-Netzwerkpakete zur Verhinderung von Angriffen auf die geschützten Systeme über das Netzwerkprotokoll UDP, indem über UDP erreichbare benötigte Dienste gezielt registriert und freigegeben werden, wobei Nachrichten explizit für diese UDP-Ports zugelassen werden, die übrigen Ports jedoch geschlossen blei-

ben, und/oder

- Längenbeschränkungen von ICMP-Paketen, wobei ICMP_Nachrichten nur in einer vorgegebenen Maximallänge als gültige Datenpakete erkannt und hiervon abweichende ICMP-Pakete verworfen werden, und/oder
- Ausschließen bestimmter externer IP-Adressen von der Kommunikation mit dem Zielsystem, und/oder
- Paket-Level-Firewall-Funktion, wobei ein- und ausgehende IP-Pakete mittels frei definierbarer Regeln untersucht und auf Grund dieser Regeln abgelehnt oder an das Zielsystem weitergeleitet werden, und/oder
- Schutz von erreichbaren Diensten des Zielsystems durch Ausschluss bestimmter Dienste und/oder Benutzer und/oder Umlenkung von Diensteanfragen auf andere Server.

10. Computerprogrammprodukt, aufweisend Computerproramm-Codes zur Erkennung und Abwehr von Angriffen auf Serversysteme von Netzwerk-Diensteanbietern und -betreibern mittels eines in ein Computer-Netzwerk einzubindenden elektronischen Gerätes, dass dieses Computerprogrammprodukt enthält, **gekennzeichnet durch** die Programmschritte

- Schutz vor DoS- und DDoS-Attacken (Flood-Attacken), wobei,
  - jeder IP Syn (IP-Verbindungsaufbauwunsch) registriert und zur Bewahrung im IP-Protokoll festgelegten Zeitbeschränkung mit einem Syn Ack beantwortet wird, während das registrierte

Syn-Paket auf Gültigkeit und die im Zielssystem verfügbaren Dienste geprüft wird und

- der Verbindungsaufbau mit dem Zielsystem initialisiert und das empfangene Datenpaket an das Zielsystem zur weiteren Bearbeitung übergeben wird, wenn die Prüfung erfolgreich abgeschlossen ist und zwischenzeitlich der wiederum von dem von außen anfragenden System auszusendende Ack sowie ein darauf folgendes gültiges Datenpaket empfangen wurde, und/oder

- Link Level Sicherheit, wobei die zu prüfenden Datenpakete direkt von der OSI-Schicht 2 (Link Level) übernommen wird, und/oder
- Untersuchung gültiger IP-Header, wobei der Aufbau jedes IP-Paketes vor dessen Weiterleitung auf das Zielsystem auf Gültigkeit überprüft und jedes ungültige IP-Paket verworfen wird, und/oder
- Untersuchung des IP-Paketes durch Überprüfung insbesondere der Länge und der Prüfsumme des IP-Paketes auf Übereinstimmung der Angaben im TCP- oder IP-Header mit dem Aufbau des IP-Paketes, und/oder
- TCP/IP Fingerprint-Schutz, wobei der als Antwort ausgehende Datenverkehr von den geschützten Systemen zu den von außen anfragenden Systemen neutralisiert wird, indem musterhafte Protokoll-Identifizierer verwendet werden, und/oder
- Sperrung aller UDP-Netzwerkpakete zur Verhinderung von Angriffen auf die geschützten Systeme über das Netzwerkprotokoll UDP, indem über UDP

erreichbare benötigte Dienste gezielt registriert und freigegeben werden, wobei Nachrichten explizit für diese UDP-Ports zugelassen werden, die übrigen Ports jedoch geschlossen bleiben, und/oder

- Längenbeschränkungen von ICMP-Paketen, wobei ICMP_Nachrichten nur in einer vorgegebenen Maximallänge als gültige Datenpakete erkannt und hiervon abweichende ICMP-Pakete verworfen werden, und/oder
- Ausschließen bestimmter externer IP-Adressen von der Kommunikation mit dem Zielsystem, und/oder
- Paket-Level-Firewall-Funktion, wobei ein- und ausgehende IP-Pakete mittels frei definierbarer Regeln untersucht und auf Grund dieser Regeln abgelehnt oder an das Zielsystem weitergeleitet werden, und/oder
- Schutz von erreichbaren Diensten des Zielsystems durch Ausschluss bestimmter Dienste und/oder Benutzer und/oder Umlenkung von Diensteanfragen auf andere Server.

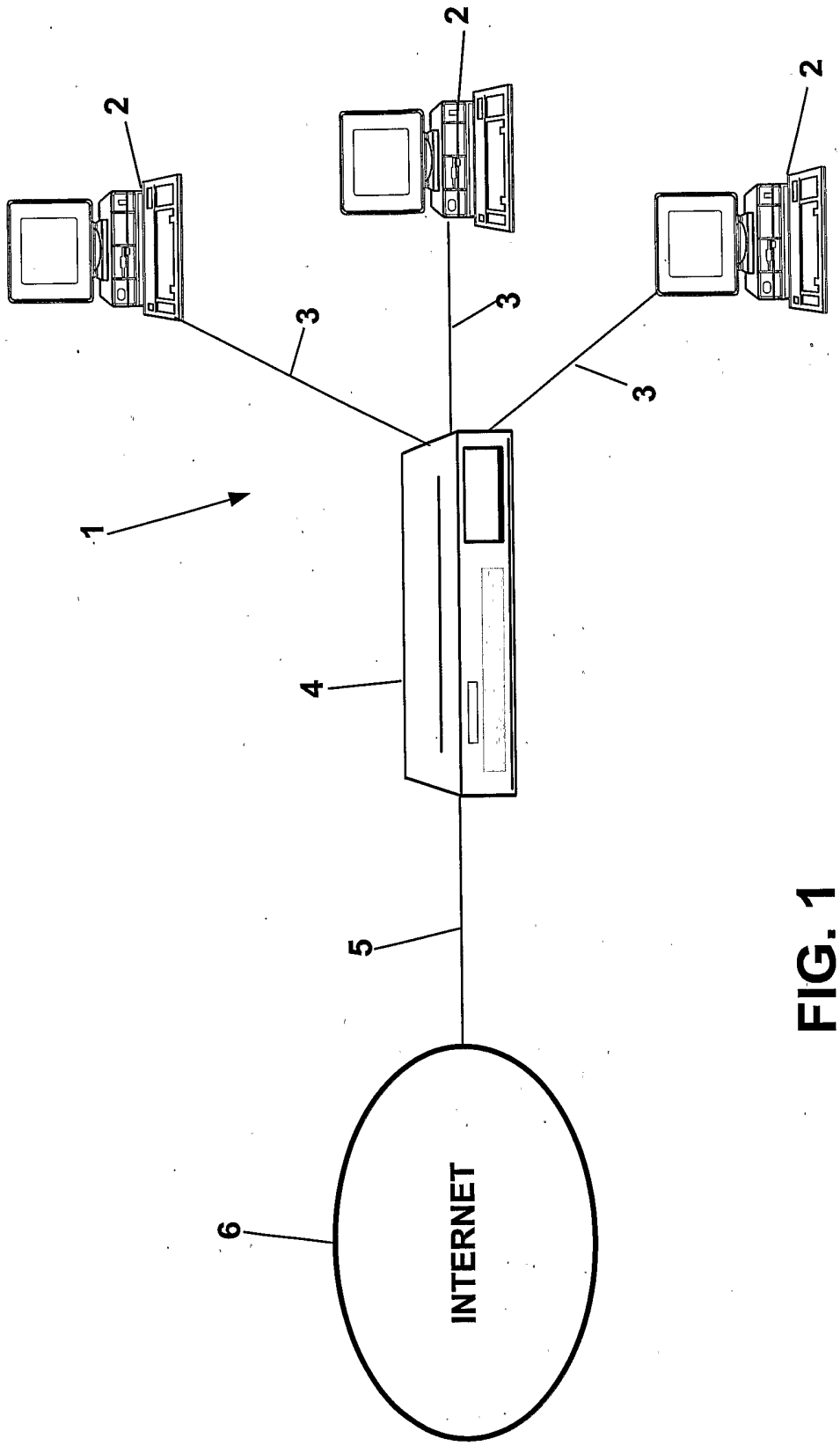


FIG. 1

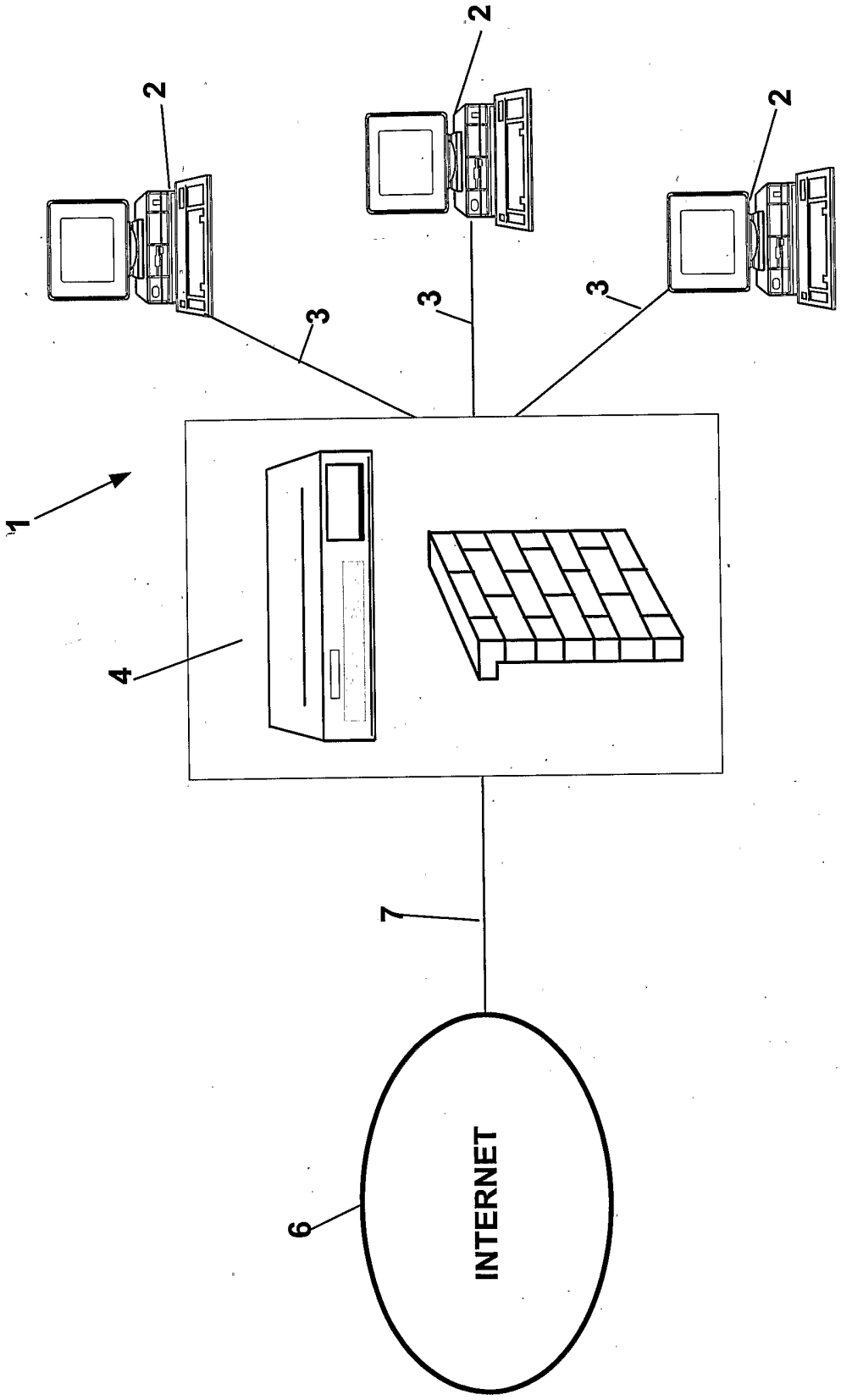


FIG. 2

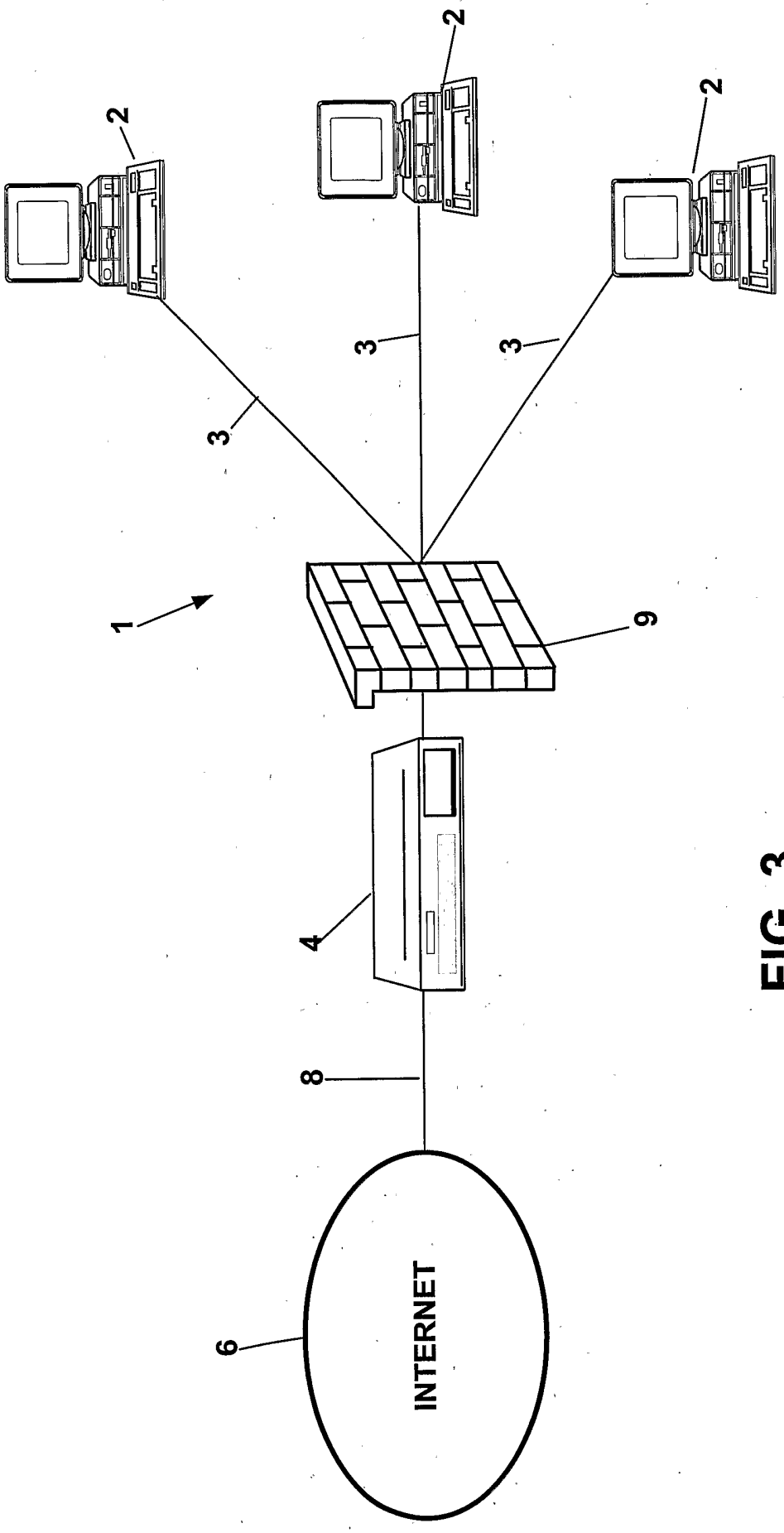


FIG. 3

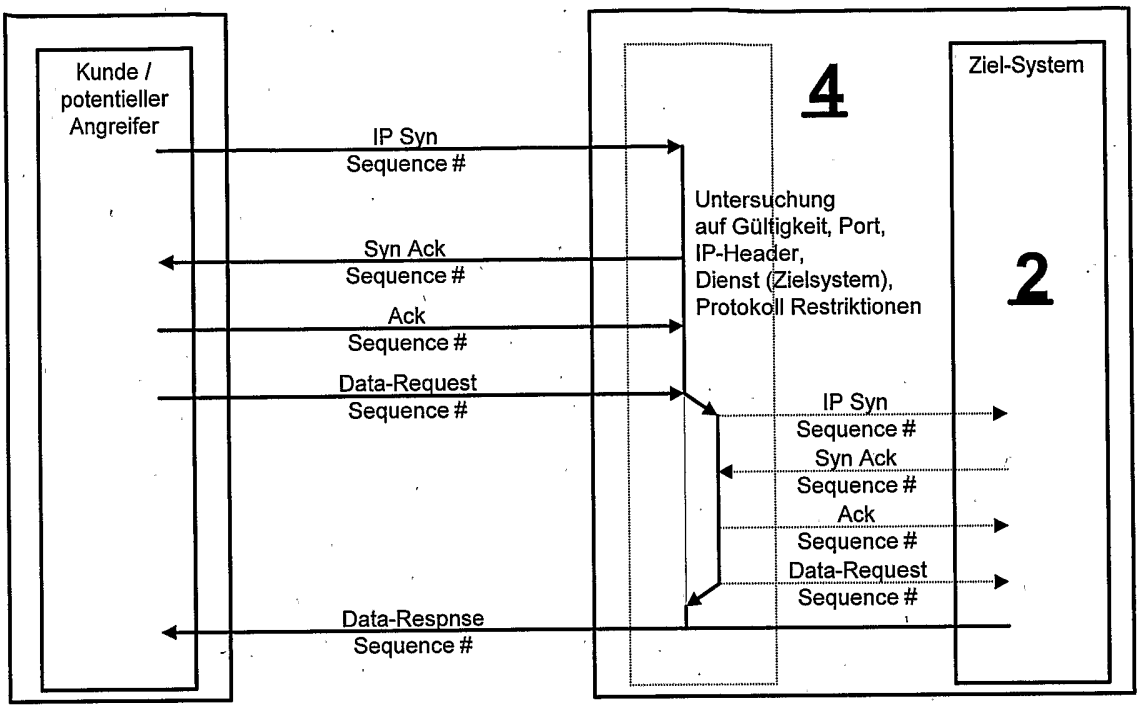

Kunde / potentieller Angreifer
IP Syn Sequence #
Syn Ack Sequence #
Ack Sequence #
Data-Request Sequence #
Data-Respnse Sequence #
4
Untersuchung auf Gültigkeit, Port, IP-Header, Dienst (Zielsystem), Protokoll Restriktionen
IP Syn Sequence #
Syn Ack Sequence #
Ack Sequence #
Data-Request Sequence #
Ziel-System
2

FIG. 4

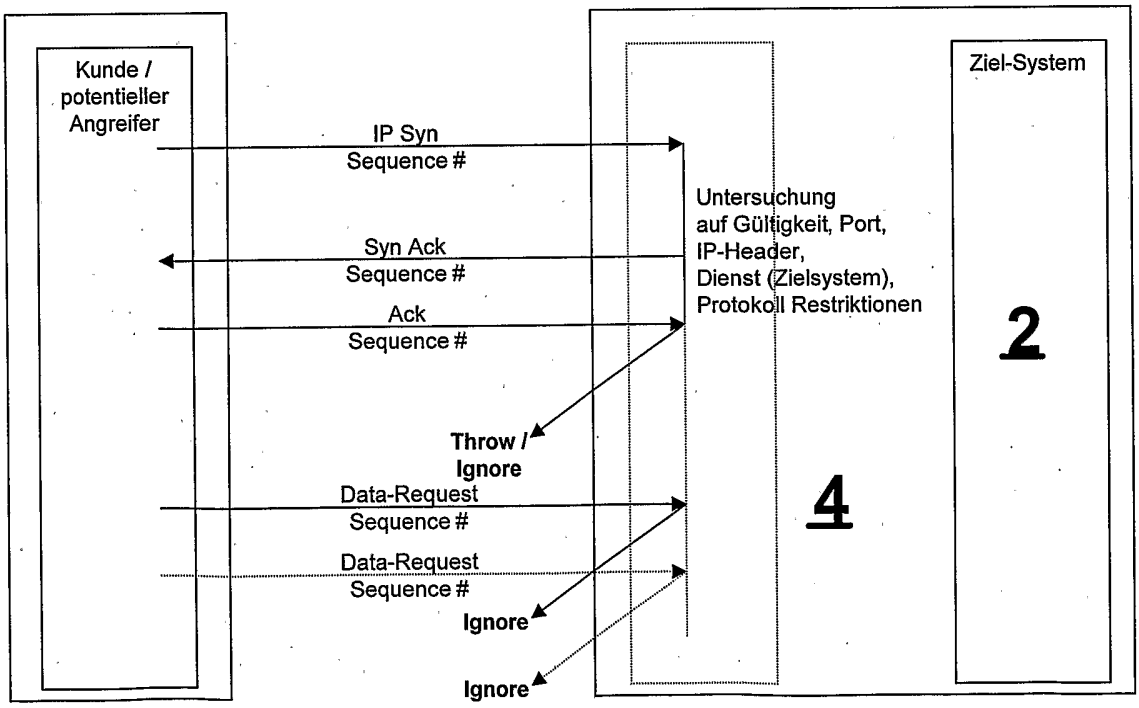

Kunde / potentieller Angreifer
IP Syn Sequence #
Syn Ack Sequence #
Ack Sequence #
Throw / Ignore
Data-Request Sequence #
Data-Request Sequence #
Ignore
Ignore
Untersuchung auf Gültigkeit, Port, IP-Header, Dienst (Zielsystem), Protokoll Restriktionen
4
Ziel-System
2

FIG. 5

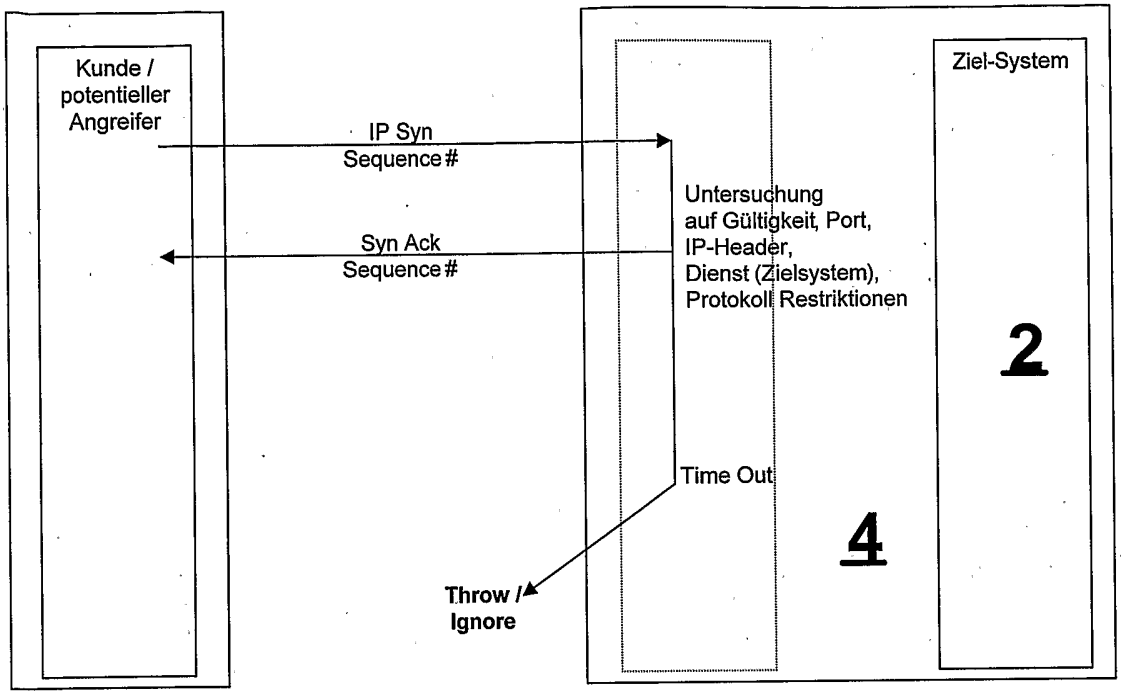

Kunde / potentieller Angreifer
IP Syn Sequence #
Syn Ack Sequence #
Untersuchung auf Gültigkeit, Port, IP-Header, Dienst (Zielsystem), Protokoll Restriktionen
Time Out
Throw / Ignore
Ziel-System
2
4

FIG. 6

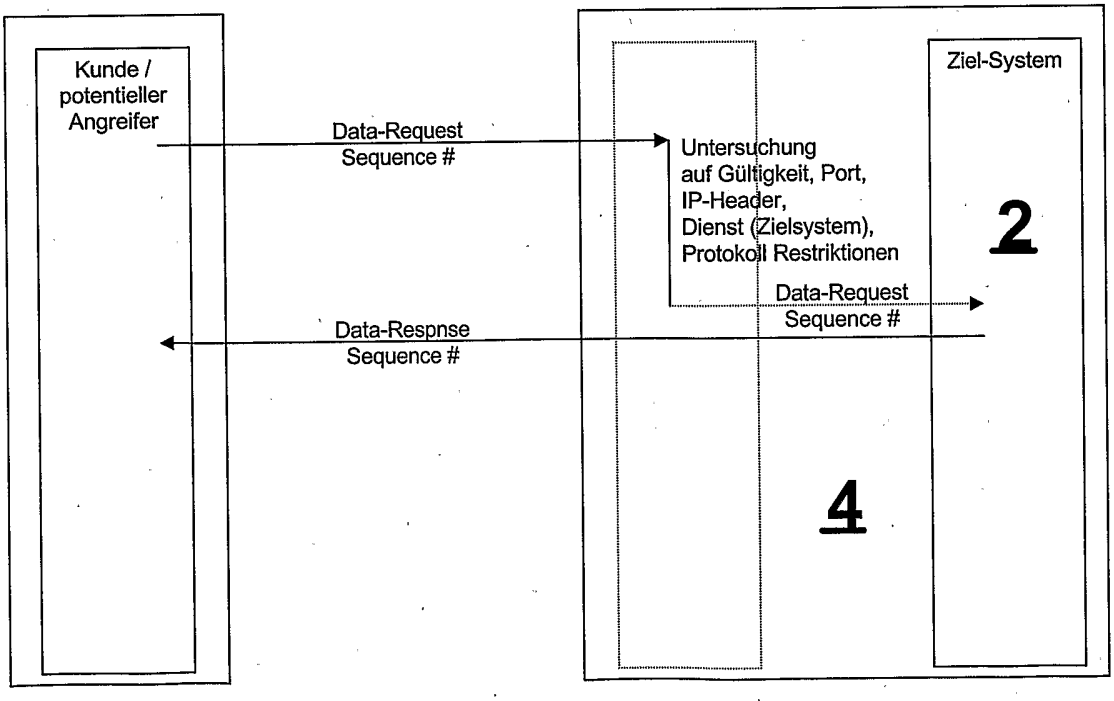

Kunde / potentieller Angreifer
Data-Request Sequence #
Data-Respnse Sequence #
Untersuchung auf Gültigkeit, Port, IP-Header, Dienst (Zielsystem), Protokoll Restriktionen
Data-Request Sequence #
Ziel-System
2
4

FIG. 7

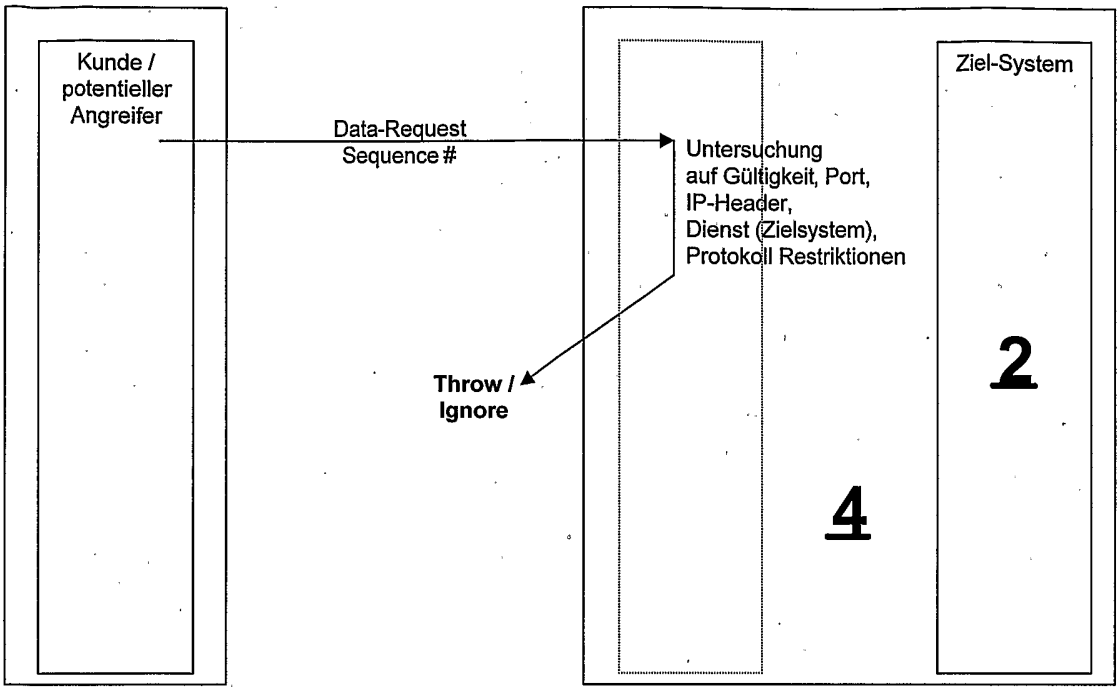

Kunde / potentieller Angreifer
Data-Request Sequence #
Untersuchung auf Gültigkeit, Port, IP-Header, Dienst (Zielsystem), Protokoll Restriktionen
Throw / Ignore
Ziel-System
2
4

FIG. 8

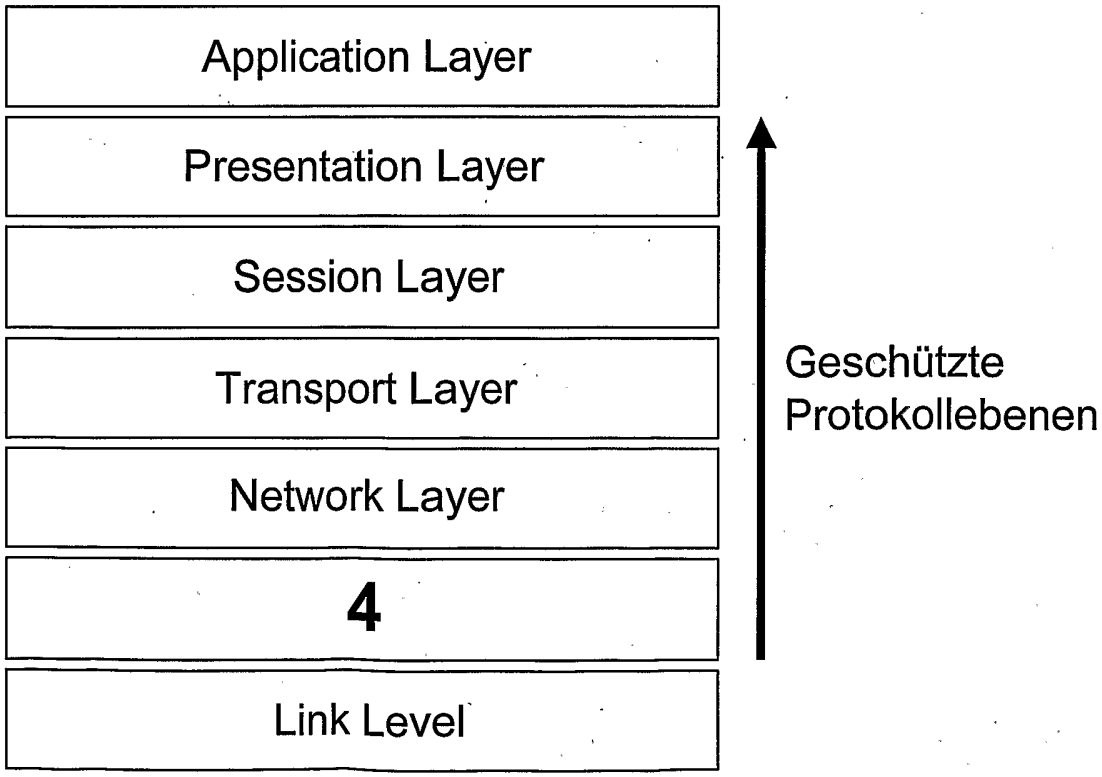

Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
4
Link Level
Geschützte Protokollebenen

FIG. 9

IP-Header

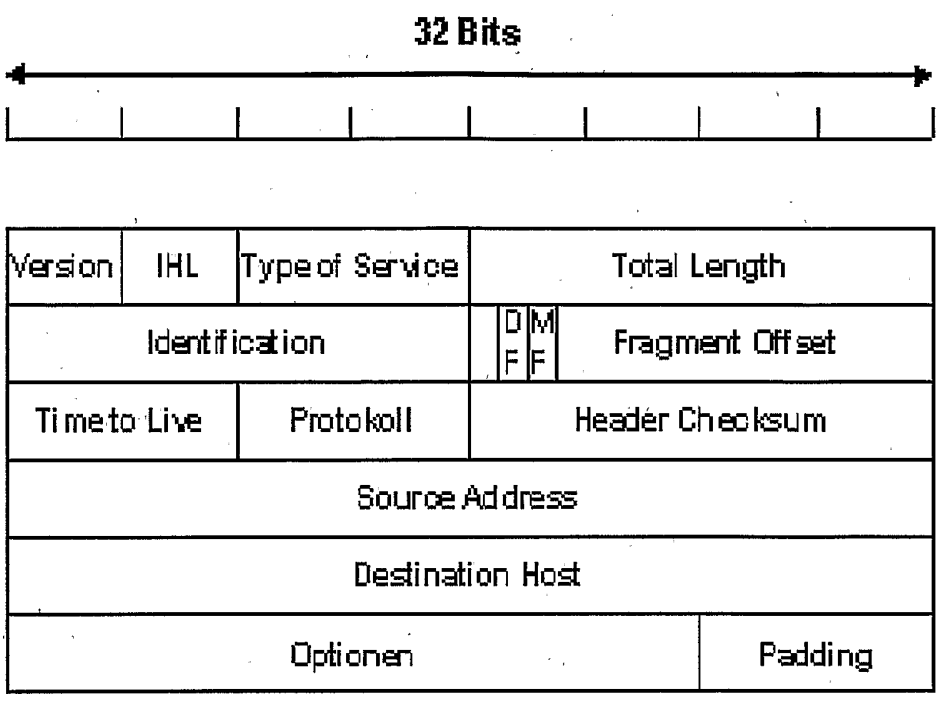
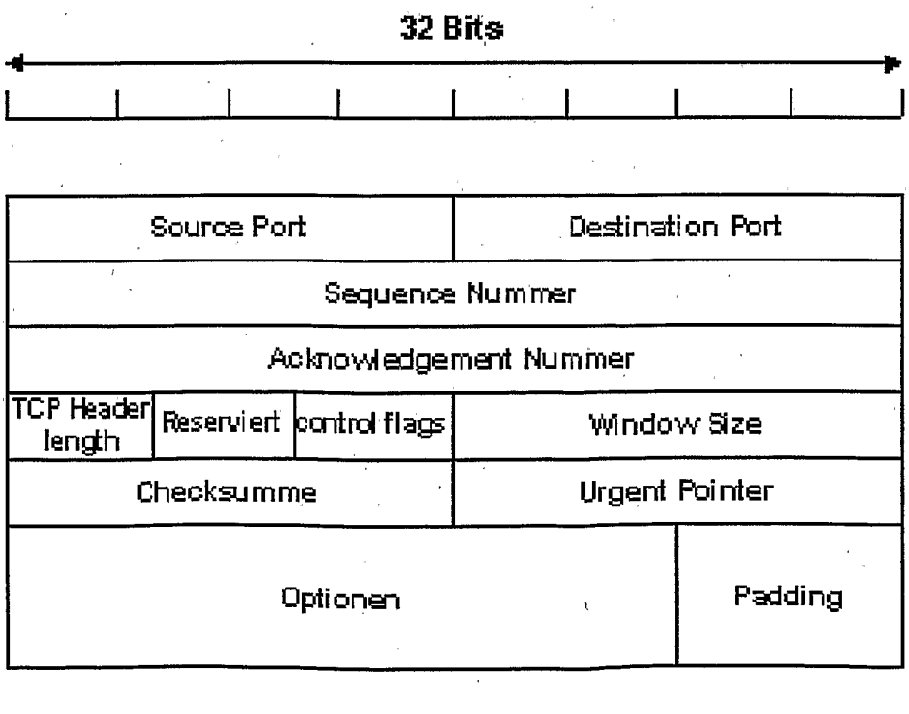


FIG. 10

FIG. 11

TCP-Header



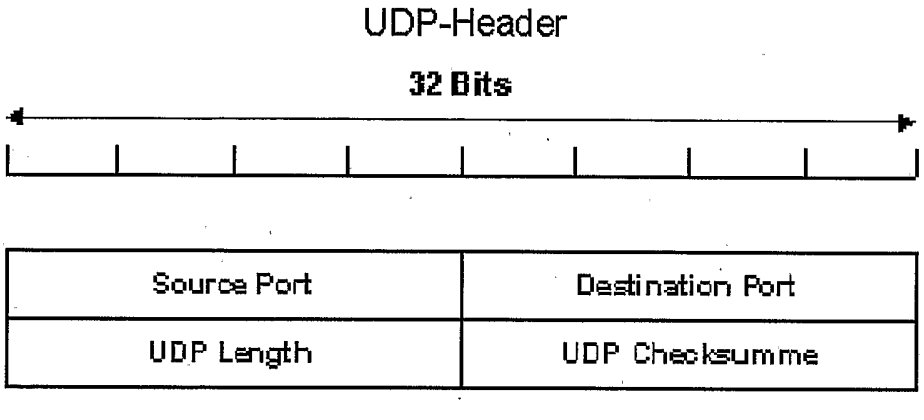
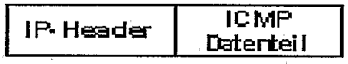


FIG. 12

FIG. 13



ICMP Typ	ICMP Code	ICMP Prüfsumme
ungenutzt		
IP-Header und 64 Bits des Original-Datagramms		

ICMP Typ	ICMP Code	ICMP Prüfsumme
Pointer	ungenutzt	
IP-Header und 64 Bits des Original-Datagramms		

ICMP Typ	ICMP Code	ICMP Prüfsumme
Identifikator	Sequenznummer	
ICMP Echo Daten		

INTERNATIONAL SEARCH REPORT

International Application No
I../EP 01/09328

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	HUNT R: "Internet/Intranet firewall security-policy, architecture and transaction services" COMPUTER COMMUNICATIONS, BUTTERWORTHS & CO. PUBLISHERS LTD, GB, vol. 21, no. 13, 1 September 1998 (1998-09-01), pages 1107-1123, XP004146571 ISSN: 0140-3664 page 1110, right-hand column, line 45 -page 1114, left-hand column, line 23	1-10
A	WO 99 48303 A (CISCO TECH IND) 23 September 1999 (1999-09-23) claims 1-3	1-10

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
2 May 2002	10/05/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Veen, G

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 01/09328

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9948303 A	23-09-1999	AU 3098299 A	11-10-1999
		WO 9948303 A2	23-09-1999

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 01/09328

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H04L29/06

Nach der internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	HUNT R: "Internet/Intranet firewall security-policy, architecture and transaction services" COMPUTER COMMUNICATIONS, BUTTERWORTHS & CO. PUBLISHERS LTD, GB, Bd. 21, Nr. 13, 1. September 1998 (1998-09-01), Seiten 1107-1123, XP004146571 ISSN: 0140-3664 Seite 1110, rechte Spalte, Zeile 45 -Seite 1114, linke Spalte, Zeile 23 ---	1-10
A	WO 99 48303 A (CISCO TECH IND) 23. September 1999 (1999-09-23) Ansprüche 1-3 -----	1-10

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
2. Mai 2002	10/05/2002

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Veen, G

INTERNATIONALER RECHERCHENBERICHT

	ionales Aktenzeichen
	PCT/EP 01/09328

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 9948303 A	23-09-1999	AU 3098299 A	11-10-1999
		WO 9948303 A2	23-09-1999