

Lizenz zum Aufpassen.



**8MAN**  
die Lösung für das  
Berechtigungsmanagement

## Haftungsbedingungen

Die in dieser Anleitung dargestellten Informationen können zu jeder Zeit und ohne weitere Hinweise geändert werden. Die Bereitstellung wird keine rechtlichen Folgen für protected-networks.com nach sich ziehen.

Die Verwendung der protected-networks.com Software 8MAN ist eine Endnutzer-Lizenzvereinbarung (EULA). 8MAN darf ausschließlich in Abstimmungen mit den vertraglichen Bedingungen genutzt werden.

Ohne vorherige schriftliche Vereinbarung von protected-networks.com darf dieses Dokument weder teilweise noch vollständig vervielfältigt, weitergegeben oder übersetzt werden.

Dieses Dokument soll verstanden werden als ein Teil einer Rahmenverordnung der Allgemeinen Geschäftsbedingungen von protected-networks.com, EULA und der Datenschutzbestimmungen die auf dieser Webseite aufgeführt sind.

## Copyright

8MAN ist eine eingetragene Handelsmarke einer Softwarelösung sowie seiner verwandten Dokumente und das geistige Eigentum von protected-networks.com.

Handelsmarke und Marke mit oder ohne ausdrückliche Anzeige sind das geistige Eigentum der jeweiligen Markeneigentümer.

protected-networks.com GmbH

Alt-Moabit 73

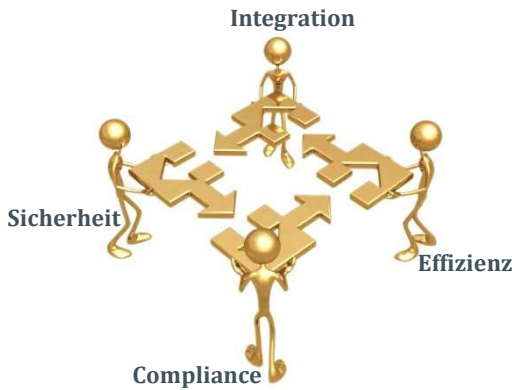
10555 Berlin

Tel.: +49 (30) 390 63 45 - 0

Web: [www.protected-networks.com](http://www.protected-networks.com)

Zuletzt geändert: Oktober 2010 - V0.3

# Berechtigungsmanagement-Lösung



Dieses Dokument bietet einen kurzen Überblick über die Beweggründe des Berechtigungsmanagements. Es wird im Detail gezeigt, was aus heutiger Sicht die Hauptgründe hierfür sind und was derzeit eine zufriedenstellende Durchführung verhindert. Es wird dargestellt, wie die so genannte „ISEC“ Lösung von protected-networks.com und die Umsetzung von 8MAN funktioniert. Im Anschluss daran folgt ein Beispielsfall, der die schnellen Einsparungen und Kosten sowie die Einbindung der gesamten Organisation aufzeigt, um vorhandene Sicherheitslücken zu reduzieren und dem „Need-to-know“-Prinzip zu verfolgen.

## Gefahr von innen

Tägliche Nachrichten: Vertrauliche Daten wurden gestohlen und erscheinen in der Öffentlichkeit oder wurden an den Wettbewerb verkauft. Der Diebstahl oder der Verlust ist hierbei weitaus bedeutsamer. Über 80% des Datenverlustes passiert aufgrund von Datenmissbrauch innerhalb des Unternehmens. Dies wurde von Analysten (IDC) und Prüfern bestätigt (KPMG).

In den meisten Unternehmen richtet sich der Großteil der Bemühungen auf die Sicherung der Netzwerke vor der Außenwelt mit beispielsweise Firewalls oder Anti-Virus-Software. Nahezu keine Anstrengung wird auf die Sicherung und Reduzierung der „Möglichkeiten“ vor Diebstahl und Datenverlust innerhalb des Unternehmens verwendet.

Hierfür gibt es vielseitige Gründe. Es ist bekannt, dass die moderne Spionage das „social hacking“ als eine Hauptbezugsquelle für Informationen nutzt. Auf der anderen Seite verhindert ein Mangel an entsprechenden Lösungen und Tools, einen Überblick über die Berechtigungssituation zu gewinnen und macht es somit nahezu unmöglich, diese Rechte zu handhaben oder in einer effizienten Weise zu verwalten.

Ein typisches Argument ist „Die unternehmenskritischen Daten sind in unserer Datenbank gesichert!“ Das scheint richtig zu sein. Es scheint auch zu stimmen, dass nur die absolute Minderheit der Mitarbeiter einen Zugang hat. Aber die zentrale Botschaft wird deutlich, wenn der Inhalt analysiert wird: Wie verändert sich das Kundenverhalten? Wie ist unser finanzieller Ausblick für die nächsten zwei Jahre? Welche Vorteile bringt die neue Technologie?



Diese Daten wie Word, Excel oder PowerPoint Files sind als unstrukturierte Daten gelagert. Eine Studie von Meryll Lynch hat ergeben, dass mehr als 80% der Daten in einem Unternehmen unstrukturiert sind! Somit sind die strategisch wichtigen Informationen über die Zukunft eines Unternehmens auf den Fileservern verfügbar. Deshalb ist es wichtig zu klären, wer hierauf Zugriff hat.



Heutzutage schafft es kein Tool, dies in einer ganzheitlichen Weise umzusetzen. Es gibt zwar einzelne Tools, die nützliche Informationen bieten, wenn Antworten zu konkreten Fragestellungen bestehen. Technische Unterbrechungen und die Unvereinbarkeit machen jedoch deren Anwendung bei Nicht-Funktionieren besonders mühsam.

Deshalb fordern Standards wie Sarbanes-Oxley (SOX) und Wirtschaftsprüfer wie KPMG eine Lösung für dieses Problem: Eine vollständige Dokumentation von "Wer hat einer konkreten Person eine Berechtigung vergeben und zu welchem Zeitpunkt?"

Einige große Unternehmen wie IBM, Computer Associates und Andere versuchen diese Probleme mithilfe der so genannten Identity Management Steuerung von oben nach unten zu lösen. Zuerst werden die Organisation, dann die Ressourcen und die bestehenden Rollen analysiert. Später werden die Rollen definiert und schlussendlich eingeführt. Dies führt jedoch nicht zu einem bedeutsamen Wechsel in der Verwaltung. Es ist weitaus schwieriger, dies zu entwickeln: Mitarbeiter entwickeln sich, Abteilungen ändern sich und Unternehmen werden gekauft. Es ist ein konstantes und lukratives Einkommen für die Beratungsunternehmen, diese Strukturen abzugleichen.

Solch eine teure und zeitintensive Investition ist für Unternehmen mit über 10.000 Angestellten bei weitem nicht bezahlbar. Und wie Forester in seinen Studien festgestellt hat, gibt es derzeit keine Produkte die für diese Art von Unternehmen geeignet sind.

Fazit: Die Bedrohung ist real und viele Unternehmen nehmen dies noch nicht ernst genug. Die Gründe hierfür können vielfältig sein: Ob es fehlende Managemententscheidungen sind, eine bestehende Lücke in den Tools oder eine ineffiziente Arbeitsgestaltung.

Die Rückverfolgung in frühere Zeiten unterstützt die rechtliche und ursächliche Analyse der Fälle von Datendiebstahl und -verlust. Die 8MAN Gruppe bietet hierfür eine schlüssige und integrierte Lösung für das Berechtigungsmanagement. Die Zeit ist reif für eine integrierte und ganzheitliche Lösung, um die Herausforderung anzunehmen.

### **Arbeiten durch "ISEC" von protected-networks.com**

Wie soll man eine Lösung im 21. Jahrhundert entwickeln in der Tools und Lösungen für nahezu jeden IT-Aspekt verfügbar sind? Die IT-Landschaft entwickelt sich: Virtualisierung, trübe Datenverarbeitung, Abwanderung und Konsolidierung sind stetige Themen für die Administratoren. Während der Aufwärtsbewegung der Wertschöpfungskette, ist das Rationalisieren und Automatisieren der „unwichtigen“ Aufgaben des Tagesgeschäfts notwendig.

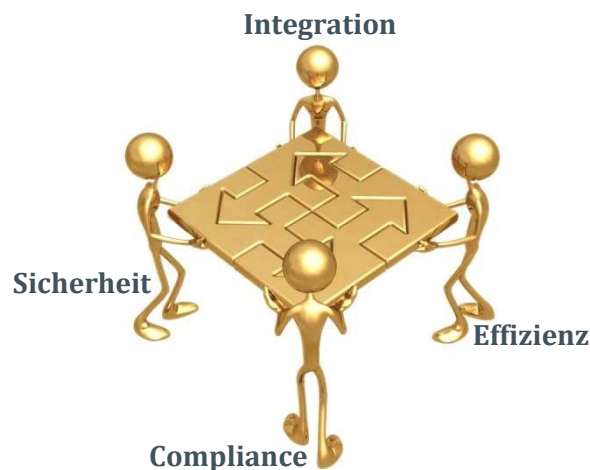


Angenommen, dass Zugangsberechtigungen keine unwichtigen Aufgaben sind, wie auch immer diese gemanagt werden, müssen die folgenden Fragen jedoch durch irgendeine Lösung beantwortet werden können.

- Wie integrieren wir den Prozess und reduzieren die Anzahl der technischen Unterbrechungen?
- Wie erhält man einen Überblick über die Dateneigentümer und deren Einfluss, ohne diese zu überladen?
- Wie kann man schnell und einfach vorhandene Lücken schließen?
- Wie erfüllen wir schnell und einfach die geforderte Einhaltung der rechtlichen Richtlinien?
- Wie führen wir einen Wechsel herbei?



Deshalb sollte jede Lösung nicht nur diese Fragen beantworten, sondern muss sich auf die folgenden Kategorien als Ganzes konzentrieren: ISEC als Integration, Sicherheit, Effizienz und Compliance.



### Integration und Transparenz

Um das Berechtigungsmanagement zu optimieren, müssen einige Elemente integriert sein: Active Directory, Fileserver und andere auf LDAP basierende Datenbanken und Ressourcen. Diese Daten müssen integriert und konsolidiert sein, um einen einfachen Überblick zu ermöglichen: Wo hat Herr Schmidt Zugang im Unternehmen?

- Zeigt in Minuten, wer Zugang zu den Daten hat.
- Visualisiert die Active Directory Gruppenstrukturen und die Verbindungen zueinander.
- Zeigt auf, über welche Gruppenstrukturen bestimmte Personen Zugang haben.
- Weist in Minuten auf die Unterschiede in den Berechtigungen zwischen den Verzeichnissen hin.



## Sicherheit und Einbindung

Benötigt wird ein klarer Überblick: Wo gibt es Sicherheitslücken? Um sie zu schließen, müssen einfache Mechanismen die Aufdeckung und Verbesserung der Situation erlauben. Dies muss entweder in der IT oder gemeinsam mit den Dateneigentümern und den Abteilungsleitern möglich sein.

- Aufdeckung und Beseitigung von möglichen Lücken auf einen Blick möglich.
- Bezieht die Dateneigentümer durch das Verschaffen eines Überblicks über die Zugangsberechtigungen auf ihre Daten ein.
- Überlässt den Dateneigentümer die Verantwortung für die korrekte Vergabe von Zugangsberechtigungen. Zeichnet und korrigiert regelmäßig den aktuellen Status auf.



## Effizienz und Effektivität

Die Effizienz wird durch das Gewähren und Aufheben von Zugangsberechtigungen oder auf Basis von temporären Berechtigungen unterstützt. Die Effektivität wird unterstrichen durch die automatische Bildung und Löschung von Gruppen die den empfohlenen Gruppenstrukturen von Microsoft und ihren Unternehmensrichtlinien entsprechen.

- Problemlose Einbindung in bereits bestehende Workflows
- Einfache Modifizierung durch Copy & Paste sowie Drag & Drop
- Berechtigte Mitgliedsgruppen oder Zugangsberechtigungen auf temporärer Basis durch die automatische Aufhebung in Minuten – eine Erinnerung hieran ist nicht mehr nötig – aufgehoben von ihrer Auslastung/Speicher
- Einfache und standardisierte Prozesse zur Reduzierung von Zeit und Kosten im Berechtigungsmanagement



## Compliance und Kontrolle

Um den Status von Zugangsberechtigungen und Gruppenstrukturen zu jeder Zeit in der Vergangenheit zu sehen, ist es notwendig, einen Überblick auf Anfrage zu erhalten. Daneben muss die aktuelle Situation nachweisbar sein: Woher kommt sie? Wer hat etwas geändert und wann? Der Wechsel des AD und der Zugangsrechte nur über die ISEC Lösung 8MAN (z. B. durch Admins, Helpdesk oder über die Dateneigentümer) ermöglicht nicht nur die Standardisierung, sondern auch die Rückverfolgung jeder Änderung und der hierzu gehörenden Erklärung.

- Aufzeichnung aller Scans der Gruppenstrukturen und Zugangsrechte in allen Ordnern zur späteren Einsicht: Wie war die Situation im 20. Jahrhundert?
- Aufzeichnung aller Änderungen von Zugangsrechten oder Gruppenstrukturen mit der Notwendigkeit der Rechtfertigung jeder Aktivität: Wer änderte was und wann?



- Zeigt vorgenommene Änderungen außerhalb von 8MAN, um sie zu akzeptieren oder abzulehnen. Was passierte außerhalb unseres Standardverhaltens?
- Erstellt vollständige Logbücher der Verzeichnisse, Nutzer und Gruppen sowie der vorgenommenen Änderungen. Was passierte in diesem Verzeichnis während des letzten Jahrzehnts?



## Praktische und direkte Beispiele

Wie "ISEC" und 8MAN das Berechtigungsmanagement in Unternehmen verändert, wird in einigen Fällen erklärt.

Authentifizierter Benutzer (b-filer01\Authentifizierter Benutzer) hat Zugriff auf die folgenden Verzeichnisse

Verzeichnis	Berechtigung	Größe
b-cluster_lab83		
b-filer01		
fileserver	Read	42.17 GB
Recordings\$		284.66 MB
User	Read and execute	0 Byte
Vorlagen	Read	683.32 MB
xfer	Modify	3.88 GB

Jeder (b-filer01\Jeder) hat Zugriff auf die folgenden Verzeichnisse

Verzeichnis	Berechtigung	Größe
b-cluster_lab83		
b-filer01		
fileserver		42.17 GB
z_InfoThek - ohne Backup	Modify	1.45 GB
z_Temp - ohne Backup	Modify	32.01 GB
Recordings\$	Modify	284.66 MB
User		0 Byte
Vorlagen		683.32 MB
xfer		3.88 GB

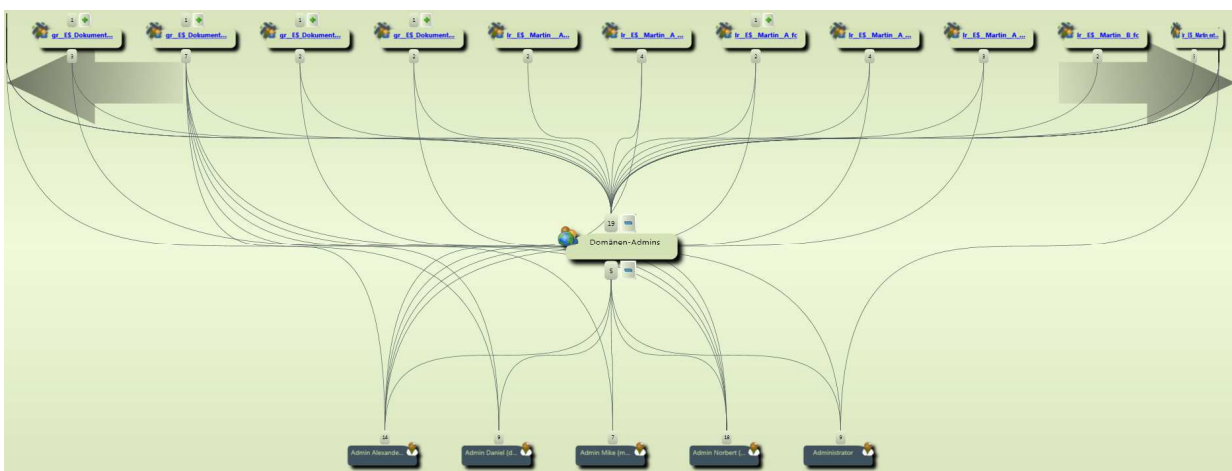
Wo hat "jeder" Zugang?

8MAN erlaubt die Suche und Darstellung „großer offener Türen“ wie Zugangsberechtigungen für jeden oder autorisierte Nutzer. Unter Verwendung des Szenarios "Wo hat ein Nutzer Zugang?", können diese Fälle in nur Minuten durch einen Klick dargestellt und korrigiert werden.

Wo hat „jeder“ Zugang im Unternehmen?

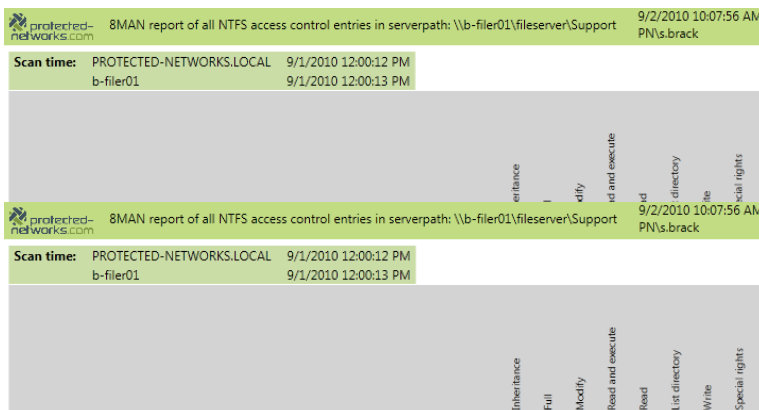
## Aufklärung der AD Gruppenstrukturen

Gruppenschleifen oder verzweigte Gruppenstrukturen können grafisch dargestellt und aufgeschlüsselt werden:



Wie sieht Ihre Struktur aus?



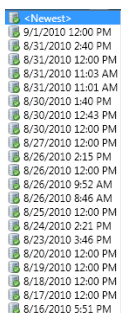


## Reports für die Abteilungsleitung

Die IT Verwaltung sollte nicht alleine eingebunden und verantwortlich für die Vergabe von Zugangsrechten auf die Unternehmensdaten sein. Ein einfacher Bericht oder ein Überblick ermöglicht die Einbindung der Abteilungsleitung, sodass sie somit ein wirkliches Eigentumsrecht an ihren Daten besitzen: Ist die Zugangsberechtigung auf den Ordner korrekt?

	Inheritance	Full	Modify	Read and execute	Read	List directory	Write	Special rights
<b>Read and execute</b>								
René Vierkorn (r.vierkorn)				✓	✓	✓		
Thomas Gomell (t.gomell)				✓	✓	✓		
<b>Read</b>								
Authentifizierte Benutzer (b-filer01\Authentifizierte Benutzer)					✓			
<b>Modify</b>								
Thomas Gomell (t.gomell)			✓	✓	✓	✓	✓	✓
Stephan Brack (s.brack)			✓	✓	✓	✓	✓	✓
Christian Zander (c.zander)			✓	✓	✓	✓	✓	✓
<b>Full</b>								
Felix Wagner (f.wagner)	✓	✓	✓	✓	✓	✓	✓	✓
Martin Geißler (m.geissler)	✓	✓	✓	✓	✓	✓	✓	✓
Mike Wiedemann (m.wiedemann)	✓	✓	✓	✓	✓	✓	✓	✓

Wann haben Sie das letzte Mal die Abteilungsleitung mit einbezogen?



## Start logging

Zu Beginn von 8MAN in ihrem Unternehmen werden alle Informationen beschafft und gelagert auf die Anfrage von den betreffenden Active Directory Informationen und Zugangsrechten auf die Verzeichnisse.

Starten Sie jetzt 8MAN und seien Sie fähig, jede Situation zurückzuverfolgen!

## Berechtigungsmanagement: Return on Invest – eine Fallstudie

Wie verbessert ISEC und 8MAN nicht nur die Zugangsberechtigungssituation, sondern auch die Kostenstruktur? Dieser Abschnitt zeigt Ihnen ein Beispiel. Das Nutzen von Microsoft Standard Tools benötigt 20 bis 30 Minuten, um einen Zugang zu bestätigen oder abzulehnen. Dabei wird angenommen, dass die empfohlene Gruppenstruktur erneuert und der Prozess dokumentiert wurde. Die Beschaffung eines Überblicks über alle Zugangsrechte auf einen bestimmten Ordner kann leicht mehr als drei Stunden andauern.

In einem Unternehmen mit mehr als 1000 Nutzern kann dies in Bezug auf die Zeit und die Kosten bei mehr als 155 Arbeitsstunden oder 50.000 EUR pro Jahr bedeutsam sein!

8MAN beschleunigt diese Aufgaben und vereinfacht den Prozess. Nutzerzeugnisse sind auf Anfrage verfügbar. 8MAN reduziert die Anstrengungen jeder Aufgabe auf wenige Minuten und beinhaltet die Dokumentation und Modifizierung von Gruppenstrukturen.



In demselben Unternehmen wird die diesbezügliche Arbeitszeit um 88%, auf 19 Arbeitsstunden reduziert.



*„Die meisten der Aufgaben der IT Domain wiederholen sich. Dank 8MAN und seiner integrierten Wizards können die Aufgaben um bis zu 90% schneller erledigt werden, während die Qualität zur gleichen Zeit verbessert wird.“ erklärt Stefan Büggemann, Chef von Worldwide IT-Operations bei ATOTECH.*

8MAN verbessert dadurch nicht nur die Sicherheit und die Prozesse, sondern erreicht auch die Amortisierung und nachhaltige Einsparung in weniger als zwei Jahren.

## Zusammenfassung

Die von protected-networks.com entwickelte ISEC Lösung 8MAN ermöglicht Unternehmen:

- Eine vollständige Transparenz sämtlicher Zugangsberechtigungen gegenüber unstrukturierten Daten durch einen Klick.
- Verbesserung der Sicherheit und die Einführung des „Need-to-know“-Prinzips bei der Einbindung der relevanten Personen in der Organisation (Dateneigentümern, Abteilungsleitern und Sicherheitsbeauftragten)
- Verbesserung der Effizienz in dem Berechtigungsmanagement. In Anlehnung zur Beschleunigung und Vereinfachung der Einführung und Wartung der komplexen Beschaffung und der Identity-Management-Lösungen.
- Compliance für interne und externe Prüfer: Wer hat welchen Zugang und warum vergeben?

Die 8MAN Lösung unterstützt die verschiedenen Nutzer in ihrer täglichen Arbeit.

**Der IT Administrator** erhält durch wenige Klicks einen Überblick über die Situation der Zugangsberechtigungen und den Beziehungen zwischen den Gruppen des Active Directory. Er kann die Wege der Zugangsberechtigungen modifizieren und verbessern, Standardeinstellungen einführen und jederzeit kontrollieren. Der **IT Helpdesk** kann Zugangsberechtigungen verwalten, wenn sie von den Nutzern per Email, Anruf oder Ticket angefragt werden. Die Nutzer müssen keine Domainadministratoren sein, können 8MAN jedoch durch ihre normalen Nutzerkonten benutzen. Durch die Nutzung von 8MAN werden alle Aktivitäten aufgenommen und können zugleich zurückverfolgt werden.

**Der Dateneigentümer** erhält auf einfache Weise Informationen darüber, wer Zugang zu seinen Daten hat. Er kann dies anerkennen oder ändern. Alles wird vollständig dokumentiert. Die Berichte können zudem digital aufgezeichnet werden.

**Der Sicherheitsbeauftragte** wird immer die Möglichkeit haben, einen vollständigen Überblick darüber zu erlangen, wer Zugang hat, wer ihn vergeben hat und wann er vergeben wurde.

Die Zurückverfolgung in frühere Zeiten unterstützt die rechtliche Verfolgung bei Datendiebstahl oder -verlust.



Die 8MAN Gruppe bietet eine schlüssige und integrierte Lösung für das Berechtigungsmanagement.



### Über protected-networks.com GmbH

protected-networks.com GmbH entwickelt integrierte Lösungen für das Berechtigungsmanagement in die Serverumwelt von Unternehmen in jedem Geschäftsbetrieb. Integriertes Datensicherheitsmanagement ist die betriebene Basiseinstellung von protected-networks.com. Sie bietet Unternehmen eine standardisierte Lösung für die Verwaltung von Zugangsberechtigungen durch aufzeichnen und berichten. Die Lösung **8MAN** ermöglicht die Visualisierung, Verwaltung, Dokumentation und Optimierung von Zugangsrechten die im IT-Umfeld bestehen. **8MAN** erweitert und optimiert nicht nur die Funktionen des Microsoft Service wie Active Directory, Fileservern und Austausch, sondern beinhaltet auch viele andere Serversysteme.



protected-networks.com GmbH

Alt-Moabit 73

10555 Berlin

Tel. 030 / 390 63 45 - 50 | Fax 030 / 390 63 45 - 51

info@protected-networks.com

www.protected-networks.com

