

Guten Tag liebe Leserin, lieber Leser,

vor Ihnen liegt die Erstausgabe von anyWARE kompakt, der Kundenzeitung der anyWARE AG.

Im Zeitalter der Informationsflut durch unterschiedlichste Medien ist es für jeden von uns schwieriger geworden, über solide Detailinformationen zu verfügen. Deshalb starten wir heute mit der gedruckten Version unserer Kundenzeitung, um ausgewählte IT-Themen für Sie begreifbarer zu machen.

Wir berichten in regelmäßigen Abständen über Standardthemen oder informieren Sie zu aktuellen Fragestellungen. Diese Ausgabe beschäftigt sich mit dem Thema „100%ige Sicherheit“.

Über 11 Jahre Business-Erfahrungen bestätigen uns, in unserem Anspruch: 100% zu leisten. Dies zeigt sich sowohl in der Auswahl von verlässlichen Produkten, von bewährten Partnern wie auch beim Einsatz unseres fundiertem Know-hows. Nur so können wir unser Tagesgeschäft erfolgreich bewältigen.

Als Unternehmer haben auch Sie stets die 100% im Blick: Sie wünschen sich 100% Auslastung, 100% Leistung, 100% Erfolg und 100% Sicherheit - gerade für Ihre Firmendaten.

Täglich werden Sie mit diesem Thema konfrontiert - bewusst oder unbewusst. Sei es durch Datenverlust, Spyware oder in Form von Phishing-Mails.

Stellt sich die Frage: Wann machen Sie Ihre IT sicher?

Ihr
Rudolf Braun Michael Steinfartz
Vorstand Vorstand

Inhalt:

Begrüßung

VPN ist DAS „Schlüssel“wort zur Anbindung zukünftiger Standorte, um Sicherheit gewährleisten zu können

Virenabwehr – Die Mainzer Kirche ist up-to-date

Trotz Backup kommt's zu Datenverlust!

Grundlagen zur Datensicherung im Serverbereich

Wie schütze ich mich vor Phishing?

Was sind Antispy-Lösungen?

Termine / Ausblick

Ansprechpartner im Bereich „Sicherheit“ bei anyWARE

Impressum

Firewallmöglichkeit wurde deshalb zusätzlich aktiviert.

Nachdem die Einwahl über die verschlüsselte VPN-Verbindung auf den ISA 2000 erfolgt ist, durchläuft der Datenstrom die weitere Firewall, die bereits vorhandene Watchguard. Damit wurde ein 2-stufiges Sicherheitskonzept mit zwei unabhängigen Firewalls realisiert. Zudem wurde der ISA 2000 in Wiesbaden mit einer zertifikatsbasierten Autorisierung konfiguriert. Die Notebooks der französischen Außendienstmitarbeiter wurden so eingerichtet, dass sie über einen verschlüsselten VPN-Tunnel auf den ISA 2000 hier in Wiesbaden zugreifen können. Die starke Verschlüsselung des VPN-Tunnels wird durch den Einsatz von sicheren Protokollen bei der Internetnutzung (wie z. B. IPSec und L2TP) realisiert. Der Leitungsinhalt ist somit durch die individuelle Verschlüsselung für Fremde nicht angreifbar. Die Daten für Bestellungen werden von nun an sicher direkt vom SQL-Server in Wiesbaden geladen. Die Bestelldaten können durch die Online-Nutzung des transaktionsorientierten Datenbankmanagementsystems zeitlich parallel im System verbucht werden. Die Bestände bleiben dadurch stets aktuell und die Zusammenarbeit zwischen der deutschen Hauptverwaltung und der

(Fortsetzung auf Seite 2)

VPN ist DAS „Schlüssel“wort zur Anbindung zukünftiger Standorte, um Sicherheit gewährleisten zu können - Auch beim Zusammenspiel von Netzwerken

Ein modernes mittelständisches Unternehmen der chemisch-pharmazeutischen Industrie, ansässig in Wiesbaden mit weltweiten Niederlassungen, ist im vergangenen Jahr zunächst mit der Bitte an uns herangetreten, die Außendienstmitarbeiter ihrer französischen Niederlassung an das Wiesbadener Firmennetzwerk sicher und zuverlässig anzubinden. Problematisch war vor allem der Prozess der Bestellungen in der Vergangenheit. Die französischen Außendienstmitarbeiter konnten ihre Bestellungen von unterwegs nur auf aufwändigen, komplizierten Umwegen nach Deutschland schicken. Zukünftig sollten Bestellungen online mithilfe einer Datenbank-Anwendung auf SQL-Basis möglich werden.

Die Überlegungen unsererseits gingen in die Richtung, die gegebene Hardware weiterhin zu nutzen, um kostspieligen Neuananschaffungen möglichst aus dem Weg zu gehen. Die Komponenten des bestehenden

Netzwerkes wurden von uns so kombiniert, dass ausschließlich Dienstleistung und keine neue Hardware notwendig waren. Vorhanden waren bereits ein Microsoft ISA 2000 Server (Microsoft Internet Security and Acceleration Server), eine Watchguard Firebox sowie die SQL- und Exchange-Infrastruktur. Neben der Watchguard Firebox als Firewall gibt es verschiedene andere Anbieter von Firewalls. Wir sind beispielsweise zertifizierter Partner von Ecos für die Produktpalette BB-5000, ein Firewallsystem für individuell anpassbare Kundenwünsche.

Was haben wir gemacht?

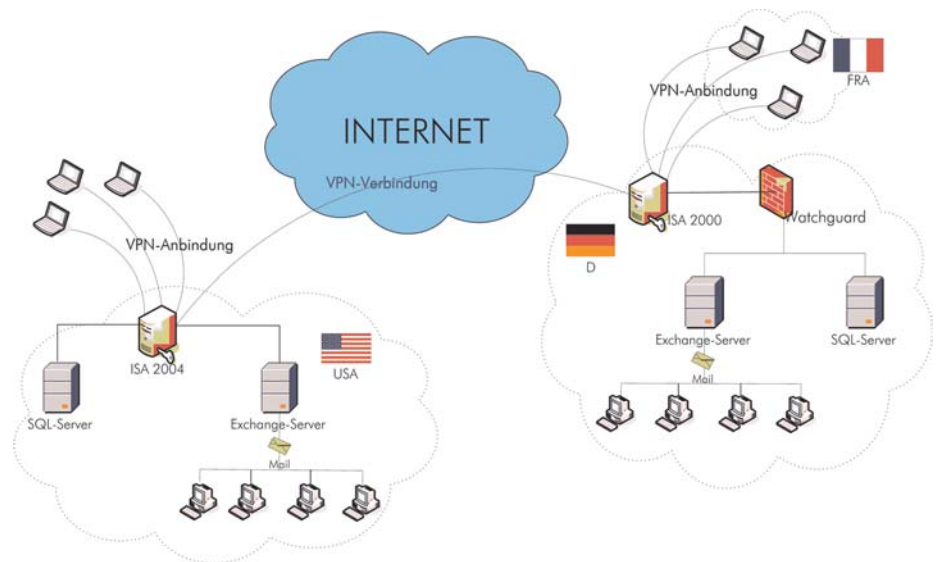
Die Anbindung der Außendienstmitarbeiter sollte zukünftig über eine sichere VPN-Verbindung (Virtual Private Network) auf den ISA 2000 Server erfolgen. Der Microsoft ISA wurde von nun an nicht mehr nur als Proxy-Server eingesetzt, sondern in seinem vollen Leistungsumfang genutzt – die

(Fortsetzung von Seite 1)

französischen Zweigniederlassung basiert endlich auf einem sehr effizienten Netzwerk-zusammenschluss.

Für die Nutzung von VPN-Gateways sind im Allgemeinen sehr teure Lizenzkosten für jeden einzelnen Anwender oder jeden Zugriff fällig. Die Anbindung der mobilen Endgeräte erfolgte hier jedoch nach dem Lizenzierungsmodell des ISA Servers anhand der eingebauten Prozessoren mit dem Grundgedanken, dass mit steigender Nutzerzahl des VPN-Gateways auch die Prozessorleistung ansteigen muss. Diese Form der Abrechnung senkt die Lizenzkosten und ermöglicht eine flexible Skalierbarkeit der VPN-Zugriffe.

Im zweiten Schritt sollte von uns die amerikanische Niederlassung an Deutschland angebunden werden. Bei der Ist-Analyse vor Ort stellte sich leider heraus, dass die Anbindung des internen Netzwerks an das Internet teilweise nicht genügend sicher erfolgte. Das musste schnellstens geändert werden. Der Zugang zum Internet und die Anbindung an Deutschland haben wir ähnlich wie die Anbindung der französischen Außendienstmitarbeiter an das deutsche Netz vorgenommen - der einzige Unter-



schied - hier wurde ein ISA 2004 eingesetzt. Die Kommunikation zwischen dem deutschen und dem amerikanischen Server und der externe Zugriff der Notebooks auf das Netz werden durch VPN-Verbindungen auf den Microsoft ISA 2004 Server ermöglicht und hier verschlüsselt getunnelt. Sichere Verbindungen bei der Verständigung sind somit gewährleistet. Der eMailversand wird

mithilfe eines Exchange-Servers sicher realisiert. Die Bestandsdaten für die Bestellungen befinden sich auch in Amerika auf einer SQL-basierenden Datenbank, die sich ständig mit der Datenbank in Deutschland abgleicht.

Weitere Informationen zum Microsoft ISA sind unter www.microsoft.com/germany/isaserver/default.aspx zu finden.

Virenabwehr – Die Mainzer Kirche ist up-to-date

Die Bedrohung durch Viren hat sich in den letzten Jahren um ca. 300% gesteigert. Die von Viren ausgehenden Gefahren nehmen stetig zu und können im schlimmsten Fall sogar existenzbedrohend für ein Unternehmen werden. Studien von Analysten/Marktbeobachtern wie beispielsweise dem Gartner-Institut belegen dies.

So ist auch eine kirchliche Einrichtung der Region darauf bedacht, sich vor Virenattacken stets aktuell und effektiv schützen zu können. In diesem Zusammenhang wurde in einem Roll-Out im März 2005 das komplette Netzwerk bezüglich der Virenschutzsoftware von uns aktualisiert.

Was bedeutet das?

Das Netzwerk der Einrichtung besteht aus ca. 15 Servern und ca. 700 Anwender-PCs, die in mehreren Subnetzen durch ein VLAN betrieben werden. Aufgrund der Vielzahl an Netzwerkteilnehmern war es dem Administrator wichtig, die Virenschutzlösung zentral zu steuern, um nicht jeden PC separat verwalten zu müssen.

Dafür aktualisierten wir das bereits vorhandene McAfee-Werkzeug mit der Verwaltungssoftware „ePolicy Orchestrator“ auf Version 3.5. Die veraltete Fassung wurde dafür komplett deinstalliert und die neue Version installiert und konfiguriert. Im nächsten Schritt wurde die alte Antivirensoftware auf allen Computern im Netzwerk komfortabel (zentral) durch die neu eingeführte Management-Konsole aktualisiert. Im

Anschluss wurde der Administrator des Systems entsprechend geschult und auf die neuen Features hingewiesen. Zeitgleich wurden sämtliche Schritte in einer Dokumentation festgehalten. Dieses Roll-Out wurde in nur zwei Tagen komplett abgewickelt.

Glossar:

VPN-Verbindung:

VPN ist die Abkürzung für „virtual private network“ und beschreibt den Transport von Daten über einen (geschützten/verschlüsselten) Kanal des öffentlichen Netzes wie des Internets. So ist es möglich, Mitarbeitern den Zugriff auf das Unternehmensnetzwerk gesichert von außen zu gewährleisten. Auch die Verbindung zwischen zwei entfernten Netzwerken (wie bei dem o.g. Projekt) ist mithilfe von „VPN-Gateways“ möglich.

Die Sicherheit der Verbindungen wird durch geheime Passwörter, Verschlüsselungen, Prüfsummen oder Zertifikate gewährleistet.

Zertifikatsbasierte Autorisierung:

Das Sicherheitskriterium der Identifizierung des Nutzers wird gewährleistet, indem die digitale Identitätsbestätigung mit einem Zertifikat vorgenommen wird.

Vorteile des McAfee ePolicy Orchestrator:

- Skalierbarkeit auf Netzwerke bis zu einer Größe von 250.000 Rechnersystemen
- Zentrale und somit komfortable Installation, Deinstallation und Konfiguration von Virenschutz- und Antispylösungen
- Die zentrale Verwaltung wird durch nur eine Konsole erleichtert und Kosten werden minimiert
- Zentrale und komfortable Konfiguration/Verwaltung von Sicherheitseinstellungen und Updates
- Multiple Domänen bei größeren Unternehmen können verwaltet werden
- Unternehmensweite Durchsetzung von Sicherheitsvorgaben
- Sicherheitslücken durch unberechtigte PCs können durch frühzeitige Warnmeldungen ermittelt und beseitigt werden
- Der „system compliance profiler“ prüft automatisiert alle Computer im Netzwerk auf das Fehlen von wichtigen Sicherheitspatches und erleichtert so dem Administrator das Auffinden von sicherheitskritischen Computern
- Individuelle Statistiken visualisieren die Systemüberwachung. Umfangreiche Auswertungen/Reports können frei generiert werden und zur stetigen Dokumentation des Sicherheitsstandes verwendet werden
- Die Verwaltung von Dritthersteller-Produkten ist möglich

Alle Netzwerkteilnehmer können nun zentral verwaltet werden. Die Aktualität jedes Virenschanners wird zentral gesteuert und ein Schädlingsbefall kann minimiert werden.

Trotz Backup kommt's zu Datenverlust!

Seit Jahren beauftragt der Geschäftsführer eines kleinen, fast mittelständischen Unternehmens, regelmäßig einen ihm bekannten externen EDV-Spezialisten damit, sich um die Installation und Konfiguration aller Firmen-PCs sowie den reibungslosen Betrieb des Unternehmensnetzwerks zu kümmern.

Dieses Netzwerk verfügt über einen MS Windows 2000-Server und 10 PCs; einige davon sind Außendienst-Notebooks. Das Unternehmen nutzt zur täglichen Auftragsbearbeitung eine gängige Branchensoftware. Auf dem Server werden daher alle relevanten Kundendaten regelmäßig gespeichert, die zur täglichen Abwicklung

benötigt werden. Der Server ist mit einem Bandlaufwerk ausgestattet, mit dem in regelmäßigen Abständen eine Sicherung auf Band (Backup) gespeichert wird. Diese Sicherungsbänder werden in einem verschlossenen Schrank im Büro des EDV-Spezialisten gelagert.

Als eines Tages der Netzwerkserver des Mittelständlers aufgrund eines Hardwarefehlers ausfällt, sollen die Daten vom letzten Backup-Band wieder eingespielt werden. Dabei stellt sich aber heraus, dass das Bandlaufwerk des Serversystems offensichtlich bereits längere Zeit defekt war, denn auf den letzten fünf Backup-Bändern waren

keine rücksicherungsfähigen Daten geschrieben worden. Die einzige noch funktionstüchtige Sicherungskopie war mehr als fünf Jahre alt und damit alle relevanten Unternehmensdaten der letzten Jahre verloren. Die Rechner wurden darauf hin komplett neu installiert.

Fazit: Selbst wenn man regelmäßig ein Backup von den zu sichernden Daten erstellt, bedeutet dies noch lang nicht, dass im Ernstfall das Rücksichern der gewünschten Daten erfolgreich umgesetzt werden kann. Sinnvoll ist es, von Zeit zu Zeit eine teilweise Rücksicherung von Backups durchzuführen, um die Funktionstüchtigkeit zu überprüfen.

Grundlagen zur Datensicherung im Serverbereich

Im Nachfolgenden haben wir Ihnen ein paar grundsätzliche Informationen rund um das Thema „Datensicherung“ zusammengestellt. Angefangen bei der Fragestellung „Welche Daten sollen gesichert werden?“, über die Methoden der Datensicherung, die Lagerbedingungen, der Datensicherungs-Software, des Aufstellens eines Notfallplans bis hin zu Datensicherungs-Strategien.

Welche Daten sollen gesichert werden?

Im Rahmen der Datensicherung werden vorsorglich alle Daten, die Sie für einen reibungslosen Betrieb Ihres Unternehmens benötigen, regelmäßig auf ein externes Datenmedium gesichert, das Sie anschließend sicher verwahren sollten.

Die drei praktikabelsten Methoden der Datensicherung sind:

- Volle Datensicherung
- Inkrementelle Datensicherung
- Differentielle Datensicherung

Wie die Bezeichnung schon sagt, werden im Rahmen einer **vollen Datensicherung** sämtliche zu sichernde Dateien auf einem Datenträger/-medium gespeichert.

Vorteile volle Datensicherung

- Alle Daten liegen komplett vor
- Sie müssen bei der Wiederherstellung / Rücksicherung nicht lange „suchen“

Nachteile volle Datensicherung

- Je nach Datenvolumen ist die Datensicherung zeitaufwendig
- Sie benötigen viel Platz auf dem Speichermedium

Als Voraussetzung für die **inkrementelle Datensicherung** wird zunächst eine Volldatensicherung durchgeführt. Danach werden nur noch die Dateien gesichert, die sich seit der letzten Volldatensicherung bzw. inkrementellen Sicherung verändert haben.

Vorteile inkrementelle Datensicherung

- Sie sparen Speicherplatz
- Sie benötigen weniger Zeit für die Datensicherung

Nachteile inkrementelle Datensicherung

- Die Datenwiederherstellung benötigt mehr Zeit, da immer erst die Volldatensicherung und anschließend alle erstellten inkrementellen Backups nacheinander rückgesichert werden müssen
- Falls eine inkrementelle Sicherung defekt ist, kann unter Umständen der volle Datenbestand nicht mehr wieder hergestellt werden

Um eine **differentielle Datensicherung** durchzuführen, müssen Sie zunächst einmal eine Vollsicherung durchführen. Danach werden bei der differentiellen Datensicherung alle Daten gesichert, die sich seit der letzten Volldatensicherung verändert haben.

Vorteile differentielle Datensicherung

- Die Wiederherstellung der Dateien ist im Bedarfsfall unkomplizierter und schneller
- Sie benötigen nur die letzte Vollsicherung und die letzte differentielle Datensicherung

Nachteile differentielle Datensicherung

- Sie benötigen mehr Zeit - im Vergleich zu der inkrementellen Datensicherung

Unterschiede gibt es auch bei den **Speichermedien** für die Datensicherung.

Welches Speichermedium genutzt wird, hängt u. a. davon ab, wie groß die Datenmenge ist, die Sie sichern wollen. Die Kapazität des in Frage kommenden externen Speichermediums ist ein weiterer entscheidender Faktor für die Auswahl.

Die Speichermedien, deren Kapazität und die Geschwindigkeit im Überblick finden Sie in der Tabelle auf Seite 4.

Hinweise zu den **Lagerbedingungen** für Speichermedien:

Die Speichermedien sollten trocken und kühl (nicht über Zimmertemperatur) gelagert werden; dabei ist darauf zu achten, dass sie keinem direkten Sonnenlicht ausgesetzt sind.

Im Zusammenhang mit den Lagerbedingungen empfiehlt es sich, einen sinnvollen **Lagerort** zu finden, der auf jeden Fall getrennt von Ihren PCs bzw. Ihrem Netzwerk sein sollte.

Wie in dem o. g. Beispiel beschrieben, ist es empfehlenswert, die Datenmedien nicht am Firmenort selbst zu lagern, sondern sie dezentral aufzubewahren. Dies kann bei Ihrem IT-Dienstleister sein oder einem Bankschließfach. Der Aufbewahrungsort der Speichermedien sollte gemäß den Lagerbedingungen zusätzlich gegen äußere Einflüsse, wie Feuer, Wasser und Diebstahl gesichert sein.

Für die professionelle Datensicherung bieten unterschiedliche Hersteller spezielle **Datensicherungs-Software** für die gängigsten Betriebssysteme an; so z. B. Symantec Veritas die Software Backup Exec für Windows Server.

Datensicherungs-Strategie

Es empfiehlt sich auch in Ihrem Unternehmen die Datensicherung anhand einer festgelegten Prozedur durchzuführen:

- Wie die Datensicherung zu erfolgen hat
- Wer für die Datensicherung verantwortlich ist
- Wann die Datensicherung durchgeführt werden soll
- Welche Daten genau gesichert werden sollen
- Welches Speichermedium zu verwenden

(Fortsetzung auf Seite 4)

(Fortsetzung von Seite 3)

Laufwerkstyp	Kapazität (unkomprimiert / komprimiert)	Geschwindigkeit (komprimiert)
DDS4	20/40	max. 100MB/Min
DDS5	36/72	max. 100MB/Min
DLT160	80/160	max. 270MB/Min
LTO1	100/200	max. 500MB/Min
LTO2	200/400	max. 1000MB/Min
LTO3	400/800	max. 2600MB/Min

ist und in welchen Intervallen es ersetzt werden soll

- Welche Backupmethode zur Datensicherung eingesetzt wird (Volldatensicherung, inkrementelle oder differenzielle Datensicherung)

cherung)

- Wo und wie die Datensicherungsmedien aufzubewahren sind
- Wie lange die Datensicherungsmedien archiviert werden

- Wann und wie die Datensicherungsmedien auf ihre Wiederherstellbarkeit überprüft werden

Unterstützende innerbetriebliche Maßnahmen

Wenn Sie sich nun gezielt mit dem Thema „Datensicherung“ auseinandersetzen, so gehören folgende begleitende Maßnahmen dazu:

- Sensibilisierung der Unternehmensleitung, Administratoren und Mitarbeiter (Anwender)
- Schulungen der Mitarbeiter
- Regelmäßige Wartung der Hardware-Komponenten
- Aktualisierung der relevanten Datensicherungs-Software

Wie schütze ich mich vor Phishing?

Als Phishing bezeichnet man das Angeln nach Passwörtern. Beim Phishing gibt es mehrere Varianten, an die Passwörter zu gelangen. Zum einen werden dem Anwender eMails mit falschen Webadressen geschickt. In diesen eMails werden die Anwender aufgefordert, den Link zu nutzen, um beispielsweise ihre Benutzerdaten des Onlinekontos zu aktualisieren. Dieser Aufforderung bitte NIEMALS nachkommen!!! Man wird auf falsche Webseiten geleitet, wo Benutzereingaben protokolliert werden. So gelangen die Angreifer an Ihre Benutzerdaten – sehr fatal. Zum anderen ist die

Gefahr eines Befalls durch Keylogger/Spyware ohne Antispy-Lösungen sehr hoch. Als Spyware bezeichnet man Software, die Informationen (z. B. das Surfverhalten) vom befallenen Computer protokolliert und aufzeichnet. Keylogger registrieren die Tastatureingaben am eigenen Rechner ungehindert und senden diese an den Angreifer unbemerkt weiter.

Durch eine geeignete Verschlüsselung der Eingabedaten, sensiblen Umgang mit Webadressen/Passwörtern sowie einer geeigneten Antispy-Lösung kann Phishing weitestgehend entgegengewirkt werden.

Termine:

07. Juni 2006, IT_Kom
 Fachmesse und Fachtagung
 Phönix-Halle Mainz
 Besuchen Sie anyWARE am Stand 40!
www.it-kom-mainz.de

Ausblick:

Die nächste Ausgabe von anyWARE kompakt beschäftigt sich schwerpunktmäßig mit dem Microsoft Exchange Server.

Was sind Antispy-Lösungen?

Als Folge unerkannter Spyware oder anderer potenziell unerwünschter Programme kann es u. a. zur Weitergabe von Informationen, Rechner- und Netzwerkstörungen, langsamerem Internetzugang, verminderter

Produktivität und vermehrten Pop-Up-Anzeigen kommen. Spezielle Antispy-Lösungen wirken dem entgegen und helfen unerwünschte Programme entweder vorbeugend zu blockieren oder schnell zu er-

kennen sowie sicher zu entfernen, noch bevor sie ihre schädlichen Aktivitäten entfalten können.

Besitzer einer McAfee Enterprise Antivirenschutzlösung können eine Antispy-Lösung günstig in den bestehenden Virenschutz integrieren.

Ansprechpartner im Bereich „Sicherheit“ bei anyWARE:

- Herr Daniel Capilla für Virenschutzlösungen
- Herr Michael Lorio für sichere Netzwerkanbindungen und sicheren eMailverkehr
- Herr Marcel Kösling für Backupsysteme

Neben vielen anderen Mitarbeitern der anyWARE AG sind auch diese drei Hauptansprechpartner aus dem Bereich „Sicherheit“ MCSE-zertifiziert.

Was bedeutet das für Sie als Kunde?

Die Mitarbeiter bestätigen durch ihre umfangreichen Zertifizierungen fundierte Kenntnisse in den Bereichen „Planung“, „Implementierung“ und „Wartung“ von Microsoft Windows basierenden Client/



Server Netzwerkinfrastrukturen.

Herr Michael Lorio ist zusätzlich **Ecos Certified Trainer (ECT)**, dies entspricht derzeit der höchsten Zertifizierungsstufe bei Ecos für die Firewall BB-5000. Weiterhin hat Herr Daniel Capilla eine Zusatzzertifizierung als **MCSE:Security** und beweist seine Kenntnisse zu den Sicherheitsanforderungen von Serversystemen mit dieser erfolgreich bestandenen Prüfung.

Impressum:

Herausgeber:
 anyWARE AG
 Holzstr. 32
 55116 Mainz
 Tel. +49 (6131) 965 96 50
 Fax. +49 (6131) 965 96 55
 eMail: feedback@anyWARE.AG
 Web: www.anyWARE.AG

Vorstand:
 Rudolf Braun (ViSdP)
 Michael Steinfartz

Redaktion:
 Jana Jabusch
 Barbara Külps (MarComInN)

Auflage:
 3000 Exemplare