(19) österreichisches patentamt

(10) **AT 501 652 A1 2006-10-15**

(12) Österreichische Patentanmeldung

(21) Anmeldenummer: **A 57/2005**

(22) Anmeldetag: **14.01.2005**

(43) Veröffentlicht am: **15.10.2006**

(51) Int. Cl.[8]: ***G06F 21/00*** (2006.01)

(73) Patentanmelder:

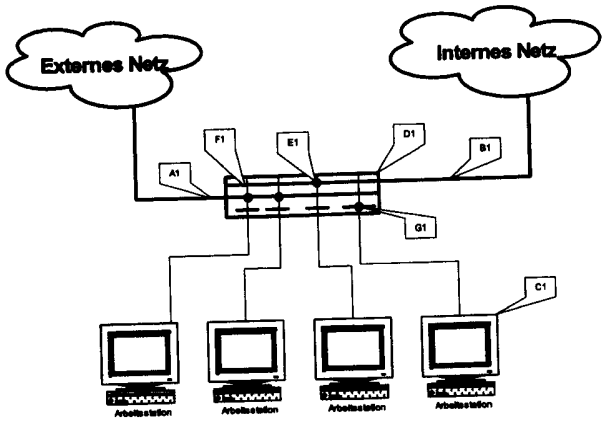
DIAPLAN ELEKTRONIC GMBH
A-9020 KLAGENFURT (AT)

(72) Erfinder:

JANSCHITZ KLAUS
KLAGENFURT (AT)
STEBE FRANZ
DIEX (AT)

(54) COMPUTERSICHERHEITSSYSTEM

(57) Computersicherheitssystem für höchstmöglichen Schutz vor Angriffen auf das interne Netzwerk mit einem jeder Arbeitsstation (C1) zugeordneten Verbindungsknoten (D1) zur Trennung und Verbindung in den gewählten Arbeitsbereich (A1, B1), welcher ein Netzwerk oder auch ein allein stehender Betrieb ist, wobei jeder Verbindungsknoten (D1) die Arbeitsstation (C1) nur mit einem Arbeitsbereich, verbinden kann. Das System besteht aus mindestens einer Einheit (D1), welche das Betriebssystem in Abhängigkeit der benötigten Ressource mit dem entsprechenden Arbeitsbereich (A1, B1) verbindet. Der Verbindungswechsel wird durch hardwaremäßiges Trennen der Verbindung durchgeführt. Das Trennen und Verbinden des Betriebssystems kann mit automatischer oder manuell geschehen. Das Betriebssystem kann einem Netzwerk verbunden werden (E1) oder komplett getrennt von allen Netzwerkverbindungen sein, (G1) Für einen automatisch Verbindungswechsel wird der Netzwerkverkehr überwacht und bei Erkennung eines benötigten Zugriffs auf eine im Netzwerk nicht vorhandene Ressource wird ein Verbindungswechsel vorgenommen. Der manuelle Verbindungswechsel kann entweder über einen Hardware oder Software Schalter erfolgen.



AT 501 652 A1 2006-10-15

diaplan elektronic gmbh
Kaufmanngasse 5
9020 Klagenfurt
E-Mail : office@diaplan.com
tele : +43 463 54510 45
fax: + 43 463 54510 15

„Computersicherheitssystem"

Zusammenfassung

Die Erfindung betrifft ein Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk insbesondere dem Schutz der Daten des internen Netzwerks mit einem jeder Arbeitsstation zugeordnetem Verbindungsknoten zur Trennung und Verbindung in den gewählten Arbeitsbereich, welcher ein Netzwerk oder auch ein allein stehender Betrieb ist, wobei jeder Verbindungsknoten die Arbeitsstation nur mit einem Arbeitsbereich, welcher ein Netzwerk oder auch ein allein stehender Betrieb ist, verbinden kann. Das System besteht aus mindesten einer Einheit, welche das Betriebssystem in Abhängigkeit der benötigten Ressource mit dem entsprechenden Arbeitsbereich verbindet. Es gibt im Normalfall mindestens zwei von einander getrennte Netzwerke. Ein Netzwerk bildet das interne Netz und eines das externe Netzwerk, welches beispielsweise mit dem Internet oder Intranet verbunden ist. Der Verbindungswechsel wird durch ein hardwaremäßiges Trennen der Verbindung durchgeführt. Das Trennen und Verbinden des Betriebssystems kann mit automatischer oder manueller Aufforderung geschehen. Das Betriebssystem kann mit einem Netzwerk verbunden werden oder komplett getrennt von allen Netzwerkverbindungen sein, wodurch die höchstmögliche Sicherheitsstufe erreicht wird. Für einen automatischen Verbindungswechsel wird der Netzwerkverkehr überwacht und bei Erkennung eines benötigten Zugriffs auf eine im Netzwerk nicht vorhandene Ressource wird ein Verbindungswechsel vorgenommen. Der manuelle Verbindungswechsel kann entweder über einen Hardware oder Software Schalter erfolgen.

NACHGEREICHT

diaplan elektronic gmbh
Kaufmanngasse 5
9020 Klagenfurt
E-Mail : office@diaplan.com
tele : +43 463 54510 45
fax: + 43 463 54510 15

Beschreibung :

Technisches Gebiet

Die Erfindung betrifft ein Computersicherheitssystem für den höchstmöglichen einfachen und sicheren Schutz eines Betriebssystems vor schädigenden Angriffen aus fremden Netzen, gemäß dem Oberbegriff des Anspruchs 1. Das System findet Anwendung für den Schutz von Firmennetzwerken sowie privaten Netzwerken und deren Internetanbindung oder anderen als unsicher eingestufte Netzwerk Verbindungen.

Stand der Technik

Das Thema Sicherheit gewinnt für Unternehmen immer mehr an Bedeutung. Die Bedrohung der IT-Systeme durch Sicherheitslücken in Betriebssystemen und Anwendungen wächst ständig. Unternehmen sind heute immer wieder neuen und schwerer zu bekämpfenden Bedrohungen durch Hacker ausgesetzt. Wo vor einiger Zeit noch die Absicherung sämtlicher Ein- und Ausgangspunkte eines Netzwerks ausreichte, sind heute umfangreichere Schutzmechanismen notwendig.
Das Internet ist einer der wichtigen Bestandteile in einem Unternehmen, gleichzeitig bildet es eine Schnittstelle für Angriffe. Die Risiken bei der Nutzung des Internets gehen vom Datendiebstahl bis zum Systemausfall was von Produktivitätsausfällen bis zum Ruin führen kann.

Schutzsysteme für Firmennetzwerke in bekannter Art und Weise für den Gebrauch in Firmennetzwerken, die durch Filterung des ein- ausgehenden Datenverkehrs, Animations-Kontrolle, Blockierung von verdächtigen Skripten und „XXX-dailer" den Zugriff auf das Firmennetzwerk begrenzen. Als Beispiele seien Firewalls PIX Stationen, welche die Schnittstelle zum Internet bilden und den unerlaubten Zugriff über gesperrte Ports verweigern.

Firewalls

Mit den am Markt erhältlichen Systemen ist es möglich, Regeln für spezifische Protokolle, Ports, Anwendungen und/oder Fern-Adressen zu definieren. Es können auch Meldungen an den Nutzer gehen, wenn Anwender versuchen eine Internet Verbindung aufzubauen.
Diese Systeme schützen das Netzwerk, indem der Zugriff auf das Netzwerk begrenzt und der Datenverkehr durchsucht wird.

diaplan elektronic gmbh
Kaufmanngasse 5
9020 Klagenfurt
E-Mail : office@diaplan.com
tele : +43 463 54510 45
fax: + 43 463 54510 15

Nachteil besteht darin, dass ein Angriff über die nicht gesperrten Zugriffsmöglichkeiten (Bsp.: https, http, FTP Ports) mit Hilfe von Betriebssystem- oder Anwenderprogramm-Lücken erfolgen kann. Diese Fehler werden oft erst im Schadensfall entdeckt und mit Updates des Herstellers behoben. Es vergeht so eine bestimmte Zeit, bis ein Update für eine Anwendung oder ein Betriebssystem zur Verfügung steht. Die Nutzer sind dann selbst verantwortlich dafür, dass alle Ihre Netzwerkteilnehmer die aktuellen Updates in das Rechnernetzwerk einspielen. Die Administration solcher Schutzsysteme ist sehr aufwendig und bedarf einer speziellen Ausbildung. Durch den Zwang der ständigen Aktualisierung der Konfiguration ist das System sehr fehleranfällig. Die Programme werden mit steigender Sicherheitsstufe komplexer und sind dadurch Netzwerk Komponenten meist nur mit Spezialwissen zu bedienen.
Für die Gewährleistung einer dem derzeitigen Stand der Technik entsprechenden Sicherheit eines Firmennetzwerks ist eine permanente, aufwendige Pflege und Überwachung notwendig, diese Wartungen und System Aktualisierungen sind daher oft extrem teuer und können daher üblicherweise nur von Grossunternehmen finanziert werden. Kleiner Unternehmen sind meist wegen des kleineren Kapitals nicht in der Lage solche Sicherheitsmaßnahmen umzusetzen.

Bekannt sind beispielsweise Systeme nach DE 19742330 C1 sie bieten ein Verfahren zum Abschotten sicherheitsrelevanter Datenverarbeitungsanlagen gegen Beeinflussungen aus anderen Datennetzen sowie hierzu geeignete Einrichtung. Um zu verhindern, dass eine mit einem öffentlichen Datennetz kommunizierende sicherheitsrelevante Datenverarbeitungsanlage auf von außen stammende Datentelegramme mit sicherheitsrelevanten Inhalt reagiert, sind die beiden Datennetze durch zwei Security translator Systeme voneinander getrennt. Dieses lässt nur Daten mit nicht sicherheitstechnischem Charakter zur Übermittlung an die sicherheitsrelevante Datenverarbeitungsanlage zu. Durch die Filterung der Datentelegramme des externen Netzwerks kann sichergestellt werden, dass keine Datentelegramme mit sicherheitsrelevanten Inhalt in das zweite Netzwerk gelangen, was das System als Sicher gegen sicherheitsrelevante Datentelegramme einstuft.
Das System besteht aus zwei securits translator was den Vorteil hat, dass die von außen anliegenden Telegramme getrennt bewertet werden können.
Die Telegramme werden von einem security translator verschlüsselt und von dem anderen entschlüsselt, wodurch das System an Sicherheit gewinnt. Durch die zyklische Prüfung der

NACHGEREICHT

diaplan elektronic gmbh
Kaufmanngasse 5
9020 Klagenfurt
E-Mail : office@diaplan.com
tele : +43 463 54510 45
fax: + 43 463 54510 15

Filter auf Übereinstimmung, wird das System ständig auf Funktionstüchtigkeit überprüft.
Nachteil des Systems ist die direkte Anbindung an das externe Netz, wodurch ein Eindringen durch einen Konfigurationsfehler, einer Lücke im Betriebsystem der Datenverarbeitungsanlage, einer Lücke im security translator System, einen Fehler eines internen Benutzers, usw. in die Sicherheitseinrichtungen von Hackern möglich ist und Daten des internen Systems verändert, gestohlen oder Steuerbefehle in das Netzwerk eingespeist werden.

Daneben offenbart die DE 102 01 655 C1 einen Multifunktions-Server, insbesondere Twin-Server, mit wenigstens zwei eigenständigen Server, die jeweils ein eigenständiges Mainboard, wenigstens eine eigene CPU, Festplatten, Speicherbausteine und /oder Netzwerkkarte aufweisen, wobei die Server in einem gemeinsamen, insbesondere in einem 19" rackfähigen, Gehäuse angeordnet sind. Auf beiden eigenständigen Servern laufen die Firewalls parallel. Durch den Ansatz der Redundanz im System ist das System zwar ausfallsicher, was ein Kennzeichen des Systems ist. Einen höchstmöglichen Schutz vor Angriffen aus einem externen Netzwerk kann das System nicht bieten, weil es direkt mit dem externen Netzwerk verbunden wird. Durch einen Konfigurationsfehler, durch Versäumnis der Aktualisierung eines Betriebsystems oder einen Benutzerfehler kann das interne Netzwerk von einem externen Netzwerk aus schädigend Angegriffen werden.
Trotz der kostengünstigen Anschaffung der Hardware des Systems, bleibt ein erhöhter Wartungsaufwand für das aktualisieren von Betriebsystemen, Virenscanner und der Administration.

Darstellung der Erfindung

Aus der bekannten Technik ist es Aufgabe der vorliegenden Erfindung eine kostengünstige, einfache und im Bezug auf den verursachten Schaden höchstmöglich sichere Lösung zum Schutz von Betriebsystemen oder Netzwerken vor schädigenden Angriffen über eine externe Schnittstelle auf das zu schützende Netzwerk oder System anzubieten. Die Erfindung baut auf einer einfachen Idee auf, das interne Netzwerk wird von der Internetschnittstelle, welche die Schwachstelle im Netzwerk bildet hardwaremäßig getrennt. Dadurch ist gewährleistet, dass ein schädigender Angriff über die externe Schnittstelle auf das zu schützende Netzwerk im Prinzip unmöglich ist

diaplan elektronic gmbh
Kaufmanngasse 5
9020 Klagenfurt
E-Mail : office@diaplan.com
tele : +43 463 54510 45
fax: + 43 463 54510 15

(physikalische Trennung der Verbindung). Die bisher bekannten Systeme aus dem Stand der Technik verbinden das gesamte Netzwerk oder die Server des Netzwerks mit dem Internet. Aufgabe der Erfindung ist es, dem Klient des internen Netzwerks eine Internet Verbindung zu ermöglichen, ohne das interne Netzwerk mit dem Internet zu verbinden. Zur Lösung dieser Aufgabe geht die Erfindung davon aus, dass zwei oder mehrere Netzwerke aufgebaut werden. Ein internes Netzwerk (interne Daten Laufwerke, interne Mails) auf das jeder Benutzer, welcher nicht mit dem Internet verbunden ist, zugreifen kann. Ein externes Netzwerk, welches zum Zugriff auf das Internet verwendet wird. Jeder Benutzer kann sich mit einem der beiden Netzwerke verbinden. Eine gleichzeitige Verbindung mit dem internen und externen Netzwerk ist nicht möglich(siehe Figur 1).

Die Aufgabe wird dadurch gelöst, dass jeder Verbindungsknoten die Arbeitsstation nur mit einem Arbeitsbereich, welcher ein Netzwerk oder auch ein allein stehender Betrieb ist, verbinden kann. Bei einem Verbindungsaufbau der Arbeitsstation mit einer externen Ressource wird die Arbeitsstation zuerst vom internen Netzwerk getrennt. Nach erfolgreicher Trennung wird die Arbeitsstation mit dem externen Netzwerk verbunden. Vor der Trennung vom internen Netzwerk werden alle Ressourcen und Informationen des internen Netzwerks von der Arbeitsstation gesichert und von der Arbeitsstation entfernt.
Der Verbindungswechsel der Arbeitsstation kann über eine Wechselschaltung erfolgen.
Die Anforderung des Verbindungswechsels kann manuell oder automatisch erfolgen. Nach dem Beenden der externen Ressource wird die Arbeitsstation vom externen Netzwerk getrennt und anschließend zertifiziert wieder mit dem internen Netzwerk verbunden. Bei der Erkennung eines Virus auf der Arbeitsstation wird diese nicht mehr mit dem internen Netzwerk verbunden. Damit ist gewährleistet, dass ein Ausfall nur auf einer Arbeitsstation eine Auswirkung hat.
Durch das physikalische Trennen der Netzwerkverbindungen kann kein direkter Zugriff auf das interne Netzwerk erfolgen. Die externe Schnittstelle, welche die Schwachstelle in der Netzwerkstruktur des derzeitigen Systemstandards bildet ist somit physikalisch vom internen Netzwerk getrennt. Damit ist ein Hacker Angriff auf das interne System im Prinzip ausgeschlossen.

Es ist bevorzugt, dass beim Trennen die internen Laufwerke entfernt werden, der Zwischenspeicher entleert und geöffnete interne Dokumente geschlossen oder zwischengespeichert werden. Damit können keine Daten in das externe Netzwerk übertragen werden und bei der Rückverbindung kann durch das

diaplan elektronic gmbh
Kaufmanngasse 5
9020 Klagenfurt
E-Mail : office@diaplan.com
tele : +43 463 54510 45
fax: + 43 463 54510 15

Zwischenspeichern der Daten eine Zeitersparnis gewonnen werden.

Es ist bevorzugt, dass vor dem Umschalten in das interne Netzwerk die Arbeitsstation auf einen Such Prozessor geschaltet wird. Der Such Prozessor kann in der Umschalteinheit integriert werden. Am Such Prozessor wird die Arbeitsstation auf Viren überprüft. Ist diese mit einem Virus infiziert, gibt es keine Freigabe für eine Verbindung mit dem internen Netzwerk. Die Arbeitsstation kann automatisch formatiert werden und ein zertifizierte neues Abbild wird auf die Arbeitsstation eingespielt. Nach erfolgreicher Neuinstallation oder Viren und Trojaner freiem System wird die Arbeitsstation wieder mit dem internen Netzwerk verbunden. Die Abbilder der einzelnen Arbeitsstationen können auf dem Such Prozessor hinterlegt werden und vor dem Umschalten einmalig automatisch gesichert werden. Der Speicherbereich für das Ablegen des zertifizierten Abbild der Betriebsysteme kann als reiner Lesespeicher ausgebildet werden, wenn eine höhere Sicherheitsstufe gefordert ist. Die Implementierung des Such Prozessors kann in der Arbeitsstation oder in einer externen Einheit erfolgen.

Erfindungsgemäß wurde gefunden, dass vor dem Verbindungsaufbau mit dem externen Netz alle Daten, welche vom internen Netzwerk stammen, entfernt werden, um keine Informationen an das externe Netz weiter zugeben. Es werden auch Informationen wie IP Adresse, Server IP, Subnet Maske und alle Informationen, welche Auskunft über das interne Netzwerk geben entfernt. Die Arbeitsstation wird nur mit dem externen Netzwerk verbunden, wenn sie komplett aus der internen Domain entfernt wurde. Damit werden keine Informationen des internen Netzwerks an die externe Schnittstelle weitergegeben.

Ein weiterer Aspekt der erfindungsgemäßen Lösung ist der, dass das Computersicherheitssystem bei der Verwendung eines eigenen externen und internen Betriebsystems für das externe und interne Betriebsystem unterschiedliche Betriebsysteme verwendet.

Entsprechend einer weiteren Ausführungsform ist das erfindungsgemäße Computersicherheitssystem frei skalierbar. Damit kann das erfindungsgemäße Computersicherheitssystem mit den Anforderungen und Erwartungen des Nutzers oder der Betreibers von einer preiswerten Einstiegslösung für Privatnetzwerke gerecht werden und bis zu großen Firmennetzwerken wachsen.

NACHGEREICHT

diaplan elektronic gmbh
Kaufmanngasse 5
9020 Klagenfurt
E-Mail : office@diaplan.com
tele : +43 463 54510 45
fax: + 43 463 54510 15

Erfindungsgemäß wurde gefunden, dass es bevorzugt ist, wenn das System abhängig von der verwendeten Hardware mit unterschiedlichen Sicherheitslevels ausgestattet ist, da dies eine individuelle Anpassung erleichtert und Kosten spart. Sie kennzeichnen die Umschaltgeschwindigkeit und den zusätzlichen Ressourcenaufwand des Systems, wobei Level 3 das günstigste Summenergebnis dieser Kriterien bildet.
Im ersten Level werden bei jedem Verbindungswechsel vom externen zum internen Netzwerk die Konfigurationsdateien des Betriebsystems durch die am Such Prozessor hinterlegten original Dateien ersetzt. Bei einer Änderung der Dateien durch einen externen Angriff auf die Workstation können diese wieder hergestellt werden.
Im zweiten Level wird bei jedem Umschaltvorgang der gesamte Parametersatz des Systems oder das gesamte Betriebsystem ersetzt, somit ist gewährleistet, dass die Workstation höchstmöglich keine infizierten Dateien oder Betriebssystem Modifikationen beinhaltet. Für diese Variante ist kein Virenscanner für die Arbeitsstation notwendig, da immer das gesamte Betriebssystem neu eingespielt wird. Im drittem Level werden auf der Workstation zwei Betriebssysteme ausgeführt, wobei eines für das interne und eines für das externe Netzwerk betrieben wird. Beim Verbindungswechsel wird auf das jeweilige Betriebssystem umgeschaltet oder gebootet. Das externe Betriebssystem wird bei jedem Verbindungswechsel zum internen Netzwerk aus neu installiert und gebootet. Das Betriebsystem befindet sich auf dem Such Prozessor der Umschalteinheit. Als mögliche Implementierung des Computersicherheitssystems kann auch das gesamte System in einem PC Gehäuse untergebracht werden. Nachdem der Trend der Miniaturisierung immer weiter voran schreitet, können aus dem jetzigen Stand der Technik mehrere Computereinheiten mit dem Computersicherheitssystem in einem PC Gehäuse abgebildet werden, wodurch sich der räumliche Bedarf und die Kosten des Systems reduzieren.
Durch die Umschalteinheit muss lediglich ein Netzwerkkabel zur Arbeitsstation gelegt werden.

Im den folgenden Absätzen werden die Sicherheitslevel genauer beschrieben und erklärt.

Level 1

Erfindungsgemäß wird der Verbindungswechsel vom internen Netzwerk wie folgt beschrieben durchgeführt.
Die Umschalteinheit bemerkt eine Anforderung einer externen Ressource durch eine manuelle oder automatische Anforderung von einer Arbeitsstation. Der Knotenpunkt der Arbeitsstation wird ermittelt und es wird der Arbeitsstation die Trennung aller internen Netzwerkverbindungen signalisiert. Der Nutzer

NACHGEREICHT

diaplan elektronic gmbh
Kaufmanngasse 5
9020 Klagenfurt
E-Mail : office@diaplan.com
tele : +43 463 54510 45
fax: + 43 463 54510 15

kann die Aufforderung für die Umschaltung bei jedem Vorgang bestätigen oder eine automatische Bestätigung wählen. Nach erfolgreicher Verbindungstrennung vom internen Netzwerk wird auf den Such Prozessor geschaltet, welcher sich ein Betriebssystemabbild von der Arbeitsstation holt. Sind die Vorgänge am Such Prozessor abgeschlossen, so wird auf das externe Netzwerk geschaltet. Der Nutzer kann nun mit der externen Ressource arbeiten. Interne Ressourcen stehen ihm während der externen Verbindung nicht zur Verfügung.

Wird von der Umschalteinheit die Beendigung der externen Ressource bemerkt, so wird die Arbeitsstation auf eine Rückschaltung auf das interne Netzwerk vorbereitet. Die Arbeitsstation wird jetzt mit dem Such Prozessor der Umschalteinheit verbunden. Die Arbeitsstation wird überprüft und die Konfigurationsdateien des Betriebssystems werden ersetzt. Ist die Arbeitsstation infiziert, so wird automatisch eine Neuinstallation vorgeschlagen und durchgeführt. Die Überprüfung der Arbeitsstation kann ganz einfach mit einem auf dem Such Prozessor hinterlegtes Abbild durchgeführt werden. Ergeben sich Unterschiede, ist der Rechner infiziert. Ein schnelles Vergleichen kann mit der Größe des Abbilds durchgeführt werden. Nach erfolgreicher Neuinstallation oder fehlerfreiem Betriebssystem wird die Arbeitsstation wieder mit dem internen Netzwerk verbunden. Dateien, welche auf der Arbeitsstation gespeichert werden oder in den Zwischenspeicher geschrieben werden, gehen dabei verloren.

Level 2

Die Umschalteinheit bemerkt eine Anforderung einer externen Ressource von einer Arbeitsstation. Der Knotenpunkt der Arbeitsstation wird ermittelt und es wird der Arbeitsstation die Trennung aller internen Netzwerkverbindungen signalisiert. Der Nutzer kann dies bei jedem Vorgang bestätigen oder eine automatische Bestätigung wählen. Nach erfolgreicher Verbindungstrennung vom internen Netzwerk wird auf den Such Prozessor geschaltet, welcher sich ein Betriebssystem Abbild vom Rechner holt. Sind die Vorgänge am Such Prozessor abgeschlossen so wird auf das externe Netzwerk geschaltet. Die Arbeitsstation wird vollständig aus der internen Domäne entfernt und bekommt eine neue Netzwerkadresse in einem anderen Netzwerkbereich als das interne Netzwerk. Alle Informationen vom internen Netzwerk auf der Arbeitsstation werden entfernt. Der Nutzer kann nun mit den externen Ressourcen arbeiten.

NACHGEREICHT

diaplan elektronic gmbh
Kaufmanngasse 5
9020 Klagenfurt
E-Mail : office@diaplan.com
tele : +43 463 5451045
fax: + 43 463 5451015

Wird von der Umschalteinheit die Beendigung der externen Ressource bemerkt, so wird die Arbeitsstation auf eine Rückschaltung auf das interne Netzwerk vorbereitet. Die Arbeitsstation wird jetzt mit dem Such Prozessor der Umschalteinheit verbunden. Die Arbeitsstation wird neu installiert mit dem Abbild, welches vor dem Umschalten am Such Prozessor hinterlegt wurde. Die installierten Abbilder können in einer zusätzlichen Partition der Festplatte oder einem anderem Speicher durchgeführt werden, um die Formatierung der Platte während des Startvorgangs des neuen Betriebssystems durchführen zu können. Nach erfolgreicher Neuinstallation wird die Arbeitsstation wieder mit dem internen Netzwerk verbunden. Dateien, welche auf der Arbeitsstation gespeichert werden oder in den Zwischenspeicher geschrieben werden gehen dabei verloren.

Level 3

Die Umschalteinheit bemerkt eine Anforderung einer externen Ressource von einer Arbeitsstation. Der Knotenpunkt der Arbeitsstation wird ermittelt und es wird der Arbeitsstation ein Umschalten des Betriebssystems signalisiert. Die Umschalteinheit kann als externes oder internes Gerät realisiert werden. Beide Betriebssysteme sind im Hintergrund gestartet und sind mit dem internen oder externen Netzwerk verbunden. Bei der Umschaltung wird auf ein laufendes Betriebssystem geschaltet. Der Nutzer kann nun mit der externen Ressource arbeiten.

Wird von der Umschalteinheit die Beendigung der externen Ressource bemerkt, so wird die Arbeitsstation auf eine Rückschaltung auf das interne Netzwerk vorbereitet. Die Arbeitsstation kann sofort mit dem internen Betriebsystem verbunden werden, weil keine Verbindung mit dem externen Betriebsystem besteht. Beim Umschalten auf das interne Betriebssystem wird das externe Betriebssystem über die Umschalteinheit neu installiert und für ein nächstes Umschalten auf die externe Ressource vorbereitet.

Eine Erweiterung der erfinderischen Lösung sieht vor, dass das jedes Netzwerk auch zusätzlich mit Schutzsystemen ausgestattet werden kann.

Ein weiterer Aspekt der erfindungsgemäßen Lösung ist der, dass die externen Daten über eine eigene Transferstation in das interne Netzwerk gebracht werden. Die Transferstation kann Files oder Emails, welche als File am Transfer Prozessor

diaplan elektronic gmbh
Kaufmanngasse 5
9020 Klagenfurt
E-Mail : office@diaplan.com
tele : +43 463 54510 45
fax: + 43 463 54510 15

hinterlegt werden in das interne Netz bringen. Jedes File wird vorher nach Viren gescannt und auf Fehler überprüft. Ist dieser Such erfolgreich und können keine Fehler entdeckt werden, so findet ein Transfer der Dateien ins interne Netzwerk statt. Aus der Sicht des Users bildet die Transferstation einen File und Mail Server, welche zum Ablegen von Informationen benützt werden kann. Der Transfer Prozessor ist in der externen oder internen Umschalteinheit integriert.

Erfindungsgemäß werden bei der Ausführung des Systems mit Level drei die Betriebssysteme vorzugsweise als Terminal Klient Betriebssysteme auf die Workstations gespielt. Diese Betriebssysteme sind sehr klein, da sie nur eine Verbindung zum Terminal Prozessor herstellen, wo die Anwendungen des Benutzers ablaufen. Die Terminal Klient Betriebssysteme können somit auf einen kleinen Speicher einer Einschubkarte, oder eines externen Gerätes (USB Stick) oder in den Bootspeicher einer bootfähigen Netzwerkkarte gebootet werden. Das externe Betriebssystem kann als einfacher Browser ausgeführt werden.

Ein weiterer Aspekt der erfindungsgemäßen Lösung ist der, dass die Umschalteinheit als Einschubkarte für einen PC ausgeführt werden kann. Dies hat den Vorteil, dass keine zusätzliche externe Hardware benötigt wird und ein bestehendes Netzwerk durch Einbau der Umschalteinheit einfach umgerüstet wird. Der Bootspeicher für die Betriebssysteme und Such Prozessor können direkt auf die Karte implementiert werden. Für kleinere Netzwerke ist diese Systemlösung kostengünstiger.

Erfindungsgemäß ist in der Umschalteinheit auch ein Such Prozessor enthalten, der die Arbeitsstation vor der Verbindung mit dem internen Netzwerk nach Viren untersucht oder je nach Ausführung die Konfigurationsdateien des Betriebssystems ersetzt oder das gesamte Betriebssystem neu installiert.

Ein weiterer Aspekt der erfindungsgemäßen Lösung ist der, dass beim Umschaltvorgang das nicht benötigte Betriebssystem im Hintergrund neu installiert und gebootet wird, was eine Zeitersparnis beim Rückschalten auf das externe System darstellt. Unter anderem können im Zuge dieser Installation auch neue Updates des Systems eingespielt werden, ohne dass der Nutzer etwas davon bemerkt.

Erfindungsgemäß ist die Steuerung der Umschaltung der beiden Netzwerke physikalisch getrennt, das heißt die Umschaltung von einer Schalthardware kann nur in eine Richtung erfolgen. Dies

diaplan elektronic gmbh
Kaufmanngasse 5
9020 Klagenfurt
E-Mail : office@diaplan.com
tele : +43 463 54510 45
fax: + 43 463 54510 15

ist durch das Basis Konzept der Idee gegeben und verhindert eine Steuerung des gesamten Umschaltvorgangs von einem Netzwerk.

Ein weiterer Aspekt der erfindungsgemäßen Lösung ist der, dass das Computersicherheitssystem mit einer eigenen Schnittstelle für die Administration des Systems ausgestattet ist. Diese Schnittstelle ist mit keinem der beiden Netzwerke verbunden und kann nur hardwaremäßig über einen Administrationsschalter bedient werden. Damit ist sichergestellt, dass ein Zugriff auf die Einstellungen des Systems nur über eine Manuelle Betätigung möglich ist.

Erfindungsgemäß wurde festgestellt, dass eine Überblendung des Bildschirminhalts mit einer Speichereinheit von großer Bedeutung ist, um dem Benutzer ein Flackern des Bildschirms nicht sichtbar zu machen. Der Benutzer bemerkt dadurch die Umschaltung nicht und kann ganz normal am PC weiterarbeiten.

Ein weiterer Aspekt der erfindungsgemäßen Lösung ist der, dass die Umschalteinheit direkt auf dem Mainboard implementiert werden kann und beim Kauf schon ein Bestandteil des PCs ist. Damit entfällt die Installation des Systems in der internen und externen Netzwerkstruktur. Besonders gut geeignet sind Mainboards, die Multiprozessorsysteme unterstützen.

Ausführungsbeispiel

Die Anordnung für das System besteht aus einem Such-, Abbild und Transfer- Prozessor und einer Schalteinheit, welche das Trennen und Verbinden der einzelnen Arbeitsstationen ermöglicht. Die Steuerungen für die Umschaltungen der Netze sind getrennt, somit kann von einem Netzwerk nur in eine Richtung geschaltet werden. Dadurch ist es einem externen Hacker unmöglich, sich die Steuerung zu Nutze zu machen, weil diese nicht mit dem externen Netzwerk in Verbindung steht.

In Figur 1 wird das Grundkonzept der Idee dargestellt. In der Figur wird das externe A1, interne B1 Netzwerk und der Betrieb allein stehend mit G1 symbolisiert. Die Arbeitsstationen C1 können nur mit dem externen oder internen Netzwerk verbunden sein. Eine gleichzeitige Verbindung mit beiden Netzwerken ist nicht möglich. Mit der Darstellung D1 wird das gesamte System der Umschalteinheit beschrieben, welches aus geschlossenen Knotenpunkten E1 und offenen Knotenpunkten F1 besteht. Die Ansteuerung dieser Knotenpunkte erfolgt über zwei voneinander getrennten Systemen. Ein Knotenpunkt zu einem Netzwerk kann

diaplan elektronic gmbh
Kaufmanngasse 5
9020 Klagenfurt
E-Mail : office@diaplan.com
tele : +43 463 54510 45
fax: + 43 463 54510 15

nur geschlossen werden, wenn der des anderen Netzwerks geöffnet ist. Dies ist durch eine hardwaremäßige Verriegelung sichergestellt.

Figur 2 zeigt die Basis des Verbindungsprinzips des Systems. Mit dem X der Figur, welches bei Markierung in A2 gezeigt wird, ist die Trennung vom internen Server dargestellt. B2 stellt die Arbeitsstation des Netzwerks dar. Eine Verbindung C2 zu einem anderen Netzwerk ist nur möglich, nachdem die Trennung A2 der Arbeitsstation vom internen Netzwerk erfolgreich durchgeführt wurde.

diaplan elektronic gmbh
Kaufmanngasse 5
9020 Klagenfurt
E-Mail : office@diaplan.com
tele : +43 463 54510 45
fax: + 43 463 54510 15

Patentansprüche

1. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk insbesondere dem Schutz der Daten des internen Netzwerks mit einem jeder Arbeitsstation zugeordnetem Verbindungsknoten zur Trennung und Verbindung in den gewählten Arbeitsbereich, welcher ein Netzwerk oder auch ein allein stehender Betrieb ist, **dadurch gekennzeichnet, dass** jeder Verbindungsknoten die Arbeitsstation nur mit einem Arbeitsbereich, welcher ein Netzwerk oder auch ein allein stehender Betrieb ist, verbinden kann.

2. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach Anspruch 1, **dadurch gekennzeichnet, dass** die Steuerung der Verbindung durch zwei getrennte Steuerungssystem realisiert ist und diese hardwaremäßig voneinander getrennt sind.

3. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder beiden der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** im System ein Such Prozessor für eine Virusprüfung implementiert ist.

4. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** ein Abbild Prozessor im System für das automatische Wiederherstellen der Arbeitsstation im System implementiert ist.

5. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** ein Transfer Prozessor im System implementiert ist, welche die gescannt Daten des externen Servers in das interne Netzwerk ohne das interne Netzwerk mit dem externen zu Verbinden speichert.

NACHGEREICHT

diaplan elektronic gmbh
Kaufmanngasse 5
9020 Klagenfurt
E-Mail : office@diaplan.com
tele : +43 463 54510 45
fax: + 43 463 54510 15

6. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** die Arbeitsstation bei benötigen einer externen Ressource zuerst die Verbindung mit dem internen Netzwerk trennt und nur bei erfolgreicher Trennung eine Verbindung mit dem externen Netzwerk aufnimmt.

7. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** vor der Rückverbindung mit dem internen Netzwerk die Arbeitsstation gesäubert wird.

8. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** keine Information vom internen System über die Arbeitsstation an die externe Schnittstelle übertragen werden kann.

9. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** eine Anforderung eines Verbindungswechsel nur in eine Richtung pro Netzwerk möglich ist.

10. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System keine direkte Verbindung des externen Netzwerks mit dem internen Netzwerk zulässt.

11. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** ein Informationstransfer der internen

diaplan elektronic gmbh
Kaufmanngasse 5
9020 Klagenfurt
E-Mail : office@diaplan.com
tele : +43 463 54510 45
fax: + 43 463 54510 15

Daten nur über einen Transfer Prozessor geht, welcher nicht mit beiden Netzwerken gleichzeitig verbunden sein kann.

12. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** es mindestens zwei Arbeitsbereiche gibt, welche nicht mit einander verbunden sind.

13. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** nur die Arbeitsstationen mit dem externen Server verbunden werden.

14. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** die Arbeitsstationen vor Verbindung mit dem externen Server vom internen Netzwerk getrennt werden.

15. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** nur bei einer Fehler und Virus freien Arbeitsstation eine Rückverbindung mit dem internen Netzwerk möglich ist.

16. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** bei Verbindungswechsel immer über den Such Prozessor geschalten wird.

17. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem

NACHGEREICHT

diaplan elektronic gmbh
Kaufmanngasse 5
9020 Klagenfurt
E-Mail : office@diaplan.com
tele : +43 463 54510 45
fax: + 43 463 54510 15

Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** bei Verbindungswechsel auf das externe Netzwerk ein Abbild oder eine Sicherung der Konfigurationsdateien der Arbeitsstation gemacht werden.

18. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System als externes oder internes Gerät ausgeführt werden kann.

19. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System mit einer USB, Firewire, Ethernet, RS232, IR , Bluetooth, WLAN und mit jeder anderen Schnittstelle ausgebildet sein kann.

20. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System am Mainboard implementiert werden kann.

21. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System bei jedem Verbindungswechsel die Konfigurationsdateien des Betriebsystems ersetzt.

22. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System bei jedem Verbindungswechsel das Betriebsystem neu installiert.

NACHGEREICHT

diaplan elektronic gmbh
Kaufmanngasse 5
9020 Klagenfurt
E-Mail : office@diaplan.com
tele : +43 463 54510 45
fax: + 43 463 54510 15

23. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System auf der Arbeitsstation mit zwei unterschiedlichen Betriebsystem arbeitet, wobei ein Betriebsystem mit dem externen und eines mit dem internen Netzwerk verbunden ist.

24. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System die Neuinstallation des externen Betriebsystems nur bei nicht benötigter externer Ressource durchführt.

25. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System die beiden Betriebsysteme im Hintergrund parallel weiterlaufen lässt.

26. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System die beiden Betriebsysteme an der Arbeitsstation bei jedem Verbindungswechsel neu einspielt.

27. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** am System die Betriebsystem als Terminalprogramme ausgeführt werden können.

28. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder

diaplan elektronic gmbh
Kaufmanngasse 5
9020 Klagenfurt
E-Mail : office@diaplan.com
tele : +43 463 54510 45
fax: + 43 463 54510 15

mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System als Einschubkarte für die Arbeitsstation ausgebildet sein kann.

29. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System den Verbindungswechsel manuell oder automatische durchführen kann.

30. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System eine hardwaremäßige Steuerung des Verbindungswechsel über eine sonder Kombination oder sonder Taste der Mouse oder Tastatur unterstützt.

31. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System das Flackern des Bildschirms beim Verbindungswechsel durch einen sanften Bildübergang ersetzt und dem Benutzer das Flackern nicht mehr sichtbar ist.

32. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System den Benutzer über jeden Verbindungswechsel informiert.

33. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System jeden Verbindungswechsel in einer Datei aufzeichnet und überwacht.

diaplan elektronic gmbh
Kaufmanngasse 5
9020 Klagenfurt
E-Mail : office@diaplan.com
tele : +43 463 54510 45
fax: + 43 463 54510 15

34. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System auf beliebig große Netzwerke erweiterbar ist.

35. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System mit einer Redundanz ausgestattet werden kann.

36. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System als Multisystem mit Parallel arbeitenden Einheiten für eine Bessere Systemleistung ausgestatte werden kann.

37. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System beliebig vielen Teilsystem kaskadiert werden kann.

38. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System durch Firmware Updates auf neuesten Stand gebracht zu werden kann.

39. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System mit einer USV Anlage verbunden sein kann und mit dieser Kommunizieren kann.

NACHGEREICHT

diaplan elektronic gmbh
Kaufmanngasse 5
9020 Klagenfurt
E-Mail : office@diaplan.com
tele : +43 463 54510 45
fax: + 43 463 54510 15

40. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System mit mehreren Schalteinheiten ausgeführt sein kann.

41. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System eine Schnittstelle bittet mit der es dem Benutzer ermöglicht ist das System nach seinen Bedürfnissen zu konfigurieren.

42. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System mit einer Schnittstelle ausgestattet ist mit der man aufgezeichnete statistische Daten aus dem System auszulesen kann.

43. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System den Netzwerkverkehr überwacht und so ein automatischer Verbindungswechsel möglich ist.

44. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System auch so eingerichtet werden kann, dass der Benutzer jeden Verbindungswechsel bestätigen muss.

45. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch**

diaplan elektronic gmbh
Kaufmanngasse 5
9020 Klagenfurt
E-Mail : office@diaplan.com
tele : +43 463 54510 45
fax: + 43 463 54510 15

gekennzeichnet, dass das System mit einem Passwort für einen Verbindungswechsel ausgestattet werden kann.

46. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** im System für jeden Benutzer ein Verbindungswechselpasswort eingerichtet werden kann.

47. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System über einen Transfer Prozessor, welcher sich im externen Server als Laufwerk zur Verfügung stellt, Dateien in das interne System mit der Umschalteinheit und dem Such Prozessor gescannte Dateien transportieren kann.

48. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System den Transfer Prozessor wie eine Arbeitsstation behandelt und bei jedem Verbindungswechsel neu installiert.

49. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System mit dem Transfer Prozessor Mails vom externen Mail Server in den internen Mail Server und umgekehrt transferieren kann.

50. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System im Fehlerfall einer Arbeitsstation diese automatisch Formattieren, Neuinstallieren und neu Booten kann.

NACHGEREICHT

diaplan elektronic gmbh
Kaufmanngasse 5
9020 Klagenfurt
E-Mail : office@diaplan.com
tele : +43 463 54510 45
fax: + 43 463 54510 15

51. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System vor dem Umschalten auf das externe System die Arbeitsstation komplett aus der internen Domäne entfernt und alle Einträge der internen Domäne sichert und anschließend entfernt.

52. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System vor dem Verbindungswechsel den Zwischenspeicher der Arbeitsstation löscht.

53. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System nur bei korrekter Entfernung aus der internen Domäne und korrekter Löschung aller Informationen des internen Netzwerk auf der Arbeitsstation ins externe Netzwerk geschalten wird.

54. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System im Online Betrieb neue Betriebssoftwareupdates einspielen kann, ohne das der Benutzer etwas merkt, welche bei jedem Verbindungswechsel das System aktualisieren.

55. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System durch die Trennung der Steuerung für den Umschaltprozess nur in eine Schaltposition von einem Netzwerk aus gebracht werden kann.

diaplan elektronic gmbh
Kaufmanngasse 5
9020 Klagenfurt
E-Mail : office@diaplan.com
tele : +43 463 54510 45
fax: + 43 463 54510 15

56. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System mit einer automatischen Betriebssoftwareupdateeinheit und Virusupdateeinheit ausgestattet werden kann.

57. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System vor Verbindungswechsel die geöffneten Dateien zwischen speichert und bei der Rückschaltung wieder öffnet.

58. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System mit einer eigenen externen Betätigung für das Umschalten jeder Arbeitsstation ausgeführt werden kann.

59. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System mit einer Verschlüsselungseinheit ausgestattet sein kann.

60. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** der Transfer Prozessor des System nicht mit beiden Netzwerken gleichzeitig verbunden sein kann.

61. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch**

NACHGEREICHT

diaplan elektronic gmbh
Kaufmanngasse 5
9020 Klagenfurt
E-Mail : office@diaplan.com
tele : +43 463 54510 45
fax: + 43 463 54510 15

gekennzeichnet, dass der Transfer Prozessor des Systems die Transferdaten in einen Zwischenspeicher lädt, wo diese gescannt werden.

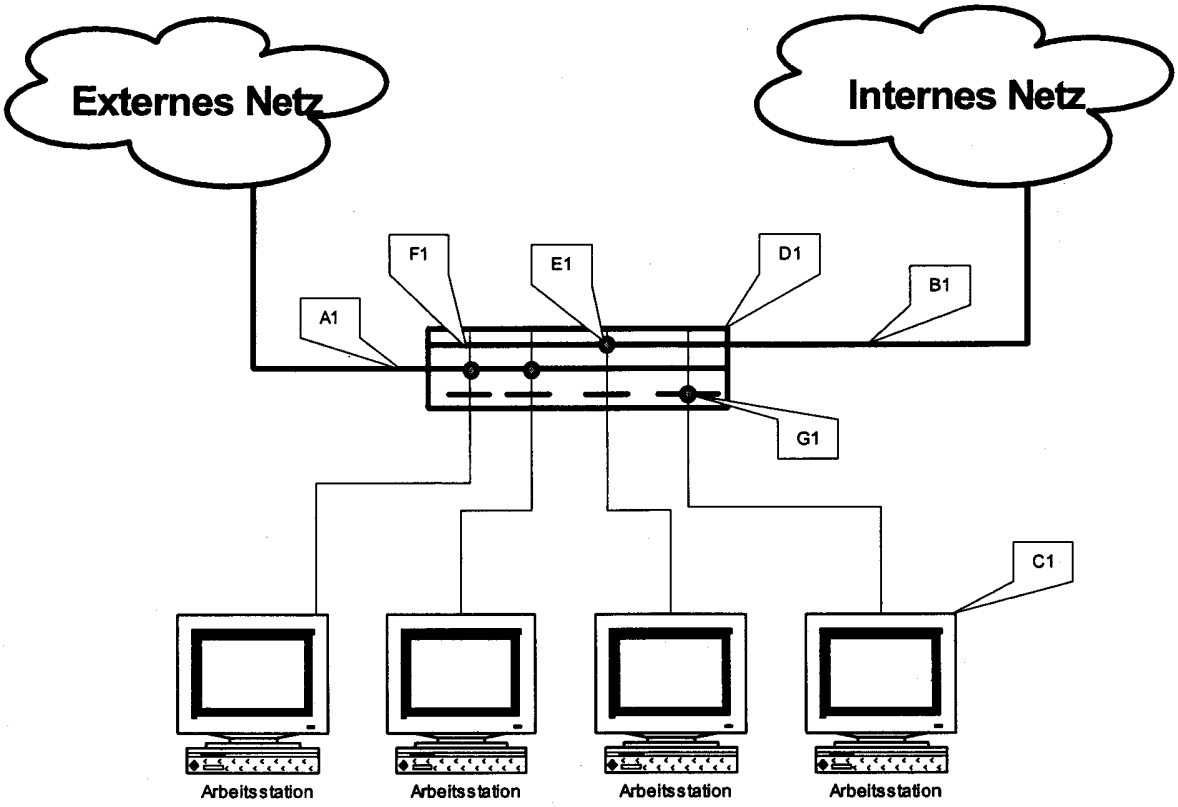
62. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** der Transfer Prozessor den Datenaustausch von Emails und Files ins interne oder den Email für den Postausgang vom internen Netzwerk dynamisch durchführen kann.

63. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das Computersicherheitssystem mit einer zweiten Einheit ausgebildet ist und beim Ausfall der ersten Einheit auf die zweite redundante Einheit umschaltet.

64. Computersicherheitssystem für höchstmöglichen Schutz vor direkten schädigenden Angriffen auf das interne Netzwerk über eine externe Schnittstelle insbesondere dem Schutz der Daten des internen Netzwerks nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** jedes der beiden redundanten Einheiten eine eigene Netzversorgung hat.

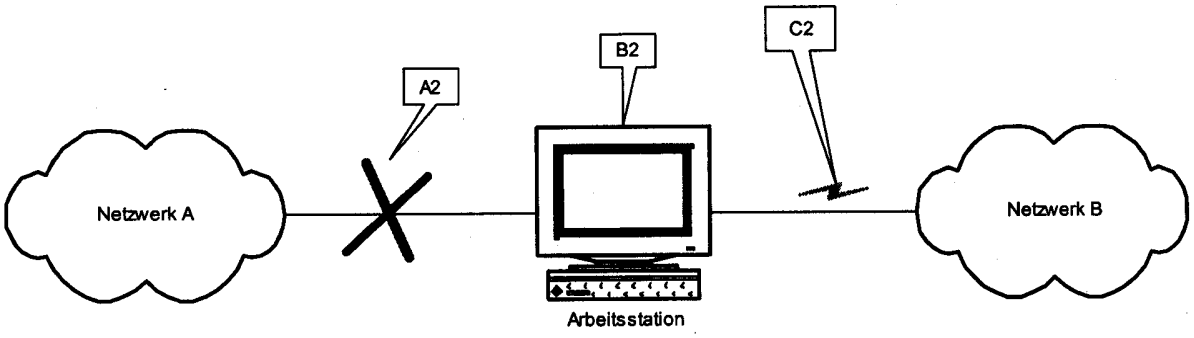
NACHGEREICHT

diaplan elektronic gmbh
Kaufmanngasse 5
9020 Klagenfurt
E-Mail : office@diaplan.com
tele : +43 463 54510 45
fax: + 43 463 54510 15



Figur 1

diaplan elektronic gmbh
Kaufmanngasse 5
9020 Klagenfurt
E-Mail : office@diaplan.com
tele : +43 463 54510 45
fax: + 43 463 54510 15



Figur 2

NACHGEREICHT

diaplan elektronic gmbh
Kaufmanngasse 5
9020 Klagenfurt
E-Mail : office@diaplan.com
tele : +43 463 54510 22
fax: + 43 463 54510 15

Patentansprüche

1. Computersicherheitssystem für höchstmöglichen Schutz vor schädigenden Angriffen auf das interne Netzwerk insbesondere dem Schutz der Daten des internen Netzwerks mit einem jeder Arbeitsstation zugeordneten Verbindungsknoten, **dadurch gekennzeichnet, dass** das System als zentrales Computersicherheitssystem ausgeführt ist, mit dem mindestens zwei Netzwerke über diesen Verbindungsknoten durch eine physikalische Schaltung der Arbeitsstation einzeln zugeschalten und die übrigen Netzwerke physikalisch getrennt sind.

2. Computersicherheitssystem nach Anspruch 1, **dadurch gekennzeichnet, dass** die Steuerung der Verbindung durch zwei getrennte Steuerungssysteme realisiert ist und diese hardwaremäßig voneinander getrennt sind.

3. Computersicherheitssystem nach einem oder beiden der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** im System ein Suchprozessor für eine Virusprüfung implementiert ist.

4. Computersicherheitssystem nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** ein Abbildprozessor im System für das automatische Wiederherstellen der Arbeitsstation im System implementiert ist.

5. Computersicherheitssystem nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** ein Transferprozessor im System implementiert ist, welcher sich in einem ersten Schritt mit dem externen Netzwerk verbindet und sich die Daten des externen Servers holt, in einem zweiten Schritt der Transferprozessor vom externen Netzwerk getrennt wird und sich mit dem Suchprozessor verbindet, welcher die Daten des externen Servers auf Viren oder böswillige Programme überprüft, ist der Inhalt sauber, wird die Arbeitsstation vom Suchprozessor getrennt und mit dem internen Netzwerk verbunden, anschließend werden die Daten ins interne Netzwerk übertragen ohne das interne Netzwerk mit dem externen Netzwerk zu verbinden.

6. Computersicherheitssystem nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** die Arbeitsstation bei Benötigung einer externen Ressource zuerst die Verbindung mit dem internen Netzwerk trennt und nur bei erfolgreicher Trennung eine Verbindung mit dem externen Netzwerk aufbaut.

diaplan elektronic gmbh
Kaufmanngasse 5
9020 Klagenfurt
E-Mail : office@diaplan.com
tele : +43 463 54510 22
fax: + 43 463 54510 15

7. Computersicherheitssystem nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** Dateien oder Emails nicht vom internen System über die Arbeitsstation an die externe Schnittstelle sondern nur über den Transfer-Prozessor übertragen werden.

8. Computersicherheitssystem nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System mindestens zwei physikalisch getrennte Netzwerke oder ein Netzwerk und einen alleinstehenden Betrieb beinhaltet, welcher physikalisch vom Netzwerk getrennt ist.

9. Computersicherheitssystem nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** eine Arbeitsstation nur mit dem internen Netzwerk verbunden wird, wenn diese vom Suchprozessor als Fehler und virusfrei erfolgreich geprüft wurde.

10. Computersicherheitssystem nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** bei Verbindungswechsel immer im ersten Schritt für eine Prüfung der Arbeitsstation, diese auf den Suchprozessor geschalten wird.

11. Computersicherheitssystem nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** bei einem Verbindungswechsel auf das externe Netzwerk ein Abbild oder eine Sicherung der Konfigurationsdateien der Arbeitsstation am Suchprozessor hinterlegt wird.

12. Computersicherheitssystem nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System mit einer USB, Firewire, Ethernet, RS232, IR, Bluetooth, WLAN und mit jeder anderen Schnittstelle für den Verbindungsaufbau ausgebildet ist.

13. Computersicherheitssystem nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System bei jedem Verbindungswechsel die Konfigurationsdateien des Betriebssystems ersetzt.

14. Computersicherheitssystem nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** im Computersicherheitssystem zwei unterschiedliche Betriebssysteme hinterlegt sind, wobei eines für den externen und das andere für den internen Betrieb vorgesehen ist.

diaplan elektronic gmbh
Kaufmanngasse 5
9020 Klagenfurt
E-Mail : office@diaplan.com
tele : +43 463 54510 22
fax: + 43 463 54510 15

15. Computersicherheitssystem nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System die Neuinstallation des externen Betriebsystems nur bei nicht benötigter externer Ressource durchführt.

16. Computersicherheitssystem nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System die beiden Betriebssysteme im Hintergrund parallel weiterlaufen lässt.

17. Computersicherheitssystem nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System die beiden Betriebssysteme an der Arbeitsstation bei jedem Verbindungswechsel neu einspielt.

18. Computersicherheitssystem nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** am System die Betriebssysteme als Terminalprogramme ausgeführt sind.

19. Computersicherheitssystem nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System den Verbindungswechsel wahlweise manuell mit einem Schalter am Rechner, welcher mit der Umschalteinheit verbunden ist, oder automatisch mit der Umschaltsteuerung durch Prüfen der Netzwerkanforderungen der Arbeitsstation durchführt.

20. Computersicherheitssystem nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System den Benutzer über jeden Verbindungswechsel informiert.

21. Computersicherheitssystem nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System jeden Verbindungswechsel in einer Datei aufzeichnet und überwacht.

22. Computersicherheitssystem nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System mit einer zweiten Einheit als Redundanz ausgestattet ist.

23. Computersicherheitssystem nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System als Multisystem mit parallel arbeitenden Einheiten für eine bessere Systemleistung ausgestattet ist

diaplan elektronic gmbh
Kaufmanngasse 5
9020 Klagenfurt
E-Mail : office@diaplan.com
tele : +43 463 54510 22
fax: + 43 463 54510 15

und mit beliebig vielen Teilsystemen der Umschalteinheit kaskadierbar ist.

24. Computersicherheitssystem nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System durch Firmware Updates auf neuesten Stand gebracht wird.

25. Computersicherheitssystem nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System mit mehreren Schalteinheiten ausgeführt ist.

26. Computersicherheitssystem nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System eine Schnittstelle bietet, mit der es dem Benutzer ermöglicht das System nach seinen Bedürfnissen zu konfigurieren.

27. Computersicherheitssystem nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System den Netzwerkverkehr überwacht und so ein automatischer Verbindungswechsel möglich ist.

28. Computersicherheitssystem nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System den Transferprozessor wie eine Arbeitsstation behandelt und bei jedem Verbindungswechsel neu einspielt.

29. Computersicherheitssystem nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System mit dem Transferprozessor Mails vom externen Mailserver in den internen Mailserver und umgekehrt automatisch transferiert.

30. Computersicherheitssystem nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System im Fall einer geschädigten oder manipulierten Arbeitsstation diese automatisch formatiert, neu installiert und neu startet.

31. Computersicherheitssystem nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System vor dem Umschalten auf das externe Netzwerk die Informationen der internen Domäne von der Arbeitsstation im Suchprozessor sichert und danach von der Arbeitsstation entfernt.

diaplan elektronic gmbh
Kaufmanngasse 5
9020 Klagenfurt
E-Mail : office@diaplan.com
tele : +43 463 54510 22
fax: + 43 463 54510 15

32. Computersicherheitssystem nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System vor dem Verbindungswechsel den Zwischenspeicher der Arbeitsstation löscht.

33. Computersicherheitssystem nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System durch die Trennung der Steuerung für den Umschaltprozess nur in eine Schaltposition von einem Netzwerk aus gebracht wird.

34. Computersicherheitssystem nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System mit einer automatischen Betriebssoftwareupdateeinheit und Virusupdateeinheit ausgestattet ist.

35. Computersicherheitssystem nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System vor Verbindungswechsel die geöffneten Dateien zwischenspeichert und bei der Rückschaltung wieder öffnet.

36. Computersicherheitssystem nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System mit einer eigenen externen Betätigung für das Umschalten jeder Arbeitsstation ausgeführt ist.

37. Computersicherheitssystem nach einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das System mit einer Verschlüsselungseinheit ausgestattet ist.

Recherchenbericht zu **A 57/2005**
Technische Abteilung 3A

österreichisches patentamt

Klassifikation des Anmeldungsgegenstands gemäß IPC[7]: IPC (8): G06F 21/00N3E1
Recherchierter Prüfstoff (Klassifikation): ECLA: G06F21/00N3E1
Konsultierte Online-Datenbank: epodoc, wpi 14
Dieser Recherchenbericht wurde zu den am ~~21~~. **Jänner 2005** eingereichten Ansprüchen **1-64** erstellt.

Kategorie*)	Bezeichnung der Veröffentlichung: Ländercode, Veröffentlichungsnummer, Dokumentart (Anmelder), Veröffentlichungsdatum, Textstelle oder Figur soweit erforderlich	Betreffend Anspruch
X	DE 199 00 744 C2 (Pütter) 21. Dezember 2002 (21.12.2002) *gesamtes Dokument*	1-64
	--	
X	DE 101 09 628 A1 (O'Lucky) 5. September 2002 (05.09.2002) *gesamtes Dokument*	1-64
	--	
X	US 2004/0111578 A1 (Goodman et al.) 10. Juni 2004 (10.06.2004) *gesamtes Dokument, insbesondere Zusammenfassung; Fig.4; Fig.8; [0009]-[0012]; [0026]-[0027]; [0029]-[0030]*	1-64
	--	
X	US 6 578 140 B1 (POLICARD CLAUDE) 10. Juni 2003 (10.06.2003) *gesamtes Dokument, insbesondere Zusammenfassung; Fig.3; Fig.4;*	1-64
	--	
A	KR 2002 089 849 A (F & F SECURETEK CO LTD) 30. November 2002 (30.11.2002) *englische Zusammenfassung*	1-64

Datum der Beendigung der Recherche:	☐ Fortsetzung siehe Folgeblatt	Prüfer(in):
14. November 2005		Dipl.-Ing. FASTENBAUER

*) **Kategorien** der angeführten Dokumente:

- **X** Veröffentlichung **von besonderer Bedeutung**: der Anmeldungsgegenstand kann allein aufgrund dieser Druckschrift nicht als neu bzw. auf erfinderischer Tätigkeit beruhend betrachtet werden.
- **Y** Veröffentlichung **von Bedeutung**: der Anmeldungsgegenstand kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren weiteren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese **Verbindung für einen Fachmann naheliegend** ist.
- **A** Veröffentlichung, die den **allgemeinen Stand der Technik** definiert.
- **P** Dokument, das **von Bedeutung** ist (Kategorien **X** oder **Y**), jedoch **nach dem Prioritätstag** der Anmeldung **veröffentlicht** wurde.
- **E** Dokument, das **von besonderer Bedeutung** ist (Kategorie **X**), aus dem ein **älteres Recht** hervorgehen könnte (früheres Anmeldedatum, jedoch nachveröffentlicht, Schutz ist in Österreich möglich, würde Neuheit in Frage stellen).
- **&** Veröffentlichung, die Mitglied der selben **Patentfamilie** ist.