AUSGABE 1/2000

TDT Gateway

Wir stellen aus: Halle 1 • Stand 8k4
CeBIT HANNOVER 24.2.–1.3. 2000

T.D.T.® Transfer Data Test GmbH

SHELL

GATEWAY

Vieles im Leben kann man heute für selbstverständlich nehmen. Zum Beispiel, dass Energieträger wie Heizöl, Benzin oder Diesel zuverlässig in den Öltanks der Verkaufsstellen von Mineralölgesellschaften vorrätig sind und auf Anruf die geforderte Menge geliefert wird. Die Transportlogistik, vom Verlassen des Öls aus den Pipelines bis zur Lieferung zu den Tankstellen, in die Betriebe oder in den Haushalt erfordert eine zuverlässige und schnelle Datenkommunikation. Neue Dienste, wie E-Commerce oder Internet stellen die Konzerne vor innovative Aufgaben, die überwiegend in Zusammenarbeit mit hochkarätigen Entwicklungshäusern gelöst werden. Um eine über Jahre bewährte EDV-Infrastruktur an neue, schnellere Weitverkehrsdatennetze anzubinden setzt die Shell Direct Services GmbH unter anderem auf TDT-Lösungen für Frame Relay und auf ein neues Inhouse-Netz.

Was bis zum Jahr 1998 Shell Mineralölhandel und Heizungs-Dienst GmbH hieß, firmiert seitdem unter Shell Direct Services GmbH. Der neue Name ist Programm, das Produkt- und Servicespektrum wird kontinuierlich ausgebaut. Mit der Bezeichnung Shell Direct kommt zum Ausdruck, den Kunden immer vor Ort zur Verfügung zu stehen. Die konsequente Hinwendung zum kompetenten Dienstleister für die Energieversorgung mit Bulkprodukten (Heizöl, Diesel-, Ottokraftstoffe) zeigt sich in der Leistungspalette.Die Shell Direct-Organisation ist als Vertriebsorganisation der Deutschen Shell AG bundesweit an mehr als 50 Standorten tätig. Für die tägliche Arbeit sind über 500 Mitarbeiter “vernetzt”. Die eigene Tankwagenflotte, mit Zentraldisposition von Hamburg aus, sorgt für einen zuverlässigen Transport des schwarzen Goldes und allen weiteren Schell-Produkten in der Bundesrepublik. Neben dem Vertrieb von Heizöl, Diesel-, Ottokraft- und Schmierstoffen baute das Unternehmen ebenso systematisch die Betreuung von Heizungsanlagen aus. Dazu gehören in erster Linie der Heizungsdienst mit den Dienstleistungen: Wartung, Modernisierung und Reparatur sowie Wärme-Contracting.

Das Wärmelieferungskonzept der Shell

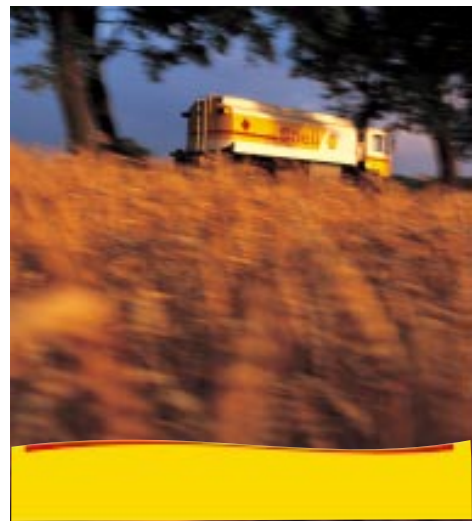
Eine von der Shell Direct Services GmbH geprägte Dienstleistung heißt Wärme-Contracting. Unter diesem “Zauberwort” bietet das Hamburger Unternehmen der Immobilien- und Baubranche die optimale Wärmeversorgung an. Das Ganze funktioniert so: Anstelle des Energieträgers (z. B. Heizöl oder Erdgas) wird dem Unternehmen oder dem Verbraucher die benötigte Wärme zur Verfügung gestellt. Um die Bereitstellung braucht sich der Kunde also nicht kümmern. Als Wärme-Contractor mietet Shell Direct den Heizraum, bringt die Heizstation auf den neuesten wirtschaftlichen Stand und stellt die dem Bedarf des Gebäudes genau angepasste Wärmeenergie zur Verfügung. Neben hohem Heizkomfort werden zusätzlich Emissionen reduziert und die Umwelt weniger belastet. Um die Finanzierung braucht sich der Kunde ebenfalls nicht zu kümmern, auch diese wird durch Shell Direct Services abgewickelt. Der Kunde zahlt nur einen vertraglich festgelegten monatlichen Wärmepreis.

Shell-Schmierstoffe

Absolute Zuverlässigkeit und Sicherheit kennzeichnen Schmierstoffe von Shell. Mit mehr als 650 Sorten, die im Werk Grasbrook hergestellt werden, bietet der Global Player ein Produktprogramm, das keine Wünsche offen lässt. Die Arbeit in Forschungszentren wie dem PAE-Labor in Hamburg bildet dafür eine wesentliche Grundlage. Ein integriertes QHSE-System (Quality, Health, Safety, Environment) setzt diesen Gedanken von der Forschung über die Produktion bis zur Auslieferung in die Tat um.

Shell-Kraftstoffe

Speziell für den gewerblichen Bedarf ist ein hochwertiger Dieselkraftstoff entwickelt worden. Längerfristige Vereinbarungen über die Lieferung von Heizöl und Kraftstoffen werden von den Shell Direct Services-Vertretungen vor Ort abgeschlossen.



Das Shell Betriebstankstellen-Konzept

wurde für Unternehmen mit einer großen Firmenfahrzeugflotte konzipiert. So übernimmt Shell Direct etwa die gesamte Planung, Installation und Belieferung. Die umweltgerechte und leicht zu bedienende Anlage wird mit dem Tankkartensystem verwaltet. Dadurch entsteht eine deutliche Kostentransparenz bei den Abrechnungen und mit Hilfe der Fuhrparkmanagement-Software wird der optimale individuelle Zuschnitt erreicht. Ein Optimum an Rentabilität ist die logische Folge. Mit der euroShell Service-Card können alle gespeicherten Informationen auf einen PC übertragen und zur Entlastung der Verwaltung ausgewertet werden. Alle Kartenbenutzer haben hier einen besonderen Vorteil: Die Software koppelt die Daten der Betriebstankstelle mit unterwegs erfolgten Tankfüllungen. So erhält das Unternehmen die besten Voraussetzungen für mehr Kostentransparenz und wirtschaftlicheren Einsatz der Fahrzeugflotte.
Die EDV-Abteilung in Hamburg koordiniert all diese Leistungen und hält die Daten für die betreffenden Niederlassungen im zentralen Rechenzentrum bereit. Sämtliche spezifischen Programme werden in der Hansestadt konzipiert, mit den Systemlieferanten entwickelt und gepflegt. So ist es nur logisch, dass zwar die Art der WAN-Anbindung den neuen Erfordernissen angepasst werden muss, die EDV-Architektur in der Zentrale davon aber unangetastet bleiben soll. Zu komplex sind die Rechenoperationen und die spezifischen Programme dafür. Die Kosten für das Umschreiben der Software und das Aufstellen einer neuen Hardware würde in keinem vernünftigen Verhältnis zu den Einsparungen stehen.
In einer Prioritätenliste wurde unter anderem die Vorgehensweise für folgende Ziele definiert: Vereinheitlichung der DFÜ-Lines durch die Installation einer neuen einheitlichen Netzwerktopologie. Die Fehlerminimierung soll dadurch erheblich reduziert und die Stabilität des Netzes gewährleistet werden. Der Einsatz auf in sich abgestimmte Komponenten bei der Datenüber-

TDT-Innovationen

- ***Handheld Desk*** mit TA und TDT-Software im Internet
- ***ALPHA-Router*** der guenstige Router mit 2 ISDN-Anschluessen
- ***Neue Functional Group im DCC System 3*** erweitert die Funktionalitaet erheblich
- ***NetMACS 3*** jetzt mehrplatzfaehig
- ***Micro TA*** fuer IP-Anwendungen

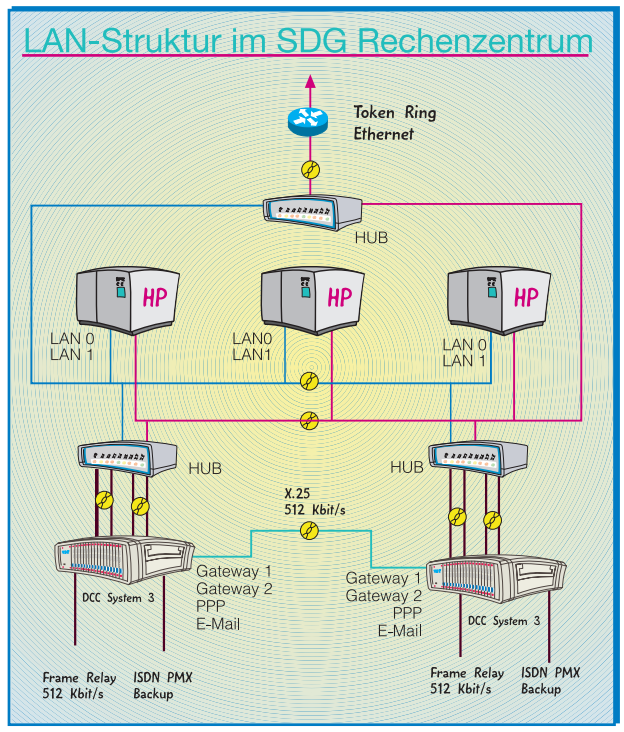
tragung beseitigt den “Wildwuchs”, der sich im Laufe von über 10 Jahren eingeschlichen hat. Die Redundanz wesentlicher Baugruppen von einem flexiblen Lieferanten sollten die Ausfallsicherheit des Netzes gewährleisten. Physikalische Netzstörungen müssen durch ein Backupkonzept überbrückt werden. Einig war man sich, dass das erhöhte Informationsbedürfnis innerhalb der SDG-Organisation (E-Mail /Intranet/Internet/E-Commerce etc.) so schnell wie möglich realisiert werden sollte.

Für das Projekt wurde neben der DeTeSystem, einer Tochter der Telekom, auch *TDT* ausgewählt, zumal Shell mit den seit 1988 installierten DCCs bisher die besten Erfahrungen gemacht hat. Die Aufgabe lautete, auf einen einfachen Nenner gebracht, das bisherige DatexP-Netz und die zahlreichen Modemdirektverbindungen durch ein Frame Relay-Netz zu ersetzen. Neben einer neuen WAN-Struktur implementierten die *TDT*-Entwickler ein völlig neues LAN-Konzept für das HeadOffice. Wichtigste Änderung: Die Zentralrechner sollen die Sessions nicht mehr über V.24 aufbauen, sondern die vorhandenen Ethernetschnittstellen nutzen. Die Priorität für die Shell-Niederlassungen lautete: Die HP-Terminals ohne eigene Intelligenz, die sich bisher über X.25 an die Zentrale anbinden ließen, werden sukzessive aus dem Betrieb genommen. Die Niederlassungen im Bundesgebiet haben in den letzten Jahren gewaltig aufgerüstet, um beim Kunden vor Ort unmittelbar reagieren zu können. PCs übernehmen immer mehr Aufgaben, die bisher vom Zentralrechner erledigt werden mussten. Die Devise lautete: Weg von einer reinen Terminalanwendung und hin zur strukturierten Vernetzung der PCs in den Niederlassungen. Zu sehr sind die Anforderungen in den Außenstellen gewachsen. In den größeren Niederlassungen konnten *TDT*-Mitarbeiter bis zu 20 PC-Arbeitsplätze vernetzen. Für die Anbindung nach Hamburg über das Frame Relay-Netz sorgen je nach Größe der Shell-Außenstellen die bewährten *TDT*-Geräte wie der SinglePAD 3 oder DCC System 3, die alle mit ISDN-Ports für ein sicheres Backup ausgestattet sind. Im Zuge der Umrüstung übernehmen *TDT*-Techniker das Einrichten der PC-Komponenten - dazu gehört auch die Adressierung der IP-Adressen der einzelnen Rechner und das Einstellen der Mailfunktionen. Damit die unter Windows 95/98 laufenden PCs das Windows-PPP-Protokoll für den Datenaustausch nutzen können, sind sie mit einer zusätzlichen Emulation (Reflection) ausgerüstet worden. Dadurch entfällt der Kauf von zusätzlichen Netzwerkkarten. Ausschließlich die NT-Rechner arbeiten mit einer LAN-Netzwerkkarte. Für die Verbindung zu den DCCs oder SinglePADs genügt im allgemeinen die COM-Port(V.24)-Schnittstelle. Mit der Konfiguration des Routings und mit Testübertragungen schließt das Team aus dem niederbayerischen Essenbach die Anbindung der jeweiligen Außenstelle an die Hamburger Zentrale via Frame Relay ab.

Einer der entscheidenden Gründe für den Einsatz der *TDT*-Geräte sind die integrierten Backupmöglichkeiten der niederbayerischen Router. Die Datensicherheit bei der Übertragung ist also gewährleistet. Der gordische Knoten den *TDT* in der Hamburger Zentrale zu lösen hatte, forderte den ganzen Erfindungsreichtum der Software-Entwickler. Die über das Frame Relay-Netz ankommenden TCP/IP-Daten werden im DCC System 3 über ein Gateway und anschließend über PPP an die Zentralrechner weitergeleitet. Die HP-Rechner kommunizieren über die Ethernetschnittstelle mit den PCs bzw. mit den DCCs von *TDT*. Eine Holdup-Funktion gewährleistet bei der neuen Lösung, dass eine bestehende Telnet-Session rechnerseitig nicht abgebaut wird, auch wenn die WAN-Verbindung nicht mehr aufrecht gehalten werden kann bzw. nicht mehr verfügbar ist. Selbst ein Ausschalten des Endgerätes darf nicht zum Beenden der Telnet-Session führen. Ein Beenden der Verbindung darf nur durch ein Logout des Hosts eingeleitet werden, da ein unangemeldeter plötzlicher Interrupt für die Zentralrechner fatale Folgen haben könnte. Bei Wiederverfügbarkeit des WAN-Netzes wird die Telnet-Session auf dem gleichen TCP-Port fortgeführt. Dadurch haben die *TDT*-Entwickler erreicht, dass die bewährten X.25/X.3-Implementierungsfunktionen auch unter TCP/IP funktionieren.

Da die Modernisierung des Netzes im ganzen Bundesgebiet nicht parallel durchgeführt werden kann, bzw. kleinere Niederlassungen auch noch mit “dummen” Terminals arbeiten, werden die asynchronen X.3-Daten im DCC einfach in IP umgesetzt. Über eine Telnet-Session, die vom DCC auf einem Server eröffnet wird, findet die Übertragung statt.
Für den Fall der Fälle, dass die WAN-Verbindung nicht mehr steht bzw. nicht mehr verfügbar ist und der Anwender seine Telnet-Session nicht selber beendet, übernimmt der Help Desk (Operator), über V.24 mit den Zentralrechnern verbunden, die Kontrolle dieser Session und beendet sie ordnungsgemäß. Den Alarm erhält er vom DCC System 3.
Nach den ersten erfolgreichen Tests läuft seit Ende 1999 der IP-Router im DCC System 3 erfolgreich in der Hamburger Zentrale. Parallel dazu ist die Neustrukturierung der Niederlassungen in vollem Gange. Das gesteckte Ziel, mit einer schnelleren und kostengünstigeren WAN-Verbindung die Kosten zu senken und die Reaktionszeit zu verkürzen, ist nach einer ersten Recherche erreicht. Die optimierte EDV- und Telekommunikationsstruktur mit ihrer WAN-Plattform ermöglicht neue Leistungen zu installieren, zum Beispiel Voice over Frame Relay. Das Frame Relay-Netz und die *TDT*-Geräte sind für die Übertragung größerer Datenmengen prädestiniert. Die Bandbreite kann per Software erweitert werden - die Commit Information Rate wird nach Bedarf einfach erhöht.
Als nächste wichtige Maßnahme in Hamburg ist die Anbindung eines UNIX lp-Systems an Remote-Drucker geplant. Der modulare Aufbau des *TDT*-Paradepferdes erlaubt die Ansteuerung eines jeden Remote-Druckers über eine definierte IP-Adresse. Das alternative Routing sorgt dafür, dass die IP-Adresse in jedem Fall zu der Zieladresse gelangt.

Darüber hinaus kann die Shell Direct Services GmbH als Tochter der Deutschen Shell AG auf die Unterstützung und Professionalität eines der größten Unternehmen der Welt zählen. Die langjährigen Erfahrungen finden in der Hamburger Zentrale Eingang und fließen in die tägliche Arbeit ein. Die Telekommunikationsübertragung, die in vielen wichtigen Bereichen mit *TDT*-Komponenten ausgestattet ist, trägt dazu bei, Informationen und Know-how in allen Bereichen des Unternehmens einschließlich der Niederlassungen gewinnbringend einzusetzen.



Kontaktadresse:
SHELL DIRECT, HAMBURG, KARSTEN MERGET
email: Karsten.K.Merget@ope.shell.com
Tel.: +49 (040) 6324 5230
Fax: +49 (040) 6324 6769

EDITORIAL

Sehr geehrte Leserinnen und Leser

Wie war das eigentlich am Tag nach der Jahrtausendwende? Haben Sie Ihre PCs hochgefahren, um die Funktionalität der Programme zu prüfen? Der in vielen Beiträgen hochstilisierte EDV-Crash zum Jahrtausendwechsel blieb einfach aus. *TDT* hat sich an solchen Spekulationen nicht beteiligt. Bereits in der letzten Switched-Ausgabe 1999 wurde darauf hingewiesen, dass es zum Jahrtausendwechsel für *TDT*-Kunden keinen Grund zur Sorge gibt. Unsere Kunden konnten beruhigt ohne teure Wartungs- und Serviceverträge die neue Arbeitswoche abwarten. Die wenigen Anrufe am 1. Januar hatten alle den gleichen Inhalt: „Ein gutes neues Jahr und auf eine weitere erfolgreiche Zusammenarbeit.”
Den zweiten Teil des Anrufes greift ein Software-Entwickler natürlich gerne auf, denn eine erfolgreiche Zusammenarbeit beruht neben zuverlässigen Hardware-Komponenten auch immer auf einer maßgeschneiderten Software. Und dafür ist unser Unternehmen prädestiniert, zumal beide Bereiche im Hause angesiedelt sind. Der Informationsfluss passiert bei *TDT* praktisch im Zimmer nebenan, der Blickwinkel für angedachte Lösungen erweitert sich. So werden wir künftig neben der reinen Datenübermittlung Anwendungen forcieren, bei denen es notwendig ist, Bild oder Sprache digital zu übermitteln. Es gibt davon so viele wie die sprichwörtlichen Sandkörner in der Wüste. Denken Sie mal darüber nach, vielleicht benötigen auch Sie in Ihrem Verantwortungsbereich die beschriebenen Ansatzpunkte. Stellvertretend für alle *TDT*-Entwickler kann ich Ihnen versichern, dass wir alle denkbaren Visionen aufgreifen und nach praktikablen Lösungen suchen.

Ihr
Helge Mader

kryptographie

TEIL 1

9 Z A 4 A S 1 G W 7 L P 8 U M 2 G K

Eine kleine Einführung in Kryptographie

Im Laufe der Geschichte hat die Menschheit immer wieder versucht ihre Gedanken, Handlungen und Absichten vor anderen zu verstecken. Die Menschen schrieben Codes, sprachen eigenartige Sprachen und erfanden mechanische Apparaturen, um eine Nachricht in einer zweiten zu verstecken, immer zu dem Zweck Informationen vom Zugriff Unberechtigter zu verbergen. Im Zeitalter des Internets und den damit verbundenen Diensten wie z.B. das Homebanking oder E-Commerce stieg das Bedürfnis der Menschen nach dem Verstecken von persönlichen oder kommerziellen Daten überproportional an. Noch nie gab es ein so riesiges Verlangen nach Verschlüsselungsmethoden die von einer so breiten Masse gefordert wird wie heute. Kryptographie hat eine noch nie dagewesene Bedeutung erlangt.

Etwas Geschichte

Krieg war immer ein Katalysator für das Vorantreiben von Entwicklungsaktivitäten in allen Wissenschaftsbereichen. Dies traf insbesondere auf die Entwicklung der Kryptographie zu. Das Wissen über feindliche Absichten war oft kriegsentscheidend. Die Deutschen hatten z.B. im Zweiten Weltkrieg eine Krypto-Maschine mit dem Namen Enigma. Diese bestand aus einer Anzahl von beweglichen Rädern die benutzt wurden, um Nachrichten zu verschlüsseln und zu entschlüsseln. Dabei wurde z.B. mit einem Rad der Buchstabe „F“ dem Buchstaben „N“ zugeordnet, mit einem weiteren Rad der Buchstabe „N“ dem Buchstaben „L“ usw. Je mehr Räder verwendet wurden, um so aufwendiger war es die Nachricht zu entschlüsseln. So komplex Enigma auch war, die Alliierten schafften es den Mechanismus zu knacken und trugen allein dadurch zu einer erheblichen Verkürzung des Krieges bei. Aber selbst im alten Rom benutzte bereits Julius Caesar einen Verschlüsselungs-Mechanismus, um Nachrichten während einer Schlacht mit seinen Feldherren auszutauschen. Die Methode war weitaus weniger komplex, etwa vergleichbar mit nur einem Rad der Enigma-Maschine.

Das 20. Jahrhundert läutete eine total neue Aera der Kryptographie ein. Plötzlich war es durch den Einsatz von Elektronenrechnern möglich hochkomplexe Kryptoalgorithmen zu verwenden, und das Entschlüsseln der oben genannten Methoden wurde zum Kinderspiel. Die Folge war ein dramatischer Fortschritt in der Entwicklung der Kryptographie bis zum heutigen Tag.

Die Enigma

Moderne Kryptographie

Computer wurden auf mathematischer Basis entwickelt, d. h. ein Computer kann nicht raten oder von einer fest vorgegebenen Route abweichen. Ein Computer vollzieht nicht mehr und nicht weniger als das was ihm durch ein mathematisches Regelwerk vorgegeben wird. Eine künstliche Intelligenz wäre, von diesen Regeln abzuweichen. Der eigentliche Kernpunkt des Computers ist der, dass er die vorgeschriebenen Rechenoperationen mit fast nicht vorstellbarer Geschwindigkeit ausführt. Nichts kann uns darauf vorbereiten was uns in Zukunft erwartet, und da die Komplexität der Sicherheits- und Kryptomechanismen mit der Geschwindigkeit der Computer wächst, haben wir nicht die geringste Vorstellung, welchen Schutz uns die gegenwärtigen Sicherheits- und Kryptomethoden in naher Zukunft bieten.

Knacken moderner Kryptographie

Es ist einleuchtend, dass die einfachste Methode einen passenden Schlüssel zu finden diejenige ist, einfach alle möglichen Schlüssel auszuprobieren. Es wird zudem klar warum die Geschwindigkeit eines Computers in der Kryptographie solch eine Bedeutung besitzt. Je schneller ein Computer die Arbeit zum Austesten eines Schlüssels verrichten kann, desto schneller kann ein passender Schlüssel gefunden werden. Dies nennt man in der Kryptographie eine „brute force attack“ (ein Vorgehen mit brachialer Gewalt), da der Rechner blind alle Möglichkeiten austestet. Für einen perfekten Kryptoalgorithmus wäre dies die einzig gangbare Methode, den passenden Schlüssel zu finden. Auf Grund der computertechnischen Erfordernisse ist die Zeit für eine „brute force attack“ stark von der Größe (Länge) des Schlüssels und von der angewandten Entschlüsselungs-Methode abhängig. Diese verliert allerdings an Aussagekraft, wenn man sich die symmetrische und asymmetrische Verschlüsselung betrachtet. Hier sind die Größen (Längen) der Schlüssel sehr unterschiedlich. Ein guter Schlüssel in der symmetrischen Verschlüsselung ist 128 Bits lang. Auf der anderen Seite ist ein schlechter oder schwacher Schlüssel für eine asymmetrische Verschlüsselung 512 Bits lang. Es wird klar, dass die Art der Verschlüsselung einen erheblichen Anteil hat, wenn man eine Aussage treffen will wie gut eine „sichere“ Nachricht verschlüsselt ist. Natürlich gibt es auch unterschiedliche Möglichkeiten eine verschlüsselte Nachricht zu „knacken“, die hier aber auf Grund ihrer Komplexität nicht weiter besprochen werden kann.

Grundsätzlich gibt es bei der Ver- und Entschlüsselung zwei Geschmacksrichtungen: symmetrische und asymmetrische. Beide haben ihr Für und Wider und beide werden gegenwärtig verwendet. Um den Unterschied zu verstehen vergleichen wir die Verschlüsselung einer Nachricht mit einem Schloss. Die Nachricht befindet sich auf einem Blatt Papier innerhalb einer Schachtel. Diese Schachtel ist mittels eines Schlüssels verschlossen. Im digitalen Sinne wäre ein Schlüssel eine Serie von Ziffern und nur die richtige Kombination der Ziffern ist in der Lage, die Nachricht zu entschlüsseln. Im Sinne der symmetrischen Verschlüsselung ist der Fall recht einfach. Man benutzt zum Öffnen der Box den gleichen Schlüssel den man auch zum Abschließen der Box benutzt hat. Im Sinne der asymmetrischen Verschlüsselung würde man zum Öffnen der Schachtel einen anderen Schlüssel verwenden als den zum Verschließen der Schachtel. Mit anderen Worten, es werden zwei unterschiedliche Schlüssel verwendet.

Im Folgenden soll eine kurze Vorstellung der bekannten Verschlüsselungsverfahren beschrieben werden:

Symmetrische Verfahren

Transpositions-Chiffren

Die Transpositions-Chiffren sind keine Codierungen, wie man sie sich üblicherweise vorstellt, jedoch spielen sie immer noch eine wichtige Rolle in der Kryptographie. Bei den Transpositions-Chiffren bleiben die zu verschlüsselnden „Buchstaben, was sie sind, sie bleiben aber nicht wo sie sind”. Es wird also lediglich die Reihenfolge der Buchstaben verändert. Eine Transpositions-Chiffre erhält man beispielsweise, indem man einen Text spaltenweise statt zeilenweise aufschreibt, dann aber zeilenweise übermittelt. Dem Empfänger müssen dann, quasi als Schlüssel, die Anzahl der Zeilen bekannt sein.

Beispiel: Aus „Dieser Text ist geheim“ wird durch Umwandlung mittels des beschriebenen Verfahrens und einer Zeilenanzahl von 5

D R I H
I T S E
E E T I
S X G M
E T E X

die auf den ersten Blick unlesbare Botschaft „DRIHITSEEETISXGMETEX“

Diese Art der Codierung wurde bereits in der Antike von den Griechen benutzt. Zum Übermitteln von Geheimbotschaften verwendete man eine sogenannte „Skytale“, einen Holzstab mit einem festgelegten Durchmesser, um den dann spiralförmig Pergamentstreifen gewickelt wurden, den der Sender dann von links nach rechts beschrieb. Die im Bild gezeigte Skytale würde dem oben beschriebenen Zeilen-/Spaltenverfahren entsprechen. Würde man den Pergament-streifen von oben nach unten lesen, erhielte man nur „ETEXSXGMITSEDRIH“, erst wenn er um eine Skytale mit gleichem Durchmesser gewickelt würde, könnte man den Text wieder lesen.

Dieses Verschlüsselungsverfahren ist allerdings nicht sehr sicher, da es durch simples Ausprobieren in relativ kurzer Zeit geknackt werden kann. Trotzdem spielen Transpositions-Chiffren auch in modernen Algorithmen eine Rolle, wo sie beispielsweise zum nochmaligen Verschlüsseln bereits mit anderen Methoden verschlüsselter Texte eingesetzt werden.

Das Gegenstück zu den Transpositions-Chiffren bilden die Substitutions-Chiffren, die im Folgenden vorgestellt werden.

Die monoalphabetische Substitution

Die monoalphabetische Substitution ist ebenfalls eines der einfachsten Verfahren, einen Text zu verschlüsseln. Wie der Name bereits ausdrückt, wird einfach jedem Buchstaben des Alphabets ein entsprechender Geheimbuchstabe zugeordnet. Dieser Geheimbuchstabe kann sich zum Beispiel aus einer Verschiebung des lateinischen Alphabets ergeben, er kann aber auch auf einer Geheimschrift mit völlig anderen Symbolen beruhen. Anders als bei den Transpositions-Chiffren bleibt also die Reihenfolge der Buchstaben erhalten, jedoch werden die Zeichen selbst verändert. Auch monoalphabetische Substitutionen wurden bereits in der Antike eingesetzt. Ein Beispiel für eine monoalphabetische Substitution ist beispielsweise der sogenannte „Caesar-Code“, der auf Julius Caesar zurückgeht. Das Geheimalphabet erhält man, indem man das Klartextalphabet um eine bestimmte Buchstabenanzahl verschiebt, also beispielsweise:

Klartext:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Geheimtext:

D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Der Schlüssel ist in diesem Falle der Anfangsbuchstabe des Geheimalphabets, also hier D. Eine andere, ebenfalls schon sehr alte Form der monoalphabetischen Substitution ist das „Atbash“. Bei diesem Verfahren wird das normale Alphabet einfach umgekehrt, d.h. aus A wird Z, aus B wird Y usw. Das Atbash-Verfahren ähnelt dem römischen Caesar-Code, ist aber jüdischen Ursprungs.

Es sind jedoch auch gänzlich andere monoalphabetische Zuordnungen denkbar. Man könnte ja einem Klartextbuchstaben jeden beliebigen anderen Buchstaben oder auch eine Ziffer oder ein geheimes Symbol zuordnen, solange dies eindeutig geschieht. Alle monoalphabetischen Substitutionen haben gemeinsam, dass sie auf äußerst einfache Art realisiert werden können. Monoalphabetische Substitutionen sind jedoch mit statistischen Verfahren ebenso einfach zu knacken, da jede Sprache eine charakteristische Buchstabenverteilung besitzt. Im Deutschen und im Englischen ist beispielsweise E der am häufigsten vorkommende Buchstabe, also wird im Geheimtext das am häufigsten vorkommende Symbol möglicherweise das E repräsentieren.

Die polyalphabetische Substitution

Die leichte Angreifbarkeit der monoalphabetischen Substitution führte dazu, dass man sich Gedanken machte, wie man die relativen Häufigkeiten der einzelnen Buchstaben im verschlüsselten Text verschleiern könnte, so daß der Angriff mittels Statistik erschwert wird.

Die homophone Chiffre

Ein erster Versuch war die sogenannte homophone Chiffrierung. Hierbei wird häufig vorkommenden Buchstaben nicht ein geheimes Äquivalent, sondern mehrere Geheimzeichen zugeordnet. Da beispielsweise das „E” ein sehr häufig vorkommender Buchstabe ist, wird man ihm z. B. 10 verschiedene Geheimzeichen zuordnen, während dem „L” z. B. nur 3 oder dem „X” nur ein Zeichen zugeordnet ist. Da die umgekehrte Zuordnung jedoch nach wie vor eindeutig sein muss, d.h. ein Zeichen des Geheimtextes darf nur genau eine Bedeutung haben, während ein Klartextzeichen natürlich mehrere zugeordnete Zeichen hat, können die Zeichen des Geheimtextes natürlich keine Buchstaben sein, es würden sich beispielsweise Zahlen oder Buchstabenpaare anbieten. Zwar verschleiert dieses Verfahren die Buchstabenhäufigkeiten ziemlich gut, allerdings ist eine Kryptoanalyse („Knacken“ des Codes) auch hier noch recht einfach möglich

MESSE-HIGHLIGHTS

ALPHA-Router

IP-Provider und Netzwerkspezialisten können auf der Messe am *TDT*-Stand die jüngste Entwicklung live erleben. Der ALPHA-Router, preismäßig liegt er unter 1.000 DM, wartet mit Features auf, die sonst nur im oberen Preissegment angesiedelt sind.
Der ALPHA-Router wurde zur WAN-Anbindung von "local area networks" (LAN) konzipiert. Mit 2 ISDN(S_0)-Schnittstellen), einer 10/100 BASE T Ethernet-Schnittstelle, zwei asynchronen V.24-Schnittstellen und einer synchronen X.21-Schnittstelle können fast alle LAN-Topologien über ein WAN verbunden werden. Alle bestehenden TDT-Protokolle und IP Router System 3-Komponenten sind im ALPHA-Router verfügbar und können vom Anwender beliebig kombiniert werden. Netzwerkmanagementfähigkeit, automatischer Backup und Fallback sind typische *TDT*-Merkmale, deren Nutzen für viele Entscheidungsträger wichtige Kriterien sind. Der ALPHA-Router läßt sich sowohl über das Netz, wie auch über einen lokalen Konfigurationsport in Betrieb nehmen.

World Wide Web für Windows CE Handheld Computer

So nützlich die PCs im Kleinstformat auch sind, ein Manko stellt sich gerade im Zeitalter des Internets heraus: Die User können im Regelfall das Internet nur über ein Modem erreichen. Was aber, wenn bereits ein ISDN-Anschluß zur Verfügung steht? Der Markt bietet zwar PCMCI-Karten (PC-Cards) in allen denkbaren Variationen - zum einen sind diese Steckkarten jedoch relativ teuer und zum anderen ist die Capi-Software für die Windows CE-Version dafür noch nicht verfügbar. Mit dem TA von *TDT* ist die Lösung jetzt gefunden. Die *TDT*-Software-Schmiede entwickelte für die TA-Serie eine spezielle Software, die den Zugang über jede ISDN-Leitung in das World Wide Web erlaubt. Die TAs ermöglichen allen Geräten, die über eine serielle Schnittstelle PPP unterstützen, den Zugang zum Internet. Die Innovation wird auf dem *TDT*-Stand in Halle 1 Stand 8k4 vorgestellt.

Neue FG - im DCC System 3 Ethernet I

Die Leistungsfähigkeit des DCC System 3 wird kontinuierlich erweitert. Rechtzeitig zur größten Computermesse der Welt können die *TDT*-Entwickler die Functional Group „**Ethernet I**" präsentieren. Damit können ab sofort viele der zur Verfügung stehenden *TDT* Functional Groups in die IP-Welt vermittelt werden.
Mit der „**Ethernet I**" FG in Kombination mit anderen FGs (e.g. Frame Relay etc.) können beliebige Router- und Gateway-Funktionalitäten im DCC System 3 geschaffen werden. Durch die offene Protokoll- und Interface-Struktur, gepaart mit der bekannten Modularität des DCC System 3 öffnet sich ein breites Anwendungsspektrum.

World Telecom in Genf

Eine mit allen wichtigen Global Players besetzte Messe zog die Entscheidungsträger in ihren Bann. Qualifizierte Gesprächspartner und eine sehr angenehme Atmosphäre kennzeichnete die Genfer Tage für die *TDT*-Crew. „Eine Messe, die internationale Maßstäbe setzt", zieht Jürgen Büttner das erfreuliche Resümee für das niederbayerische Unternehmen.

Wir stellen aus: Halle 1 • Stand 8k4

CeBIT HANNOVER 24.2.–1.3. 2000

Die Richtung stimmt . . .

Telekommunikation mittels digitaler Datenübertragung heißt die Zielrichtung von TDT. Nicht erst seit das Internet einem breiten Publikum den Nutzen digitaler Datenübertragung täglich vor Augen führt, hat sich TDT dieses Themas angenommen und die Produktpalette danach ausgerichtet. Zuverlässigkeit und Skalierbarkeit der Datenübertragung sind dabei die bestimmenden Merkmale. Da die Anwendungen mit dem TCP/IP-Protokoll zunehmend auch alle Sicherheitsmerkmale erfüllen, können unsere Kunden in den TDT-Entwicklungen neben den bewährten Protokollen auch auf TCP/IP-Anwendungen zurückgreifen. Überzeugen Sie sich doch persönlich auf der Messe, wie wir Produkte innerhalb weniger Monate zur Serienreife entwickelt haben. Dabei freuen wir uns auf einen anregenden Dialog und versprechen Ihnen, Ihre Erfahrungen und Wünsche in das Portfolio unserer Produkte aufzunehmen. Um Sie möglichst umfassend über das breite Leistungsspektrum der Telekommunikationsanwendungen informieren zu können, bitten wir um eine Terminabsprache, denn wir möchten, dass Sie nicht nur gut bewirtet, sondern auch bestens informiert werden.

Bis zur CeBIT verbleibe ich recht herzlich

Ihr

Michael Pickhardt

NetMACS ist jetzt mehrplatzfähig

Die neue Version kann von beliebigen Stellen im LAN erreicht und bedient werden. Darüber erleichtert in Kürze eine neue Konfigurationsoberfläche die intuitive Benutzerführung. Alle NetMACS User können sich die neue K.O.-Update downloaden. Der genaue Zeitpunkt wird auf unserer Internetpage http://www.tdt.de bekannt gegeben.

Die TDT-Website näher am Backbone

Da die 64kbit-Standleitung gerade in Stoßzeiten manchmal überlastet war, hat sich die Geschäftsleitung entschlossen, dieses Nadelöhr zu beseitigen. Der komplette Internetauftritt liegt auf einem Server, der direkt an einem Backbone der Telekom angeschlossen ist. Ein schnellerer Durchsatz in Spitzenzeiten ist dadurch für die vielen Besucher unserer Seiten garantiert.
Die bisher ohnehin wenigen Ausfallzeiten sind dadurch zusätzlich gleich gegen null gesunken.

TA MICRO goes IP

Als konsequente Weiterentwicklung des mittlerweile zigtausendfach verkauften TA MICRO präsentiert sich der neue MICRO Router (70 mm x 60 mm). Als OEM Einbau-Router reicht für den Betrieb der Anschluss an eine Stromversorgung. Zudem ist der MICRO Router pinkompatibel zum TA MICRO. Die Neuentwicklung verfügt über eine Ethernet-Schnittstelle, eine ISDN-Schnittstelle sowie zwei serielle Schnittstellen (V.24 und TTL). Zusätzlich steht ein 15-bit breiter I/O-Port zur Verfügung, welcher zum Beispiel eine effektive und kostengünstige Anbindung an Überwachungs- und Funktionseinheiten im Maschinen- und Anlagenbau erlaubt. Je nach Anwendung können die seriellen Ports mit unterschiedlichen Protokoll-Modulen bestückt werden, zum Beispiel Frame Relay, X.25 oder X.3 asynchron.

IP-Pocket Guide nun schon in der 3. Auflage

Die *TDT*-Pocket Guides gehen sprichwörtlich weg wie die warmen Semmeln. Mit jeder neuen Auflage werden die kleinen aber feinen Führer aktualisiert, so dass die Pocket Guides immer up to date sind. Jetzt in neuer aktualisierter Auflage: Der Frame Relay Pocket Guide

Die komplette Reihe über X.25 • Frame Relay • ISDN und IP können bei *TDT* gegen eine Gebühr von DM 5.- pro Pocket Guide angefordert werden.

T.D.T.-LEISTUNGSSPEKTRUM

CPU Unit innerhalb des DCC System 3

Auf der CPU Unit des DCC System 3 befindet sich die gesamte Software einer Functional Group wie z. B. die Protokoll-Software-Module (IP, Frame Relay etc.). Jede CPU Unit kann eine Reihe von unterschiedlichen Interface Units bedienen. Die Protokoll-Software gibt der Functional Group in der Regel ihren Namen. Folgende CPU Units stehen zur Verfügung:

- X.25 CPU Unit (max. 512 Kbit/sec)
- X.75 CPU Unit (max. 512 Kbit/sec)
- X.3/Terminal CPU Unit (max. 512 Kbit/sec)
- Ethernet I CPU Unit (10/100 Mbit/sec)
- HDLC CPU Unit (max. 512 Kbit/sec)
- E1 und FE1 CPU Unit (max. 2 Mbit/sec)
- Frame Relay CPU Unit (max. 512 Kbit/sec)
- AMP CPU Unit (max. 512 Kbit/sec, 700 Kanäle)
- ISDN BRI TE CPU Unit (2 ISDN Ports)
- ISDN BRI CPU Unit (1, 2 oder 4 ISDN Ports)
- ISDN PRI CPU Unit
- Crypto und Crypto Manager CPU Unit
- CSM CPU Unit (Central Site Modem mit 4 Modems max. 33,6 Kbits/sec)
- V110 CPU Unit

I M P R E S S U M

Herausgeber	T.D.T. Transfer Data Test GmbH Siemensstraße 18 84051 Essenbach Tel. 08703/9 29-00 Fax 08703/9 29-201
Verantwortlich für den Inhalt	Michael Pickhardt, Geschäftsführer H. J. Büttner
Gesamtproduktion	Werbeagentur J. Wimmer Ulmenstraße 21 84051 Essenbach Tel. 0 87 03/9 13 60 Fax 0 87 03/9 13 61
Auflage:	*12.500 Exemplare*