AUSGABE 1/03

ZUKUNFT

T.D.T.®
Transfer Data Test GmbH

Wir laden ein
12.3.–19.3.2003
Halle 1 Stand 8k4

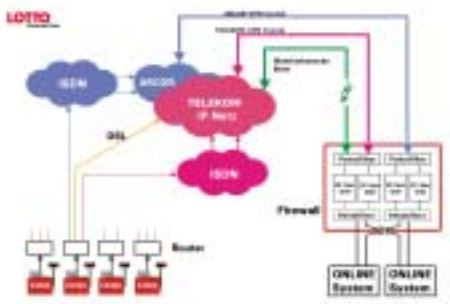
LOTTO SETZT AUF INTERNET

Als eigenständiges Unternehmen richten die Lotto-Gesellschaften Deutschlands ihren Fokus auf eine effektive Geschäftsstrategie und Gewinnmaximierung aus. Dabei unterliegen die Einnahmen einem gnadenlosen Prinzip: Nicht getätigter Wochenumsatz ist unwiderbringlich verloren und bedeutet Mindereinnahmen. Deshalb ist bei der Datenübermittlung die hohe Verfügbarkeit und zunehmend eine hohe Bandbreite für den Geschäftserfolg unerlässlich. Diese Kernaussage trifft gerade in Spitzenzeiten, kurz vor Abgabeschluss der Lottoscheine und Sportwetten, zu. Lotto Rheinland-Pfalz GmbH, deren

Gesellschafter die Landessportverbände sind, hat die Zeichen der Zeit erkannt und das Ziel neu definiert: Mehrumsatz durch zusätzliche „Spiel-Angebote" und höchste Verfügbarkeit mittels Internet-Datenübertragung mit den Sicherheitsmechanismen VPN und IPSec. Die neue Technik muss die durchschnittlich 100.000 Übertragungen pro Tag erheblich günstiger übertragen und die ohnehin schon sehr geringe Ausfallrate gleichzeitig halbieren. Um dieses ehrgeizige Ziel zu erreichen, hat sich die Geschäftsleitung in Koblenz das niederbayerische IT-Unternehmen T.D.T. ins Boot geholt.

Lotto-Toto ist in Deutschland ein Begriff, den nahezu alle Bürger kennen. Die Abwicklung übernehmen die Lotto-Gesellschaften verschiedener Bundesländer, die bei der Datenübertragung der Annahmestellen in die jeweiligen Zentralen auf unterschiedliche Lösungen setzen. Lotto Rheinland-Pfalz entschied sich schon früh für eine spezielle X.25-Variante, deren Erneuerung oder Ablösung vor der Tür stand. Die bisherige Datenübertragung der Außenstellen in Rheinland-Pfalz und Luxemburg zu speziellen X.25-Konzentratoren in Koblenz, um von dort aus in das LAN zu routen, konnte und wollte man nicht mehr fortsetzen. Die Abhängigkeit von sehr wenigen Partnern war zu hoch.

Dem X.25-Netz erwuchsen in den vergangenen Jahren ernsthafte Konkurrenten, spätestens mit dem Einzug der IP-Technik. So konnte daran gedacht werden, die langsame und teure X.25-Datenübertragung durch einen genauso sicheren aber erheblich schnelleren und flexibleren Datentransfer zu ersetzen. Weiterer wichtiger Ansatzpunkt war: Die neue Technik muss von vielen Anbietern beherrscht werden, damit auch langfristig eine günstige Kostenstruktur gewährleistet ist. Die Zeichen standen also auf Erneuerung und die Voraussetzungen dafür waren gegeben: Mit dem Neubau des Rechenzentrums 1996 wurde auch eine zukunftsorientierte Infrastruktur installiert, die weit über die damaligen Bedürfnisse hinausreichte. Die Zentrale in Koblenz ist mit einem eigenen Glasfaserring ausgestattet, alle wichtigen Systeme sind redundant ausgelegt und garantieren höchste Sicherheitsstandards. An dieses Rechenzentrum waren bis zur aktuellen Umstellung ca. 1.600 Außenstellen mit X.25-Terminals angeschlossen. Die als Sonderlösung konzipierten Geräte mit X.25-Anschluss werden praktisch nicht mehr hergestellt oder nur zu einem nicht vertretbaren hohen Preis. Der Schritt zu preiswerter, zukunftssicherer Technik und Software und der Datenübertragung via IP war somit die logische Konsequenz. Schon schwieriger gestaltete sich die Suche nach geeigneten Partnern. Es mussten Unternehmen gefunden werden, die IPSec bis in das letzte Bit beherrschen und darüber hinaus hohe Kompetenz in allen Fragen zu X.25 nachweisen konnten. „Nach langen Recherchen im Internet stieß ich unter anderem auch auf *TDT*" erinnerte sich Gas-



Das neue „Lotto-Netz" von Rheinland-Pfalz

par Soproni, Leiter Zentrale IT. „Ein Gespräch mit Lotto Hannover bestätigte mir, dass wir auf der richtigen Spur sind - und so entstanden die ersten Kontakte." Schnell erkannte man das Potential, das *TDT* in punkto X.25 aufweisen konnte und die Konzepte zur IPSec waren in sich sehr schlüssig. Kein anderes Unternehmen konnte zum damaligen Zeitpunkt XoT, das über IPSec weitertransportiert werden sollte, anbieten. Das war genau die Lösung, die im ersten Schritt von Ressortleiter Informationstechnologie Manfred Härtel angedacht war. Der lang- und mittelfristige Umbau des Netzes konnte geplant werden, ohne die über 1.600 Endgeräte in den Annahmestellen sofort ersetzen zu müssen. Man wusste, dass die eingesetzten Geräte mit X.25-Anschluss in den Außenstellen noch über mehrere Jahre ihre Dienste tun werden und die HP-Großrechner in der Zentrale mit dem XoT-Modul ohnehin schon bestückt waren. Die Konfiguration war in kürzester Zeit vorgenommen. Exakt hier setzte das *TDT*-Konzept an. In enger Zusammenarbeit mit Lotto Rheinland-Pfalz entwickelte das Unternehmen, das dieses Jahr 25 Jahre Bestehen feiert, unter Federführung von Entwicklungsleiter Siegfried Vogl einen Router unter dem pragmatischen Namen „Lotto-Router". Schon bei der Ausarbeitung und regelmäßigen Abstimmung des Pflichtenheftes war klar, dass Spezial-Featers entwickelt werden würden, die in den bisher bekannten Router-Modellen nicht zu finden sind.

Einer der „unbezahlbaren" Mehrwertdienste, den auch weltweit führende Anbieter mit ihren Standardlösungen nicht oder nur zu teuren Preisen anbieten konnten, ist das Providerswitching, das mehrere Datenstrecken unterschiedlichster „Transportstrecken-Provider" auswählen kann, z.B. Internet, asynchrone Modemleitung, oder GPRS.

Die Datenübermittlung via IPSec

Die *TDT*-Router übernehmen die X.25-Daten der Endgeräte, verpacken sie in IP-Daten und routen sie zu der Koblenzer Zentrale. Hinter dieser einfachen Beschreibung steckt ein Bündel komplexer Aufgaben. Das angeschlossene Terminal schickt einen Verbindungswunsch zu den „Lotto-Routern". Der Router hält diesen Verbindungsaufbau hoch und sucht sich einen Transportweg zum XoT-Gateway des Rechenzentrum aus. Ist der Call erfolgreich, reicht die Software den

X.25-Call durch. Sollte die Leitung tot oder blockiert sein, sucht sich der „Lotto-Router" einen anderen Provider und auch andere Transportwege, im Notfall sogar über ein angeschlossenes Modem. In diesem Fall wird in letzter Konsequenz eine asynchrone X.25-Strecke aufgebaut. Zusätzlich wichtet die eingebaute Intelligenz die Verbindungswege, um den effektivsten Transportweg auszuloten. Somit können günstige dynamische Adressen vergeben werden. Das Halten des Verbindungsaufbaus Terminal/Router ist eine Aufgabe, die Rücksicht auf das besondere Umfeld von IPSec erfordert. Da der Router (alle Clients sind als Road-Warrior definiert) bei jeder Anwahl eine andere IP-Adresse erhält, bauen IPSec-Anwendungen einen Tunnel auf. Die Zentrale „sieht" nur statische, fest an den Router vergebene IP-Adressen, und IPSec kann durch das Road-Warrior-Verfahren mit den dynamischen Adressen umgehen. Auf Grund zusätzlich übertragener Informationen erfolgt eine Authentifizierung dieser Außenstelle (Zertifikat). Darüber hinaus greifen noch mehrere Sicherheitsmechanismen, so kommen die Calls zum Beispiel durch das VPN-Gateway (Gegenstelle des IPSec-Tunnels), durch redundant ausgelegte Gateways und durch die Load Sharer bzw. Load Balancers, welche die Verteilung der Lasten auf diverse Rechner vornehmen. Das komplizierte Gebilde von Gateways und Load Balancern erforderte einen hohen Programmieraufwand, damit der Datenfluss zu den Außenstellen gewährleistet ist. Die Load Sharer halten auf Ebene 3 die Verbindung (das ist nicht selbstverständlich) - und über diesen Tunnel wird ein weiteres virtuelles Netz gelegt. Diese Konfiguration müssen die Router von *TDT* erkennen bzw. unterstützen, damit die Adresszuordnung geregelt ist.

Das Rechenzentrum in Koblenz

Parallel zur Installation der Router musste auch die Kommunikations-Infrastruktur in Koblenz neu strukturiert werden und mit externen Partnern eine kluge und langfristig angelegte Lösung gefunden werden. Die eigentlichen Applikationen im Rechenzentrum laufen weiterhin unter X.25. Die HP-Großrechner, durch ein zusätzliches Softwaremodul XoT-fähig gemacht, übernehmen wie bisher alle Aufgaben. Skeptiker, die vor der Lösung warnten, wurden eines Besseren belehrt. Das Problem, wie die zentralseitigen Rechner wissen sollen wohin die Pakete zurückgeroutet werden müssen, wenn dynamische Adressen eingesetzt werden, konnte wiederum durch IPSec und ein geschicktes Routing-Konzept gelöst werden.

Firewall und Sicherheit

Mit Akribie wurde und wird das Thema Datensicherheit behandelt. Nur auf den ersten Blick stellt das Versenden der Daten über das öffentliche Internet ein Risiko dar. Durch VPN und IPSec ist es allemal möglich, die Daten so zu verschlüsseln, dass Missbrauch ausgeschlossen ist. Und die Datensicherheit in der Zentrale wird durch mehrere unabhängige Firewalls schon seit Jahren auf denkbar höchstem Niveau gepflegt. Die Einteilung in Zonen, so ist zum Beispiel der Online-Lotto-Spielbetrieb eine eigene Zone, lässt Angriffe auf das gesamte Netz nicht zu.
Ebenso können die im Worst-Case anzunehmenden DoS-Attacken auf das IP-Netz immer nur eine Verbindung zu einem Provider lahmlegen, nie aber gleichzeitig beide. Damit ist mit der IP-Variante nicht nur die Verfügbarkeit gegenüber dem X.25-Netz gestiegen, sondern auch dessen Sicherheit. Falls es in IP-Netzen durch den Ausfall wichtiger Komponenten bei einem Provider zu kurzzeitigen Störungen kommt, zeigt sich die volle Leistungsfähigkeit des Routers: Innerhalb von Sekunden schaltet er zum Beispiel vom Telekom-Netz auf das Arcor-Netz um oder umgekehrt. Bei zwei völlig unabhängige Providern multipliziert sich die Verfügbarkeit auf nahezu hundert Prozent.

Gegen Attacken schützen

Die Authentisierung der Daten gewährleistet die absolute Vertraulichkeit und ebenso die Authentizität der Daten. Somit ist durch IPSec eine größere Sicherheit als bei X.25 gegeben. Moderne Verschlüsselungs- und Authentifizierungstechnologien auf der Basis von Algorithmen, ermöglichen Sicherheitsstandards, die, mathematisch nachgewiesen, nicht zu knacken sind.
Dank IPSec kann man ein virtuelles Netz aufbauen, da die Router von der Zentrale aus virtuell angesprochen werden - mit virtuellen IP-Adressen. Neben TCP-Protokollen können auch UDP-Protokolle getunnelt werden. In der Konsequenz kann durch IPSec das Netz wie ein LAN behandelt werden, um zum Beispiel die Konfiguration für die Router zu realisieren oder eine Problemanalyse durchzuführen.

Sicherheit groß geschrieben

Die redundante Sicherung der hochsensiblen Daten erfolgt in einem zweiten Gebäude, weit genug vom Hauptsitz entfernt, damit zum Beispiel bei einem Flugzeugabsturz, nur eines der beiden Gebäude getroffen werden kann. Hochsensible Feuerwarnanlagen und Dieselaggregate bei Stromausfall runden die umfangreichen Sicherheitsmaßnahmen ab.

Zusätzliche Bandbreite

Durch die Anbindung der Provisions- und Vertriebsstellen an das ISDN-Netz hat sich die Bandbreite schlagartig erhöht. War ursprünglich die Steigerung von 2.400 Baud auf 9.600 Baud durch X.31 das Nonplusultra, so toppt die ISDN-Verbindung zu den Knoten die Bandbreite natürlich um ein Vielfaches. Auch hier bewährte sich, das Design in Modellrechnungen zu testen und dann mit zuverlässigen Partnern die Installation der Geräte vorzunehmen. Das Rechenzentrum simulierte das künftige Netz und hat alle möglichen Varianten berechnet, z.B.: Wie kommt unser Rechenzentrum unter VMS und Linux mit der Flut der Daten zurecht?

Die Einführung des neuen Systems

Die Installation der TDT-Lotto-Router wurde gewissenhaft vorbereitet. Zwei PCs, sogenannte „Ammen", befüllten die Router mit den entsprechenden Daten für die jeweilige Außenstelle. Das Aufstellen der Geräte war die Aufgabe der Telekom-Techniker, da damit auch die Prüfung des ISDN-Anschlusses gegeben war. Mögliche Fehlerquellen konnten somit ausgelotet und sofort an Ort und Stelle behoben werden. Die Telekom ist eine zuverlässige Größe und es macht einfach Sinn, vorhandenes Know-how und Equipment zu nutzen, resümiert Manfred Härtel. Unsere Job besteht vornehmlich im Design des Netzes und dem Betrieb der zentralen und dezentralen Komponenten. Die Hotline in Koblenz trug dazu bei, dass die Agenturen bei Fragen umfassend beraten und unterstützt wurden. Die Desktop-Betreuer arbeiten schon seit Jahren mit einem speziellen Fern-Management-System, so dass die Betreuung zur Umstellung eigentlich nur eine weitere Routinearbeit war.

Die Test- und Befüllungsstation für die „Lotto-Router" mit einem der beiden „Ammen-PCs"

ISDN und DSL

Da die Timeout-Zeiten der Geschäftsstellen im Durchschnitt zwischen 30 Sekunden und 3 Minuten liegen, müssen sich die Außenstellen bei ISDN zum Teil bis zu 40-mal pro Tag reconnecten und das führt zu Aufbauzeiten, auch wenn diese mit weniger als 5 Sekunden sehr kurz sind. Die Entscheider von Lotto Reinland-Pfalz treiben deshalb den DSL-Anschluss voran. Auf Grund einer anderen Tarifierung mit Mindestnutzungszeit bei DSL werden die Reconnects auf meist eine Anwahl pro Tag minimiert. Die logische Folge, die Zeiten für die Kunden werden auf ein Minimum reduziert, zumal durch die „gelöteten" Verbindungen (keine Wählleitung) bei DSL der Aufbau noch schneller erfolgt.
Die Kombination macht es aus: DSL mit einer „festen Verbindung" und ISDN mit dem Vorteil der flexiblen Rufleitung. Alle Berechnungen zeigen, dass die Umrüstung auf DSL die Kosten reduzieren wird. Somit wird ein optimierter Mix von ISDN und DSL die Netzstrukur kennzeichnen. Keines für sich alleine ist gut genug, beide ergänzen sich optimal.

Amortisation, Rendite und höhere Umsätze

Die Renditeberechnung ist mehr als erfüllt worden. Eine Investition in die Router wird durch die Kosteneinsparungen innerhalb des berechneten Zeitraums mehr als kompensiert. Die Amortisationszeit liegt je nach Außenstelle zwischen 12 und 16 Monaten. Obwohl Neuland betreten worden ist, hat sich das Konzept als absolut richtig bewährt. Die umsichtigen Recherchen und Modellberechnung haben sich als Volltreffer erwiesen. Die Verfügbarkeit ist dank der Providersteuerung höher als bei der X.25-Lösung. Langfristig setzt man mit Linux auf das richtige System, denn allein unter Linux realisierte Lösungen können kostengünstig entwickelt werden. IP und IPSec werden sich auch weiterhin so dynamisch wie in den letzten Jahren entwickeln. Um höhere Umsätze generieren zu können, sollen besonders Sportwetten in das Angebot aufgenommen werden und dafür muss man gerüstet sein.
Noch wichtiger war für Gaspar Soproni und Manfred Härtel, die Präsentation des Spielgeschäftes und die Kommunikation zu trennen. Die Terminals in den Außenstellen sind relativ teures mechanisches Equipment mit einer Lebensdauer von bis zu 10 Jahren und mehr. Die Entwicklung der IT-Technik wird jedoch in erheblich kürzeren Intervallen stattfinden. „Würden wir uns für Terminals mit IP-Anschlüssen entscheiden, können wir auf die schnellen technologischen Änderungen nicht reagieren", führt dazu Gaspar Soproni aus. „Deshalb gilt für uns die Devise: Beides voneinander getrennt. Wir wollen ein Netzwerk, basierend auf Lösungen mit Standards, die von möglichst vielen Firmen in Deutschland angeboten werden. Dann sind wir immer auf der sicheren Seite."

Technik mit allen Raffinessen bei Lotto

Lotto-Router und Annahmegerät
Fotoersatz für Außenansicht Koblenz

Der Erfolg von Lotto Rheinland-Pfalz basiert natürlich nicht nur auf überragende IT-Kenntnisse und einer ausgezeichneten IT-Ausstattung. 1.600 Außenstellen bedeuten 1.600 verschiedene Partner mit ebenso vielen unterschiedlichen Anforderungen. Insgesamt 12 Bezirksstellen unterstützen die Zentrale in allen Bereichen. Ein Bündel von durchdachten Maßnahmen, wie Schulungen, regelmäßige Infos, rechtzeitige Lieferung von Werbematerial und der Einsatz von Field-Technikern vor Ort sichert die Zufriedenheit der Partner. Die Wartungs- bzw. Reparaturabteilung in Koblenz steht in engen Kontakt zu den Stellen und den Service-Technikern vor Ort. Alle üblichen Komponenten können innerhalb einer Stunde repariert bzw. ersetzt werden.

Die Zukunft hat begonnen

So kann man die Planungen von Lotto Rheinland-Pfalz GmbH beschreiben. Mittel- und langfristige Planungen laufen nicht nebeneinander sondern greifen ineinander. Durch die neue Netzstruktur können zum Beispiel die Außenstellen bei Werbe- und Marketingmaßnahmen erheblich besser mit Daten versorgt, und die Kunden vor Ort dadurch intensiver und gezielter angesprochen werden. Neue Angebote werden höhere Kapazitäten beanspruchen und flexiblere Maßnahmen verlangen. Mit Linux als „Schlüsseltechnologie" und IPSec als „Sicherheitsmedium" ist für eine genügend große Anzahl leistungsfähiger Programmierer und Unternehmen gesorgt. Für *TDT* wiederum eine Chance mehr, vorhandene Kapazität und Know-how für ein Unternehmen mit zukunftsorientierter Geschäftpolitik einzusetzen.

Kontaktadressen: Lotto Rheinland-Pfalz GmbH

Gaspar Soproni
Tel.: 02 61 / 94 38 - 411
Fax.: 02 61 / 94 38 - 640
mailto:
gaspar.soproni@lotto-rlp.de
http://www.lotto-rlp.de

Manfred Härtel
Tel.: 02 61 / 94 38 - 4 60
mailto:
manfred.haertel@lotto-rlp.de
http://www.lotto-rlp.de

EDITORIAL

All-inclusive ist angesagt

Sehr geehrte Leserinnen und Leser,
Business und Kommunikation sind zwei untrennbare Größen, denn ohne Informationsaustausch entstehen keine Geschäfte. Deshalb fordern Sie zurecht die Anbindung an ein Kommunikationsnetz durch funktionelle und hochverfügbare Lösungen.
Im Laufe von 25 Jahren hat sich *TDT* als klassischer Hardwareproduzent und Supportdienstleister für eigene Produkte einen ausgezeichneten Ruf aufgebaut, trotzdem werden wir unser Portfolio mit neuen Dienstleistungen erweitern. Ob für exklusive VPN-Lösungen, von der Beratung und Ausschreibungsunterstützung, bis zur komplett gemanagten Kundenlösung: Sie möchten eine Komplettlösung mit Entscheidungshilfen und einem kompetenten „Sorglos-Paket"?
Wie eine aufwändige Markt- und Kundenbefragung uns eindeutig bestätigte, fordern Sie neben einer exzellenten IT-Hardware auch einen auf Ihre Bedürfnisse abgestimmten Support zu einem angemessenen Preis. Die Umsetzung Ihrer Forderungen zeichnet sich klar durch die neuen *TDT*-Produkte ab. Die neue R500-Serie, die modulare Plattform M3000 und das Gateway für die „Zentrale Seite" G5000 sind die optimierte Hardware für sichere, zuverlässige VPN-Verbindungen über jedes Backbone, natürlich auch über das öffentliche Internet. Die fehlenden Komponenten für eine zuverlässige Komplettlösung ist das Stück Kupfer. Genau diese Komponente wird *TDT* künftig zusätzlich bereitstellen. Das Produktmanagement setzt dabei auf starke Partner und Carrier-unabhängige Konzepte. Dieses Vorgehen garantiert die zur Zeit günstigste verfügbare Lösung am Markt. Informieren Sie sich bei *TDT*.

Herzlichst: Ihr Wolfgang Rau
Produktmanagement

Virtual Private Network (VPN)

Teil 3

Lösungen mit IPSec – ein investitionssicheres System zur Realisierung von kostengünstigen, flexiblen Unternehmensnetzen

Safety First, Handling Third

„Virtual Private Network“ (VPN) Lösungen mit IPSec – ein investitionssicheres System zur Realisierung von kostengünstigen, flexiblen Unternehmensnetzen

1. **VPN Einteilung, Anforderungen und Einsparungspotentiale**
2. **Vorteile von IPSec gegenüber anderen VPN-Protokollen**
3. **IPSec im Detail, Bausteine und Verfahren**
4. **Manuelle Konfiguration von IPSec**
5. **Automatische Verteilung von Sicherheitsvereinbarungen und Schlüssel mit IKE**
6. **IPSec und NAT**
7. **IPSec im PKI (Personal Key Infrastruktur) Umfeld**

Im dritten Teil werden Gesichtspunkte zur Handhabung von VPNs mit IPSec beleuchtet (Punkt 4 und 5)

4. Manuelle Konfiguration von IPSec

Bei einer manuellen Konfiguration müssen alle Informationen auf beiden Seiten der Security Gateways eingetragen werden. Die Informationen werden unter den Security Parameter Index (SPI) hinterlegt. Für eine bidirektionale Verbindung sind auf jeder Seite zwei statische Security Associations (SAs) nötig, eine für den eingehenden und eine für den abgehenden Datenverkehr. Dieses Vorgehen ist sehr aufwändig. Es müssen folgende Parameter hinterlegt werden:

- Verschlüsselungsalgorithmus
- Hashalgorithmus
- Verschlüsselungs-Key
- Authentifizierungs-Key

Folgende IPSec-Features können nicht benutzt werden:

- Replay-Schutz (Überlaufen der Packet-Counter)
- Perfect Forward Secrecy (Statische Schlüssel)

Das „Internet Key Exchange“ (IKE) Protokoll beseitigt diese Nachteile und regelt die automatische Generierung von SA und Schlüsselmaterial.

5. Automatische Verteilung von Sicherheitsvereinbarungen und Schlüssel mit IKE

Der Unterschied zur Manuellen Konfiguration ist nicht nur die automatische Generierung und Verteilung des Schlüsselmaterials für die geforderten kryptongrafischen Methoden, sondern auch die automatische Etablierung und das Löschen von SA. Damit können SA vor einem Überlauf des Replay–Schutzes neu generiert werden. Die Datenverbindung wechselt auf die neu generierte SA und der Packet-Counter beginnt wieder mit 0. Eine SA wird nach Ablauf einer zu vereinbarenden Datenmenge oder Zeitdauer gelöscht. Zum Verbindungsaufbau via IKE-Protokoll **müssen** folgende Informationen ausgetauscht werden:

- Authentifizierungsmethode: *Pre-Shared-Key*
- Verschlüsselungsalgorithmus: *DES*
- Hashalgorithmus: *SHA-1, MD5*
- Diffie-Hellmann-Gruppe (Oakley-Gruppe): *1*

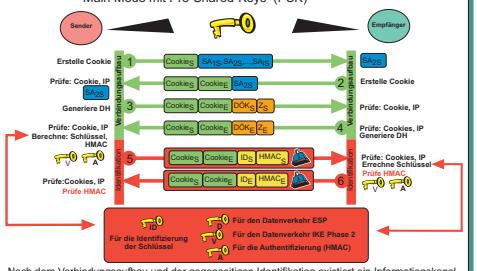
Die oben aufgeführten Größen müssen nach einer laut RFC [12] implementiert werden. Weitere Methoden sollten implementiert werden, z.B:

- Authentifizierung mit Signaturen [15], Public-Keys, Verbesserte Methode mit Public-Keys
- Hashalgorithmus mit Tiger
- Verschlüsselungsalgorithmus mit 3DES
- Diffie-Hellmann-Gruppe 2

Natürlich gibt es heute bessere Methoden als in [12] gefordert. Vor kurzem hat das NIST den neuen Advanced Encryption Standard (AES) festgelegt mit dem Algorithmus von J. Daemen and V. Rijmen. Dieser symmetrische Verschlüsselungsalgorithmus löst den veralteten 3DES (Data Encryption Standard) ab und ist von der Verschlüsselungsleistung bei einer vergleichbaren Sicherheit mehr als doppelt so schnell. Folgende Varianten gibt es: AES-128, AES-192, und AES-256 mit 128, 192 und 256 Schlüssel. Der SHA-1 Hash-Algorithmus verwandelt Daten um einiges schneller in eine Zufallszahl als MD-5 Algorithmus. Die Oakley-Gruppe 1 erzeugt ein 768 Bit langes asymmetrisches Schlüsselpärchen, die Schlüssel von Oakley-Gruppe 2 sind 1024 Bit lang und umso sicherer. Dazu ist zu beachten, dass die asymmetrische Verschlüsselung mit einem längeren Schlüssel auch langsamer ist.

Um die Auswirkung diese Einstellungen zu verstehen, muss man sich den Verbindungsaufbau mit IKE (Internet Key Exchange) im Detail ansehen.

Abb. 1: IKE Verbindungsaufbau Phase 1
Main Mode mit Pre-Shared-Keys (PSK)

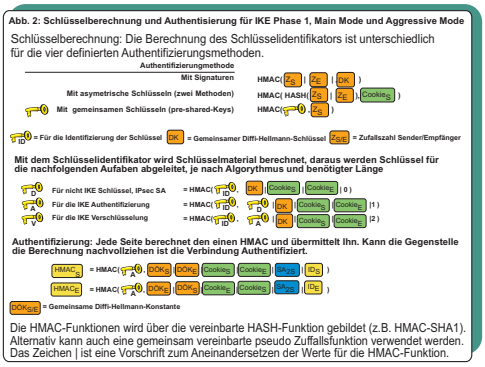


Nach dem Verbindungsaufbau und der gegenseitigen Identifikation existiert ein Informationskanal. In Phase 2 werden eine oder mehrere SA für die Datenverbindung ausgehandelt. Der Informationskanal ist bidirektional und kann zu mehreren Gegenstellen existieren. Zur Identifikation der Verbindung dient die IP-Adresse der Gegenseite und beide Cookies.

Der Verbindungsaufbau mit IKE erfolgt nach dem “Internet Security Association and Key Management Protocol“ (ISAKMP) [11] in zwei Phasen. In Phase 1 wird eine sichere Verbindung über den UDP Pot 500 aufgebaut. Nach erfolgreichem Abschluss von Phase 1 existiert auf beiden Seiten eine sogenannte ISAKMP SA. Diese ISAKMP SA besitzt auf beiden Seiten den gleichen SPI und wird von beiden Seiten zur Aushandlung zukünftiger SA für den Datenverkehr in Phase 2 benutzt. Die Authentifizierung in Phase 1 kann in Main- oder Aggressiv-Mode durchgeführt werden.

Beispielhaft ist in Abb.1 der automatische Verbindungsaufbau mit IKE. Die Authentifizierung erfolgt mit Pre-Shared Keys. Die Cookies werden im ISAKMP Header übertragen und dienen beiden Seiten zusammen mit der IP-Adresse zur Identifikation der Verbindung, bis die ISAKMP SA ausgehandelt ist und der SPI diesen Zweck für Phase 2, den sogenannten Quick-Mode, übernimmt. Damit können Verbindungswünsche von unterschiedlichen Gegenstellen zugeordnet werden bis zur Etablierung der ISAKMP SA und den zugehörigen SPI. Zugleich ist dies der kritische Punkt beim Verbindungsaufbau.

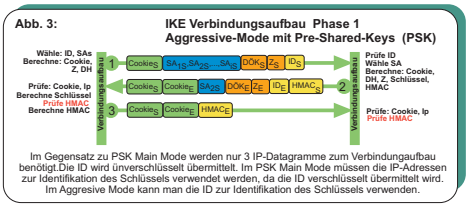
Abb. 2: Schlüsselberechnung und Authentisierung für IKE Phase 1, Main Mode und Aggressive Mode



Die HMAC-Funktionen wird über die vereinbarte HASH-Funktion gebildet (z.B. HMAC-SHA1). Alternativ kann auch eine gemeinsam vereinbarte pseudo Zuffallsfunktion verwendet werden. Das Zeichen | ist eine Vorschrift zum Aneinandersetzen der Werte für die HMAC-Funktion.

Bei einem „Denial of Service“ Angriff versuchen viele Angreifer mit einer Flut von Verbindungswünschen den IKE-Dienst auszuschalten. Durch die Cookies kann das Gateway ungültige Datenpakete ignorieren bevor der Austauch des Datenpaketes 4 stattfindet. Das Datenpaket 4 erfordert CPU-Zeit um Diffie-Hellman [DH] Konstanten zu berechnen oder bei anderen Authentifizierungsmethoden Verschlüsselungen durchzuführen. Die Angreifer müssen also in die Vorleistung gehen. Mit Datenpaket 5 authentifiziert sich der Sender, mit Packet 6 der Empfänger, damit steht die ISAKMP SA mit zugehöriger SPI. Das Datenpaket wird mit dem D-Schlüssel verschlüsselt, damit kann die Identität des Senders nicht von einem Schnüffler (Sniffer) gelesen werden. Dieser sichere Datenkanal wird in Phase 2 zum Aufbau der SA für den Datenverkehr benutzt. Bei einer intelligenten Konfiguration der Parameter für die Lebensdauer der ISAKMP SA können mehrere SA für die Verschlüsselung des Datenkanals übertragen werden, auch kann ein Dynamisches Re-Keying für den Datenverkehr durchgeführt werden. Dieses Vorgehen minimiert Verbindungszeiten wenn z.B. eine SA für den Datenverkehr abgelaufen ist. In Abbildung 2

Abb. 3: IKE Verbindungsaufbau Phase 1
Aggressive-Mode mit Pre-Shared-Keys (PSK)

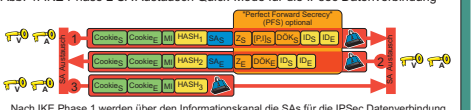


Im Gegensatz zu PSK Main Mode werden nur 3 IP-Datagramme zum Verbindungaufbau benötigt.Die ID wird unverschlüsselt übermittelt. Im PSK Main Mode müssen die IP-Adressen zur Identifikation des Schlüssels verwendet werden, da die ID verschlüsselt übermittelt wird. Im Aggresive Mode kann man die ID zur Identifikation des Schlüssels verwenden.

sind die Verfahren zur Berechnung des Schlüsselmaterials dargestellt. Phase 1 ist entscheidend für die Sicherheit der Datenübertragung. Um die Sicherheit zu beurteilen muss man wissen welche Größen in die Berechnung des Schlüsselmaterials eingehen, diese gilt es besonders zu schützen. In Abbildung 2 ist die Berechnung gezeigt.

Man sieht, dass für die Authentifizierung nach allen 4 Methoden von beiden Partnern der $HMAC_{S/E}$ nachvollzogen werden muss. Dies ist ein mit Schlüssel A gebildeter Hash. In die Bildung dieses Fingerabdrucks gehen beide öffentliche Schlüssel nach DH ($DÖK_{S/E}$), die Cookies, die SA und die Kennung ($ID_{E/S}$) der Partner ein. Um diesen Hash nachvollziehen zu können benötigt man den D-Schlüssel, der aus dem ID-Schlüssel abgeleitet wird. In die Berechnung des ID-Schlüssels gehen in Summe bei allen 4 Methoden die Zufallszahlen $Z_{E/S}$, die öffentiche DH-Konstante (DÖK), das Sender Cookie und der Pre-Shared-Key ein. Um eine Beurteilung der Sicherheit durchführen zu können muss man die Übertragung dieser Daten beurteilen. Bei allen 4 Authentifizierungsverfahren werden die Cookies und die ISAKMP SA Vorschläge offen übertragen, es geht auch nicht anders. Es bleibt also zu überprüfen wie die Zufallszahlen, die DH-Parameter und die ID (Identifikation) bei der Übertragung geschützt werden.

Abb. 4: IKE Phase 2 SA Austausch Quick-Mode für die IPsec Datenverbindung



Nach IKE Phase 1 werden über den Informationskanal die SAs für die IPSec Datenverbindung vereinbart. Beide Seiten können mit den Austauch beginnen. Jede Seite übermittelt der Gegenstelle eine eindeutige SPI. Diese SPI wird in den IPSec Headern AH und ESP, im folgenden Datenverkehr übermittelt und dient der Gegenseite zu Identifikation der eben vereinbarten SA. Der Message Identifier MI kenzeichnet die jeweilige Session.

Damit kann eine Aussage über die Sicherheit der 8 Authentifizierungsmethoden a priori getroffen werden. Das ergibt eine Matrix von 8 Methoden und 3 Parameter. In Abbildung 3 ist IKE Phase 1 im Aggressive-Mode gezeigt. Wie man sieht werden alle Parameter für die Berechnung des Schlüsselmaterials offen übertragen.

In Tabelle 1 werden alle Kombinationen gegenübergestellt. Während bei den Authentifizierungsmethoden mit PSK und Signaturen der Aggressive-Mode bedenklich ist, ist er bei den beiden Methoden mit asymmetrischer Verschlüsselung gleichwertig. Die verbesserte Authentifizierungsmethode mit Public-Keys im Aggressive-Mode ist das sicherste und schnellste Verfahren für IKE Phase 1. Natürlich müssen beide Partner diese Methode unterstützen. Das ist jetzt genau der Punkt an dem Zertifikate ins Spiel kommen. Um die Daten des Partners lesen zu können, brauchen beide den öffentlichen Schlüssel der Gegenstelle. Diese Schlüssel werden in Zertifikaten hinterlegt. In diesen Zertifikaten ist zugleich die Identität des Besitzers eingetragen. Damit der Empfänger das richtige Zertifikat finden kann, sendet er einen Hash seines Zertifikats. Der Empfänger findet in seinem Zertifikatspeicher anhand dieses Fingerabdrucks das richtige Zertifikat, überprüft die Gültigkeit und entschlüsselt die Daten und umgekehrt, das war es. Bei der ordinären Public-Key-Methode sind dazu zwei asymmetrische Ver- und Entschlüsselungen notwendig. Beim verbesserten Public-Key Verfahren wird nur die Zufallszahl $Z_{E/S}$ asymmetrisch verschlüsselt, alle anderen Daten werden mit einem symmetrischen Verschlüsselungsverfahren übertragen. Der symmetrische Schlüssel wird aus der verschlüsselt übertragenen Zufallszahl und den Cookies errechnet, damit wird es schneller.

Tabelle 1:

	PSK		Signaturen		Public Key		Public Key Verbessert	
	Main Mode	Aggr. Mode	Main Mode	Aggr. Mode	Main Mode	Aggr. Mode	Main Mode	Aggr. Mode
$DH_{E/S}$	⊘	⊘	⊘	⊘	⊘	⊘	🔒	🔒
$ID_{E/S}$	🔒	⊘	🔒	⊘	🔒	🔒	🔒	🔒
$Z_{E/S}$	⊘	⊘	⊘	⊘	🔒	🔒	🔒	🔒
$HASH_{E/S}$	🔒		✍🔒	✍	🔒	🔒	🔒	🔒

⊘ =Unverschlüsselt 🔒 =Verschlüsselt ✍ =Signiert

Damit haben wir jetzt IKE Phase 1 abgeschlossen. Es folgt Phase 2, der im Quick-Mode. Jetzt werden die SA für den Datenverkehr ausgetauscht, jeweils eine SA für die abgehenden und eine für die eingehenden Daten. Damit haben wir insgesamt auf jeder Seite drei gültige SA. Wird die ISAKMP SA ungültig, muss mit Phase 1 neu begonnen werden. Eine sinnvolle Konfiguration der Gültigkeitsparameter für die ISAKMP SA, Zeit oder Datenmenge wird empfohlen. Damit kann man unnötig lange Verbindungsaufbauzeiten vermeiden. Das besondere am Quick-Mode ist die „Perfect Forward Secrecy“ (PFS). Ohne PFS werden neue Schlüssel aus den Vorgängern abgeleitet. Mit PFS wird jedes Mal ein neuer Diffie-Hellman Austausch gestartet, damit können unabhängige Schlüssel generiert werden. Natürlich kostet das Rechenzeit. Die Entschlüsselung aufgezeichneter Daten ist dann jedoch erheblich schwerer.

Weitere Informationen zu diesem Thema können Sie auf der TDT-Internetseite (www.tdt.de) als PDF-Datei downloaden.

Neue T.D.T.-Entwicklungen

Serie M3000

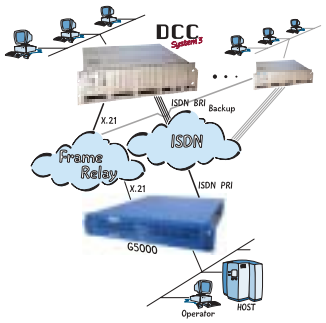
Die Serie M3000 - das neue Lego-System von *TDT* . Mit der neuen Serie M zielt *TDT* auf Firmen mit einem Gespür für eine investitionssichere, sich schnell amortisierende Anlage. Die Serie M dient zur Aufnahme von bis zu vier aktiven Kommunikations-Modulen. Damit kann sich der Kunde sein System anforderungsgerecht zusammenstellen und damit gezielt Kosten sparen. Die Module decken das Spektrum vom reinen ISDN-Router über DSL bis hin zum 2 Mbit/s Frame Relay-Anschluss ab. Weitere Module sind in der Planung. Das System ist erweiterbar, da neue Technik einfach durch den Einbau weiterer Module integriert werden kann. Motor dafür ist ein auf Linux basierendes Betriebssystem. Protokolle wie X.25, IP, IPSec usw. sind bereits integriert. Jedes aktive Kommunikations-Modul kann auch als Einzelgerät bezogen werden.

G5000

Deutsche Shell AG setzt auf die neue T.D.T.-Plattform G5000

Die Anforderung bestand darin, eine Telnet-Session hostseitig auch dann nicht abzubauen, wenn die WAN-Verbindung abbricht oder das Endgerät abgeschaltet wird. Ein Beenden der Telnet-Session, so die Forderung, darf nur durch einen Logoff am Host erfolgen. Ein unkontrollierter Abbruch hätte fatale Folgen. Steht die WAN-Verbindung wieder zur Verfügung, wird die Telnet-Session wieder auf dem gleichen Port fortgesetzt. Zudem ist es für den Administrator möglich, über einen Quereinstieg die Session ordnungsgemäß abzubauen. Neben einer klassischen Backup-Lösung, der Frame Relay-Anbindung mittels ISDN PRI, verfügt das Gateway über eine kundenspezifische Holdup-Funktion.

Die auf Kundenanforderung skalierbare Plattform für spezielle Anwendungen auf der Hostumgebung bietet erhebliche Vorteile: z.B. High Speed-Anbindungen mit Frame Relay, ISDN, PRI, X.25 und DSL, sowie Firewalling und IPSec Gateways mit bis zu 2.000 Tunnels.



GPRS-Lösungen

Lotto Hessen nutzt GPRS

Für Lotto Hessen stellt GPRS eine wichtige Möglichkeit dar, das Backup über ein alternatives Netz zu transportieren. Die Diskussion über Sicherheit fand rasch ein Ende, da *TDT* den Sicherheitsstandard IPSec einsetzt. Verschlüsselung (3DES, AES), Authentifizierung und Datenintegrität sind damit voll gewährleistet.

GPRS ist die Abkürzung für General Packet Radio Service und bietet GSM-Mobilfunknetzbetreibern erstmals die Möglichkeit, paketorientierte Datendienste anzubieten.

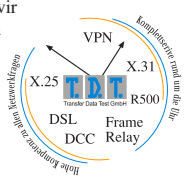
GPRS unterstützt sehr viele Datenübertragungsprotokolle, unter anderem IP und X.25. Somit kann der Mobilfunkteilnehmer mit fremden Datennetzen, wie z.B. das Internet oder firmeninterne Intranets, kommunizieren. GPRS öffnet die unendlichen Weiten des World Wide Web. Im Gegensatz zu den bisherigen GSM-Übertragungsverfahren wird bei GPRS nicht die Verbindungsdauer berechnet, sondern die tatsächlich übertragene Datenmenge. Man kann also online bleiben - solange keine Daten übertragen werden, fallen auch keine Mehrkosten für den Teilnehmer an.

GPRS ermöglicht es den Teilnehmern Daten mit öffentlichen Datennetzen auszutauschen. Um höhere Datenraten zu erzielen, können mehrere Zeitschlitze miteinander kombiniert werden, maximal acht. Pro Zeitschlitz lassen sich je nach Fehlerschutzmechanismen bis zu 20 kbit/s übertragen, wobei im Normalfall 14,4 kbit/s pro Zeitschlitz die Maximalrate ist, um zu hohe Bitfehlerraten zu vermeiden.

24-Stunden-Service

T.D.T. baut seine Service-Leistung aus

Der zuverlässige und schnelle *TDT*-Support kann ab sofort rund um die Uhr genutzt werden. Gerne unterbreiten wir für Ihre Konfiguration ein attraktives Angebot. Besuchen Sie uns auf der CeBIT, mailen Sie uns oder nutzen Sie die Antwortkarte. Wir reagieren prompt.



CeBIT mit neuen Akzenten

Investitionen, die sich jetzt lohnen

Mit einer noch nie dagewesenen Produktinnovation wird *TDT* seine Kunden in den kommenden Monaten und Jahren begleiten. VPN, IPSec und Linux sind die Zutaten, die wir seit geraumer Zeit erfolgreich mixen und Ihnen damit den Datentransfer nicht nur flexibler sondern auch günstiger ermöglichen werden. Die Lösungen haben es in sich und nutzen unter anderem konsequent die starken Seiten des Internets: VPN und IPSec. Im bewährten *TDT*-Stil sorgen wir dafür, dass die aktuellen Lösungen langfristig skalierbar sind und auf einer zukunftssicheren Plattform programmiert werden. So wichtig Internet künftig auch sein wird, so ernst nehmen wir die Probleme unserer Kunden, die ihre IT-Struktur mit vorhandener Technik und Geräten noch über längere Zeiträume nutzen möchten.

Denn seit nahezu 25 Jahren begleiten wir sie mit bewährten Entwicklungen und gerade die Anbindung von X.25-Lösungen an das IP-Netz ist eine Aufgabe, die untrennbar mit dem Namen *TDT* gekoppelt ist.

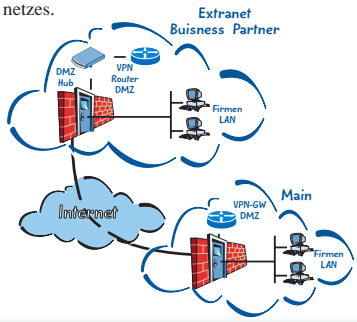
Dies gilt natürlich ebenso für unsere umfassenden und kompetenten Dienstleistungen, über die wir uns mit Ihnen unter anderem gerne auf unserem Stand in Halle 1 (Stand 8k4) unterhalten möchten. Wie echte bayerische Dienstleistung auf der CeBIT-Messe aussehen und sogar schmecken kann, erfahren Sie durch unsere Bewirtung mit original bayerischen Spezialitäten.

Herzlichst

Michael Pickhardt *Jürgen Büttner*

Kostenreduzierung durch Internet dank **smart**VPN

Unternehmen mit hohen Datentransferkosten, bedingt durch teure Netze, Standleitungen und Telefonverbindungen, können ihre Ausgaben mit der Internetlösung von I.T.E.N.O.S. und *TDT* erheblich reduzieren. Mit **smart**VPN stellen Ihnen die beiden Solution-Partner ein VPN Netz auf Basis des Internets mit geringen Transferkosten und erheblichem Mehrwert zur Verfügung. Die sichere Übertragung der Daten sowie deren Authentifizierung und Integrität wird durch den Einsatz der IPSec suite gewährleistet. Die Clients können über DSL oder ISDN an das **smart**VPN angebunden werden. Ein Backup über GPRS bietet maximale Verfügbarkeit des Datendienstes. Die Komplettlösung beinhaltet ein skalierbares Servicepaket einschließlich Netzwerkmanagement und Faultmanagement. Alles in allem reduziert **smart**VPN als Gesamtlösung die Transferkosten nachhaltig und erweitert gleichzeitig die Bandbreite und Verfügbarkeit Ihres Firmennetzes.



Neue ALPHA Com-Serie

Mit den neu entwickelten ALPHA-Geräten ist die Anbindung synchroner oder asynchroner Endgeräte an eine Ethernet/IP-Netzwerkumgebung möglich.

Die Schnittstellen
ALPHA Com$_{sync}$ ➢ serielle, asynchrone
ALPHA Com$_{async}$ ➢ synchrone (V.24)

Zudem erlaubt der ALPHA Com$_{async}$ kundenspezifische Protokolle zu implementieren, um verschiedensten Endgeräten den Zugang zu einem IP-Netz zu ermöglichen.

Die Einsatzmöglichkeiten sind unter anderem: Steuerung und Überwachung von industriellen Prozessen • Geldausgabeautomaten • Wetterstationen • POS-Terminal Cluster per LAN • Fernwartung und Gebührenerfassung • Erfassung von Verbrauchsdaten • Aufzugsysteme • Gebäudetechnik u.v.m.

25 Jahre T.D.T.

Am 2. Mai feiert *TDT* sein 25-jähriges Betriebsjubiläum und das gesamte Team ist stolz auf diesen Anlass. Es ist nicht nur für Kunden, sondern auch für die Mitarbeiter beruhigend zu wissen, dass *TDT* alle wichtigen IT-Entwicklungen rechtzeitig erkennt und die Firmenpolitik danach ausrichtet. Firmenchef Michael Pickhardt wiederum weiß um die Qualität und das Engagement seiner Mitarbeiter und so können sich alle schon mal auf eine Firmenfeier mit Event-Charakter freuen. Unter dem Motto: Der Alltag ist zukunftsorientiert, die Feste feiern wir wie vor 500 Jahren, wird *TDT* seinen Gästen ein Spektakel der besonderen Art bieten.

Ihr Votum: SWITCHED weiterhin in bewährter Form

Wir bedanken uns für die vielen Antworten, die wir zur Umfrage, ob SWITCHED künftig per eMail oder wie bisher in Papierform versendet werden soll, erhalten haben. Als kleines Dankeschön hat jeder Einsender den IP-Sec-Pocket-Guide erhalten.

Das Ergebnis der Zuschriften hat uns in der Beibehaltung der bisherigen Aufmachung und Zusammenstellung der Beiträge bestärkt. Rund 98 % der Einsender finden diese gelungen und nur 2 % halten diese für verbesserungsfähig. Der überwiegende Teil, 63 % der Einsender, liest alle Beiträge, 30 % lesen vorrangig die Seite 3 und 7 % beschränken sich nur auf die Titelstory. Wir wollten von Ihnen auch wissen, wie die SWITCHED künftig erscheinen soll. Der überwiegende Teil der Einsender bevorzugt nach wie vor die SWITCHED in Papierform, annähernd 73 %. Unsere Hauszeitschrift wird Ihnen daher auch in Zukunft im bekannten DIN-A3-Format per Post zugeschickt. Eine Zusendung per E-Mail (PDF-File) ist vorerst nicht geplant.

T.D.T.-Support und VPN

Zusätzlich führten wir eine telefonische Befragung unter unseren Kunden durch. Wir bedanken uns für die gute Zusammenarbeit und die freundliche Auskunft, die uns überwiegend erteilt wurde. In dieser Telefonaktion wurden zum einen die in unserer Datenbank gespeicherten Angaben mit den Kunden abgeglichen und ergänzt. Zum anderen wurden Fragen zu *TDT* allgemein und zu dem Thema VPN im Besonderen gestellt. So stellte sich beispielsweise heraus, dass 68 % der Befragten mit unserem Hotline-Service sehr zufrieden sind und nur 7 % Verbesserungswünsche äußerten. Eine große Anzahl von 25 % der Befragten hat diesen Service hingegen noch nie genutzt. Ist VPN ein Thema für unsere Kunden? Sind wir mit unseren Neuentwicklungen auf der richtigen Spur? Diese Fragen können wir nun mit JA beantworten. Annähernd 82 % der Befragten nutzen bereits das Internet zur Datenkommunikation. Dabei ist die Sicherheit der übertragenen Daten für rund 80 % sehr wichtig. VPN mit IPSec ist somit ein interessantes Thema für unsere Kunden, denn die Sicherheit des Datentransfers hat auch für uns oberste Priorität.

IMPRESSUM

Herausgeber	T.D.T. Transfer Data Test GmbH Siemensstraße 18 Gewerbegebiet Altheim 84051 Essenbach ☎ + 49 (0) 8703 9 29-100 🖷 + 49 (0) 8703 9 29-101 ✉ info@tdt.de www.tdt.de
Verantwortlich für den Inhalt	Michael Pickhardt, Geschäftsführer H. J. Büttner, Vertriebsleiter
Gesamtproduktion	Werbeagentur J. Wimmer Ulmenstraße 21 84051 Essenbach ☎ + 49 (0) 8703 913-60 🖷 + 49 (0) 8703 913-61 ✉ jwimmer@rze.de
Auflage	12.000 Exemplare
Ausgabe 1/2003	Auf Umweltpapier gedruckt