(19) Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 101 46 397 B4** 2004.09.30

(12) # Patentschrift

(21) Aktenzeichen: **101 46 397.9**
(22) Anmeldetag: **20.09.2001**
(43) Offenlegungstag: **30.04.2003**
(45) Veröffentlichungstag
der Patenterteilung: **30.09.2004**

(51) Int Cl.[7]: **G06F 15/177**

Innerhalb von 3 Monaten nach Veröffentlichung der Erteilung kann Einspruch erhoben werden.

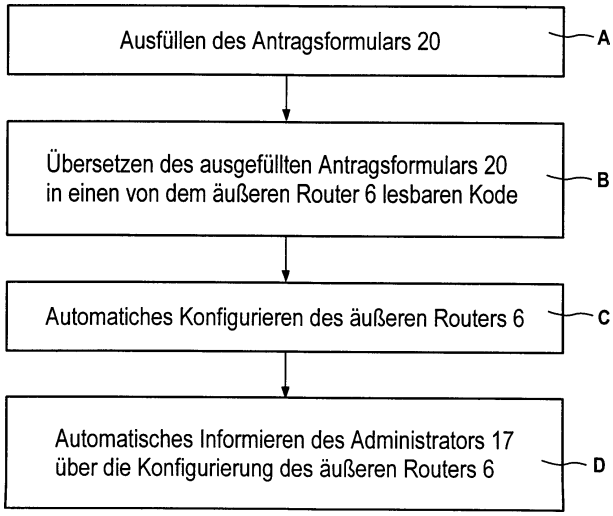
(71) Patentinhaber:
Siemens AG, 80333 München, DE

(72) Erfinder:
Exenberger, Gerald, 91088 Bubenreuth, DE;
Welsing, Stephan, 91315 Höchstadt, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:
EP 06 58 837 A2

(54) Bezeichnung: **Verfahren, Rechnerprogramm, Datenträger und Datenverarbeitungseinrichtung zum Konfigurieren einer Firewall oder eines Routers**

(57) Hauptanspruch: Verfahren zum Konfigurieren einer Firewall (8) oder eines Routers (5, 6), wobei ein erster Rechner (7a bis 7c) oder ein erstes Rechnernetz (1) über die Firewall (8) oder den Router (5, 6) mit einem zweiten Rechnernetz (2) verbunden ist und der Router (5, 6) oder die Firewall (8) derart konfiguriert werden, dass eine Rechnerkommunikation zwischen einem Rechner (11) des zweiten Rechnernetzes (2) und dem ersten Rechner (7a bis 7c) oder einem vorgegebenen Rechner des ersten Rechnernetzes (7a bis 7c) ermöglicht wird, aufweisend folgende Verfahrensschritte:
a) Ausfüllen eines vorgefertigten und der jeweiligen Rechnerkommunikation zugeordneten Antragsformulars (20), wobei das Antragsformular (20) auf einer einmalig erstellten und der jeweiligen Rechnerkommunikation zugeordneten technischen Risikoanalyse basiert,
b) automatisches Übersetzen des ausgefüllten Antragsformulars (20) in einen für die Konfigurierung der Firewall (8) oder des Routers (5, 6) geeigneten Kode und
c) automatisches Konfigurieren der Firewall (8) oder des Routers (5, 6) in...



Beschreibung

[0001] Die Erfindung betrifft ein Verfahren, ein Rechnerprogramm, einen Datenträger und eine Datenverarbeitungseinrichtung zum Konfigurieren einer Firewall oder eines Routers.
[0002] Die Hauptaufgabe einer Firewall ist der Schutz eines lokalen Rechnernetzes, das z.B. ein Intranet eines Industrieunternehmens sein kann, gegenüber Angriffen aus einem externen Rechnernetz, wie beispielsweise dem Internet. Ein Angriff ist beispielsweise ein Versuch eines sogenannten Hackers von dem Internet unbefugt auf das Intranet zuzugreifen, um beispielsweise unbefugt Daten aus dem Intranet zu erhalten oder einen sogenannten Computervirus in das Intranet einzuschleusen. Um den Angriff abzuwehren, verhindert die Firewall eine beliebige Kommunikation der einzelnen Rechner des lokalen Rechnernetzes mit Rechnern des externen Rechnernetzes. Eine Firewall kann beispielsweise zwischen dem lokalen und dem externen Rechnernetz geschaltet sein, um nur bestimmten, aufgrund einer Konfiguration der Firewall vorgegebenen Anwendern Zugriff von dem externen auf das lokale Rechnernetz zu gestatten. Dies ist beispielsweise bei einer sogenannten Partneranbindung, bei dem Rechner verschiedener Rechnernetze miteinander kommunizieren, bei einem Heimarbeitsplatz oder bei einer Außendienstanbindung über Modems oder ISDN (Integrated Service Digital Network) nötig. Die Firewall kann aber auch derart konfiguriert sein, dass nur bestimmte Anwender des lokalen Rechnernetzes mit Rechnern des externen Rechnernetzes kommunizieren können. Eine Firewall kann aber auch die direkte Kommunikation eines einzelnen Rechners mit einem Rechnernetz verhindern (vgl. z.B. Stefan Strobel "Firewalls", zweite aktualisierte und erweiterte Auflage, Heidelberg, dpunkt-Verlag, 1999, oder "Computer-Fachlexikon", Microsoft Press Deutschland, Unterschleißheim, 2000).
[0003] Ein Router ist eine Vermittlungseinrichtung in einem Rechnernetz, die eine möglichst effiziente Übermittlung von Daten von einem Rechner zu einem anderen Rechner des Rechnernetzes z.B. aufgrund eines einem von dem Rechner an den anderen Rechner übermittelten Datensatz zugeordneten Protokoll, welches beispielsweise ein sogenanntes Internet Protokoll (IP) sein kann, gewährleistet. Ein Router kann auch verschiedene Rechnernetze, wie beispielsweise das lokale und das externe Rechnernetz, miteinander verbinden. Ein Router kann auch derart konfiguriert sein, dass er auch eine Firewall Funktionalität aufweist. Dies ist beispielsweise möglich, wenn mittels des Routers ein sogenanntes IP-Filter realisiert ist. Ein Router mit einem IP-Filter leitet dann nur Datensätze eines vorbestimmten Typs, vorbestimmter Quell- und/oder Zieladressen, vorbestimmter Quell- und/oder Zielports oder auch eventuell Datensätze mit vorbestimmten Flags weiter.
[0004] Bevor der Anwender beispielsweise von einem Rechner des externen Rechnernetzes auf bestimmte Rechnerprogramme des lokalen Rechnernetzes zugreifen kann, muss die Firewall bzw. der Router in geeigneter Weise konfiguriert werden. Dies macht in der Regel ein speziell geschulter sogenannter Administrator, der auch für einen reibungslosen Betrieb des lokalen Rechnernetzes zuständig ist. Bevor der Administrator die Firewall oder den Router geeignet konfiguriert, stellt der Anwender in der Regel einen Antrag, um auf das gewünschte Rechnerprogramm zugreifen zu dürfen. Der Administrator überprüft daraufhin, ob der Anwender überhaupt auf das von ihm genannte Rechnerprogramm zugreifen darf und führt anschließend eine technische Risikoanalyse durch, mit deren Hilfe mögliche Sicherheitsrisiken zumindest eingeschränkt werden sollen. Aufgrund der technischen Risikoanalyse soll beispielsweise sicher gestellt werden, dass der Anwender nur auf das von ihm gewünschte Rechnerprogramm Zugriff oder dass ein Nichtberechtigter aufgrund einer nachlässig durchgeführten technischen Risikoanalyse Zugriff auf ein Rechnerprogramm oder einen Rechner des lokalen Rechnernetzes hat. Aufgrund der technischen Risikoanalyse bestimmt der Administrator beispielsweise geeignete IP- oder Portfilter oder auch ein geeignetes host routing. Anschließend konfiguriert der Administrator die Firewall bzw. den Router in geeigneter Weise, so dass der Anwender auf das von ihm gewünschte Rechnerprogramm zugreifen kann.

Stand der Technik

[0005] Dieser Prozess kann jedoch relativ zeitaufwändig sein und kann in der Regel nur von einem Spezialisten, wie dem Administrator, durchgeführt werden. Aus der EP 0 658 837 A2 ist ein Verfahren zur Kontrolle der Netzwerk-Sicherheit durch Verwendung von Paketfiltern bekannt. Die Konfiguration wird durch Eingabe von Sicherheits-Regeln in einer grafischen Benutzeroberfläche definiert und durch einen Paketfilter-Generator in Paketfilter-Kode übersetzt. Dadurch wird dem Systemadministrator eine einfache Kontrolle der Konfiguration ermöglicht, ohne dass er selbst Kode schreiben müsste.

Aufgabenstellung

[0006] Die Aufgabe der Erfindung ist es, ein Verfahren anzugeben, das eine Voraussetzung schafft, eine Firewall oder einen Router in flexibler und zeitnaher Anpassung an Nutzerbedürfnisse und in zeitsparender Weise zu konfigurieren.
[0007] Die Aufgabe wird gelöst durch ein Verfahren zum Konfigurieren einer Firewall oder eines Routers, wo-

bei ein erster Rechner oder ein erstes Rechnernetz über die Firewall oder den Router mit einem zweiten Rechnernetz verbunden ist und der Router oder die Firewall derart konfiguriert werden, dass eine Rechnerkommunikation zwischen einem Rechner des zweiten Rechnernetzes und dem ersten Rechner oder einem vorgegebenen Rechner des ersten Rechnernetzes ermöglicht wird, aufweisend folgende Verfahrensschritte:

a) Ausfüllen eines vorgefertigten und der jeweiligen Rechnerkommunikation zugeordneten Antragsformulars, wobei das Antragsformular (**20**) auf einer einmalig erstellten und der jeweiligen Rechnerkommunikation zugeordneten technischen Risikoanalyse basiert,

b) automatisches Übersetzen des ausgefüllten Antragsformulars in einen für die Konfigurierung der Firewall oder des Routers geeigneten Kode und

c) automatisches Konfigurieren der Firewall (**8**) oder des Routers (**5**, **6**) in Abhängigkeit von dem Kode.

[0008] Erfindungsgemäß wird also vor der Konfigurierung ein vorgefertigtes und der Rechnerkommunikation zugeordnetes Antragsformular ausgefüllt. Unter der Rechnerkommunikation zugeordnet wird verstanden, dass mittels des Antragsformulars Angaben gemacht werden, die nötig für die gewünschte Rechnerkommunikation sind. Diese Angaben sind beispielsweise eine Zieladresse oder eine ISDN Nummer desjenigen Rechners, mit dem kommuniziert werden soll, ein eventuelles Authentifzierungs-Schema wie beispielsweise CHAP (Challange Handshake Authentication Protocol), VPNs (virtuelles Privatnetz), etc.. Mittels des Antragsformulars sollen jedoch ferner keine Angaben gemacht werden können, aufgrund derer die Firewall oder der Router anders als für die gewünschte Rechnerkommunikation konfiguriert werden kann. Das erfindungsgemäße Verfahren kann beispielsweise dann besonders zeitsparend für die Konfiguration sein, wenn verschiedene Anwender Zugang zu demselben Rechnerprogramm bzw. Rechner wünschen. Dann müssen nämlich große Teile der technischen Risikoanalyse nur einmal durchgeführt werden, da viele Einstellungen, wie insbesondere IP- oder Portfilter für die verschiedenen Anwender gleich oder zumindest ähnlich sind. Folglich ist für eine bevorzugte Variante der Erfindung vorgesehen, das Antragsformular auf einer einmalig erstellten und der Rechnerkommunikation zugeordneten technischen Risikoanalyse zu basieren.

[0009] Nach dem Ausfüllen des Antragformulars wird erfindungsgemäß das Antragsformular automatisch in den für die Konfigurierung der Firewall oder des Routers geeigneten Kode übersetzt. Die Übersetzung wird vorzugsweise mittels eines geeigneten Rechnerprogramms automatisch durchgeführt. Somit entfällt ein manuelles Übersetzen des Antragsformulars durch den Administrator. Vielmehr kann, wie es nach einer weiteren Ausführungsform der Erfindung vorgesehen ist, die Firewall oder der Router nach der Übersetzung in den Kode automatisch konfiguriert werden.

[0010] Der Hauptvorteil des erfindungsgemäßen Verfahrens ist somit, dass bei einer Konfigurierung der Firewall oder des Routers lediglich ein Antragsformular, das der Rechnerkommunikation zugeordnet ist, ausgefüllt werden muss. Die Übersetzung in den Kode und eventuell das Konfigurieren wird anschließend automatisch durchgeführt. Dadurch ergibt sich nicht nur eine Zeitersparnis bei der Konfigurierung der Firewall bzw. des Routers, sondern auch eine sichere Konfigurierung der Firewall bzw. des Routers, da keine manuellen Schritte, die eventuell fehlerbehaftet sein können, zwischen dem Ausfüllen des Antragsformulars und der Konfigurierung nötig sind. Außerdem muss nur einmal die technische Risikoanalyse durchgeführt werden.

[0011] Gemäß einer Variante der Erfindung wird nach der automatischen Konfigurierung der Firewall oder des Routers automatisch ein Administrator, der das erste Rechnernetz oder den ersten Rechner pflegt, von der Konfigurierung informiert. Der Administrator des ersten Rechnernetzes oder des ersten Rechners, also diejenige Person, die für den reibungslosen Betrieb des ersten Rechnernetzes bzw. des ersten Rechners zuständig ist, wird somit zuverlässig über eine veränderte Konfiguration der Firewall oder des Routers in Kenntnis gesetzt.

[0012] Nach Ausführungsformen der Erfindung ist das erste und/oder das zweite Rechnernetz ein Intranet, ein ISDN-Netz (Integrated Service Digital Network) oder das Internet.

[0013] Wie bereits oben stehend beschrieben, wird das Antragsformular vorteilhaft in den Kode mittels eines Rechnerprogramms übersetzt. Gemäß weiteren vorteilhaften Varianten der Erfindung ist das Rechnerprogramm auf einem Datenträger gespeichert bzw. auf einer Datenverarbeitungseinrichtung installiert.

Ausführungsbeispiel

[0014] Ein Ausführungsbeispiel ist exemplarisch in den schematischen Zeichnungen dargestellt. Es zeigen:

[0015] **Fig.** 1 ein das erfindungsgemäße Verfahren veranschaulichendes Szenario,

[0016] **Fig.** 2 ein das erfindungsgemäße Verfahren veranschaulichendes Flussdiagramm und

[0017] **Fig.** 3 ein Antragsformular.

[0018] Die **Fig.** 1 zeigt eine typische Struktur einer Anbindung eines lokalen Rechnernetzes, das im Falle des vorliegenden Ausführungsbeispiels ein Intranet **1** eines medizintechnische Geräte herstellenden Industrieunternehmens ist, an ein externes Netz. Im Falle des vorliegenden Ausführungsbeispiels ist das externe Netz ein ISDN-Netz (Integrated Service Digital Network) **2**. Eine solche Struktur ist im Prinzip beispielsweise in Stefan

Strobel "Firewalls", zweite aktualisierte und erweiterte Auflage, Heidelberg, dpunkt-Verlag, 1999, auf Seite 210 abgebildet.

[0019] Im Falle des vorliegenden Ausführungsbeispiels umfasst das Intranet **1** mehrere PCs, von denen in der **Fig.** 1 exemplarisch PCs **3a** bis **3c** dargestellt sind. Die einzelnen PCs **3a** bis **3c** sind für den Fachmann in allgemein bekannter Weise miteinender beispielsweise mittels eines in der **Fig.** 1 nicht dargestellten BUS verbunden.

[0020] Um einen direkten Datenverkehr zwischen den PCs **3a** bis **3c** des Intranets **1** mit dem ISDN-Netz **2** zu verhindern, um somit z.B. einen unter Umständen kostspieligen Datenverkehr von dem Intranet **1** ins ISDN-Netz **2** zu minimieren oder einen Zugang von dem ISDN-Netz **2** in das Intranet **1** zu beschränken bzw. zu überwachen, können die PCs **3a** bis **3c** des Intranets **1** nur über eine sogenannte demilitarisierte Zone (DMZ) **4** mit dem ISDN-Netz **2** kommunizieren. Die DMZ **4**, die auch als Firewall-Netz bezeichnet wird, umfasst im Falle des vorliegenden Ausführungsbeispiels einen inneren Router **5**, einen äußeren Router **6** und mehrere Server, von denen in der **Fig.** 1 exemplarisch Server **7a** bis **7c** dargestellt sind.

[0021] Der innere Router **5** ist dabei mit dem Intranet **1** verbunden und ermöglicht eine Kommunikation der einzelnen Rechner **3a** bis **3c** mit den Servern **7a** bis **7c**. Der äußere Router **6** ist dagegen mit dem ISDN-Netz **2** verbunden und erlaubt lediglich eine Kommunikation einzelner an das ISDN-Netz **2** angeschlossener Rechner mit den Servern **7a** bis **7c**. Somit gibt es keine direkte Verbindung zwischen dem ISDN-Netz **2** und dem Intranet **1**. Vielmehr können die PCs **3a** bis **3c** nur über die Server **7a** bis **7c** mit an das ISDN-Netz **2** angeschlossen Rechnern kommunizieren. Um einen zusätzliche Schutz des Intranets **1** und der Server **7a** bis **7c** zu erhalten, sind die Server **7a** bis **7c** zusätzlich mit einer Firewall **8** geschützt, der zwischen dem inneren Router **5**, dem äußeren Router **6** und den Servern **7a** bis **7c** geschaltet ist.

[0022] Der innere Router **5** und die Firewall **8** sind im Falle des vorliegenden Ausführungsbeispiels derart konfiguriert, dass Mitarbeiter **9** des Industrieunternehmens mittels der PCs **3a** bis **3c** Zugriff auf für sie bestimmte und in den Servern **7a** bis **7c** der DMZ **4** gespeicherten Daten, Rechnerprogramme, Anwendungen usw. haben. Der äußere Router **6** in Verbindung mit der Firewall **8** sind dagegen derart konfiguriert, dass nur bestimmte und in den Servern **7a** bis **7c** gespeicherte Rechnerprogramme, Dateien, Anwendungen usw. von dem ISDN-Netz **2** zugänglich sind. Eine Kommunikation einer des Mitarbeiter **9** mit einem der PCs **3a** bis **3c** mit einem an das ISDN-Netz **2** angeschlossenen Rechner ist also nur über die DMZ **4** und insbesondere nur über einen der Server **7a** bis **7c** möglich.

[0023] Wie bereits erwähnt, stellt im Falle des vorliegenden Ausführungsbeispiels das Industrieunternehmen medizintechnische Geräte wie beispielsweise ein in der **Fig.** 1 dargestelltes Magnetresonanzgerät **10** her. Im Falle des vorliegenden Ausführungsbeispiels wurde das Magnetresonanzgerät **10** an ein Krankenhaus **12** verkauft und befindet sich in einem Untersuchungsraum **13** des Krankenhauses **12**.

[0024] Im Falle des vorliegenden Ausführungsbeispiels umfasst das Magnetresonanzgerät **10** einen Rechner **11**, der u.a. in für den Fachmann bekannter Weise das Magnetresonanzgerät **10** im Betrieb geeignet steuert. Der Rechner **11** des Magnetresonanzgerätes **10** ist ferner an ein lokales Rechnernetz (Krankenhausnetz) **14** des Krankenhauses **12** angeschlossen, wobei das Krankenhausnetz **14** wiederum mit einem Router **15** mit dem ISDN-Netz **2** verbunden ist.

[0025] Im Falle des vorliegenden Ausführungsbeispiels ist ferner in dem Server **7a** der DMZ **4** ein Servicerechnerprogramm gespeichert, das u.a. für eine Fernwartung des Magnetresonanzgerätes **10** geeignet ist. Mittels dieses Serviceprogramms kann ein Techniker **16** des Industrieunternehmens das Magnetresonanzgerät **10** in für den Fachmann geläufiger Weise von der Ferne testen, wenn der innere Router **5**, der äußere Router **6**, die Firewall **8** und der Router **15** geeignet konfiguriert sind. Der Techniker **16** kann dann also mit einem der PCs **3a** bis **3c** auf das in dem Server **7a** gespeicherte Servicerechnerprogramm zugreifen und mit dem Rechner **11** des Magnetresonanzgerätes **10** kommunizieren.

[0026] Im Falle des vorliegenden Ausführungsbeispiels ist der Techniker **16** dafür zuständig, von dem Industrieunternehmen verkaufte Magnetresonanzgeräte von der Ferne zu warten, weshalb der innere Router **5** und die Firewall **8** bereits derart konfiguriert sind, dass der Techniker **16** mit einem der PCs **3a** bis **3c** auf das im Server **7a** gespeicherte Servicerechnerprogramm zugreifen kann; die Firewall **8** ist ferner auch schon derart konfiguriert, dass ein Senden und Empfangen von dem Servicerechnerprogramm zugeordneten Datensätze an das bzw. von dem ISDN-Netz **2** ermöglicht ist, da der Techniker **16** im Falle des vorliegenden Ausführungsbeispiels bereits weitere, in der **Fig.** 1 nicht dargestellte und mit dem Magnetresonanzgerät **10** vergleichbare Magnetresonanzgeräte aus der Ferne mit einem der PCs **3a** bis **3c** wartet. Somit braucht also nur noch der äußere Router **6** derart konfiguriert werden, dass eine Fernwartung des Magnetresonanzgerätes **10** ermöglicht wird. Der Routen **15** ist im Übrigen schon in geeigneter Weise von einem in der **Fig.** 1 nicht dargestellten Angestellten des Krankenhauses **12** konfiguriert worden.

[0027] Aus diesem Grund ruft der Techniker **16** im Falle des vorliegenden Ausführungsbeispiels mit einem der PCs **3a** bis **3c**, im Falle des vorliegenden Ausführungsbeispiels mit dem PC **3a**, ein in einem der Server **7a** bis **7c** gespeichertes und in der **Fig.** 2 gezeigtes Antragsformular **20** auf, welches, nachdem der Techniker **16** seine Zugangsberechtigung mit einer Eingabe eines ihm zugeordneten Kennwortes verifizierte, auf einem Monitor

des PCs **3a** erscheint. Das in der **Fig.** 2 dargestellte Antragsformular **20** ist dafür vorgesehen, den äußeren Routen **6** derart zu konfigurieren, dass ein an das ISDN-Netz **2** angeschlossener Rechner mit dem Server **7a** mittels des Servicerechnerprogramms kommunizieren kann. Da das Antragsformular **20** bereits dem Servicerechnerprogramm zugeordnet ist, sind Angaben, auf welchen der Server **7a** bis **7c** zugegriffen werden soll, unnötig. Das Antragsformular **20** umfasst im Wesentlichen nur noch Angaben über den gewünschten Zielrechner. Das Antragsformular **20** erlaubt also keine Angaben, die einen Zugriff auf einen anderen Server als den Server **7a** der DMZ **4** oder ein anderes als auf das in dem Server **7a** gespeicherten Servicerechnerprogramm zulassen. Das Antragsformular **20** wurde im Übrigen aufgrund einer einmalig durchgeführten technischen Risikoanalyse erstellt und ist bereits als ausgefüllt dargestellt.

[0028] Nachdem der Techniker **16** das Antragformular **20** auf dem PCs **3a** geladen hat, füllt er es aus (Schritt A des in der **Fig.** 3 dargestellten Flussdiagramms):

Im Falle des vorliegenden Ausführungsbeispiels wird der Techniker mittels des Antragformulars **20** aufgefordert, die ISDN Nummer desjenigen Rechners, mit dem er kommunizieren möchte, und das entsprechende ISDN-Netz anzugeben. Der Techniker **16** muss ferner Angaben über die Art des Netzes (ISDN Protokoll Type), also ob es sich beispielsweise um das europäische ISDN-Netz handelt, geben. Ferner werden Angaben über einen CHAP (Challange Authentication Protocol), Benutzername (Username), ein CHAP-Passwort, die IP Adresse des Ziel Routers, der Ziel Router Netzmaske, des Zielnetzwerkes und der Zielnetzwerk-Maske verlangt.

[0029] Im Falle des vorliegenden Ausführungsbeispiels möchte der Techniker **16** mit dem Rechner **11** des Magnetresonanzgeräts **10** kommunizieren, weshalb er das Antragsformular **20** in entsprechender Weise mit der ISDN-Nummer des Rechners **11** ausfüllt. Ferner ist der Rechner **11** mittels des Routers **15** an das Krankenhausnetz **14** angeschlossen, so dass der Techniker **16** die IP Adresse des Routers **15** und dem Krankenhausnetz **14** zugeordnete Kodes angibt.

[0030] Nachdem der Techniker **16** das Antragsformular **20** ausgefüllt hat, sendet er das ausgefüllte Antragsformular an den Server **7a**. Der Server **7a** umfasst im Falle des vorliegenden Ausführungsbeispiels eine Festplatte **7a'**, in der ein geeignetes Rechnerprogramm gespeichert ist, das, nachdem der Server **7a** das ausgefüllte Antragsformular **20** empfangen hat, die Angaben des ausgefüllten Antragsformular **20** automatisch in einen von dem äußeren Router **6** lesbaren Kode übersetzt (Schritt B des in der **Fig.** 3 dargestellten Flussdiagramms). Dieser Kode lautet im Falle des vorliegenden Ausführungsbeispiels folgendermaßen, wobei nur die relevanten Befehle angegeben sind:

```
....
.......
dialer map ip 194.138.39.9 name rd_erlangen1 00080007774968
isdn switch-type basic-net3
ppp authentication chap
username rd_erlangen1 password 148"§Qas
ip route 194.138.39.0 255.255.255.0 194.138.39.9
ip route 194.138.39.9 255.255.255.255 BRI0
.....
..
```

Anschließend konfiguriert im Falle des vorliegenden Ausführungsbeispiels das Rechnerprogramm automatisch den äußeren Router **6** aufgrund des eben genanten Kodes, so dass der Techniker **16** mit einem der PCs **3a** bis **3c** das Magnetresonanzgerät **10** warten kann (Schritt C des in der **Fig.** 3 dargestellten Flussdiagramms).

[0031] Nach der Konfigurierung des äußeren Routers **6** generiert im Falle des vorliegenden Ausführungsbeispiels das Rechnerprogramm automatisch eine E-Mail, um eine Administrator **17**, der für das Intranet **1** verantwortlich ist, von der Konfigurierung des äußeren Routers **6** zu informieren (Schritt D des in der **Fig.** 3 dargestellten Flussdiagramms).

[0032] Neben einer Konfiguration des äußeren Routers **6** mittels des Antragsformulars **20** sind in dem Server **7a** oder den Servern **7b** oder **7c** weitere Antragsformulare gespeichert, mit deren Hilfe der innere Router **5** oder die Firewall **8** automatisch konfiguriert werden können.

[0033] Für das erfinderische Verfahren ist jedoch eine automatische Konfigurierung des äußeren Routers **6** nach der automatischen Übersetzung des ausgefüllten Antragsformulars **20** in den Kode optional. Auch eine Benachrichtigung des Administrators **17** von der Konfiguration des äußeren Routers **6** ist optional.

[0034] Die in der **Fig.** 1 dargestellten Rechnernetze sind ebenfalls nur von exemplarischer Natur.

Patentansprüche

1. Verfahren zum Konfigurieren einer Firewall (**8**) oder eines Routers (**5**, **6**), wobei ein erster Rechner (**7a** bis **7c**) oder ein erstes Rechnernetz (**1**) über die Firewall (**8**) oder den Router (**5**, **6**) mit einem zweiten Rechnernetz (**2**) verbunden ist und der Router (**5**, **6**) oder die Firewall (**8**) derart konfiguriert werden, dass eine Rechnerkommunikation zwischen einem Rechner (**11**) des zweiten Rechnernetzes (**2**) und dem ersten Rechner (**7a** bis **7c**) oder einem vorgegebenen Rechner des ersten Rechnernetzes (**7a** bis **7c**) ermöglicht wird, aufweisend folgende Verfahrensschritte:
a) Ausfüllen eines vorgefertigten und der jeweiligen Rechnerkommunikation zugeordneten Antragsformulars (**20**), wobei das Antragsformular (**20**) auf einer einmalig erstellten und der jeweiligen Rechnerkommunikation zugeordneten technischen Risikoanalyse basiert,
b) automatisches Übersetzen des ausgefüllten Antragsformulars (**20**) in einen für die Konfigurierung der Firewall (**8**) oder des Routers (**5**, **6**) geeigneten Kode und
c) automatisches Konfigurieren der Firewall (**8**) oder des Routers (**5**, **6**) in Abhängigkeit von dem Kode.

2. Verfahren nach Anspruch 1, bei dem nach der automatischen Konfigurierung der Firewall (**8**) oder des Routers (**5**, **6**) ein Administrator (**17**), der das erste Rechnernetz (**1**) oder den ersten Rechner (**7a**) pflegt, von der Konfigurierung informiert wird.

3. Verfahren nach einem der Ansprüche 1 bis 2, bei dem das erste Rechnernetz ein Intranet (**1**), ein ISDN-Netz (Integrated Service Digital Network) oder das Internet ist.

4. Verfahren nach einem der Ansprüche 1 bis 3, bei dem das zweite Rechnernetz ein Intranet, ein ISDN-Netz (Integrated Service Digital Network) (**2**) oder das Internet ist.

5. Rechnerprogramm, das ein Übersetzen des Antragsformulars (**20**) nach Anspruch 1 bis 4 implementiert.

6. Datenträger (**7a'**), auf dem das Rechnerprogramm nach Anspruch 5 gespeichert ist.

7. Datenverarbeitungseinrichtung (**7a**), auf der das Rechnerprogramm nach Anspruch 5 installiert ist.

Es folgen 2 Blatt Zeichnungen

Anhängende Zeichnungen

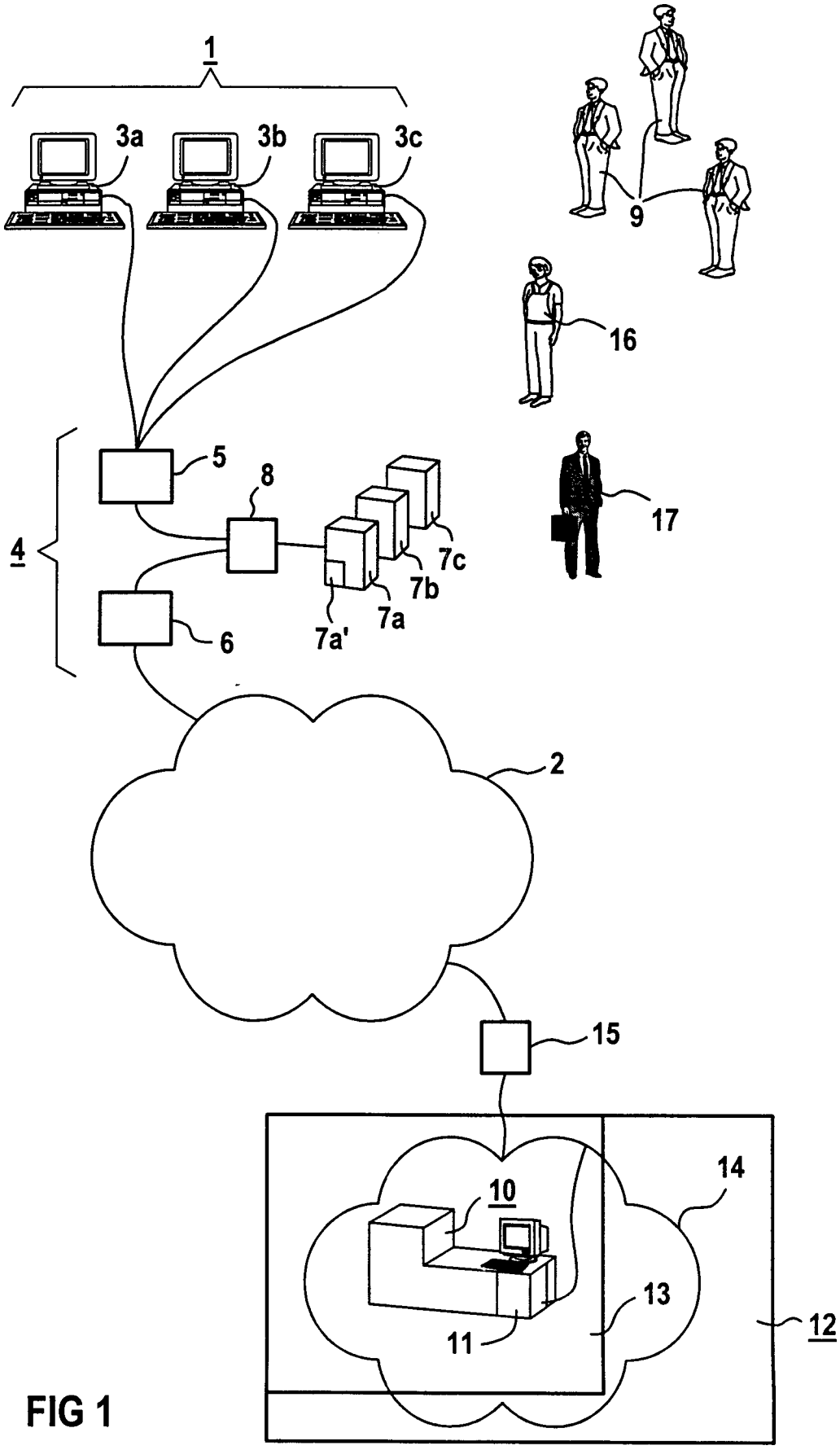


FIG 1

Antragsformular 20

ISDN Nummer:	00080007774968
ISDN Protokoll Type:	basic-net3
Authentifikation:	chap
CHAP Username:	rd_erlangen1
CHAP Passwort:	148"§Qas
IP Adresse Ziel Router:	194.138.39.9
Ziel Router Netzmaske:	255.255.255.255
Zielnetzwerk:	194.138.39.0
Zielnetzwerk-Maske:	255.255.255.0

20

FIG 2

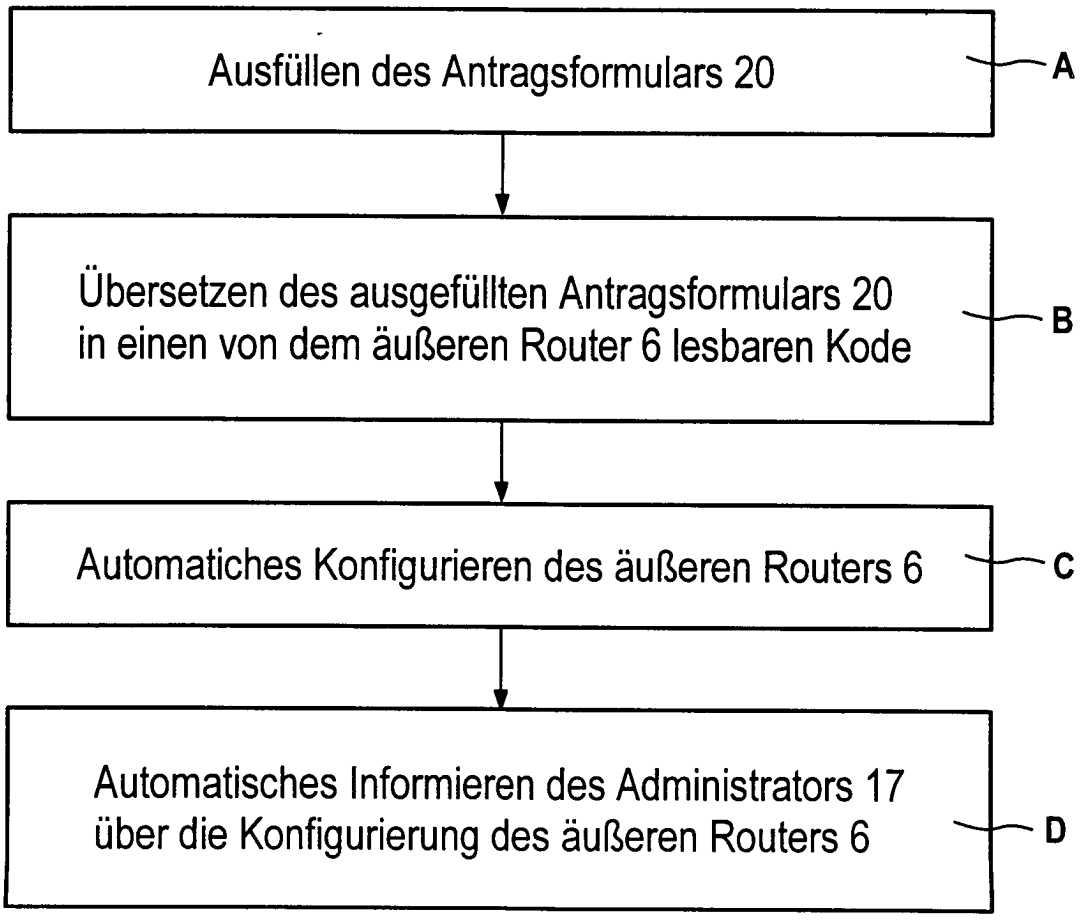


FIG 3