

CONNECTIONS

NETZWERKLÖSUNGEN FÜR EUROPA • DEN NAHEN OSTEN • AFRIKA

Aviapartner

Vertrag mit AT&T um weitere
fünf Jahre verlängert

Seite 8



Cisco

Die fünf wesentlichen Elemente
der Netzwerksicherheit

Seite 10



Wie Sie Ihr Netzwerk vor Angriffen schützen



Inklusive:

 Ein Überblick über die

AT&T Security Services

Aufruf an alle Geschäftsreisenden

Bestellen Sie noch heute Ihre AT&T Corporate Calling Card:

- Sofortige Einsparungen bei Anrufen
- Bequeme Abrechnung
- Weltweiter Zugang
- Kostenverwaltung online
- Hochwertiger Kundendienst

Rufen Sie jetzt an:

+44 (0) 191 224 6800



Oder registrieren Sie sich online unter
www.att.com/business_traveler/calling_card/#signup

Nº

5

2002



Die drei wichtigsten Herausforderungen für Ihre Geschäftsabläufe: **Sicherheit, Sicherheit und nochmals Sicherheit**



In der heutigen Geschäftswelt müssen wir uns mehr denn je auf die Bedeutung aller Sicherheitsaspekte konzentrieren: auf die wirtschaftliche Sicherheit ebenso wie auf die – in Folge des 11. September wieder deutlich ins allgemeine Bewusstsein getretene – physische Sicherheit, als auch die finanzielle Sicherheit von Geschäftspartnern und Lieferanten.

Diese Ausgabe von Connections spiegelt diese Überlegungen wider. Für uns ist es – gerade in diesen unsicheren Zeiten – sehr wichtig, mit unseren Kunden in Europa zusammenzuarbeiten und gemeinsam den Weg der Stabilität und Stärke weiterzugehen. Wir alle sind stolz auf den guten Ruf und die Beständigkeit von AT&T in einer Zeit, wo sogar einige der größten Firmen aus der Branche an ihren zu ehrgeizigen Wachstumsplänen und mangelhafter Verwaltung scheitern.

In der vorliegenden Ausgabe erfahren Sie mehr über unsere neusten Aktivitäten, durch die wir den Anforderungen unserer Kunden in punkto Sicherheit in Zukunft noch besser gerecht werden können – wie zum Beispiel die Einführung einer Reihe verwalteter Sicherheitslösungen für Geschäftskunden in EMEA.

Netzwerke sind heute das neuralgische Zentrum fast aller unserer Geschäftsprozesse. Umso wichtiger ist es daher, dass diese Sicherheitslösungen auf mehreren Ebenen wirksam vor Risiken wie Hackern, Naturkatastrophen und durch menschliche Fehler ausgelöste Schäden schützen. Wir bieten Ihnen integrierte Services, mit denen Sie zunächst das Risiko einschätzen und dann die zum Schutz des Unternehmens erforderlichen Sicherheitslösungen planen, verwalten und einsetzen können.

Lesen Sie außerdem, wie AT&T selbst auf die Probe gestellt wurde, als wir auf die unvorhergesehenen Ereignisse der Flutkatastrophe in Mitteleuropa und die damit verbundenen Schäden reagieren mussten.

Unser eigener Katastrophenplan musste in Prag und Dresden in die Tat umgesetzt werden, als das Hochwasser unaufhaltsam anstieg und unser Netzwerk sowie die Kunden in der Region bedrohte. Bei dieser Gelegenheit möchte ich unser Team ausdrücklich loben, das die Krise schnell und effizient bewältigt, den Schaden für die Kunden gering gehalten und den Service mit minimaler Unterbrechung wiederhergestellt hat.

Neben unseren neuen Security Services stellen wir Ihnen unsere Professional Services vor: Während manche Mitbewerber bemüht sind im professionellen Dienstleistungssektor Fuß zu fassen, genießen wir den großen Vorteil, bereits eines der etabliertesten Outsourcing- und Consulting-Unternehmen zu sein – und dafür haben wir mit AT&T Solutions in den letzten zehn Jahren hart gearbeitet.

Mit den zunehmend anspruchsvolleren Bedürfnissen der Kunden bieten wir unsere Services nicht mehr ausschließlich für die größten Unternehmen, sondern für ein immer breiteres Spektrum unterschiedlichster Kundengruppen an. Dabei müssen wir nicht extra eine neue Infrastruktur zur Unterstützung dieser Services aufbauen, da wir bereits über das notwendige Know-how, die erforderlichen Ressourcen und die entsprechende Reichweite verfügen.

All unsere Services werden von einem der fortschrittlichsten globalen Netzwerke der Welt gestützt – ein Netzwerk, in das wir weiterhin investieren und das ständig erweitert wird. In den letzten Ausgaben von Connections konnten Sie von den aggressiven Rollout-Plänen der neusten MPLS-Technologie in der Region lesen. In dieser Ausgabe schildern wir Ihnen, wie die Realisierung noch beschleunigt werden konnte. In der „Last Minute“-Beilage erfahren Sie außerdem, wie wir die Anzahl der Einwahlknoten für unsere Remote Access Internet Dial Services auf über 4.200 in mehr als 140 Ländern verdoppelt haben.

Ich denke, der beste Beweis für unsere Kompetenz sind letztendlich Sie – auch in dieser Ausgabe lassen wir unsere Kunden für uns sprechen. Große europäische Firmen wie BASF, Carraro, Wolford und Aviapartner schildern ihre praktischen Erfahrungen mit AT&T, und es heißt ja bekanntlich, Taten sagen mehr als Worte.

Mit den besten Grüßen

Jon Stretch
Vice President
AT&T Business, EMEA

Setzen Sie Ihre Sicherheit nicht aufs Spiel

Nicht nur Unternehmen wissen, wie wertvoll Informationen sind. Leider ist das auch Hackern und anderen Kriminellen im Internet bekannt. Die von ihnen verursachten Sicherheitsverletzungen können Verluste bei Produktivität, Markenimage und Vertrauen zur Folge haben, was wiederum zu finanziellen Schäden führt. Die Risiken, denen Unternehmen heutzutage ausgesetzt sind, stehen daher im Mittelpunkt des Interesses von Industrie und Medien.

Die Umfrage „2002 Computer Crime and Security Survey“, durchgeführt von CSI/FBI, macht das besonders deutlich. Zum Beispiel haben 90% der Befragten (in erster Linie große Unternehmen und Behörden) in den letzten zwölf Monaten Sicherheitsverletzungen ihres Computersystems festgestellt und 80% bestätigten daraus resultierende finanzielle Einbußen. Bereits im fünften Jahr in Folge geben immer mehr Befragte (74%) ihre Internet-Verbindung als häufigste Angriffsstelle an.

Bedrohungen oder tatsächliche Verletzungen der Sicherheit werden weiter zunehmen, da Unternehmen aller Größenordnungen immer mehr Geschäftsprozesse online abwickeln und Verbindungen zu Internet, Intranet und auch Remote Access immer häufiger nutzen. Und mit der zunehmenden Komplexität von E-Business-Modellen steigt auch die Komplexität der erforderlichen Sicherheitslösungen.

Mit Technik allein kann man jedoch Internet-Angriffe nicht verhindern. Sicherheitsverfahren müssen fortwährend neu bewertet und angepasst werden – ein langwieriger Prozess.



Gleichzeitig müssen Unternehmen für ein neues Sicherheitssystem viel investieren bzw. hohe Wartungskosten für vorhandene Lösungen kalkulieren.

Outsourcing des Security Managements

Angesichts dieser Situation wenden sich viele Firmen an externe Anbieter, um die Sicherheit ihrer EDV zu erhöhen und gleichzeitig die Kosten einzudämmen. Das gilt besonders für Unternehmen, denen intern das nötige technische Fachwissen fehlt, sowie für Organisationen, bei denen Sicherheit nicht in den Hauptkompe-

tenzbereich fällt. Aus der Zusammenarbeit mit externen Anbietern ergeben sich aber noch andere Vorteile, wie z.B. die Tatsache, dass diese mit den neuesten Sicherheitstechnologien und gesetzlichen Regelungen vertraut sind.

Sie sind auch für jene Unternehmen hilfreich, deren wachsendes Serviceangebot die Kapazitäten der internen Fachkräfte überschreitet. In diesem Fall können die externen Anbieter Tools zur Verfügung stellen, die den Firmen die Kontrolle über ihre gesamte Sicherheitsinfrastruktur ermöglicht.

Die Vorteile liegen auf der Hand

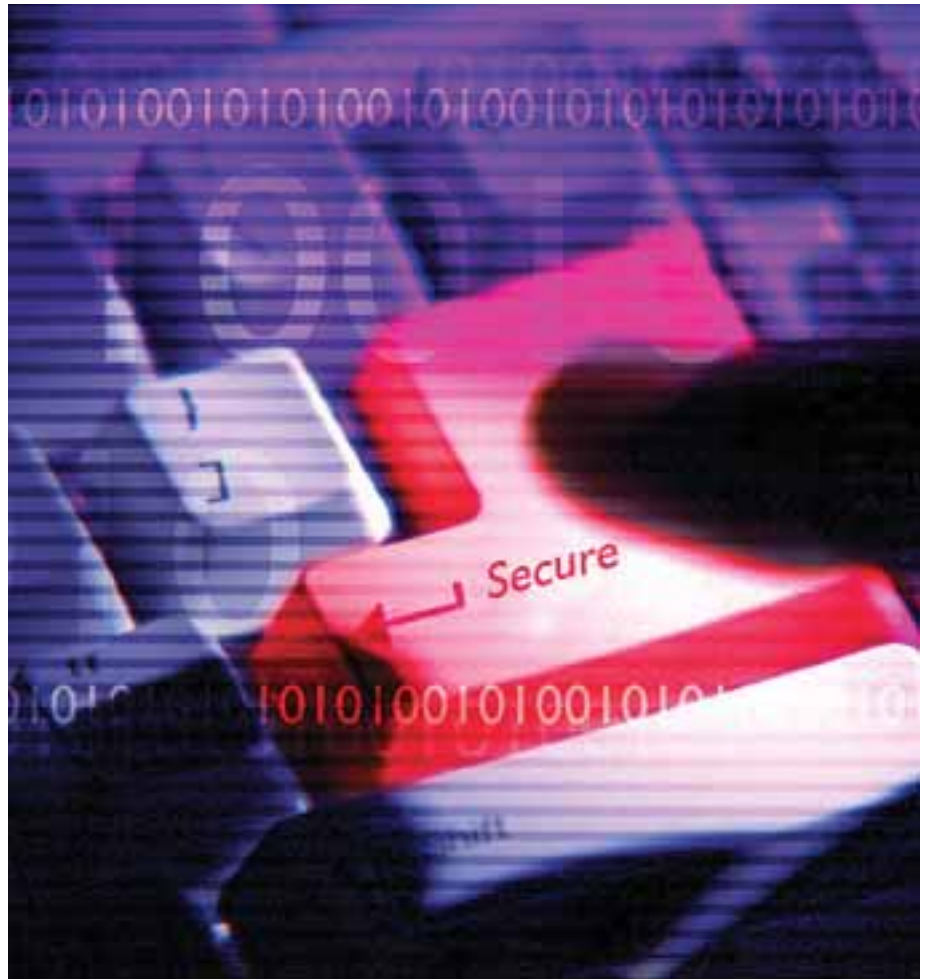
Eine verwaltete Sicherheitslösung kostet oft bedeutend weniger als die Beschäftigung interner Mitarbeiter, da sich Unternehmen die Beschaffung von Informationen und Fachwissen zu den neusten Technologien ersparen können.

Bei der Nutzung verwalteter Services von einem externen Anbieter werden außerdem Fehler bei der Konfiguration reduziert, die unter Umständen zu Sicherheitslücken im Netzwerk führen können. Des Weiteren profitieren Sie von seiner Erfahrung in Bezug auf Angriffe und Bedrohungen, die täglich analysiert werden.

Serviceanbieter können Lösungen mit Hilfe ihrer bewährten Abläufe außerdem schneller einrichten als die meisten Unternehmen. Natürlich profitieren Sie als Kunde auch von den erfahrenen Experten. Indem Sie wiederkehrende Überwachungsaufgaben extern durchführen lassen, können Sie schließlich Ihre internen Ressourcen auf Ihr Haupttätigkeitsgebiet konzentrieren.

Die Vorzüge von AT&T

AT&T arbeitet eng mit führenden Technologieanbietern wie Check Point, Nokia, Sun und Cisco zusammen und bietet eine umfangreiche Palette vollständig verwalteter Security Services, die Installation, Konfiguration, Überwachung und Verwaltung des Equipments umfassen – und das alles aus einer Hand. Es handelt sich dabei um einen End-to-End Service, bei dem es für Sie in allen Sicherheitsangelegenheiten nur eine Kontaktperson gibt – das spart Zeit und den lästigen Aufwand im Umgang mit mehreren Herstellern. Darüber hinaus sind natürlich die langjährige Erfahrung und das Fachwissen von AT&T im Bereich Security Management von entscheidendem Vorteil.



Kundendienst und technischer Support sind feste Bestandteile aller Managed IP Security Services von AT&T, die Ihnen jederzeit zur Verfügung stehen. Neben der Überwachung und Wartung von Netzwerken beraten Sie unsere erfahrenen Sicherheitsexperten im AT&T Security Network Operations Center jeden Tag rund um die Uhr.

Weitere Informationen zu den AT&T Security Services finden Sie unter:
www.att.com/emea/deutsch/services/security.html

Was ist IPSec?

IPSec (Internet Protocol Security) ist ein technischer Standard, der auf die relativ niedrigen Sicherheitslevels von Datenpaketen zugeschnitten ist, die per Internet Protocol (IP) über das Internet versendet werden. Die Sicherheitsmängel traten in erster Linie auf, weil das Internet ursprünglich nicht als öffentliches Netzwerk konzipiert wurde; die Sicherheit bei der Übertragung der Daten über das Netz war daher gegenüber der Sicherheit an den Endpunkten der Kommunikation zweitrangig. Infolgedessen wurden Datenübertragungen über das Internet zwischen Ausgangs- und Zielort leider anfällig für Störungen.

Beim so genannten „Spoofing“ werden Datenpakete abgefangen und durch falsche ersetzt,

wodurch ein unbefugter Benutzer Zugang zum Netzwerk erhalten kann. Mit IPSec werden Authentifizierungs- und Verschlüsselungsoptionen auf die einzelnen Datenpakete, nicht auf die gesamte Verbindung angewendet, wodurch einige dieser Fehlerquellen ausgeräumt werden können. Das Versehen der Datenpakete mit einem Authentication Header (AH) erhöht die Sicherheit, da die Identität des Absenders überprüft und damit die Wahrscheinlichkeit des Spoofings verringert wird. IPSec ermöglicht die Verschlüsselung einzelner Datenpakete und erhöht die Anzahl der Verschlüsselungsoptionen für einen Kommunikationskanal, so dass Hacker eine sichere Kommunikationskette nicht durch einfaches Knacken eines einzelnen Verschlüsselungscodes entziffern können.

Die Herausforderungen des Security Managements

- *Erkennung von Fehlalarmen*
- *Situationsvergleiche zur Vorhersage von Angriffen*
- *Effektive Gegenmaßnahmen*
- *24x7 Monitoring*
- *Management mehrerer Notfälle*
- *Aktualisierung der Intrusion Detection Datenbank*
- *Management globaler Katastrophen-Szenarien*

EINE WICHTIGE ADRESSE

www.eexposecurity.com

e expo SECURITY

Besuchen Sie den Stand von AT&T und **informieren** Sie sich über unser **Sicherheitsangebot**

e expo SECURITY ist völlig neuartig: eine virtuelle Ausstellung und e-Learning-Konferenz, die sich e-Sicherheitslösungen widmet und viele der führenden Technologie- und Serviceanbieter aus aller Welt zusammenbringt.

e expo SECURITY ist DIE Wissensquelle für „e-bewusste“ Führungskräfte. Unabhängig von Ihrem Tätigkeitsbereich – Management, Technologie, Informatik, Finanzen – ist auch für Sie sicher etwas Interessantes dabei.

Mit e expo SECURITY müssen Sie nicht zu einem Veranstaltungsort reisen, Zeit und Kosten aufwenden und Unannehmlichkeiten auf sich nehmen. Stattdessen werden Ihnen Fachwissen, Lösungen und Interaktionsmöglichkeiten geboten – egal wo Sie sich aufhalten, rund um die Uhr.



Überblick über die **AT&T** Security Services

Jetzt erhältlich in EMEA:

Network Vulnerability Assessment

Dieser Service umfasst Sicherheitsbewertungen und Untersuchungen des Netzwerks, um Schwachstellen im Netzwerk, im Betriebssystem oder in Anwendungen von mit dem Internet verbundenen Systemen aufzudecken. Eine erweiterte Form dieses Services ist der versuchte externe Angriff, bei dem AT&T Schwachstellen in der Netzwerksicherheit eines Kunden sucht und auswertet.

Managed Firewall

Firewalls schützen interne und externe Netzwerkgrenzen, indem die Arten von Netzwerkprotokollen und -verkehr definiert werden, die diese Grenzen überschreiten dürfen. AT&T richtet Firewalls an Kundenstandorten ein und verwaltet sie über das eigene Netzwerk.

VPN Services

AT&T bietet VPN-Lösungen zur Sicherung der Internet-Kommunikation eines Kunden. Verwaltete Tunneling- und Verschlüsselungstechnologien unter Verwendung des IPSec-Protokolls gewährleisten dabei erhöhte Internet-Sicherheit und Datenschutz. Einige VPN-Services unterstützen auch 3DES-Sicherheitsalgorithmen und Hardware-Verschlüsselung. Service Level Agreements (SLAs) und VPN Tunnel Measurement-Reports garantieren außerdem die Performance des Netzwerks für den AT&T-Teil des Internet.

Professional Services

Im Rahmen von AT&T Security Consulting können die Kunden aus einer ganzen Reihe von Services und Komponenten für ihre Sicherheitsanforderungen wählen, wie z.B. Entwicklung von Sicherheitsrichtlinien und -plänen, Firewall-Analyse, Auswertung von Sicherheitsschwachstellen und Erkennung systemfremder Modems.

Weitere Informationen zu den AT&T Security Consulting Services finden Sie in der „Last Minute“- Beilage dieser Ausgabe von Connections.

Demnächst in EMEA:

Managed Authentication

Dazu gehört die Verwaltung der Prozesse und Technologien zur Überprüfung der Identität eines Benutzers, der versucht, Zugriff auf das System oder auf Anwendungen zu erhalten. Die Managed Authentication umfasst oftmals zwei Stufen und erfordert neben dem Passwort häufig eine weitere Autorisierung, wie beispielsweise den Besitz eines Token/einer Smart Card oder die Übereinstimmung von biometrischen Daten.

Managed Intrusion Detection Services (MIDS)

Hierbei geht es um die Erkennung von unberechtigten Zugriffsversuchen auf Netzwerke, Systeme, Services, Anwendungen oder Daten. ID-Systeme basieren auf Netzwerk- und Hostüberwachungen und vergleichen oft den überwachten Verkehr oder Aktivitäten mit bekannten Angriffsprofilen.

Eine langjährige **Beziehung** mit einem der **führenden** Industriekonzerne Italiens

Der Carraro-Konzern konstruiert, produziert und vertreibt Automobilsysteme für Traktoren, Baugeräte, Industrie-Gabelstapler, leichte Nutzfahrzeuge und Autos. Über 2.100 Arbeitnehmer sind in zehn Fertigungswerken des Unternehmens in Italien und im Ausland beschäftigt. Die Fabriken befinden sich vor allem in Nordost-Italien, einer Gegend, die jahrelang zu den fortschrittlichsten und aktivsten Industriezentren Europas gehörte. Weitere Werke liegen in anderen Teilen Europas, den USA, Lateinamerika und Asien.

Achsen und Getriebe sind der Hauptgeschäftsbereich des Konzerns, wobei auch die Produktion von VCPs für Autos, Kupplungen, Getriebe und andere mechanische Komponenten zur Produktpalette des Unternehmens gehören. Führende Autohersteller bevorzugen die Produkte von Carraro und 82,3 % des Konzernumsatzes werden heute in Übersee erwirtschaftet.

Anpassung an das Unternehmenswachstum

Carraro ist seit über zehn Jahren Kunde von IBM/AT&T und hat in dieser Zeit seine Geschäftsaktivitäten, seinen Umsatz und seine globale Reichweite erheblich gesteigert. Gleichzeitig ist auch das Angebot von AT&T zu einer umfangreichen Service-Palette angewachsen.

AT&T migriert zum Beispiel die zehn nationalen und internationalen Werke, die mit dem Hauptsitz in Campodarsego in Verbindung stehen, von Managed Data Network Services (MDNS) auf Enhanced Virtual Private Network (EVPN). Dieser vollständig verwaltete,

weltweit einheitliche VPN Service kombiniert die Flexibilität von Any-to-Any-Verbindungen mit der Zuverlässigkeit, Qualität und Sicherheit eines Multi-Protocol Label Switching (MPLS)-basierten, IP-fähigen Netzwerks.

AT&T hat außerdem TCP/IP Dial Services in Dual Access Mode eingerichtet, damit zum Beispiel die Manager, Außendienstmitarbeiter und Techniker einfachen Zugang zum Heimatstandort und den Niederlassungen in aller Welt haben. Das ist eine Zusatzoption zu den Global Managed Internet Services (GMIS) für dedizierte und zuverlässige High Speed Internet-Verbindungen.

Erfolg führt zu Erfolg

Im Laufe der Jahre ist die Beziehung zwischen Carraro und AT&T immer stärker geworden. „Ich kann versichern, dass Carraro ein zufriedener Kunde ist, dem wir einen wirklich weltweiten Global Network Outsourcing Service bieten konnten und mit dem wir eine enge Geschäftsbeziehung pflegen, die auf deut-



„Wir sind immer auf der Suche nach neuen Möglichkeiten, die Entwicklungen in der Technologie zu nutzen – und AT&T hilft uns dabei.“

Eugenio Nalin, IT Manager von Carraro

lichen Vorteilen basiert,“ so Gastone Tempesta, Client Solution Executive von AT&T in Padua.

„Ich bin mit der Entwicklung dieser Beziehung sehr zufrieden,“ fügt Eugenio Nalin, IT Manager von Carraro, hinzu. „Wir sind immer auf der Suche nach neuen Möglichkeiten, die Entwicklungen in der Technologie zu nutzen – und AT&T hilft uns dabei. Ich muss mich nicht extra an sie wenden, sie kommen auf mich zu, wenn es neue Lösungen gibt, die für uns hilfreich sein könnten, denn sie kennen unser Unternehmen ganz genau und wissen, was für uns interessant ist. Ich vertraue ihrem Urteil. Es ist eine Beziehung, von der beide Seiten profitieren, eine richtige Partnerschaft.“

Weitere Informationen über Carraro finden Sie unter: www.carraro.com



Von Netzstrümpfen

Der Name Wolford steht für Qualität – ihre Strümpfe, Strumpfhosen und Bodys werden weltweit von 1,5 Millionen Frauen getragen. Das österreichische Unternehmen mit Sitz in Vorarlberg führt heute über 250 Boutiquen in großen Städten auf der ganzen Welt und Niederlassungen in elf Ländern in Asien, Europa und Nordamerika.

Mit dem stetigen Wachstum von Wolford im Laufe der Jahre nahm auch die Anzahl der Lager ständig zu, und diese waren immer schwieriger zu verwalten. Daher wurde beschlossen, die Lagerdisposition zu vereinfachen, so dass Wolford jetzt, anstatt mehrere Lager in verschiedenen Ländern zu unterhalten, nur ein zentrales Lager in Bregenz hat, wo alle Aufträge bearbeitet werden, und das sind im Durchschnitt 800 pro Tag. Um dies zu verwirklichen, erklärt IT Manager Kurt Gobber, war ein inter-

Global, einheitlich und einfach

BASF IT Services B.V.

BASF IT Services bietet internen Kunden sicheren Zugriff auf die BASF-interne Rechnerumgebung. Möglich wird das durch die Remote Access Services von AT&T. Mit RAS steht ein technisch flexibler Zugang zum BASF-Intranet zur Verfügung, der Kosten spart und sichere, stabile Verbindungen ermöglicht.

Böse Überraschungen in Form überteuerter Hotel-Telefonrechnungen gehören zum Alltag weltweit agierender Großunternehmen. Dennoch kann es sich heute kaum jemand leisten, den Anschluss an das Tagesgeschäft zu verlieren. „Im Grunde war es ein Witz: wir hatten die modernste Computer- und Kommunikationstechnik, leistungsfähige Datenbanken, sichere Firewalls – und konnten keinen vernünftigen Zugriff von außen auf diese Ressourcen bieten,“ sagt Harald Endres, Manager Network Services, BASF IT Services GmbH in Ludwigshafen. Das musste sich ändern.

Mehr Funktionen für's gleiche Geld

Auf der Suche nach einer Lösung trugen die Planer von Anfang an der weltweiten Aufstellung der BASF Rechnung. Global, einheitlich und einfach – so lautete die Vorgabe, als BASF IT Services eine Ausschreibung startete. Als schließlich AT&T den Zuschlag für das Projekt bekam, hatten auch pragmatische Erwägungen die Planer der BASF IT Services geleitet. „AT&T hatte weltweit am meisten Einwahlknoten ins Internet“, so Harald Endres. Andere Anbieter hätten anstelle der eigenen Knoten Verträge mit lokalen Service Providern abgeschlossen. Bei diesem Verfahren witterten die IT-Experten

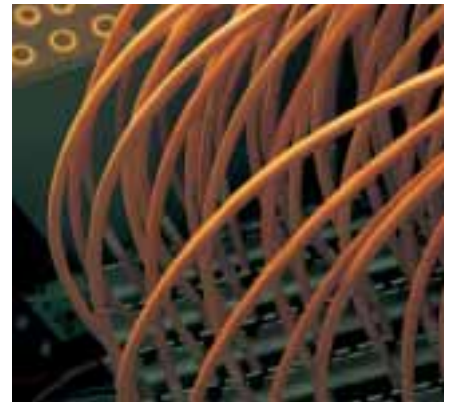
von BASF IT Services jedoch potenzielle Qualitätsunterschiede.

Remote Access für über 5000 Nutzer

Der gleiche Datentransfer, der einem Mitarbeiter vor der Installation von AT&T RAS eine Hotelrechnung von 280 Dollar beschert hätte, kostete jetzt lediglich 45 Dollar. Die Verbindung über das Internet war damit nicht nur deutlich preiswerter, sondern auch schneller und stabiler.

Dafür wurden nur zwei neue Programme installiert: Ein „Dialer“, der auf dem Notebook auch die weltweiten Einwahlnummern hinterlegt hat. Diese Einwahl-Software startet für den Verbindungsaufbau das zweite Programm, das Nortel zu der Lösung beigetragen hat. „Das Prinzip ist einfach und verschafft uns ein hohes Maß an technischer Flexibilität“, erklärt Harald Endres.

Registrieren Sie sich für das kostenlose 50-Tage-Testangebot von Internet Dial Remote Access!
www.att.com/emea/deutsch/remote



Mehr als 2.000 BASF-Mitarbeitern wird RAS bereits als Alternative zu dem herkömmlichen Verfahren angeboten. In den kommenden Monaten sollen rund 5.000 BASF-Mitarbeiter europaweit RAS-Nutzer werden. Als Unterstützung steht den Anwendern der globale Helpdesk-Service zur Verfügung.

„Wir haben mit der AT&T-Lösung ein Sicherheits- und Technologie-Bündel, ein richtig dickes Service-Paket für unsere Kunden realisiert,“ so Harald Endres. Und zukunftsweisend ist der Ansatz ebenfalls, hat doch Remote Access den Grundstein gelegt für vielfältige alternative Arbeitsmodelle wie etwa das Home Office.

BASF IT Services B.V. ist im April 2001 durch den Zusammenschluss aller IT-Aktivitäten der BASF-Gruppe in Europa entstanden. Ziel war es, das IT-Know-how im Konzern zu bündeln und externen Kunden ebenso wie der BASF Aktiengesellschaft innovative IT-Lösungen anzubieten. Derzeit werden Netze und Großrechner für rund 50.000 Nutzer an mehr als 250 Standorten in Europa betrieben.

Weitere Informationen über BASF IT Services finden Sie unter:
www.basf-it-services.com

und Netzwerken

nationales Netzwerk mit schnellen, zuverlässigen Datenwegen erforderlich. „Wir konnten es uns nicht erlauben, dass das Netzwerk, über das wir unser komplettes Bestellsystem abwickeln, Schwachstellen aufweist.“ Das Global Network von AT&T lieferte die Lösung.

Auftritt des globalen Partners

„Wir haben uns aus zwei Gründen für AT&T entschieden,“ fährt Kurt Gobber fort. „Zum einen wegen der globalen Tätigkeiten des Unter-

nehmens und der wirklich weltweiten Präsenz, zum anderen aufgrund der Qualität, der Sicherheit und der garantierten Verfügbarkeit. Dank AT&T konnten wir die elf Landesniederlassungen von New York bis Tokio über ein Frame Relay-Netzwerk mit dem Hauptsitz verbinden.“

Die Frame Relay-Lösung von AT&T brachte für Wolford wesentliche Vorteile. Lagerhaltungskosten wurden gesenkt und Lieferungen beschleunigt, mit dem Ergebnis, dass bereits ein

weiterer Ausbau des Netzwerks geplant ist. Dabei sollen auch die Wolford-Boutiquen einbezogen werden, um einen kontinuierlichen Datenfluss und reibungslose Abläufe zwischen den Verkaufsstellen und dem Hauptsitz und Lager in Vorarlberg zu gewährleisten.

„In AT&T haben wir einen zuverlässigen Netzwerkpartner gefunden, der genauso global denkt wie wir und uns auch in Zukunft tatkräftig zur Seite stehen wird“, so Kurt Gobber.

Weitere Informationen über Wolford finden Sie unter: www.wolford.com

Aviapartner bestätigt sein Vertrauen in AT&T



„Der Aufbau eines Netzwerks erfordert viel Zeit, Arbeit und Kapital. Daher ist es für uns von ausschlaggebender Bedeutung, mit einem zuverlässigen Partner zusammenzuarbeiten, der über einen guten Ruf in der Branche verfügt und uns auch langfristig zur Seite steht. AT&T erfüllt diese Kriterien in jeder Hinsicht.“

Im Mai verlängerte Aviapartner, Anbieter einer breiten Palette von Flughafendienstleistungen, seinen Vertrag mit AT&T um weitere fünf Jahre. Gegenstand des Vertrags ist die Verwaltung und Entwicklung von Apnet, dem vor drei Jahren von AT&T für Aviapartner eingerichteten Netzwerk.

Europaweite Qualität

Aviapartner befasst sich mit der Betreuung von Passagieren, der Abfertigung von Flugzeugen und dem Transport von Gepäck, Frachtgut und Briefsendungen an 32 europäischen Flughäfen. Allein im vergangenen Jahr wurden 14 Mio. Passagiere betreut und 147.000 Flugzeuge sowie 660.000 Tonnen Fracht abgefertigt. Ein Arbeitsvolumen in dieser Größenordnung setzt einen erstklassigen Kundendienst voraus, daher benötigte Aviapartner ein internationales Netzwerk, mit dem das Unternehmen seinen Kunden europaweit standardisierte Lösungen bieten kann.

AT&T konnte sich den ursprünglichen Vertrag mit einer WAN-Lösung (Wide Area Network) sichern, die alle Flughäfen miteinander vernetzt und den 4.200 Mitarbeitern ermöglicht, eine Verbindung zum Internet herzustellen, per E-Mail zu kommunizieren und überall mit den gleichen Anwendungen zu arbeiten. Auf diese Weise kann allen Fluggesellschaften der gleiche, erstklassige Service geboten werden. Für Rudolf Demeulenaere, Country Manager von AT&T Belgien & Luxemburg, beweist die Entscheidung von Aviapartner einmal mehr, dass „wir einen herausragenden Service haben, der zuverlässig und sicher ist. Darüber hinaus bestärkt diese Entscheidung unser Vorhaben einer schnellen Expansion in Europa.“

Die europäische Kommunikationsplattform von Aviapartner wird vom belgischen Zaventem aus betreut, wo etwa 35 Mitarbeiter spezielle Anwendungen entwickeln sowie Hardware-, Software- und Helpdesk-Services bereitstellen. Mittlerweile liegen die Betreuung von Apnet sowie die Verantwortung für das Netz und die Firewall ganz bei AT&T, wodurch eine optimale Daten-



Das Leistungsangebot von Aviapartner setzt erstklassigen Kundendienst voraus.

übertragung zwischen den unterschiedlichen Plattformen auf den Flughäfen sichergestellt ist.

Zuverlässigkeit, Sicherheit und Verfügbarkeit

Das Virtual Private Network (VPN) von Aviapartner basiert auf einer hierarchischen Architektur, die modernste Technologien und Geräte zusammenführt und eine Vielzahl von Zugriffsmethoden sowie Voice over IP (VoIP) und Quality of Service (QoS) unterstützt. Mit der Nutzung verschiedener Zugangsanbieter sowie ISDN-Backup wird eine hohe Verfügbarkeit gewährleistet, die ein solches Netzwerk erfordert. Der neue Vertrag stellt sicher, dass Apnet auch weiterhin Zuverlässigkeit, Sicherheit und Verfügbarkeit auf höchstem Niveau bietet.

Die Fähigkeit zur schnellen Integration eines neuen Flughafens in das Netzwerk hat für Jaak Aendeckerk, Vice President Information and

Technology von Aviapartner, oberste Priorität. „Unser Ziel ist es, neuen Fluglinien die gleichen umfassenden Services wie unseren Stammkunden zu bieten“, so Aendeckerk. „AT&T wird diesem Anspruch gerecht, da man in der Lage ist, unserem Apnet-Netzwerk im Handumdrehen neue Standorte hinzuzufügen. Der Aufbau eines Netzwerks erfordert viel Zeit, Arbeit und Kapital“, so Aendeckerk weiter. „Daher ist es für uns von ausschlaggebender Bedeutung, mit einem zuverlässigen Partner zusammenzuarbeiten, der über einen guten Ruf in der Branche verfügt und uns auch langfristig zur Seite steht. AT&T erfüllt diese Kriterien in jeder Hinsicht. Daher stehen wir auch heute noch mit voller Überzeugung hinter unserer damaligen Entscheidung.“

Weitere Informationen über Aviapartner finden Sie unter: www.aviapartner.aero

...AT&T PEOPLE...AT&T PEOPLE...AT&T PEOPLE...AT&T PEOPLE...AT&T PEOPLE...

Was ist der Unterschied zwischen AT&T und dem Kilimandscharo?

Bei AT&T kommt es in erster Linie auf Geschwindigkeit an, für den Kilimandscharo trifft genau das Gegenteil zu. Zu dieser Feststellung gelangte der österreichische Customer Enablement & Order Management Manager Walter Maurer bei seiner Tour in dieser Region.

Maurer und seine Kameraden wollten sich in den ersten vier Tagen erst akklimatisieren und bestiegen zunächst den Mount Meru (mit 4.566 Metern der zweithöchste Berg der Region). Dann folgte die große, sieben Tage dauernde Tour – der Aufstieg auf den Uhuru Peak, mit

5.896 Metern der höchste Punkt des Kilimandscharo. Sie benötigten fünfeinhalb Tage für den Aufstieg, jedoch nur anderthalb Tage für den Abstieg. Tatsächlich dauerte der letzte Tag des Aufstiegs ganze 14 strapaziöse Stunden und begann um 1.30 Uhr nachts, um der schlimmsten Tageshitze zu entgehen, die am Kilimandscharo über 30°C erreichen kann und nachts auf -15°C absinkt.


Bei Unternehmungen dieser Art ist Teamwork von großer Bedeutung, und Walter Maurers Fähigkeiten in diesem Bereich wurden während seiner Zeit bei AT&T, zuletzt als Mitglied des Teams der ENX v2-Zertifizierung, oft unter Beweis gestellt.

Die ENX- oder European Network Exchange-Zertifizierung ist ein wichtiger Faktor, da AT&T hiermit in der Lage ist, Kunden aus der Automobilindustrie den Zugang zu einem branchenspezifischen Netzwerk zu ermöglichen. Dieser Zugang ist Grundvoraussetzung für einige der großen Akteure der Branche, die diesen Zugriff für Partner und Zulieferer zur Voraussetzung machen. Die ENX Plattform kann als ein eigenständiges, nur bestimmten Mitgliedern zugängliches Netzwerk innerhalb des gesamten AT&T-Netzwerks beschrieben werden. Mit der Zertifizierung ist AT&T in der Lage, ENX-Services gemäß dem ENX-Vertrag anzubieten, wodurch unsere Fähigkeiten, auch Kunden aus dem Automobilssektor zu betreuen, weiter ausgebaut werden.



Eine zähe Truppe


Drei mutige Mitarbeiterinnen von AT&T Frankreich haben sich für die zweite „Ariel Adventure“ angemeldet, die im Dezember 2002 auf der schönen Insel La Réunion stattfindet. Zum Team gehören Anne Auble, AT&T Network Architect und verantwortlich für technische Netzwerklösungen während der Vertriebsphase, Céline Chauveau, regionale Ansprechpartnerin im Contract Management Center für AT&T Southern Region, und Frédérique Nicoli, AT&T Global Account Manager: Als Wettkampf in der freien Natur wird „Ariel Adventure“ das Durchhaltevermögen der aus je drei Frauen bestehenden Teams über einen Zeitraum von sechs anstrengenden Tagen auf die Probe stellen:


 22 km-Strecke für zwei Frauen zu Fuß und die dritte zu Pferd

 Orientierungsmarsch über eine 25 km lange Strecke

 25 km mit dem Mountainbike

 ein weiterer 25 km langer Orientierungsmarsch

 ein kombinierter Wettkampf aus Bergsteigen, Dschungelmärschen und Bogenschießen

 ein etwas (aber nur etwas) weniger anstrengender Tag bestehend aus 5 km Fußmarsch und 15 km Kanufahrt

Das von AT&T gesponserte Team mit dem passenden Namen „A Tough Tribe“ (eine zähe Truppe) ist eines von 65 Teams aus ganz Frankreich. Die Frauen trainieren ihre Kondition und ihren Teamgeist schon seit Juni, als das abenteuerlustige Trio am „SFR Raid“ teilnahm, einem Wettbewerb über 60 km, der sich aus Orientierungsmarsch, Fahrrad- und Kanufahrten zusammensetzte, und bei dem sich das Team einen herausragenden zweiten Platz erkämpfen konnte.

Mit ihrem Ehrgeiz und ihrer Entschlossenheit haben Anne, Céline und Frédérique durchaus Chancen, im Dezember ein beeindruckendes Finish zu liefern. **Die Ergebnisse unseres Teams können Sie (in französischer Sprache) unter www.arielaventure.com verfolgen.**



Experten gefragt Richard Palmer Jr., Vice President und General Manager des Geschäftsbereichs VPN und Security Services von Cisco Systems.

Aufbau einer umfassenden Sicherheitsstrategie

Die Zielsetzung der Netzwerksicherheit besteht darin, Netzwerke und Anwendungen gegen Angriffe zu schützen und gleichzeitig die Verfügbarkeit und Vertraulichkeit der Daten sicherzustellen. Da immer mehr Firmen ihre Netzwerke ausdehnen, gewinnen auch die Technologien zur Netzwerksicherheit zunehmend an Bedeutung. Ohne geeignete Sicherheitsvorkehrungen stehen Unternehmen ständig vor der Gefahr von Sicherheitsverletzungen, die ernstzunehmende Schäden oder auch den Verlust von Netzwerkressourcen zur Folge haben können.



Den Kunden von AT&T Business steht eines der sichersten und modernsten IP-Netzwerke der Welt zur Verfügung, genauer gesagt ein MPLS-Netzwerk, das weltweit qualitativ hochwertige Sprach-, Daten und Internetdienste bereitstellt. VPN-Services, Firewall-Services und andere Angebote können als Teil der aus einer Hand gebotenen Managed Security Services von AT&T integriert werden.

Beispielsweise nutzt der verbreitete I-VPN-Service von AT&T ausgereifte Tunneling- und Verschlüsselungstechnologien auf Basis des IPsec-Protokolls, um Unternehmen dabei zu helfen, Benutzer mit verteilten Ressourcen zu verbinden. Der EVPN-Service von AT&T integriert MPLS-basierte Sicherheitsfunktionen auf dem gleichen Niveau wie Frame Relay oder ATM, wodurch Kunden in der Lage sind,

sichere Intranetlösungen auf globalem Niveau aufzubauen. Als qualifizierter Service Provider im Cisco Powered Network-Programm setzt AT&T bei seinem Sicherheitsangebot auf eine übergreifende Cisco-Infrastruktur.

Das Bewusstsein für Sicherheit schärfen
Vernetzte Anwendungen bieten zwar neue Möglichkeiten und Chancen, stellen jedoch auch ein nicht zu unterschätzendes Sicherheitsrisiko dar. Wenn Unternehmensnetzwerke für immer mehr externe Benutzer geöffnet werden, bieten sie auch zunehmend mehr Angriffsfläche. Intelligent geführte Unternehmen setzen daher auf einen Layer-basierten Ansatz zum Schutz der Sicherheit und verlassen sich nicht ausschließlich auf eine einzige Technologie zur Lösung aller Sicherheitsprobleme (siehe Info-Box).

Zu den am häufigsten auftretenden Angriffen gehören DoS-Attacks (Denial of Service) sowie das Knacken von Codes und Kennwörtern um Root-Zugriff auf Netzwerkressourcen zu erhalten.

Bei DoS-Attacks werden Netzwerkressourcen lahm gelegt, so dass sogar autorisierte Benutzer nicht mehr auf Anwendungen zugreifen können. Bei Angriffen auf die Kennwortsicherheit versucht der Hacker, das



Kennwort eines autorisierten Benutzers herauszufinden, um auf diese Weise Zugriff auf dessen Netzwerkressourcen zu erhalten. So verschaffte sich ein Hacker im Dezember 2000 beispielsweise Kennwörter des Medical Centers der University of Washington und erhielt vertrauliche Daten von 5.000 Patienten.

Vernetzte Computer, auf denen E-Business-Anwendungen ausgeführt werden, weisen eine noch höhere Zahl potenzieller Schwachstellen auf. Hacker nutzen häufig die Sicherheitslücken von ungeschützten Betriebssystemen oder Anwendungen und können so ernsthafte Sicherheitsverletzungen verursachen. Abhängig vom Niveau des Angriffs variieren die Konsequenzen von leichter Belästigung bis zur vollständigen Lahmlegung des Systems. Die Kosten für die Wiederherstellung von Daten und Systemen reichen von einigen hundert bis hin zu mehreren Millionen Euro.

Ein effektives Sicherheitskonzept sollte von Netzwerkarchitekten und IT-Sicherheitsteams gemeinsam entwickelt werden. Die Zugriffsmöglichkeiten und die Sicherheitsanforderungen für jeden IT-Service sollten klar definiert sein und das Netzwerk sollte modular unterteilt werden, um eindeutig identifizierbare Vertrauensebenen zu ermöglichen. Die Zielsetzung besteht hierbei in der Schaffung von Sicherheitsebenen, so dass ein Eindringling, der die erste Hürde überwunden hat, dennoch nur auf einen begrenzten Teil des Netzwerks zugreifen kann.

CISCO SYSTEMS



EMPOWERING THE
INTERNET GENERATION

DoS	Denial of Service
EVPN	Enhanced Virtual Private Network
IP	Internet Protocol
IPSec	Internet Protocol Security
I-VPN	Internet Virtual Private Network
MPLS	Multi-Protocol Label Switching
GRE	Generic Routing Encapsulation
L2TP	Layer 2 Tunneling Protocol

Weitere Informationen über die Sicherheitslösungen von Cisco finden Sie unter:
www.cisco.com/warp/public/44/solutions/network/security.shtml

Wesentliche Elemente der Netzwerksicherheit

Eine vollständige Sicherheitslösung umfasst fünf Schlüsselkomponenten:

1 Identität – Hiermit ist eine korrekte und positive Identifizierung des Netzwerkbenutzers, von Hosts, Anwendungen, Services und Ressourcen möglich. Kennworttools und Authentifizierungsprotokolle wie RADIUS, TACACS+ und Kerberos werden häufig in Kombination mit neueren Technologien wie digitalen Zertifikaten, Smartcards und Verzeichnisdiensten eingesetzt.

2 Peripheriesicherheit – Hiermit wird der Zugriff auf wichtige Netzwerkanwendungen, Daten und Services gesteuert, so dass nur legitimierte Benutzer und Informationen in das Netzwerk gelangen können. Die Peripheriesicherheit wird in der Regel mithilfe von Zugriffsteuerungslisten und statusbehafteten Firewalls in Netzwerk-Routern und Switches sowie mit dedizierten Firewalls, Virenscannern und Inhaltsfiltern gewährleistet. AT&T verwendet die Cisco-Modellreihe Secure PIX® Firewall, um einen einzelnen Sicherungspunkt in der Peripherie des Kunden Netzwerks aufzubauen. Mit der PIX-Technologie werden konsistente Sicherheitsrichtlinien für die Kommunikation in weiträumig verteilten Intranets, Extranets und über das Internet durchgesetzt.

3 Datenschutz – Der Schutz von Daten ist immer dann von Bedeutung, wenn vertrauliche Informationen vor Ausspähsversuchen geschützt werden müssen. Mit IPsec wird sichergestellt, dass nur autorisierte Benutzer im Transfer befindliche Daten lesen können, während Tunneling-Technologien wie GRE und L2TP verwendet werden, um einen effektiven Datenschutz zu ermöglichen.

4 Sicherheitsüberwachung – Um die Sicherheit des Netzwerks auch langfristig gewährleisten zu können, ist es unabdingbar, den Status der Sicherheitsvorkehrungen regelmäßig zu prüfen und zu überwachen. Scanner für Netzwerksicherheitslücken decken Schwachstellen auf, Einbruchserkennungsprogramme überwachen die Systeme und reagieren umgehend auf sicherheitsrelevante Ereignisse.

5 Richtlinienverwaltung – Wenn Größe und Komplexität eines Netzwerks zunehmen, wächst auch der Bedarf an Tools für eine zentralisierte Richtlinienverwaltung. Fortschrittliche Tools zur Analyse, Interpretation, Konfiguration und Überwachung des Status von Sicherheitsrichtlinien, die zudem mit Browser-basierten Benutzeroberflächen ausgestattet sind, steigern die Nutzbarkeit und Effektivität von Netzwerksicherheitslösungen.

Seiner Zeit voraus: das MPLS-Netzwerk von AT&T

Die Arbeit am MPLS-basierten Global Network von AT&T geht zügig voran. In EMEA werden Ende 2002 insgesamt 80 neue MPLS-Knoten – 20 mehr als ursprünglich geplant – in Betrieb genommen, und die Implementierung des Netzwerks soll bereits Mitte 2003, also ein Jahr früher als vorgesehen, abgeschlossen sein.

AT&T baut seine Position aus

Obwohl es auf dem globalen Telekommunikationsmarkt zurzeit turbulent zugeht und sogar einige namhafte Unternehmen der Branche vor ernsthaften Problemen stehen, kann AT&T dank der langfristig ausgelegten Investitionsstrategie seine Position weiter ausbauen.

Mit diesem innovativen MPLS-basierten Netzwerk bietet AT&T seinen globalen Kunden jetzt die Vorteile einer integrierten Plattform für verschiedene Dienstleistungen, die das gesamte Spektrum des Datentransfers abdeckt – von reinen Transport-Services bis hin zu Managed Services und Outsourcing.

Der Ausbau des Netzwerks umfasst auch private Leitungen, wodurch das bestehende Leistungsangebot in Hinblick auf Bandbreite, Redundanz und Flächendeckung deutlich verbessert wird. Auf dieser Grundlage kann das Netzwerk jetzt flexibel für Sprach- und/oder Datenverbindungen eingesetzt werden.

Beste Verbindungen im AT&T Global Network

Die Investitionen in das Netzwerk ermöglichen AT&T in EMEA, nun auch verstärkt Netzwerk-Transport Services anzubieten. Die Merkmale dieser Services auf einen Blick:

- Zuverlässiges, einheitliches und globales Datennetzwerk
- Flexible und skalierbare Einsatzmöglichkeiten
- Weltweit einheitliche Netzwerkarchitektur
- Lokale Unterstützung vor Ort
- Zukunftssichere Technologieplattform
- Weltweit einheitliche Prozesse und Abläufe

Europäische Kunden profitieren bereits

Durch den Ausbau des Netzwerks steht nun auch europäischen Unternehmen die Flexibilität der Netzwerk-Transport-, Managed- und Outsourcing Services von AT&T auf einer integrierten Plattform zur Verfügung.

Neben diesen Leistungen bietet AT&T seinen Kunden noch einen weiteren, überaus wichtigen Vorteil – die Gewissheit, mit dem zuverlässigsten Anbieter der Welt zusammenzuarbeiten.

Wussten Sie schon, ...

dass das AT&T Global Network an einem durchschnittlichen Arbeitstag ca. 2,175 Trillionen Bytes an Daten verarbeitet?

Die neuste Pressemitteilung zum Rollout des MPLS-Netzwerks finden Sie unter:
http://att.emeamarketing.net/press/releases/230702_agm.html

Harte Zeiten – mit vollem Einsatz gemeistert

Connections ist eine Veröffentlichung von AT&T Business © AT&T. Veröffentlicht von: AT&T Marketing & Communications EMEA, Quadrant House, Thomas More Square, 17 Thomas More Street, London E1W 1YE, Großbritannien.

Bitte beachten Sie: Produktinformationen (zum Zeitpunkt der Drucklegung korrekt) können jederzeit geändert werden. Unser Dank gilt allen, die zu dieser Ausgabe beigetragen haben, insbesondere Carraro, BASF IT Services, Wolford, Aviapartner und Cisco Systems.

So kontaktieren Sie uns

www.att.com/emea und dann auf EMEA-Standorte klicken

Oder e-mailen Sie uns:
InfoRequest@emea.att.com

Bleiben Sie auf dem Laufenden

Besuchen Sie die Website von AT&T EMEA unter: www.att.com/emea

Wartungs- Informationen

Die *Wartungswochenenden* sind in erster Linie reserviert für *Änderungsmaßnahmen*, die von der Gesetzgebung vorgeschrieben sind (z.B. *Powerdowns aus Sicherheitsgründen*). Darüber hinaus können sie für *Änderungen genutzt werden*, die (aufgrund ihres Schwierigkeitsgrades) nicht während der üblichen *Wartungsfenster an Werktagen* vorgenommen werden können.

Geplante *Wartung am Wochenende*

Die nächste geplante *GSDA-Wartung* findet am *Samstag, den 8., und Sonntag, den 9. März 2003* von *22.00 bis 05.00 MEZ* statt.

©2002 AT&T. Alle anderen Marken, eingetragenen Marken und Dienstleistungsmarken sind Eigentum der jeweiligen Inhaber. Einige Dienstleistungen, Eigenschaften und Funktionen sind nicht in allen Ländern verfügbar. Länderspezifische Informationen erhalten Sie von Ihrem zuständigen AT&T Ansprechpartner für Marketingdienstleistungen.

005/GER02



Durch schnelle Maßnahmen wie die Sicherung wichtiger Einrichtungen und die Umleitung der Datenwege auf nicht betroffene Knoten konnte auch in den kritischsten Zeiten des Hochwassers, als die Pegelstände 2,5 m erreicht hatten, eine akzeptable Verbindung gewährleistet werden.

In diesem Sommer erlebte die Tschechische Republik die schwersten Überschwemmungen der Geschichte. Mehr als ein Drittel des Landes war betroffen, dreizehn Menschen starben, Zehntausende mussten ihre Häuser verlassen und Tausende wurden im letzten Moment von Hubschraubern gerettet.

Ein Team der Prager Niederlassung von AT&T stellte sich dieser Krise mit außerordentlicher Entschlossenheit und arbeitete mindestens 16 Stunden am Tag. Diese Mitarbeiter – unterstützt von einem Team des Geschäftsbereichs Central European Region Network Operation – reagierte umgehend auf die Hochwasserwarnungen der tschechischen Regierung und begann damit, Vorkehrungsmaßnahmen zu treffen, um die Auswirkungen auf technische Einrichtungen und damit auch die Netzausfälle für die Kunden so gering wie möglich zu halten. Andere Mitarbeiter

unterbrachen ihren Urlaub, um sich ganz der schnellstmöglichen Wiederherstellung des Backbones zu widmen.

Petr Lukas, Country Manager von AT&T, berichtet stolz: „Unsere Kunden sind sehr dankbar für unsere außergewöhnlichen Bemühungen und unser proaktives Engagement, mit dem wir sicherstellten, dass ihre Geschäftsabläufe von dieser Katastrophe so wenig wie möglich beeinträchtigt wurden.“



Die überschwemmten Büroräume von AT&T.