LENTE

COMPACT

TELECOMMUNICATIE

1993/1

KWARTAALBLAD EDP-AUDITING

Compact ®
Jaargang 20, nummer 1
Een uitgave van KPMG Klynveld EDP Auditors en Samsom BedrijfsInformatie, werkmaatschappij van Wolters Kluwer NV.
Het blad verschijnt 4 x per jaar.

Redactie
D. Steeman RE RA (hoofdredacteur)
drs. R.G.A. Fijneman RE RA
prof. A.W. Neisingh RE RA
drs. P. Veltman RE RA

Redactiesecretariaat
Mw. A.M.F. Hofland,
KPMG Klynveld EDP Auditors,
K.P. van der Mandelelaan 41,
3062 MB Rotterdam
Tel.: 010 - 453 47 40
Fax : 010 - 453 47 77

Vormgeving
Bureau Karakter, Delft

Aan dit nummer werkten mee
drs. ing. D. Brouwer
ir. E.J. Evelo
M. Kennett BA
J.L. Ramos Najera
H. Reijn
drs. T.P. de Vries
E. Zegwaart

Abonnementen
f 135,- per jaar incl. BTW. Losse nummers f 45,- incl. BTW. Abonnementen kunnen schriftelijk tot uiterlijk één maand voor de aanvang van een nieuw abonnementsjaar worden opgezegd. Bij niet tijdige opzegging wordt het abonnement automatisch met een jaar verlengd.

Abonnementsadministratie
Samsom BedrijfsInformatie,
Postbus 4,
2400 MA Alphen aan den Rijn
Tel.: 01720 - 6 68 00
Fax : 01720 - 7 59 33
Adreswijzigingen - ook tijdelijke - moeten minstens 8 weken voor de verschijningsdatum bekend zijn.

Uitgever
J.R.M. Masselink

Lid van de Nederlandse organisatie van tijdschriftuitgevers NOTU

ISSN 0920 - 1645

INHOUDSOPGAVE

REDACTIONEEL

Het blad wil een bijdrage leveren aan de ontwikkeling van het vakgebied EDP-auditing door het publiceren van actuele artikelen op deelterreinen van EDP-auditing en advies, zoals: ● beoordeling automatiseringsorganisaties en -systemen ● risicobeheersing ● telecommunicatie-adviezen ● beveiligingsonderzoeken ● quality assurance ● opleidingen en trainingen ● privacy-wetgeving ● computercriminaliteit en nieuwe regelgeving. Behalve voor EDP-auditors kan dit blad ook interessant zijn voor EDP-deskundigen en gebruikers van informatiesystemen. De in dit tijdschrift weergegeven meningen mogen niet worden gezien als officiële zienswijze van KPMG Klynveld EDP Auditors.

Het blad Compact is met de meeste zorg samengesteld. Niettemin is het niet geheel uitgesloten dat de geboden informatie enkel en alleen door tijdsverloop en/of andere oorzaken minder juist is. Noch KPMG Klynveld, KPMG Klynveld EDP Auditors, noch de redacteuren persoonlijk, noch uitgeverij Samsom BedrijfsInformatie BV, deel uitmakend van Wolters Kluwer NV, aanvaarden enige aansprakelijkheid, hoe ook genaamd, uit welken hoofde dan ook voor enig gevolg rechtstreeks of indirect voortvloeiend uit het gebruik van de informatie.

De redactie stelt gaarne ruimte in Compact beschikbaar voor reacties en/of ervaringen van lezers. Auteurs die overwegen een bijdrage te leveren, wordt verzocht kennis te nemen van de aanwijzing voor auteurs, die bij het secretariaat verkrijgbaar is.

De term *telecommunicatie* heeft de laatste decennia een enorme verandering doorgemaakt qua betekenis, qua waardering en qua betrokkenheid.
Tot en met de jaren zeventig werd bij dit woord gedacht aan telefooncentrales, de PTT, telex en dergelijke; een wereld waarvan slechts een handjevol specialisten kennis had en die ver afstond van de primaire bedrijfsvoering in een onderneming. Telefoon was er gewoon; het was een puur faciliterende voorziening.

Door steeds verdergaande ontwikkelingen in de informatietechnologie, miniaturisering van elektronische schakelingen en automatisering van test- en fabricageprocessen van deze elektronica, wordt de van oudsher analoge wereld van elektronische schakelingen vervangen door een digitale. Digitale technieken zijn beter en sneller te ontwerpen en goedkoper toe te passen.
Ook de telefooncentrale-apparatuur maakte deze ontwikkeling door, waardoor de centrales niet alleen kleiner en goedkoper werden, maar waardoor tevens het gat tussen de werelden van de computers en netwerken enerzijds en van de telefonie anderzijds slonk, want digitaal gesproken is een bit een bit, of ze nu onderdeel uitmaakt van een X.25-packet of van een gedigitaliseerd telefoongesprek. De integratie van spraak en data heeft er inmiddels toe geleid dat veel leveranciers, inclusief de zich van oudsher op spraak richtende PTT's, zich op deze gecombineerde markt hebben gestort. De markt van informatietransport, van nieuwe produkten en van nieuwe diensten. De moderne telecommunicatiemarkt.

Een belangrijke katalysator voor de moderne telecommunicatiemarkt is standaardisatie. Op alle niveaus van het ISO-model voor Open Systems Interconnection is en wordt gewerkt aan standaarden, op basis waarvan vervolgens leveranciers hun produkten ontwikkelen. Op toepassingsniveau is inmiddels door het International Telegraph and Telephone Consultative Committee (CCITT) een raamwerk van standaarden ontwikkeld onder de verzamelnaam X.400, op basis waarvan elektronische postsystemen op een afgesproken manier wereldwijd met elkaar zouden kunnen communiceren. Maar ook op het gebied van netwerkbesturingssystemen en encryptie-apparatuur heeft standaardisatie geleid tot een breed aanbod van produkten.

Ook binnen organisaties is een integratie in gang gezet. Waar eerder de spraak- en datacommunicatie - door geheel gescheiden afdelingen - afzonderlijk werden aangepakt, is er vandaag in de meeste organisaties op z'n minst sprake van overleg tussen afdelingen en is er veelal nog slechts sprake van één afdeling die zich met de totale telecommunicatie-infrastructuur van de onderneming bezighoudt.

In strategie en beleid, hoe om te gaan met informatietechnologie, wordt het gezamenlijk nut van een adequate telecommunicatie-infrastructuur onderkend. Zij kan leiden tot een efficiëntere bedrijfsvoering, tot een voorsprong op de concurrentie of simpelweg tot grotere overlevingskansen.
De behoefte van ondernemingen om tijdig de juiste informatie beschikbaar te hebben, heeft het gebruik van telecommunicatievoorzieningen enorm doen toenemen. In eerste instantie het gebruik van de lokale PC-netwerken, maar de laatste jaren steeds meer de verbindingen tussen locaties: de Wide Area Netwerken.
Met dit toenemend gebruik ontstaat een toenemende mate van afhankelijkheid van netwerken. Veel bedrijven claimen inmiddels slechts voor korte tijd zonder netwerkvoorzieningen te kunnen voortbestaan. Ook de behoefte aan goede beveiliging van deze voorzieningen - betrouwbaarheid, vertrouwelijkheid, beschikbaarheid - zou met deze ontwikkeling moeten toenemen. Het toepassen van de juiste encryptietechnieken, het op de juiste wijze inrichten van de beheerorganisatie, het correct installeren van netwerkbesturings-software en het regelmatig afwegen van de restrisico's in deze netwerkinfrastructuur tegen de geïnventariseerde bedreigingen en genomen maatregelen: het is niet een kwestie van keuze. Alle genoemde activiteiten dienen samen met vele andere door het management van ondernemingen te worden onderkend en actief ondersteund in de bedrijfsvoering.

De EDP-auditor komt in zijn werk regelmatig in aanraking met telecommunicatie-omgevingen, soms in de conventionele, soms in meer moderne zin.
Geïntegreerde bekabelingssystemen, waarover zowel spraak als datacommunicatie plaatsvindt, computernetwerkkoppelingen, die deels over de verbindingen van andere leveranciers zijn gerealiseerd, moderne telefooncentrales die het knooppunt zijn in een landelijk telecommunicatienetwerk voor spraak- en datatoepassingen, speciale verbindingen tussen bank en klant, waarlangs dagelijks voor miljoenen aan financiële transacties worden verzonden: in al die gevallen zal de EDP-auditor inzicht moeten hebben in de functionaliteit van de toegepaste componenten, maar veel meer nog in de problematiek rond het ontwerpen, exploiteren en beheren van dergelijke voorzieningen, waardoor een betrouwbaar en veilig informatietransport kan worden gegarandeerd.
De redactie is van mening dat dit nummer van Compact kan bijdragen tot het verdiepen en verbreden van dit inzicht.

Graag wil ik - mede namens de overige redactieleden - mijn dank betuigen aan de heer H. Veenman, senior manager bij KPMG Klynveld Management Consultants en adviseur op het gebied van telecommunicatie en beveiliging, onder wiens inhoudelijke verantwoordelijkheid dit nummer tot stand is gekomen.

D. Steeman

Netwerkmanagement, de organisatorische opzet en financiële beheersing

Ir. E.J. Evelo

Investeren in netwerkvoorzieningen dient wel overwogen te gebeuren, de eenmalige kosten zijn vaak hoog. Maar de regelmatig terugkerende kosten van onderhoud, huur, mensen en middelen zijn vaak vele malen hoger. Beheersing van deze kosten begint bij een goede organisatie, waarin taken en verantwoordelijkheden, maar ook services en service levels helder zijn gedefinieerd.

INLEIDING

Toenemend belang van netwerken

Het belang van communicatienetwerken in de totale IT-functie van bedrijven neemt toe. Met de vorming van resultaatverantwoordelijke business units ontstaan kleinere werkeenheden met eigen IT-toepassingen en een veelheid aan relaties met in- en externe informatiesystemen. Een beperkt aantal centrale systemen wordt vervangen door kleinere decentrale, gekoppelde systemen. Koppelings- en integratieproblemen nemen zienderogen toe.

De impact van netwerken op het bedrijfsproces verandert van ondersteunend technisch middel tot onderscheidend strategisch voordeel. Integratie van externe en interne bedrijfsprocessen maakt het mogelijk aanzienlijke tijdwinsten en kostenreducties te boeken, en nieuwe onderscheidende toegevoegde waardediensten te introduceren. Duidelijk voorbeeld hiervan is de toepassing van EDI in elektronisch bestellings- en betalingsverkeer.

Noodzaak tot kostenbeheersing

Het aandeel van de netwerkkosten in de totale bedrijfskosten stijgt navenant. Met de huidige scepsis rond verdergaande investeringen in IT nemen ook de aarzelingen toe inzake investeringen in netwerken. Voorts blijkt uit onderzoek dat deze investeringen slechts een klein deel (minder dan 25 procent) vertegenwoordigen van de uitgaven aan netwerken. Een adequate beheersing van de (stijging van de) netwerkkosten is dus een absolute noodzaak.

Deze noodzaak tot kostenbeheersing staat in contrast met het nijpend tekort aan deskundig personeel. Beheersing van de exploitatiekosten van netwerken vereist goed opgeleid en getraind personeel, dat niet alleen kennis heeft van de onderliggende technische materie, maar ook begrip heeft van en voor de organisatorische aspecten, de financieel-economische overwegingen en de strategische consequenties.

Uitbesteding

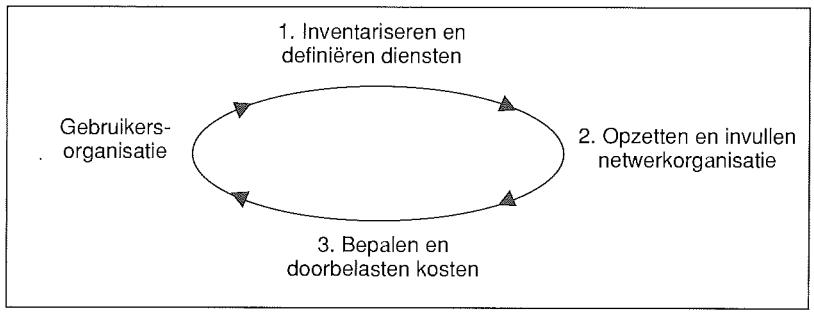
Steeds meer bedrijven kiezen vanuit deze optiek van schaarste aan mensen en middelen voor uitbesteding van de exploitatie van netwerken. Deze keuze is schijnbaar in tegenstelling met het geschetste toenemende belang van netwerken op de primaire bedrijfsprocessen, maar sluit goed aan op de bredere trend: 'back to the core'.

De kernvraag van dit artikel is daarmee hoe gegeven de beperkingen in de beschikbaarheid van personele en financiële middelen de mogelijkheden van netwerken maximaal kunnen worden benut.

Zoals de titel van dit artikel reeds aangeeft is het antwoord op deze kernvraag geschreven vanuit de organisatorische en financiële invalshoek. Daarmee wordt het belang van adequate technische (hulp)middelen niet ontkend, maar hierover wordt reeds uitgebreid gepubliceerd. Het zijn juist de organisatorische opzet en financiële beheersing van de exploitatie van netwerken die enigszins onderbelicht blijken.

AANPAK

De kernvraag rond de organisatorische opzet en de financiële beheersing van de exploitatie van netwerken wordt in dit artikel beantwoord vanuit het globale raamwerk zoals opgenomen in figuur 1.



Figuur 1. Raamwerk.

Doelstelling is te komen tot een beheerste exploitatie van netwerken door een optimale afstemming tussen diensten, organisatie en kosten met behoeften van gebruikersorganisaties.

Met het inventariseren en definiëren van de te leveren diensten is duidelijk welke kwaliteiten en kwantiteiten aan services door de gebruikersorganisatie(s) worden gewenst (en welke niet). Aan de orde komen de gangbare diensten. Voorts is aandacht besteed aan het gebruik van Service Level Agreements (SLA's).

Vervolgens kan de organisatie worden ingericht met het opzetten en invullen van het netwerkmanagement. Aan de orde komen een organisatiemodel met functies, taken en werkzaamheden, en enkele kengetallen gerelateerd aan de kosten en de omvang van het netwerk. Verder wordt ingegaan op de vrijheidsgraden en bijbehorende overwegingen zoals centraal versus decentraal en eigen versus derden.

Ten slotte kunnen de kosten worden geïnventariseerd en vertaald in commerciële tarieven. Aan de orde komen een kostenmodel, een tariefstructuur en enkele overwegingen bij de vertaling van kosten in tarieven.

Stappenplan
Genoemd raamwerk is zeer wel bruikbaar voor de inrichting en beheersing van het netwerkmanagement. Door het inventariseren en definiëren van de diensten wordt duidelijk welke services dienen te worden geleverd. Vervolgens kan per service worden bepaald welke taken en (hulp)middelen hiertoe noodzakelijk zijn. Deze taken kunnen vervolgens in een organisatorisch kader worden geplaatst. Ten slotte kunnen de kosten van deze organisatie met bijbehorende (hulp)middelen aan geleverde services worden toegerekend. De gebruikersorganisatie zal vervolgens een afweging maken tussen de geleverde service en de in rekening gebrachte kosten, wat kan leiden tot bijstelling van de gehele cyclus van service, organisatie en tarief.

In veel gevallen is sprake van een bestaande organisatie en heeft het bovenstaande stappenplan het karakter van een heroriëntatie en aanscherping van services, organisatie en tarieven. Een analyse van kosten en gebruikerssatisfactie kan dan een goede aanleiding zijn tot bijstelling van services, organisatie en tarieven. Hiertoe wordt in principe dezelfde methodiek gebruikt als voor het in eerste instantie inrichten van het netwerkmanagement, alleen wordt begonnen met stap 3: het bepalen (en doorbelasten) van de kosten, en het vervolgens uitvoeren van stap 1 en 2. Dit artikel is geschreven in de (chrono)logische volgorde, te beginnen met de specificatie van de diensten, vervolgens de inrichting van de organisatie, en ten slotte de doorbelasting van de kosten.

DIENSTEN

Netwerkmanagement is een eerste voorwaarde voor een beheerste exploitatie van netwerken. De opzet en invulling van dit netwerkmanagement wordt bepaald door de kwaliteit en kwantiteit van de te leveren netwerkdiensten. Voor het definiëren van deze netwerkdiensten is een overzicht van gangbare netwerkservices opgesteld. Voor ieder van de daarin opgenomen services kunnen bijbehorende kwaliteiten en kwantiteiten worden bepaald en, eventueel aangevuld met niet-standaarddiensten, worden vastgelegd in een Service Level Agreement.

Door het nadrukkelijk inventariseren van de behoeften van gebruikersorganisaties en het op basis van die behoeften definiëren van de kwaliteiten en kwantiteiten van de te leveren netwerkservices, wordt voorkomen dat diensten worden geleverd waaraan geen of nauwelijks behoefte bestaat en waar dus onvoldoende financiële dekking voor is. Evenzo wordt voorkomen dat diensten worden aangeboden van een te gering kwaliteitsniveau, bijvoorbeeld onvoldoende beschikbaarheid. Voorts kunnen kostenconsequenties van differentiaties in service level, zoals verschillende beschikbaarheden, zichtbaar worden gemaakt.

In de praktijk blijkt dat gebruikersorganisaties niet altijd in staat zijn hun behoeften te formuleren. Vaststelling van te ondersteunen applicaties en vertaling naar netwerkservices is een lastige zaak, maar noodzakelijk voor een goede definitie van de netwerkservices. Enige begeleiding in de vorm van advisering door de netwerkorganisatie is dan gewenst. Het voorschrijven of opleggen van netwerkservices moet worden voorkomen. Genoemde (netwerk)services, service levels en bijbehorende agreements worden in de volgende subparagrafen kort toegelicht.

Services en service levels

Voorafgaand aan de inrichting van de organisatie voor de exploitatie van netwerken is het gewenst een duidelijk, volledig en juist beeld te hebben van de eisen en wensen c.q. behoeften van de gebrui-

kersgroepen. Daartoe is de onderstaande checklist van gebruikelijke netwerkservices opgesteld.
Netwerkservices:
- aansluiting/wijziging;
- onderhoud;
- help desk;
- (management)rapportage en -advies;
- kostenspecificatie;
- beveiliging.

Aansluiting/wijziging
Kern van genoemde netwerkservices is het leveren van aansluitingen c.q. verbindingen. Gangbare aansluitingen en/of verbindingen en bijbehorende services zijn bijvoorbeeld:
- WAN-verbinding;
- LAN-koppeling;
- terminal-aansluiting;
- file transfer;
- E-mail.

Voor ieder van de genoemde aansluitingen c.q. verbindingen zal (in overleg met de gebruikersorganisatie) moeten worden bepaald welke technische infrastructuur vereist is.

Onderhoud
Onderhoud staat voor het inspecteren van en het preventieve en correctieve onderhoud aan aansluitingen c.q. verbindingen gericht op de continuïteit c.q. beschikbaarheid van een technische infrastructuur. Zwaartepunt van het onderhoud is de melding, diagnose, opheffing en gereedmelding van storingen.

Help desk
De help desk is een vorm van gebruikersondersteuning, waar (eind)gebruikers direct met hun vragen en opmerkingen terecht kunnen. Deze betreffen storingen, bedieningsfouten, instructies, rapportages, kleine wijzigingen en dergelijke.

Managementrapportage en advies
De managementrapportage en het bijbehorende advies hebben betrekking op het (ongevraagd) informeren en adviseren van het management van betrokken gebruikersorganisaties.
De rapportage heeft de vorm van een terugblik op geleverde diensten in relatie tot afgesproken kwaliteiten en kwantiteiten, zoals levertijd, beschikbaarheid en capaciteit.
Het advies analyseert de desbetreffende rapportages en formuleert aanbevelingen omtrent het (optimale) gebruik van verbindingen. Voorts wordt in het advies (vooruit)geblikt naar nieuwe toepassingsmogelijkheden, additionele diensten, etc.

Kostenspecificatie
Kostenspecificatie betreft het op het verzoek en naar de wens van de gebruikersorganisatie specificeren (en tariferen) van de kosten van verbindingen in vaste en/of variabele componenten met als doel de (interne) doorbelasting van de kosten en de sturing van het gebruik.

Beveiliging
Beveiliging is een netwerkservice die zich richt op de betrouwbaarheid, vertrouwelijkheid en continuïteit van verbindingen, in het bijzonder gericht op de informatiestromen over deze verbindingen. Aan de beveiligingsaspecten van netwerken wordt in ruime mate aandacht besteed in andere artikelen in deze Compact.

Voor ieder van de genoemde services is het essentieel in overleg met de gebruikersorganisaties na te gaan wat hun exacte behoeften zijn en welke eisen zij stellen aan de service in kwestie. Daartoe is een goed beeld van de te ondersteunen applicaties en bedrijfsprocessen onontbeerlijk.

Service Level Agreement

Voor het beheren van de services en het handhaven van service levels kan gebruik worden gemaakt van Service Level Agreements (SLA's). In deze SLA's worden de rechten en plichten van betrokken partijen (dienstaanbieder en gebruiker) eenduidig vastgelegd. Dit voorkomt een groot probleem rond de exploitatie van netwerkservices: onduidelijkheid en misinterpretatie van afspraken en normen.

Eén van de grootste val;kuilen rond SLA's is het onvoldoende meetbaar normeren van de te leveren prestaties.

Voor een SLA kan de onderstaande beknopte inhoudsopgave gehanteerd worden:
1. services/diensten: zie voorgaande subparagraaf;
2. service levels/kwaliteiten en kwantiteiten: definitie en controle;
3. voorwaarden en condities: garanties en aansprakelijkheden;
4. prijzen: vaste/variabele tarieven;
5. procedures: melding, wijziging, storing, rapportage en dergelijke.

Afweging tussen prijs en prestatie
SLA's hebben het belangrijke voordeel dat door de gebruikersorganisatie een afweging kan worden gemaakt tussen de gewenste kwaliteit c.q. prestatie en de bijbehorende prijsstelling. Zonder SLA's zijn gebruikersorganisaties voortdurend ontevreden en willen zij almaar meer en beter.

Meetbare normen
Eén van de grootste valkuilen rond SLA's is het onvoldoende meetbaar normeren van de te leveren prestatie. Ondanks de afspraken blijven gebruikersgroepen ontevreden omdat hun perceptie van

de dienstverlening een andere is dan die van de netwerkorganisatie. Vraag is iedere keer weer hoe de (eind)gebruiker de kwaliteit beoordeelt en welke operationele normen daarvoor in aanmerking komen.

Ter illustratie is voor de service Onderhoud in figuur 2 een invulling gegeven aan de belangrijkste meetbare aspecten van een SLA.

Onderhoud:	
– serviceperiode:	kantoortijden, (plus), 7 x 24 uur
– responstijden:	0.5, 2, 4, 8 en 16 uur
– reparatietijden:	4, 8, 16 en 24 uur
– beschikbaarheden:	99.nn% plus definitie
– escalatieprocedure:	acties plus condities
– risicodekking:	loon-, materiaal- en voorrijkosten
– rapportage/overleg:	vorm, inhoud en periodiciteit
– prijs:	vaste en variabele tarieven
– boeteclausule:	n-maal maandelijkse vergoeding

Figuur 2. Onderhoud.

Sanctiemogelijkheid
Het opnemen van een sanctiemogelijkheid is wenselijk om de dienstenaanbieder daadwerkelijk te kunnen afrekenen op geleverde prestatie. Zonder een garantiestelling, boetebeding of andere sanctie blijven de gemaakte afspraken altijd enigszins vrijblijvend. In uitzonderlijke situaties kan de gebruikersorganisatie gebruik maken van de (eventuele) mogelijkheid het contract te beëindigen en elders zaken te doen. In alle gevallen is een nauwe betrokkenheid van het topmanagement noodzakelijk voor het daadwerkelijk kunnen uitoefenen van genoemde rechten.

ORGANISATIE

Om genoemde services en service levels vastgelegd in Service Level Agreements te kunnen realiseren en beheersen is, naast een technische infrastructuur met bijbehorende (netwerkmanagement) tools, een netwerkorganisatie noodzakelijk. Daartoe is een organisatiemodel ontwikkeld dat de desbetreffende functies, taken en werkzaamheden uitgebreid beschrijft en in hun onderlinge relatie plaatst.

Om een dergelijke organisatie vervolgens te kunnen kwantificeren zijn proefondervindelijk enige kengetallen genormeerd en gerelateerd aan het netwerk en de netwerkkosten. Aldus kan de omvang van de personele bemanning in orde van grootte worden bepaald.

In de uiteindelijke organisatievorm zitten enkele vrijheidsgraden die een nadere toelichting behoeven. Kenmerkend voor deze organisatievorm zijn de mate van decentralisatie en uitbesteding. Beide vrijheidsgraden worden toegelicht aan de hand van een overall organisatorisch kader dat de werking van bijbehorende sturende mechanismen, zoals business plannen en SLA's, illustreert.

Genoemd organisatiemodel, kengetallen en vrijheidsgraden worden achtereenvolgens in de volgende subparagrafen beschreven.

Organisatiemodel

Voor het opzetten, invullen (en toetsen) van een organisatie voor de exploitatie van netwerken is een organisatiemodel ontwikkeld. Dit organisatiemodel beschrijft de functies, taken en werkzaamheden van de netwerkorganisatie.

Het doel van het organisatiemodel is het op een logische en heldere manier beschrijven van de relevante functies in het kader van netwerkmanagement. Het model is in principe geen blauwdruk voor de uiteindelijke organisatievorm. Die is mede afhankelijk van de mate van decentralisatie en uitbesteding, zoals beschreven in een volgende paragraaf.

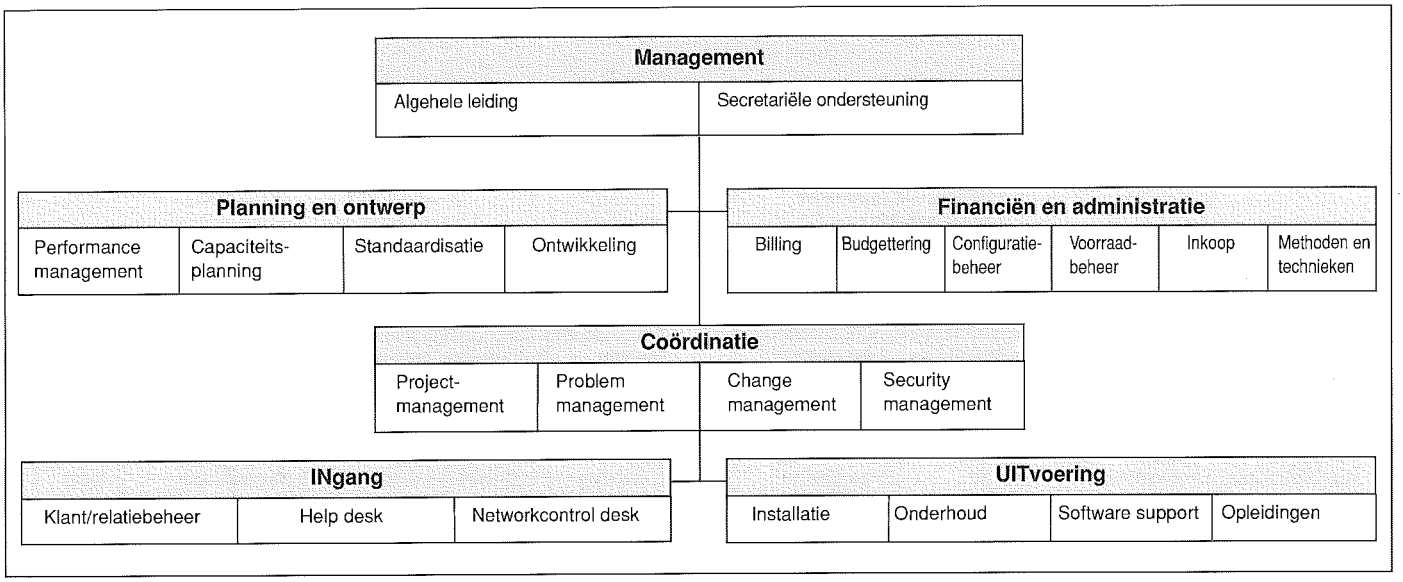
Het model blijkt in de praktijk soms overcompleet; niet alle genoemde taken en bijbehorende werkzaamheden worden door de netwerkorganisatie zelf uitgevoerd. Sommige taken zijn ondergebracht bij andere specialistische (staf)afdelingen, zoals Inkoop of Facturering, en andere taken zijn uitbesteed aan derden, zoals Installatie, Onderhoud of Opleiding.

Aan de hand van het in figuur 3 opgenomen organisatiemodel kunnen voor de (in de vorige stap) gedefinieerde services en service levels de taken worden gegroepeerd rond herkenbare en benoembare functies. Het model plaatst deze taken en werkzaamheden in hun onderlinge verband.

Functies, processen en niveaus
Het organisatiemodel is opgebouwd uit twee staffuncties, te weten Planning en ontwerp/Financiën en administratie, en drie lijnfuncties, te weten Ingang/Coördinatie/Uitvoering onder een overall Managementfunctie.

In het model zijn twee assen opgenomen:
- een horizontale proces-as herkenbaar aan Ingang/Coördinatie/Uitvoering en Planning en ontwerp/Financiën en administratie;
- een verticale niveau-as herkenbaar aan Management/Coördinatie/Uitvoering.

Opgemerkt moet worden dat niet alle taken en werkzaamheden van Financiën en administratie een tactisch of strategisch karakter hebben; dit geldt bijvoorbeeld voor configuratie- en voorraadbeheer. Ter wille van de symmetrie van het model is deze staffunctie naast Planning en ontwerp geplaatst.



Figuur 3. Organisatiemodel.

Overwegingen
Coördinatie en Uitvoering zijn gescheiden opgezet omdat Uitvoering zich met name leent voor uitbesteding. Alle overige lijnfuncties zijn minder geschikt voor volledige uitbesteding. Zonder een eigen Ingang zijn de werkzaamheden van derden onbeheersbaar, terwijl zonder een eigen Coördinatie het overzicht en de controle ontbreekt. De staffuncties kunnen eventueel onder eigen verantwoordelijkheid worden uitbesteed aan derden (bijvoorbeeld door inhuur van benodigde expertise).

De Ingang is verbijzonderd om een duidelijk herkenbare klanteningang te hebben die verantwoordelijk is voor de directe contacten met gebruikersorganisaties en die gedurende het gehele proces, van bijvoorbeeld wijziging en storingsopheffing, de contacten onderhoudt met gebruikers. Voorts geeft een afzonderlijke Ingang de mogelijkheid de schaarse expertise efficiënt te benutten door het scheiden van netwerkspecialisten en gebruikers. Netwerkspecialisten worden niet voortdurend lastig gevallen door gebruikers omdat simpele vragen worden afgevangen door de help desk. De toegevoegde waarde van deze help desk moet echter onmiskenbaar zijn, daar anders de gebruiker zal trachten direct contact te zoeken met de netwerkspecialist.

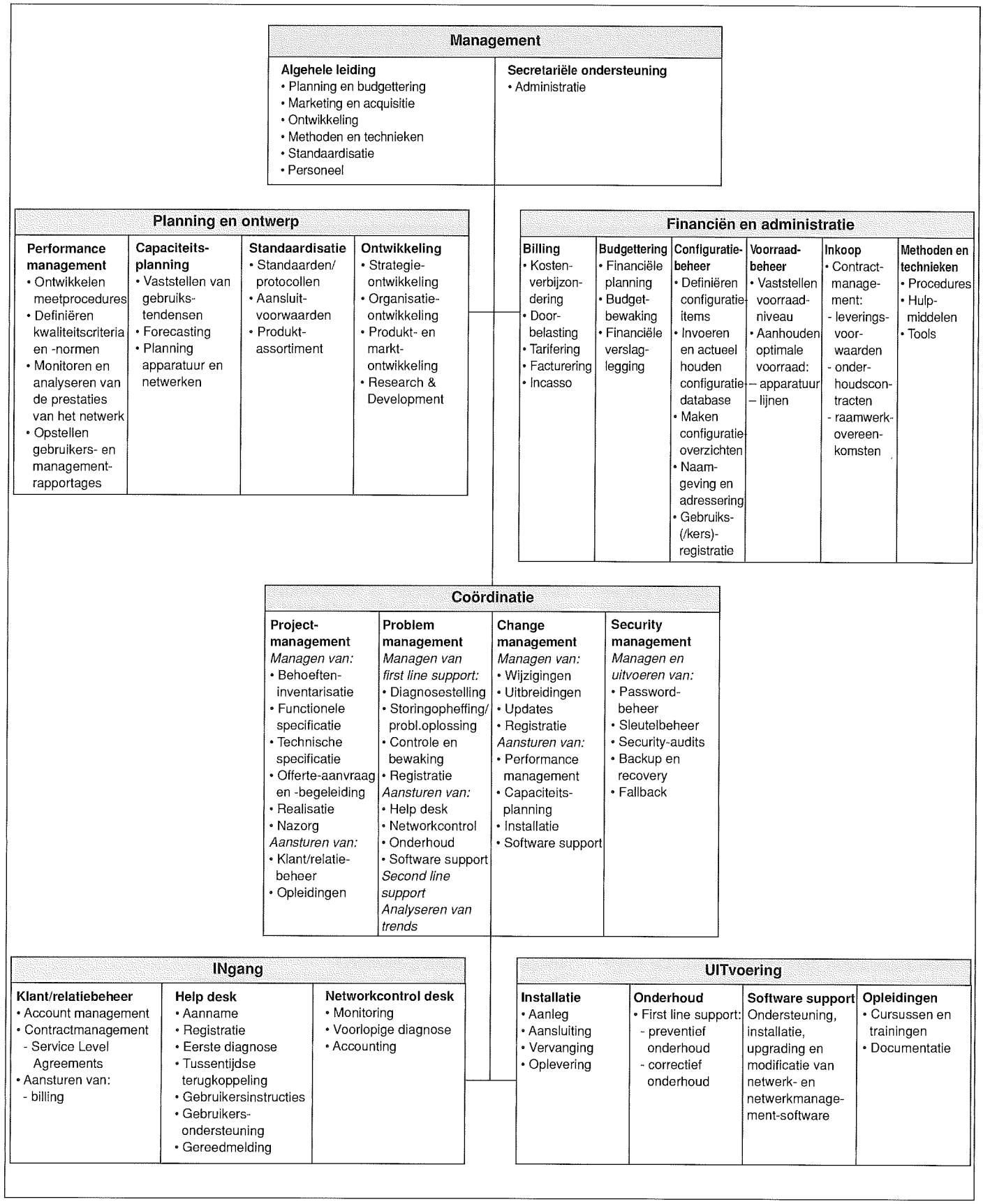
De help desk reageert op een verzoek van de gebruiker (van buitenaf), de networkcontrol desk op basis van het (continu) monitoren van het netwerk (van binnenuit). De help desk is de ingang voor kleine ad hoc-wijzigingen, het klant/relatiebeheer voor projectmatige wijzigingen. Deze projectmatige wijzigingen worden vervolgens onder verantwoordelijkheid van het projectmanagement in samenwerking met het change management gerealiseerd.

Tussen de vier opgenomen coördinatiefuncties bestaan vele verbanden en geen strikte scheidingen. Iedere functie heeft een hoofdaandachtsgebied en zal voor de invulling van dit werkveld veelvuldig gebruik maken van de andere coördinatiefuncties. Het projectmanagement is verbijzonderd om projectmatige werkzaamheden adequaat te kunnen sturen onder verantwoordelijkheid van ervaren projectmanagers.

Kwaliteitszorg
De kwaliteitszorg is ondergebracht bij de staffunctie Performance management. Hoewel kwaliteit in principe onderdeel is van de lijn, worden in het model de afwijkingen gepresenteerd c.q. gesignaleerd door de staf. Afwijkingen ten opzichte van de norm leiden tot acties bij Coördinatie dan wel Management.

Verbindende schakel in dezen is de managementinformatie. Voornaamste probleem is niet het genereren van de benodigde informatie, maar het selecteren, aggregeren en comprimeren tot de minimaal benodigde managementinformatie. Norm en afwijking zijn daarbij essentieel.
De gebruikersoptiek is het uitgangspunt. Op basis van de afgesproken services en overeengekomen service levels kan de kwaliteit van dienstverlening worden gemeten en beoordeeld. Het klant/relatiebeheer verkoopt de diensten, Coördinatie begeleidt de realisatie en Uitvoering verzorgt de produktie. Het gehele proces van verkoop, realisatie tot beheer moet voldoen aan de kwaliteitsnormen van de gebruiker, zoals vastgelegd in het Service Level Agreement.

Aansturing
De aansturing van de staffuncties vindt plaats vanuit de lijn en is als volgt verdeeld:
- Performance management en Capaciteitsplanning vanuit Change management;



Figuur 4. Uitwerkingen organisatiemodel.

- standaardisatie en ontwikkeling vanuit Management;
- Billing vanuit Klant/relatiebeheer;
- Budgettering en Methoden en technieken vanuit Management;
- Configuratiebeheer, Voorraadbeheer en Inkoop vanuit alle coördinatiefuncties.

De aansturing van Ingang en Uitvoering geschiedt vanuit de coördinatiefuncties en is als volgt opgezet:
- Klant/relatiebeheer vanuit Projectmanagement;
- Help desk en networkcontrol desk vanuit Problem management;
- Installatie vanuit Change management;
- Onderhoud vanuit Problem management;
- Software support vanuit Problem en Change management;
- Opleidingen vanuit Projectmanagement.

Opgemerkt moet worden dat niet iedere taak of functie synoniem is met één of meer medewerkers. Het model geeft slechts een functionele beschrijving van de te verrichten taken en werkzaamheden.

In figuur 4 zijn de uitwerkingen van taken in werkzaamheden opgenomen. Voor ieder van de genoemde taken is aan de hand van enkele kernbegrippen de essentie van de taak geschetst. Enkele van de aangebrachte scheidingen behoeven wellicht een nadere toelichting.

Eerste-, tweede- en derdelijnsondersteuning
De eerste-, tweede- en derdelijnsondersteuning is gescheiden opgezet. De eerstelijnsondersteuning wordt ingevuld door Onderhoud onder de functie Uitvoering. De tweedelijnsondersteuning is ondergebracht bij Problem management onder de functie Coördinatie. De derdelijnsondersteuning is bij voorbaat uitbesteed aan de leverancier respectievelijk de producent.

Accounting, Billing en Budgettering
Accounting, Billing en Budgettering is verdeeld over de functies Ingang en Financiën en administratie. Accounting (onderdeel van Networkcontrol desk) richt zich op het bijhouden van de tellers van het daadwerkelijk gebruik van het netwerk. Billing vertaalt deze tellers en overige indicatoren in facturen. Budgettering is verantwoordelijk voor het opstellen en bewaken van de budgetten.

Van produkt- naar procesoriëntatie
Zoals reeds opgemerkt is het model soms overcompleet. Alle in de checklist genoemde netwerkservices zijn opgenomen in het organisatiemodel, met dit verschil dat het organisatiemodel procesgeoriënteerd is en de checklist produktgeoriënteerd. Gelijksoortige processen voor een bepaalde service, zoals de aanname van storingsmeldingen en wijzigingen, zijn bij elkaar ondergebracht.

De werkwijze bij de invulling van het organisatiemodel is om voor de (in overleg met de gebruikersorganisaties) gedefinieerde services de taken te bepalen zoals procesgewijs geclusterd in het organisatiemodel. Deze taken laten zich het handigste vaststellen door het aflopen van de diverse uitwerkingen van het organisatiemodel. Vervolgens kunnen de resterende relevante taken overeenkomstig het model worden georganiseerd.

Kengetallen

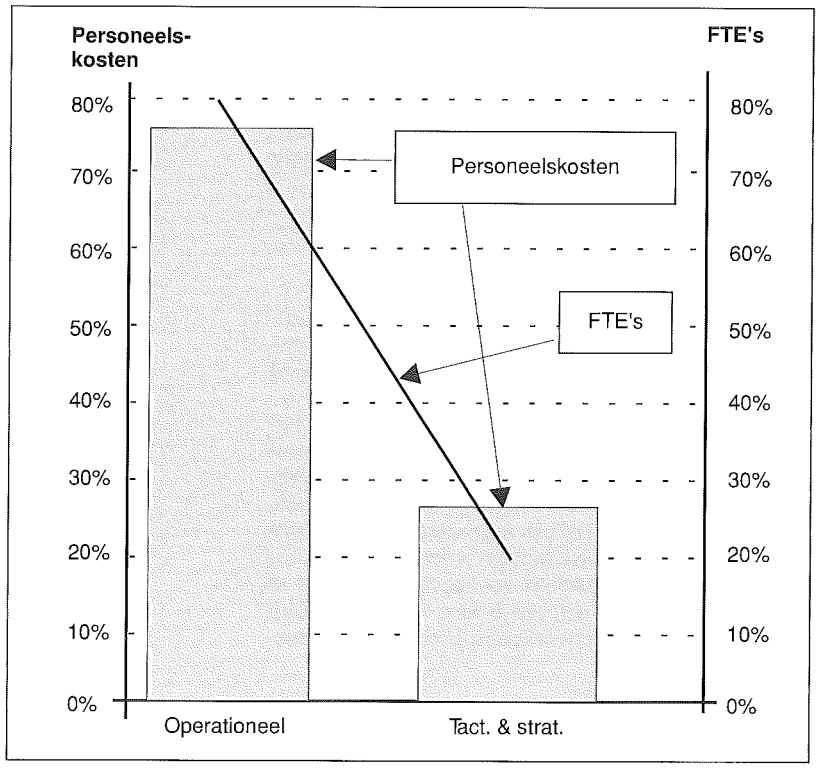
Om het geschetste organisatiemodel te kunnen dimensioneren zijn proefondervindelijk enkele kengetallen bepaald. Deze kengetallen zijn gebaseerd op verhoudingen in kosten.
De waarde van deze kengetallen is voorlopig beperkt, doch ander referentiemateriaal is nog onvoldoende aanwezig. Netwerken kennen vele vrijheidsgraden die van invloed zijn op de personele invulling van de netwerkorganisatie. Door deze netwerken te categoriseren en verschillen in omvang, maximale capaciteit en bezetting hieruit te elimineren, ontstaat een eenduidig verband tussen netwerkkosten en netwerkcomplexiteit en -performance.

De uitdaging is een verhouding te definiëren tussen netwerkkosten enerzijds en netwerkvariabelen anderzijds.

De uitdaging is een verhouding te definiëren tussen netwerkkosten enerzijds en netwerkvariabelen anderzijds. Voor LAN's wordt daarbij gebruik gemaakt van kosten per aansluiting. In de literatuur wordt gesproken over honderden tot enkele duizenden guldens per aansluiting. Voor WAN's maken wij gebruik van kosten per Datapackets Per Second (DPPS). Nader onderzoek blijft vereist.

Operationele, tactische en strategische personeelskosten
Indien in het voorgaande organisatiemodel de personele kosten van Ingang, Coördinatie en Uitvoering worden gerekend tot de operationele kosten en de personele kosten van de overige functies (Planning en ontwerp, Financiën en administratie, en Management) worden gerekend tot de tactische en strategische kosten, dan blijkt uit onderzoek naar de kosten van WAN's dat de operationele (personeels)kosten een factor drie groter zijn dan de tactische en strategische (personeels)kosten.

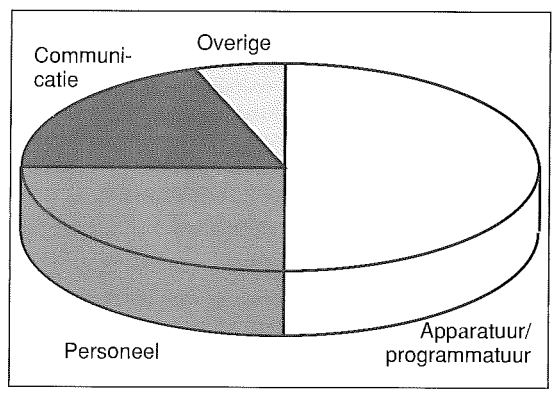
In personele bezetting (FTE's; dit is Full Time Equivalent) is deze verhouding één staat tot vier. Dit wordt veroorzaakt door de hogere loonkosten per medewerker voor de tactische en strategische functies.



Figuur 5. Verhoudingen operationele/tactische/strategische personeelskosten.

Apparatuur-, programmatuur-, communicatie- en personeelskosten
Uit onderzoek naar de exploitatiekosten van WAN's kan een eerste verhouding worden afgeleid tussen genoemde kostencomponenten. Een toelichting op het gehanteerde kostenmodel is opgenomen in de paragraaf Kosten en doorbelasting. De aangetroffen verdeling van de exploitatiekosten is als volgt:
- apparatuur- en programmatuurkosten 40 tot 60 procent;
- personeelskosten 20 tot 30 procent;
- communicatiekosten 15 tot 25 procent;
- overige kosten 0 tot 5 procent.

Figuur 6. Verhoudingen apparatuur- en programmatuur/communicatie/personeelskosten.



Deze verdeling biedt de mogelijkheid de personeelskosten in orde van grootte te bepalen en bij een gegeven of geprognotiseerde apparatuur- en programmatuurlast te voorspellen.

Decentralisatie en uitbesteding

In het beschreven organisatiemodel zitten behoudens de omvang en verdeling van de personele bemanning ook enkele vrijheidsgraden ten aanzien van de exacte plaats van de desbetreffende verantwoordelijkheden en bevoegdheden. Aan de orde zijn de mate van decentralisatie en de mate van uitbesteding.

Decentralisatie en uitbesteding zijn onderwerpen die ieder op zich een artikel rechtvaardigen. In dit artikel willen we nu eens niet vervallen in de gebruikelijke plussen en minnen door voor genoemde functies de mogelijkheid of wenselijkheid van decentralisatie en uitbesteding te behandelen. In plaats daarvan richten we ons op de beschrijving van een overall organisatorisch kader, dat de mogelijkheden tot decentralisatie en uitbesteding illustreert.

In de volgende alinea's wordt dit kader inclusief bijbehorende sturingsmechanismen, zoals Service Level Agreements en business-plannen, kort toegelicht.

Van stafafdeling naar resultaatverantwoordelijke facilitaire functie
In de organisatie van de exploitatie van netwerken zien we een belangrijke verandering, gedreven vanuit het kwaliteitsbesef van het corporate management. Netwerken moeten zich steeds meer bewijzen en het credo 'van ondersteunend middel naar onderscheidend voordeel' waarmaken. In plaats van bij een ondersteunend staforgaan (bijvoorbeeld de Interne Dienst of de Dienst Automatisering) wordt de verantwoordelijkheid voor de exploitatie van netwerken ondergebracht bij een resultaatverantwoordelijke facilitaire (netwerk) functie.

Deze facilitaire functie c.q. dit facilitair bedrijf levert op aanvraag specifieke voorzieningen, zoals lokale netwerken aan de eveneens verbijzonderde business units. Voorts levert dit facilitair bedrijf verplicht enkele algemene voorzieningen, zoals telefonie of overkoepelende netwerken aan corporate. Aldus ontstaat de in figuur 7 opgenomen driehoeksverhouding.
Om deze driehoek goed te laten functioneren is een aantal sturingsmechanismen onmisbaar.

Service Level Agreements
In het Service Level Agreement tussen een business unit en het facilitair bedrijf staat beschreven welke specifieke services en service levels onder wat voor condities worden geleverd.
In het Service Level Agreement tussen corporate en het facilitair bedrijf staat vervat welke algemene services en service levels onder wat voor condities worden geleverd.

Als uitgangspunt zijn alle services specifiek voor een business unit, immers de netwerkkosten moeten worden opgebracht door de renderende bedrijfsonderdelen. Naarmate business units soortgelijke wensen hebben en het draagvlak voor een specifieke service toeneemt, ontstaat de mogelijkheid een algemene service te definiëren die financieel-economisch aantrekkelijk kan worden aangeboden aan de desbetreffende business units.

Discussiepunt is veelal welke specifieke services tevens als algemene services kunnen worden beschouwd, met andere woorden welke specifieke services komen in aanmerking voor levering aan meerdere business units en welke (mate van) standaardisering mag daarvoor worden gehanteerd om de beheersbaarheid en daarmee de kosten enigszins in bedwang te houden.

In de praktijk leidt dit tot enkele algemene services waarvoor leverings- en afnameplicht bestaat, zoals telefonie. Daarnaast zijn er diverse specifieke services die op maat en in concurrentie met eigen decentrale of derde aanbieders worden geleverd. Uitgangspunt is dat een specifieke service slechts tot algemene service kan worden verheven indien hiertoe bij de business units een breed draagvlak bestaat.

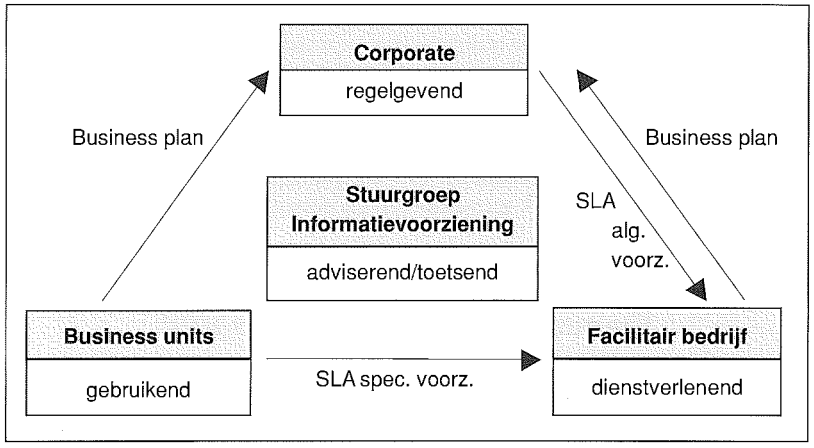
Om wildgroei en daarmee een onbeheersbare toename van de kosten te voorkomen is het essentieel dat de business units en het facilitair bedrijf worden afgerekend op hun resultaat en dat ineffectieve of inefficiënte oplossingen tot uitdrukking komen in dit resultaat.

Business-plannen
In de business- c.q. informatieplannen van de business units worden vanuit de primaire en secundaire processen de toepassingen van IT beschreven. Deze IT-toepassingen vormen een belangrijke basis voor de definitie van de benodigde netwerkservices.

In het business-plan van het facilitair bedrijf wordt aangegeven welke services en service levels het facilitair bedrijf tegen welke condities wil aanbieden, welke investeringen daartoe op wat voor termijn benodigd zijn en welk resultaat daarvan mag worden verwacht.

Door corporate dient een afstemming tot stand te worden gebracht tussen de diverse plannen van de business units onderling en in relatie tot het plan van het facilitair bedrijf. Voordelen voor één business unit moeten worden gerelateerd aan mogelijke nadelen voor andere business units en daarmee het concern als geheel. Dit kan betekenen dat de plannen van enkele business units (in overleg) worden bijgesteld om het ontstaans- dan wel bestaansrecht van een breder draagvlak en mogelijkerwijs een algemene service te rechtvaardigen.

Stuurgroep Informatievoorziening
Veelal zal corporate zich laten adviseren door een stuurgroep Informatievoorziening. Deze stuurgroep bevindt zich tussen afnemers (business units en corporate) en aanbieder (facilitair bedrijf) in en dient door alle betrokken partijen als onafhankelijk te worden ervaren en het algemeen bedrijfsbelang te behartigen.



Figuur 7. Driehoeksverhouding.

Gedwongen winkelnering
Een belangrijke vraag bij de inrichting van geschetste driehoek is de concurrentiepositie van het facilitair bedrijf. Voor de specifieke wensen van de business units is het marktmechanisme aantrekkelijk. Enerzijds voorkomt dit (te) hoge prijzen van het facilitaire bedrijf, anderzijds ontslaat dit het facilitaire bedrijf van de verplichting tot levering. Voor de algemene voorzieningen voor corporate is het onverstandig buiten de deur zaken te doen. Daarmee vervalt de bestaansgrond voor het facilitair bedrijf. Desgewenst kan gekozen worden voor uitbesteding van een aantal (veelal operationele) facilitaire taken.

Voorkomen moet worden dat het facilitair bedrijf blijft zitten met enkele kostbare, door corporate zwaar gesubsidieerde bijzondere voorzieningen, terwijl de lucratieve algemene voorzieningen buiten de deur worden ingekocht.

Centraal/decentraal/derden
Voor de specifieke voorzieningen is in principe sprake van decentralisatie. De business unit bepaalt op welke wijze zij de desbetreffende voorziening willen (laten) invullen. In sommige gevallen kan het financieel-economisch aantrekkelijk zijn zaken te doen met het facilitaire bedrijf dat soortgelijke voorzieningen levert en eventuele koppelings- en integratieproblemen oplost. In andere gevallen kan het aantrekkelijk zijn buiten de deur zaken te doen. En soms geniet een eigen invulling de voorkeur.

Voor de algemene voorzieningen is in principe sprake van centralisatie. Deze voorzieningen worden (veelal verplicht) geleverd door het facilitaire bedrijf en (veelal verplicht) afgenomen door corporate en de business units. Eventueel kunnen enkele operationele facilitaire taken worden uitbesteed aan derden.

Voor de uiteindelijke organisatievorm betekent decentralisatie dat (een deel van) het organisatiemodel eveneens wordt georganiseerd bij de afzonderlijke business units. Veelal betreft dit de invulling van een eigen help desk plus eerstelijnsondersteuning en een Informatiemanagementfunctie waar gecombineerd de planning en ontwikkeling van IT-toepassingen en netwerken wordt voorbereid.

Voordelen voor één business unit moeten worden gerelateerd aan mogelijke nadelen voor andere business units en daarmee het concern als geheel.

Uitbesteding
Met de opzet van een resultaatverantwoordelijke facilitaire functie en het aangaan van contractuele relaties zoals SLA's, ontstaat de mogelijkheid facilitaire taken uit te besteden aan derden dan wel (delen van) deze facilitaire functie te laten overgaan naar derden. Met het toekennen van een eerste en eigen verantwoordelijkheid aan de business units ontstaat eveneens een mogelijkheid tot uitbesteding.

In dit artikel is niet of nauwelijks ingegaan op de vraag welke taken zich vervolgens bij uitstek lenen voor uitbesteding. Er is slechts gepoogd een kader te scheppen waarbinnen uitbesteding op een verantwoorde wijze aan de orde kan komen.

KOSTEN EN DOORBELASTING

In het voorgaande deel is aandacht besteed aan het definiëren van de services en service levels en het daarop inrichten van de netwerkorganisatie. Ten slotte zullen, overeenkomstig het aanvankelijk geschetste stappenplan, de kosten van deze organisatie met bijbehorende (hulp)middelen moeten worden toegerekend aan de geleverde services.

Deze toerekening valt uiteen in twee delen:
1. het bepalen van de kosten;
2. het vertalen van de kosten in tarieven.

Tussen kosten en tarieven zit een aanmerkelijke stap die de netwerkorganisatie de gelegenheid biedt het gebruik van services enigszins te sturen.

Voor het bepalen van de kosten is een kostenmodel ontwikkeld. Dit model is een afgeleide van het veel gehanteerde Index-model [Inde89] en beschrijft de exploitatielasten van netwerken.
Voor het vertalen van de kosten in (commerciële) tarieven zijn enkele overwegingen opgenomen die aan de hand van een tariefstructuur kort worden toegelicht.

Kostenmodel

Voor de financiële beheersing van het netwerkmanagement is het essentieel te beschikken over een model dat de bijbehorende kosten op eenduidige manier in kaart brengt. Door het meten, analyseren en vergelijken van deze kosten kunnen trends worden voorspeld en afwijkingen ten opzichte van de norm worden geconstateerd.

Zoals hiervoor is aangegeven is het ontwikkelde kostenmodel gebaseerd op het Index-model. Uit de praktijk blijkt dat dit Index-model soms onnodig complex is, en differentiaties aanbrengt die in de praktijk niet of nauwelijks te achterhalen zijn. Aan de hand van enkele nadere studies hebben wij het in figuur 8 opgenomen kostenmodel opgesteld.

Dit model beschrijft de exploitatiekosten van netwerken onderverdeeld naar apparatuur-, programmatuur-, communicatie- en personeelskosten. De overige kosten van interne faciliteiten zoals huisvesting en dergelijke blijken in de praktijk gering (minder dan vijf procent) en worden daarom in het model niet meegenomen.

De eenmalige (aanschaf)kosten worden wel geïnventariseerd, maar (in de vorm van afschrijvingen) verwerkt in de periodieke exploitatielasten. In sommige gevallen is sprake van lease en kunnen de aanschafkosten niet worden bepaald. De leasecomponent kan dan worden meegenomen in de exploitatielasten.

Het onderscheid tussen apparatuur en programmatuur is lastig te hanteren. De programmatuur valt uiteen in systeem- en applicatieprogrammatuur. Systeemprogrammatuur is veelal opgenomen in de aanschafprijs van de apparatuur. Applicatieprogrammatuur betreft de netwerk- en communicatie-software. In het model zijn de apparatuur- en programmatuurkosten niet onderscheiden.

Facturen netwerkleverancier
In de praktijk blijkt dat facturen van netwerkleveranciers veelal onvoldoende aanknopingspunten bieden voor het onderscheiden van leveringen en diensten. Op één en dezelfde periodieke factuur staan bijvoorbeeld de kosten van uitbreidingen, upgrades en onderhoud (in totaliteit) opgenomen. In de onderhandelingen met de leverancier dient daarom bij voorkeur te worden afgedwongen dat de opbouw van de factuur naar de inzichten van de afnemer kan worden opgesteld. Dit kan tot aanzienlijke besparingen in de kosten van doorbelasting leiden.

Specificatie en differentiatie
Met het geschetste kostenmodel kunnen de totale exploitatiekosten van het netwerk worden bepaald. Vervolgens dienen deze totale kosten te worden toegerekend aan de afzonderlijke services. Hiertoe moeten de kostendragende services en de kostendragende eenheden worden bepaald.

Voor genoemde gangbare netwerkservices is dit met name de service Aansluiting c.q. verbinding.

Kostendragende eenheden zijn bijvoorbeeld de duur of capaciteit van de verbinding en/of de omvang van het verkeer. Met het bepalen van deze kostendragende services en bijbehorende eenheden begeven we ons op het raakvlak met de tarifering. De kostendragende eenheden hoeven echter niet per definitie ook de tariefbepalende eenheden te zijn. Eventueel kan worden gekozen voor vereenvoudiging, waarbij de variatie in kosten wordt teruggebracht van volledig variabel tot beperkt variabel (bijvoorbeeld een vaste prijs tot een bepaald maximum, daarboven een surplus afhankelijk van het gebruik).

De uiteindelijke verdeling van de kosten blijft altijd enigszins discutabel. Doelstelling is niet de kosten minutieus toe te rekenen, maar de kosten op een rechtvaardige wijze te verdelen zonder daarbij hoge kosten te moeten maken om exacte verdelingen te kunnen vaststellen.

	Aanschaf	Gebruik	Toelichting
1. Apparatuur & Programmatuur	• Aanschafkosten • Installatiekosten • Initiële kosten	• Hard/software onderhoud • Verzekeringen • Licenties	• Netwerk & netwerk-beheer
2. Personeel	• Ontwerp • Selectie • Installatie • Eigen ontwikkelingen • Training en vorming • Werving	• Netwerk-management • Reis- en verblijfkosten • Opleiding	• Eigen en derden
3. Communicatie	• Initiële aansluitkosten	• Maandelijkse lijnkosten • Verkeerskosten	• Centraal en lokaal
	Subtotaal aanschaf	***Subtotaal gebruik***	
		Afschrijvingen +	
		Totale exploitatiekosten	

Figuur 8. Kostenmodel.

Tariefstructuur

Om de exploitatielasten te kunnen doorbelasten dienen de geïnventariseerde kosten in tarieven te worden vertaald. Daartoe kan gebruik worden gemaakt van de in figuur 9 opgenomen eenvoudige tariefstructuur.

Tarieven zijn in principe opgebouwd uit de volgende drie componenten:
1. vaste tarieven (eenmalig en periodiek);
2. variabele tarieven;
3. kortingen.

Verbindingen
Voor de primaire service Aansluiting c.q. verbinding van de netwerkorganisatie is deze structuur nader uitgewerkt:
- vaste tarieven zijn eenmalig (aansluiting) en/of periodiek (abonnement);
- variabele tarieven zijn gerelateerd aan de duur of capaciteit van de verbinding (aantal minuten/aantal Kb/s) en/of de omvang van het verkeer (aantal Kb). Voorts kan het tijdstip (binnen/buiten kantooruren) en de bestemming (Nederland/Europa/Verenigde Staten /etc.) een rol spelen;
- kortingen zijn veelal afhankelijk van de hoeveelheid verkeer.

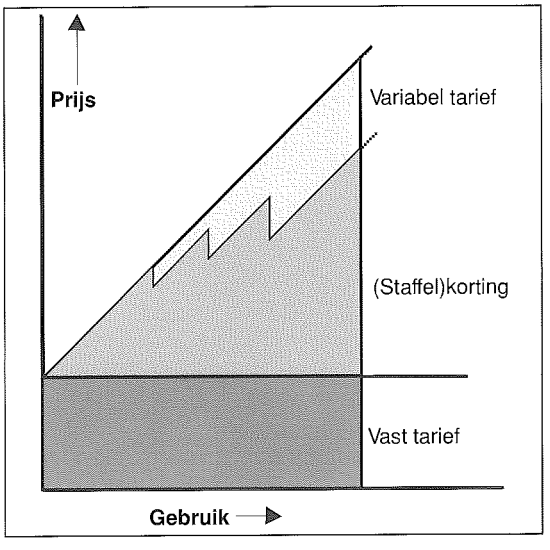
Door de prijzen van aansluitingen (eenmalige kosten), abonnementen (periodieke kosten) en berichten (variabele kosten) te variëren kunnen tariefscenario's worden doorgerekend bij verschillende afzetprognoses. Voorts kan de gevoeligheid van dit resultaat voor afwijkingen in de afzetprognoses worden bepaald. Aldus kunnen mogelijke consequenties van een bepaalde tariefstelling worden voorspeld en worden meegewogen in de uiteindelijke keuze.

Deze keuze wordt mede gestuurd vanuit de volgende beginselen inzake vaste en variabele tarieven en kortingen.

Vaste tarieven
Lage eenmalige tarieven bevorderen de toegankelijkheid van de service omdat de aanvangsinvestering voor de gebruikersorganisatie gering blijft.

Hoge vaste tarieven beperken het ondernemingsrisico van de netwerkleverancier omdat bij voorbaat duidelijk is welke inkomsten genoten zullen worden voor een bepaalde service.

Figuur 9. Tariefstructuur.



Ir. E.J. Evelo
Is senior organisatie-adviseur bij KPMG Klynveld Management Consultants en verantwoordelijk voor het adviesgebied Netwerken. Hij heeft zich gespecialiseerd in de organisatorische en financiële aspecten rond netwerkmanagement.

Variabele tarieven
Lage variabele tarieven verminderen de onzekerheden in de begroting van de gebruikersorganisatie omdat onafhankelijk van het daadwerkelijk gebruik de kosten kunnen worden begroot.

Hoge variabele tarieven bevorderen de efficiency van het verkeer omdat wijzigingen in de omvang van het verkeer (direct) zijn terug te lezen in de hoogte van de factuur.

Kortingen
Kortingen dienen alleen te worden verleend bij daadwerkelijke kostenreducties, zoals schaalgroottevoordelen, omdat anders het risico bestaat dat uitsluitend gereduceerde services worden afgenomen, hetgeen tot een exploitatietekort kan leiden.

Beslisboom
In de praktijk dient voor de service waarvan het tarief moet worden vastgesteld een reeks van vragen te worden beantwoord die in de vorm van een beslisboom leiden tot een voorzet voor een tariefstructuur. Deze vragen zijn deels van commerciële aard (strategie en marketing) en deels van technische aard (kostenopbouw en beheersing).

Leidraad is dat de kosten gepaard gaande met de tarifering in redelijke verhouding moeten staan tot het (extra) inzicht dat en de beheersing die zij de gebruikersorganisatie biedt. Kosten die niet beïnvloedbaar zijn door de gebruikersorganisatie zijn niet relevant vanuit de optiek van kostenbeheersing en voegen weinig toe aan de waarde van de factuur.

SAMENVATTING

In dit artikel is gepoogd een aanpak te schetsen voor een beheerste exploitatie van netwerken. Deze aanpak heeft als kern een optimale afstemming tussen gebruikersorganisatie en netwerkorganisatie door het in overleg definiëren van de services, het daarop afstemmen en inrichten van de organisatie en het zichtbaar maken en doorbelasten van de bijbehorende kosten.

Voor het inventariseren en definiëren van de services en service levels is een checklist van gangbare netwerkservices aangereikt en de inhoud van een Service Level Agreement geschetst.
Voor het inrichten van de netwerkorganisatie is een organisatiemodel toegelicht en is de werking van enkele sturende en beheersende mechanismen rond decentralisatie en uitbesteding beschreven.
Voor het bepalen en doorbelasten van de kosten is een kostenmodel aangereikt en zijn enkele overwegingen rond de vertaling van kosten in tarieven gegeven.

De invalshoek van dit artikel is beperkt tot de organisatorische en financiële aspecten van het netwerkmanagement, omdat vanuit deze optiek belangrijke kostenreducties en effectiviteitsverbeteringen kunnen worden gerealiseerd. De technische infrastructuur en bijbehorende (netwerkmanagement)tools vormen de basis voor de netwerkservices; de organisatorische opzet en financiële beheersing bepalen het uiteindelijke rendement.

In de komende jaren zullen de exploitatiekosten van netwerken blijven toenemen. Alleen door beheerste groei kunnen deze kosten worden opgebracht door afnemende gebruikersorganisaties. Dit vraagt om een voortdurende afstemming tussen gebruikersorganisatie en netwerkorganisatie, waarbij de gebruikersorganisatie zich desgewenst laat adviseren door de netwerkorganisatie, zonder dat deze gaat overheersen en voorschrijven.

In de praktijk zien wij helaas nog al te vaak een centrale netwerkorganisatie die vanuit haar ivoren toren weet wat goed is voor haar afnemers en naarmate de complexiteit van de problematiek toeneemt steeds rigider gaat optreden. Hoewel deze netwerkorganisatie de exploitatie van de desbetreffende services soms uitstekend beheerst, komt de kernvraag rond de definitie, organisatie en doorbelasting van services onvoldoende aan de orde, waardoor de afstemming tussen vraag en aanbod ontbreekt. Dit artikel biedt daartoe een eerste handvat.

LITERATUUR

[Inde89] *The Costs of Network Ownership,* Index Group 1989.

en telecommunicatie, de organisatorische ontwikkeling

H. Reijn

Dat het van belang was de beheersorganisatie van de netwerkvoorzieningen binnen Akzo aan te passen aan de eisen die vanuit het management aan deze voorzieningen worden gesteld, is door Akzo in een vroeg stadium onderkend. Een kijkje in de keuken van Akzo Information Services, het resultaat van een lange periode van organisatorische veranderingen.

INLEIDING

Eind jaren tachtig bestaat bij Akzo geen herkenbare organisatie voor telecommunicatie. Taken op dit gebied zijn ondergebracht op verscheidene plaatsen binnen de vijf verschillende divisies, bij locatiediensten en bij het corporate rekencentrum in Arnhem. De divisionele en lokale EDP (Electronic Data Processing)-afdelingen zijn verantwoordelijk voor de datacommunicatie rondom de beheerde computersystemen. Sterk PTT-gerichte diensten als spraak, telex en facsimile worden geleverd door locatiediensten, veelal vanuit de Technische Dienst.

Deze structuur weerspiegelt de Akzo-organisatie in die tijd: een eilandenrijk van verschillende ondernemingen, werkmaatschappijen, landenorganisaties en divisies, relatief licht gestuurd door het hoofdkantoor in Arnhem. Automatisering is in hoge mate gedecentraliseerd, met vele lokale rekencentra en kleine EDP-afdelingen.

In Arnhem is een - klein - corporate rekencentrum ondergebracht, Akzo Data Services (ADS), verantwoordelijk voor het leveren van computer- en netwerkservices gebaseerd op IBM-mainframe-technologie. Deze services worden in principe geleverd aan alle Akzo-bedrijven die daar in aanvulling op hun eigen automatiseringsmiddelen gebruik van willen maken.

Het ADS-netwerk, met vaste verbindingen binnen Nederland en een aantal Europese landen, is vrijwel geheel een traditioneel IBM SNA (Systems Network Architecture)-netwerk, zoals dat ook nu nog bij veel organisaties rondom mainframes wordt aangetroffen. De computer vormt het hart van de afdeling, het netwerk is een afgeleide van de computer. Organisatorisch is de netwerkgroep (drie personen) een onderafdeling van de computerservices-afdeling van het rekencentrum.

Hoe van deze structuur werd gekomen tot de huidige IT-infrastructuur, waarvan het netwerk te zamen met de daaraan gekoppelde computers het middelpunt vormt, wordt in dit artikel beschreven.

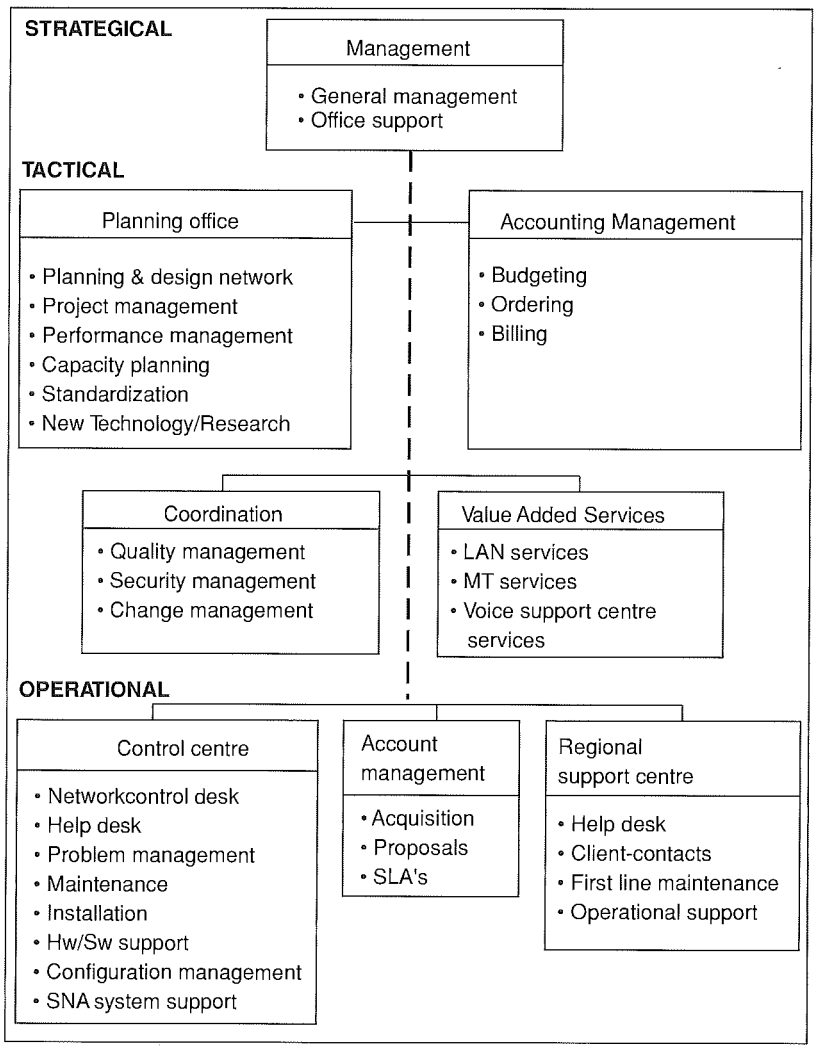
TELECOMMUNICATIE, EEN NIEUW TAAKVELD

In deze paragraaf wordt beschreven welke gebeurtenissen de aanzet vormden voor de organisatorische verandering van Akzo Data Services (ADS).

Eerste stap

De eerste stap naar een verandering in deze situatie wordt gezet als het management van ADS, nu zes jaar geleden, besluit een deskundige op het gebied van telecommunicatie binnen de afdeling te halen. Aanleiding hiertoe is de vraag die vanuit de Technische Dienst in Arnhem wordt gesteld voor assistentie bij de keuze en implementatie van een nieuw huistelefoonsysteem, een PABX (Private Automated Branch eXchange). De leverancier van de PABX begint bij het voortraject van de keuze te praten over zaken als digitaal, ISDN, datacommunicatie, lokale netwerken en software. Onderwerpen die voor de TD nieuw zijn. De vraag om assistentie vanuit het computercentrum is derhalve logisch. Echter, het computercentrum beschikt niet over kennis op dit terrein en besluit deze van buiten te halen. Zo ontstaat binnen ADS een nieuw taakveld: telecommunicatie.

Figuur 1. De organisatie van TS.



Voorzien wordt dat dit werkveld in de toekomst belangrijk gaat worden, en dat het verstandig is om naast de kennis en ervaring die de afdeling reeds bezit op het gebied van computers, ook te investeren in kennis op het gebied van telecommunicatie. Dit beleid wordt in daden omgezet door veel tijd en ook geld te besteden aan het opleiden van de medewerkers voor wat betreft met name het managen van telecommunicatie. Niet zozeer de kennis op het gebied van 'hoe werkt het' wordt verbreed, maar veeleer ligt het accent op de vragen 'wat kun je ermee' en 'hoe kun je telecommunicatie inzetten ter verbetering van de bedrijfsvoering'.

Nadat op deze wijze een kleine kiem wordt gelegd in het computercentrum, ontpopt dit zich als een groeikern. De eerstvolgende stap is dat na ongeveer anderhalf jaar de telecommunicatie- en de datacommunicatiedeskundigen worden samengebracht in een nieuwe groep: Telecommunicatie Services (TS). Deze groep, waarin dus ook de medewerkers zijn ondergebracht die het 'mainframenetwerk' opereren, wordt organisatorisch naast de computerservices geplaatst, waarmee het rekencentrum in feite uit twee hoofdafdelingen gaat bestaan, telecommunicatie- en computerservices. Dit alles binnen de afdeling ADS, het corporate rekencentrum.

In de hierop volgende periode groeit de Telecommunicatie Services-groep van drie naar vijftien medewerkers. Deze toename komt tot stand door medewerkers die elders in de organisatie werkzaam zijn op het gebied van telecommunicatie, te concentreren in de nieuwe groep. Op deze wijze wordt de groep versterkt met kennis op LAN-gebied, electronic mail, telefonie, Wide Area Netwerk (WAN)-expertise (anders dan alleen SNA) en bekabeling. Ruim de helft van de groep heeft een academische of HBO-vooropleiding. Twee medewerkers van de groep hebben een post-academische opleiding tot 'Master of Business Telecommunications' afgerond, verscheidene de post-HBO-opleiding 'Digitale Telecommunicatie'. In figuur 1 is de organisatie van TS schematisch weergegeven.

Cultuurverandering

Geleidelijk aan wordt vervolgens een belangrijke cultuurverandering ingezet. Het betreft de verandering van specifiek produktgericht naar meer dienstgericht werken. Veel van de medewerkers die naar de TS-groep zijn gekomen, hebben vanuit de oude organisatie een sterke relatie met een produkt, waardoor men geneigd is, altijd als oplossing alleen het eigen produkt te kiezen. De PROFS-deskundige biedt geen electronic mail-dienst aan, maar een produkt. De SNA-deskundige kent geen andere oplossingen voor Wide Area Netwerktransportdiensten dan de IBM-oplossingen, etc. Gevolg van deze verandering is dat de TS-groep diensten gaat aanbieden als datatransport, local-

netwerkontwerp, electronic mail, EDI en algemene adviesdiensten.

Het moge duidelijk zijn dat de verantwoordelijkheid van de Telecommunicatie Services-groep nu dus zowel het datacommunicatietaakveld als ook de diensten op het gebied van spraak, tekst en video omvat. In veel bedrijven echter worden met de term telecommunicatie alleen de traditionele PTT-diensten aangeduid, zonder de koppeling naar de datacommunicatiewereld. Vaak bestaan er wel telecommunicatie-afdelingen, maar die hebben geen of weinig binding met de rekencentra-organisatie. Binnen Akzo is de weg gevolgd van een opbouw van een telecommunicatie-afdeling vanuit de rekencentra-organisatie.

Tot nog toe kan deze verandering binnen Akzo probleemloos worden uitgevoerd. Het volledige veranderingsproces voltrekt zich binnen de centrale afdeling en de verantwoordelijkheden van noch divisies noch Technische Diensten worden op enigerlei wijze aangetast. Integendeel, de TS-groep in Arnhem bezit kennis die een duidelijke meerwaarde biedt voor de decentrale afdelingen, en deze afdelingen maken daar met plezier gebruik van. Vanuit de Akzo-organisatie neemt de vraag naar expertise op het totale gebied van telecommunicatie toe, zoals was voorzien, en de TS-groep geeft hier invulling aan.

Ook is de TS-groep in staat te reageren op de veranderingen bij de nationale PTT. Van oudsher werden alle contacten met de PTT lokaal afgehandeld. Echter, de structurele wijzigingen aan PTT-zijde, zoals het vrij worden van de markt voor randapparatuur, inclusief PABX-systemen, en de toenemende concurrentie maken het voor een bedrijf als Akzo aantrekkelijk om richting PTT niet meer als vele - kleine - individuele lokale klanten op te treden, maar als één grote klant.

Illustratief voor de veranderingen die zijn opgetreden op het telecommunicatiegebied in de laatste jaren is het volgende voorbeeld. Bij het eerste contact over de nieuwe PTT-ontwikkelingen bij de centrale inkoopafdeling van Akzo was men daar geenszins bereid om ook maar enige tijd in onderhandelingen met PTT Telecom te steken. Dit werd als geheel nutteloos gezien. Vandaag de dag werken er twee gespecialiseerde corporate inkopers op het terrein van de telecommunicatie. Hun inzet heeft inmiddels geleid tot een aantal Akzo-contracten met leveranciers, waarvan enkele een wereldwijde dekking hebben. De telecommunicatiekosten zijn hierdoor significant en aantoonbaar gedaald.

TOPMANAGEMENT BETROKKEN

Naast de geschetste ontwikkelingen die kunnen worden gezien als komende van onder uit de organisatie, wordt ook op Akzo-management-niveau en specifiek bij het IT-topmanagement duidelijk dat telecommunicatie een steeds belangrijker aandachtsgebied wordt en dat het belang van telecommunicatie voor de business van Akzo sterk groeiende is. Steeds vaker echter wordt men ook geconfronteerd met de 'eilandensituatie' waarin Akzo nog altijd verkeert. Met name op het gebied van de datacommunicatie blijken de vele gekozen 'eilandoplossingen' te leiden tot grote koppelingsproblemen, terwijl juist het netwerk de rol van 'enabler' - iets wat iets mogelijk maakt - wordt toegedacht.

Het belang van telecommunicatie voor de business van Akzo is sterk groeiende.

Het besef groeit dat er een Akzo-beleid moet worden ontwikkeld voor telecommunicatie. Een eerste aanzet daartoe wordt gegeven door een onderzoek van een externe consultant die in nauw overleg met de Corporate IT policy-groep en het CTC (Communication Technology Committee) een telecommunicatiebeleid formuleert.

Het CTC bestaat uit een aantal personen uit de verschillende divisies, verantwoordelijk voor data- en telecommunicatie. Het CTC wordt voorgezeten door de manager van de centrale TS-groep, en rapporteert aan het IT Committee. Het IT Committee is samengesteld uit de divisionele IT-managers. Het CTC heeft als taak ontwikkelingen op telecommunicatiegebied binnen Akzo te coördineren en het te voeren beleid voor te bereiden voor het IT Committee. Tot dit moment echter was de CTC met name een operationeel gerichte groep, waarin de dagelijkse problemen van netwerkbeheerders werden besproken.

Hoewel het beleid nooit formeel wordt aanvaard, is het zeker een stap in de goede richting. De discussie over de juistheid en haalbaarheid van de aanbevelingen leidt de aandacht af van de dagelijkse problematiek en verlegt deze naar de toekomst. Tactiek en strategie hebben veel aan belangrijkheid gewonnen. Akzo beseft dat het kunnen bereiken van beschikbare informatie voor de business, snel en betrouwbaar, vraagt om geplande telecommunicatievoorzieningen.

Naar een corporate-netwerk

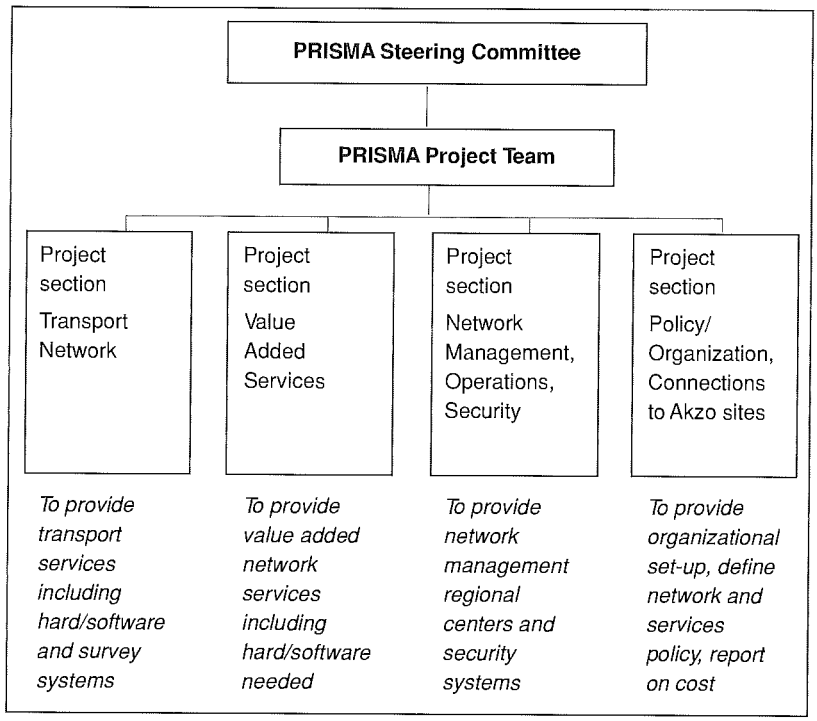
De discussie over een adequate telecommunicatiestrategie wordt in hoge mate beïnvloed door belangrijke organisatorische ontwikkelingen bij Akzo. Akzo's topmanagement heeft besloten een Corporate Identity-programma door te voeren met als doel Akzo veel meer als één bedrijf te laten opereren en daar waar mogelijk synergie-effecten te benutten. Tevens wordt de divisionele organisatie veranderd in een Business Unit (BU)-organisatie, waarbij de ruim veertig BU's, gebaseerd op specifieke produkt/markt-combinaties, de nieuwe basiselementen van de Akzo-organisatie vormen. Ondersteunende afdelingen aan de BU's worden in

de nieuwe structuur ondergebracht als Service Units (SU). De BU's zijn geclusterd in vier nieuwe Groepen, die de oude divisiestructuur vervangen.

Dit, gevoegd bij de algemene trend naar internationalisering en globalisering van Akzo's business, de verkoop en acquisitie van bedrijven inclusief het uitwisselen van bedrijfsonderdelen (swaps), geeft aanleiding tot vele nieuwe wensen en eisen op het gebied van communicatie, zowel binnen Akzo als tussen Akzo en business-relaties (klanten, toeleveranciers, banken en dergelijke).

Eind 1990 wordt een 'Decision Paper Telecommunication Strategy' opgesteld en door de Raad van Bestuur bekrachtigd, waarin belangrijke beslissingen voor heel Akzo op telecommunicatiegebied worden geformuleerd. Telecommunicatie wordt hierin gedefinieerd als alle vormen van elektronische communicatie. De volledige verantwoordelijkheid voor het beleid op telecommunicatiegebied wordt in de IT-kolom gelegd. De noodzaak tot een corporate-netwerk wordt onderschreven, waarbij tot het corporate-netwerk ook de organisatie voor ontwikkeling en beheer van dit netwerk wordt gerekend. Er wordt besloten dat de operationele kosten voor het corporate-netwerk in rekening moeten worden gebracht bij de gebruikers. De TS-groep van ADS krijgt opdracht invulling te geven aan de besluiten.

Figuur 2. Organisatie van het PRISMA-project.



PRISMA

Het antwoord op de vraag naar een corporate-netwerk wordt gevonden in de vorm van het PRISMA-project. PRISMA (Plan to Realize Infrastructural Services and Management for Akzo) omvat alle telecommunicatiediensten - spraak, data, tekst en beeld - tussen alle Akzo-locaties wereldwijd en Akzo en de 'buitenwereld'. Doelstelling van het project is om de telecommunicatie-infrastructuur van Akzo te verbeteren, met name op het gebied van de vereiste interconnectie, tegen voor Akzo lagere kosten.

In zekere zin is het PRISMA-project binnen Akzo uniek. Het is één van de weinige projecten, en zeker binnen de IT-kolom, waarbij alle Akzo-onderdelen actief participeren, en de scope wereldwijd is.

Het projectvoorstel wordt goedgekeurd inclusief de projectorganisatie (zie figuur 2), de planning en het benodigde budget. Een gebruikelijke organisatie, zeker binnen Nederland, met een Stuurgroep, een Projectgroep en een aantal deelprojecten wordt opgezet. In de Stuurgroep zijn naast een tweetal IT-managers ook twee Business Unit-managers opgenomen waarmee nogmaals het belang van een corporate-telecommunicatie-infrastructuur voor Akzo's business wordt onderstreept.

Het project wordt opgehangen aan de Corporate IT-manager, buiten het directe management van het corporate-rekencentrum om. Deze keuze wordt bewust gemaakt. Steeds duidelijker wordt merkbaar dat de Telecommunicatie Services-groep van het rekencentrum een eigen werkveld heeft gekregen en dat ook het stadium van ontwikkeling van de dienstverlening heel anders is als dat van de reeds veel langer bestaande computerservices. De dynamiek van de telecommunicatie-ontwikkelingen is groter en vereist derhalve een ander management dan het meer op continuïteit en stabiliteit gerichte rekencentrummanagement. Daarnaast wordt de groep nog door veel klanten gezien als de groep die alleen maar de communicatie van het rekencentrum zelf verzorgt, terwijl de taak van de TS-groep inmiddels veel breder is. De ophanging van het PRISMA-project buiten het rekencentrum om kan worden gezien als de volgende stap naar een organisatorische plaats van de Telecommuni-catie Services naast de computercentrumorganisatie en niet meer erbinnen.

Heel nadrukkelijk wordt het project binnen Akzo niet vanuit een technische invalshoek gepresenteerd, maar vooral vanuit een organisatorisch perspectief en het belang van een gezamenlijke infrastructuur voor de business. Als je wilt communiceren moet het kunnen. Welke technologie waarvoor wordt gebruikt, is van ondergeschikt belang. De belangrijkste voordelen die Akzo in het vooruitzicht worden gesteld, zijn een kwaliteitsverbetering op het gebied van datacommunicatie door het geleidelijk opheffen van de 'eilandenstructuur', en een kostenbesparing op het gebied van spraakcommunicatie.
Het PRISMA-project heeft een duur van twee jaar.

Het eerste jaar wordt vooral benut voor het verder uitwerken en detailleren van de plannen, het tweede jaar is het jaar van de realisatie. Gestart wordt begin 1991 en eind 1992 zal het project moeten worden afgesloten. Ongeveer vijfendertig tot veertig mensen leveren een bijdrage, werkzaam bij ofwel een divisie ofwel de centrale TS-groep. Gedurende het project wordt de Akzo-organisatie regelmatig geïnformeerd over de doelstellingen en voortgang van het project. Hiertoe is een separaat Public Relation (PR)-programma ontwikkeld.

Van project naar netwerk

De resultaten van het project eind 1992 zijn zoals gepland. Er is een privé corporate-datacommunicatienetwerk ontworpen en geïnstalleerd dat zich uitstrekt over de meeste Westeuropese landen en Noord-Amerika. Vele Akzo-locaties zijn inmiddels op dit netwerk aangesloten. De projectnaam PRISMA, die binnen Akzo enige bekendheid heeft gekregen, zal na afloop van het project de naam blijven van dit Akzo Corporate Netwerk. Een organisatie is opgebouwd die het netwerk na afloop van het project zal exploiteren. In feite is dat de TS-groep, aangevuld met regionale netwerkcoördinatoren, die gedelegeerde taken van de centrale groep voor een bepaalde regio van de wereld uitvoeren.

PRISMA wordt binnen Akzo aangeboden in volledige concurrentie met externe netwerkleveranciers als PTT's en Value Added Netwerk-leveranciers. In principe is de klant vrij om PRISMA te kiezen. Er is geen 'gedwongen winkelnering'. Derhalve is voor PRISMA een tariefstructuur gekozen die volledig vergelijkbaar is met de tariefstructuren van 'derden'. Bij de start kent PRISMA een vast, capaciteitsafhankelijk, abonnement per aansluiting en een variabel, volume- en tijdafhankelijk tarief. De variabele tariefcomponent is tevens afhankelijk van de afstand waarover wordt gecommuniceerd: nationaal, continentaal of intercontinentaal. In de toekomst zal mogelijk een verdere differentiatie worden aangebracht, om concurrerend en marktconform te blijven in vergelijking tot externe aanbieders.

DE SERVICES VAN DE TELECOMMUNICATIE SERVICES-GROEP

De dienstverlening van de centrale TS-groep omvat een groot aantal werkterreinen en taakgebieden.

Werkterreinen
Wide Area Networks (SNA, DECnet, X.25)
Local Area Networks (Token Ring, Ethernet, Novell)
Message Transfer Services (electronic mail)
Terminal access, terminal emulatie
File transfer
Videoconferencing
PABX-systemen, PABX-koppelingen
Gebouw- en locatiebekabeling
Koppeling electronic mail met X.400, telex, telefax
Opstellen telecommunicatiestrategie
Voice mail, voice response
IBM/Digital-connectivity

Taken
Adviseren, consultancy
Ontwerpen
Configureren
Installeren, implementeren
Beheren
Introduceren nieuwe services.

Naast dit datacommunicatienetwerk is er een voice competence center opgericht dat alle telecommunicatie-ontwikkelingen op het gebied van spraak en gerelateerde diensten coördineert. Akzo-contracten zijn door het competence center in samenwerking met Akzo's Corporate inkoopafdeling afgesloten met verschillende PTT's voor virtuele netwerkdiensten en de aanschaf en het onderhoud van PABX-systemen.

Een Message Transfer Service ter ondersteuning van de electronic mail policy is gerealiseerd, welke gebruik makend van het datacommunicatietransportnetwerk verschillende electronic mail-omgevingen met elkaar verbindt. Nieuwe services als videoconferencing en voice mail zijn geïntroduceerd en worden op bruikbaarheid voor de business beproefd.

Gezien vanuit organisatorisch perspectief is het belangrijk hierbij op te merken dat de beslissingsbevoegdheid over de inrichting van de telecommunicatie-infrastructuur in hoge mate is gecentraliseerd. Op deze wijze kan langzaam maar zeker de puzzel die Akzo's telecommunicatie-infrastructuur was, in elkaar worden gelegd tot een gestandaardiseerd, betrouwbaar platform voor IT-applicaties.

AKZO INFORMATION SERVICES

Vrijwel parallel namelijk aan het PRISMA-project heeft een veel ingrijpender reorganisatie plaatsgevonden van de IT-organisatie binnen Akzo. De belangrijkste redenen voor deze verandering zijn een gewenste verbetering van de prijs/prestatie-verhouding van IT-toepassingen voor Akzo en de overtuiging dat IT inmiddels zo wezenlijk is geworden voor de bedrijfsvoering van Akzo dat de bestaande organisatie van IT niet voldoende in staat is daaraan invulling te blijven geven.

De Europese IT-organisatie is opgesplitst in een Informatie Management (IM)-functie op Corporate-, Groeps- en Business Unit-niveau en een apart bedrijf, Akzo Information Services (AIS) voor alle serviceverlening op IT-gebied. De IM-organisatie blijft onderdeel van Akzo's business-onderdelen (Holding, Groep, Business Unit) en zal optreden als inkoper van IT-services. Akzo Information

H. Reijn
Is sinds 1986 werkzaam bij Akzo, waar hij startte als telecommunicatie-consultant, met als specialistische gebieden telefonie en PABX-systemen. In 1988 werd hij tevens verantwoordelijk voor een deel van Akzo's datacommunicatienetwerken. Als projectleider PRISMA werd hij belast met het realiseren van het Akzo Corporate Netwerk. Vanaf de oprichting van Akzo Information Services in 1992 is hij als manager Facilities verantwoordelijk voor inrichting en beheer van de IT-faciliteiten (netwerken en computersystemen) van Akzo in West-Europa.

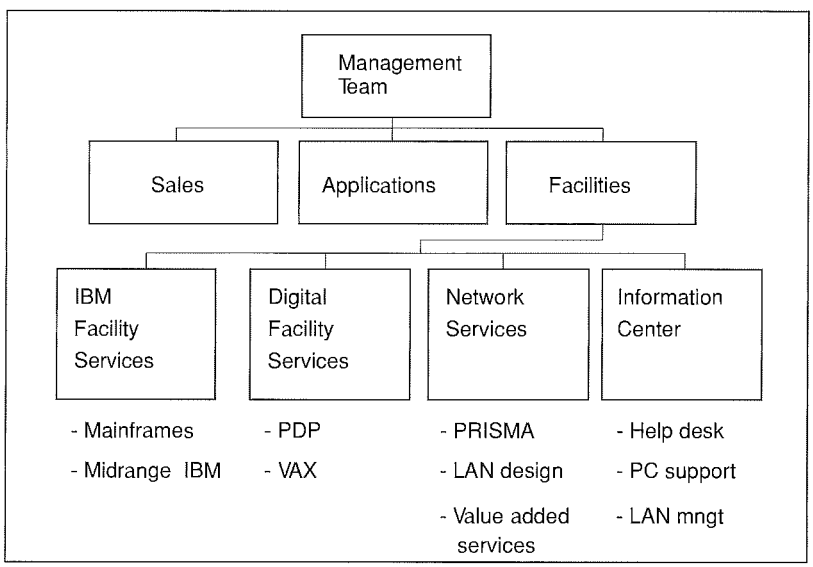
Services, een Service Unit op Corporate-niveau, zal aan Akzo IT-services verlenen op basis van een normale klant-/leverancier-verhouding. AIS zal in volledige concurrentie met 'derden' haar services aanbieden. Ook mag AIS zelf actief zijn op de externe, niet-Akzo, markt.

AIS is operationeel vanaf september 1992. De meeste Westeuropese EDP-service-afdelingen alsmede Akzo Systems maken inmiddels deel uit van AIS, waardoor een bedrijf is gevormd met ongeveer zeshonderd medewerkers opererend in Nederland, België, Frankrijk en Duitsland.

Intern is AIS georganiseerd in een drietal sectoren (zie figuur 3): Sales, Applications en Facilities. Stafafdelingen zijn gevormd voor Control, Quality en Personnel. Sales is verantwoordelijk voor de klantrelaties, Applications bouwt, implementeert en onderhoudt applicatieprogramma's en pakketten. Facilities is verantwoordelijk voor het opereren en beheren van Akzo's IT-infrastructuur, dat wil zeggen de computersystemen en netwerken.

De Facilities-organisatie is onderverdeeld in vier units, die elk volledig resultaatverantwoordelijk zijn. Deze units zijn IBM Facility Services, Digital Facility Services, Network Services en Information Center. IBM en Digital Facility Services verzorgen alle computerservices op de twee nu binnen Akzo meest voorkomende computerplatforms. De Network Services-groep is verantwoordelijk voor het PRISMA-netwerk, ontwerp van lokale netwerken, en alle eerder genoemde telecommunicatieservices. De Information Center-unit ten slotte verzorgt de help desk-functie, personal computer support en alle op locaties noodzakelijke operationele functies.

Figuur 3. Organisatie van Akzo Information Services.



CONCLUSIE

Binnen AIS heeft de 'oude' TS-groep nu een volwaardige plaats gekregen onder de nieuwe naam Network Services, met als opdracht de volledige telecommunicatie-infrastructuur voor Akzo in te richten en te beheren. Hetgeen als project is gestart, wordt nu voortgezet binnen de nieuwe IT-organisatie.

Moderne telecommunicatieservices zijn essentieel om efficiënt de nieuwe, internationale en vaak wereldwijde informatiestromen voor Akzo's managementprocessen te ondersteunen. Daarnaast kan telecommunicatie een zeker zo belangrijke rol gaan spelen in de dagelijkse operaties van Akzo's nationale en internationale bedrijfsvoering.

De besluitvorming over de netwerkinfrastructuur is vergaand gecentraliseerd om ervoor te zorgen dat de doelstelling van de infrastructuur - het realiseren en garanderen van vrije informatiestromen - wordt bereikt. De organisatorische plaats van telecommunicatie is de laatste jaren voortdurend aangepast aan het groeiende belang van telecommunicatie voor Akzo. Niet langer de computer vormt het middelpunt van de IT-infrastructuur, maar het netwerk te zamen met de daaraan gekoppelde computers. Het goed beheren en beheersen van deze totale IT-infrastructuur is de opdracht voor de komende jaren. Organisatorisch is Akzo daarop voorbereid.

SURFnet, beveiliging in een open netwerk

E. Zegwaart

Van oorsprong was het SURFnet-netwerk een open netwerk. Door de introductie van nieuwe diensten en toepassingsgebieden veranderden de eisen die aangesloten instellingen aan de beveiliging van SURFnet stelden.
In de periode 1991-1992 heeft SURFnet bv zich door middel van het project Administratieve Automatisering en Beveiliging bezonnen op de vraag hoe in een open netwerk met beveiliging moet worden omgegaan.

INLEIDING

Begin 1992 was het weer raak, opnieuw werd de doelgroep van SURFnet geconfronteerd met berichten in de pers over hackers en gekraakte computersystemen (onder meer bij de Vrije Universiteit en de Rijksuniversiteit Groningen). Tonnen schade zouden er zijn geleden.

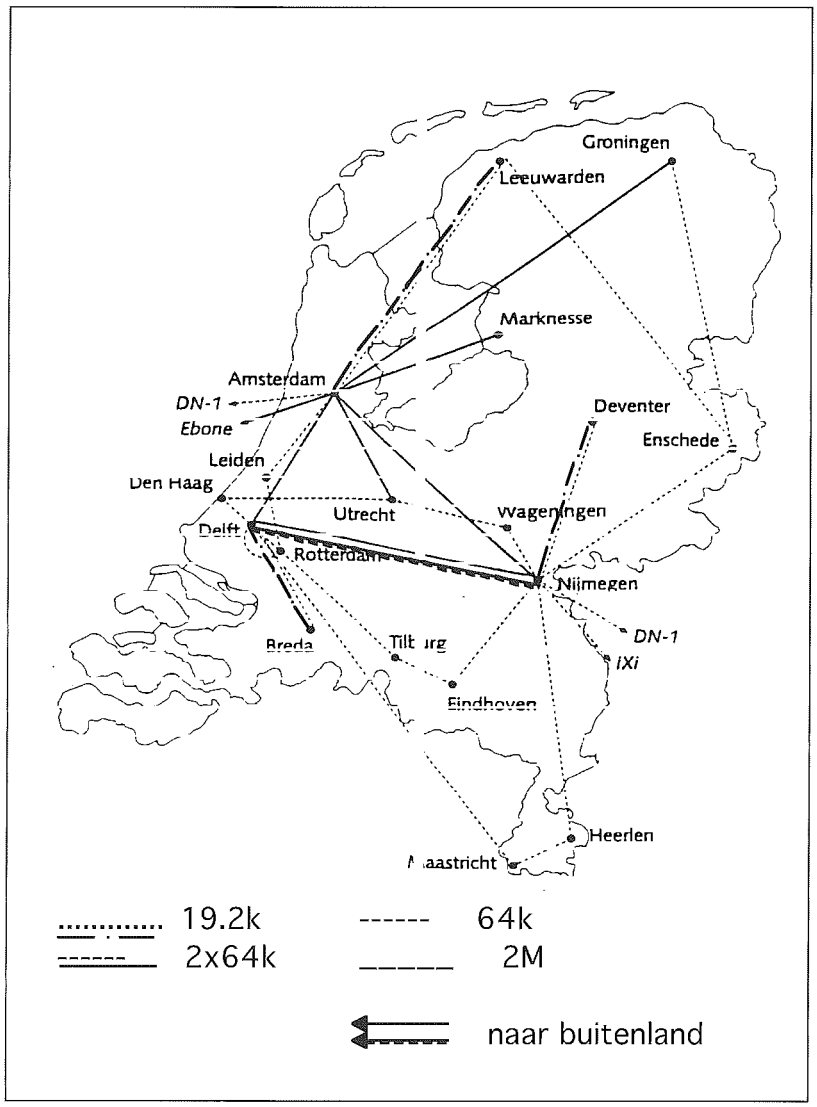
SURFnet is vanaf het begin per definitie een open netwerk geweest. Het woord open heeft hier twee betekenissen. Allereerst wordt met open bedoeld dat het netwerk op niet-leveranciersgebonden protocollen is gebaseerd, waardoor het mogelijk is verschillende computersystemen aan het netwerk te koppelen. Een andere betekenis van open is dat in principe iedereen die dat wenst en daartoe gerechtigd is, in de gelegenheid moet kunnen worden gesteld vanaf de eigen werkplek (PC, werkstation, mini-computer en mainframe) met elke willekeurige ander informatie te kunnen delen en uitwisselen. Het ligt voor de hand dat bij deze opzet van SURFnet de kans op oneigenlijk gebruik reëel aanwezig is.

In dit artikel zal worden ingegaan op beveiligingsaspecten binnen het SURFnet en bij de op SURFnet aangesloten instellingen. Er zal worden aangegeven waar zwakke plekken zijn en welke maatregelen er zijn genomen of zouden moeten worden genomen om veilig gebruik te kunnen maken van elektronische diensten.

WAT IS EN DOET SURFNET BV?

In 1985 werd het Meerjarenplan 'Samenwerking ... Reken maar', het zogenaamde SURFplan door de regering goedgekeurd [SURF85]. SURF staat voor Samenwerkingsorganisatie Universitaire Rekenfaciliteiten. Dit plan had tot doel 'het Wetenschappelijk Onderwijs en Onderzoek inclusief de daarbij behorende ondersteuning op een hoger niveau te brengen door een geavanceerd stelsel van computerdienstverlening'. De regering - de ministeries van Onderwijs en Wetenschappen, Economische Zaken en Landbouw en Visserij - stelden ten bate van de realisering van het SURFplan aanzienlijke middelen beschikbaar. Eén van de concrete activiteiten die hieruit voortvloeiden was de inrichting van een landelijk computernetwerk dat als basis kon dienen voor elektronische dienstverlening aan eindgebruikers. Via dit netwerk zouden dan instellingen, waaronder universiteiten, hogescholen, grote en kleine onderzoeksinstellingen, technologische instituten, academische ziekenhuizen en de research-centra van het bedrijfsleven en later ook bibliotheken langs elektronische weg informatie kunnen delen en uitwisselen.

Figuur 1. SURFnet-backbone (status oktober 1992).



In 1986 werden de eerste voorzieningen gerealiseerd als SURFproject. Op 1 januari 1989 is SURFnet bv officieel opgericht. Aandeelhouders van SURFnet bv zijn Stichting SURF (waarin de belangen van de gebruikers zijn vertegenwoordigd; 51%) en PTT Nederland NV (49%). SURFnet bv heeft het karakter van een not-for-profit-organisatie. Dit betekent dat er niet wordt gestreefd naar winstmaximalisatie, maar naar een zo breed mogelijk pakket van diensten tegen een zo laag mogelijk tarief.

De SURFnet-organisatie kent naast een directie, financiële en administratieve ondersteuning de volgende afdelingen: Advisering, Gebruiksondersteuning, Netwerkmanagement en Ontwikkeling (in totaal zijn er 22 mensen werkzaam). SURFnet bv is verantwoordelijk voor strategische en tactische aangelegenheden met betrekking tot de geboden dienstverlening. Het operationele beheer van de netwerkvoorzieningen is aan externe partijen (subcontracters) uitbesteed. De verschillende afdelingen begeleiden (potentiële) organisaties bij het inrichten, het optimaliseren en het gebruik maken van de elektronische diensten. De basisdiensten bestaan uit elektronische post (E-mail), het overzenden van gegevensbestanden en het op afstand raadplegen van informatiediensten. Om deze basisdiensten heen zijn diverse toepassingen beschikbaar, zoals elektronische discussielijsten en elektronische tijdschriften, maar ook information-navigators [Vers92] waarmee gezocht kan worden in (meta)gegevens.

Het SURFnet is gekoppeld aan (inter)nationale publieke netwerken (onder andere Datanet-1, Videotex en X.400) en aan andere research-netwerken [Quat90] [Malk91] (onder andere Internet, Bitnet, EARN en EUnet). Wereldwijd kunnen op dit moment al miljoenen mensen via research-netwerken onderling informatie uitwisselen. Op het landelijke SURFnet zijn meer dan 120 organisaties aangesloten. Eind 1991 kende SURFnet zo'n 25.000 gebruikers, eind 1993 verwachten we er in het totaal meer dan 50.000. Deze gebruikers zijn voor het verrichten van hun dagelijkse werkzaamheden op de een of andere manier afhankelijk van elektronische diensten. Of dit nu medewerkers zijn die bij het RCC mutaties aanbrengen in persoonsgegevens, die financiële gegevens muteren in een financieel administratief systeem, die betalingsmutaties versturen naar de BankGiroCentrale, die catalogiseren bij de bibliotheekinformatiedienst PICA, die gegevens uitwisselen met wetenschappers elders ter wereld of gewoon per elektronische post verslagen en rapporten uitwisselen met anderen, zij profiteren allen van SURFnet.

In de beginjaren is vooral nadruk gelegd op connectiviteit met andere netwerken. Minder aandacht werd besteed aan beveiliging en beschikbaarheid van de voorzieningen. Voor de gebruikers van het eerste uur, hoofdzakelijk wetenschappers, was dit geen groot probleem. De mogelijkheid van elektronisch communiceren werd ten op-

zichte van het traditionele postverkeer als een superieur alternatief gezien. In toenemende mate ging men het netwerk echter ook gebruiken voor ondersteunende functies binnen personele, studenten- en financiële administraties, waarbij de nadruk door de aard van de gegevens veel meer op beveiliging ligt, zoals bijvoorbeeld exclusiviteit bij personele gegevens en integriteit bij financiële gegevens.

Deze ontwikkeling heeft ertoe geleid dat SURFnet sinds 1989 extra aandacht is gaan besteden aan het aspect beveiliging van netwerken. Veel van de hierna weergegeven ervaringen zijn afkomstig uit het project 'Administratieve Automatisering en Beveiliging' [SURF93] dat door SURFnet bv in opdracht van de Stichting SURF sinds 1 januari 1991 wordt uitgevoerd (het project loopt tot 1 april 1993).

In het vervolg van dit artikel wordt aangegeven op welke wijze SURFnet bv op dit moment omgaat met beveiliging. In de eerste paragraaf zal een aantal serieus te nemen bedreigingen worden weergegeven, daarna wordt aangegeven welke maatregelen SURFnet bv zelf heeft getroffen; in de daarop volgende paragraaf wordt aangegeven welke maatregelen binnen de aangesloten instellingen kunnen worden getroffen. Extra aandacht wordt besteed aan netwerktechnische aspecten, in het bijzonder aan die welke voor andere organisaties ook relevant kunnen zijn.

BEDREIGINGEN

Het optreden van netwerkbedreigingen [SURF92] is sterk afhankelijk van technologische ontwikkelingen en het kennisniveau van de netwerkgebruikers. Een voorbeeld: het afluisteren van een op Ethernet gebaseerd LAN werd vijf jaar geleden niet als een grote bedreiging gezien. Op dit moment zijn er echter public domain-pakketten verkrijgbaar waarmee een gebruiker eenvoudig alle in gebruik zijnde passwords kan onderscheppen. De kans op het manifest worden van deze bedreiging is hierdoor de afgelopen jaren aanzienlijk toegenomen. Een belangrijke conclusie die hieruit kan worden getrokken, is dat de kans dat een bedreiging zich manifesteert in de tijd gezien variabel is. Netwerken worden dus eigenlijk continu bedreigd door moeilijk eenduidig vast te stellen kansen op deze bedreigingen. De conclusie die hieruit kan worden getrokken, is dat netwerken met enige regelmaat onder de loep moeten worden genomen en dat het niet kan blijven bij een eenmalige evaluatie.

Binnen het SURFnet worden geen grote bedreigingen onderkend met betrekking tot de exclusiviteit en integriteit van gegevens en middelen. Het afluisteren en veranderen van gegevens op een Wide Area Netwerk blijkt technisch veel moeilijker te realiseren (inbraak in gebouwen, opgraven van kabels, installeren van geavanceerde aftap-apparatuur, enz.) dan het afluisteren van een lokaal netwerk. Het ligt dan ook voor de hand om, indien applicaties een zeer hoge mate van vertrouwelijkheid vereisen, encryptie toe te passen op de hogere lagen van het OSI-netwerkmodel. Bij voorkeur eind-tot-eind, zodat alle tussenliggende communicatie veilig is.

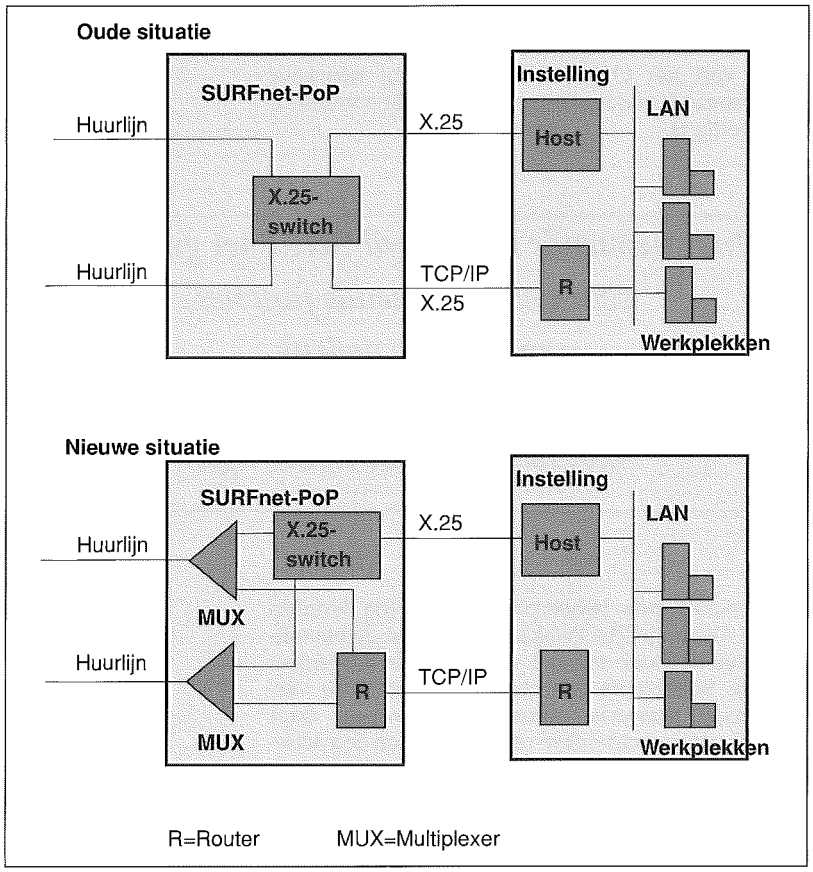
In toenemende mate werd SURFnet gebruikt voor ondersteunende functies, waarbij de nadruk door de aard van de gegevens veel meer op beveiliging ligt.

De verschillende beheerpartijen moeten worden gezien als mogelijke zwakke plekken in de beveiligingsketen. Door middel van formele afspraken met de beheerders (subcontracters) van de verschillende netwerkcomponenten, controle door middel van maandelijkse rapportages en een actieve begeleiding vanuit SURFnet-netwerkmanagement worden deze bedreigingen tot een aanvaardbaar niveau gereduceerd. Verder zijn er in het netwerk backup-voorzieningen aangebracht die ervoor moeten zorgen dat de beschikbaarheid van de diensten op de behoefte van de afnemers is afgestemd.

Cijfers van het Amerikaanse CERT Coördinatie Centrum [Holb91], waarover straks meer, geven aan dat tachtig procent van de problemen die het tegenkomt, te maken heeft met het onzorgvuldig gebruik van wachtwoorden. Een belangrijke oorzaak hiervoor is de onbekendheid bij veel medewerkers hetgeen negatieve gevolgen heeft bij het onjuist gebruik van wachtwoorden. De negatieve gevolgen van virusinfecties kennen veelal dezelfde oorzaak. Gesteld kan worden dat veel bedreigingen hun oorsprong kennen in de gebruikers van computer- en netwerkvoorzieningen. Niet de techniek, maar de gebruikers van deze techniek zijn een zwakke schakel in de beveiligingsketen. Dit is ook de reden waarom SURFnet bij het realiseren van een hoger beveiligingsniveau het accent van mogelijke maatregelen zo dicht mogelijk bij de gebruiker legt.

BEVEILIGING BINNEN SURFNET

SURFnet bv stelt in haar aansluitvoorwaarden formele eisen waaraan instellingen moeten voldoen. Deze hebben onder andere betrekking op het treffen van maatregelen ter voorkoming van oneigenlijk gebruik door een instelling, het opvolgen van richtlijnen voor het dagelijks beheer en de aansprakelijkheid van een instelling indien er direct of indirect schade ontstaat door verwijtbaar oneigenlijk of verkeerd gebruik. Daarnaast wordt in de aan-



Figuur 2. Oude en nieuwe situatie SURFnet-Point-Of-Presents (wide area backbone.).

sluitvoorwaarden aangegeven welke verplichtingen SURFnet heeft. SURFnet bv heeft onder andere een inspanningsverplichting zowel het netwerk en de aansluitingen op het netwerk als de ter beschikking gestelde diensten en faciliteiten naar behoren te laten functioneren. SURFnet bv dient tevens gegevens, indien deze bij de uitvoering van haar taak aan SURFnet bv bekend worden, met vertrouwelijkheid te behandelen. De wetgeving op dit gebied (de Wet Persoonsregistraties (WPR) en de Wet Computercriminaliteit) wordt gezien als een duidelijk maatschappelijk signaal ten aanzien van de normen waaraan een burger zich dient te houden.

Het SURFnet

SURFnet maakt op dit moment gebruik van twee typen netwerkprotocollen. Dit zijn X.25 (1984) en Internet-IP. Deze protocollen dienen als basis (carrier) voor diverse services en applicaties, onder meer DECnet, TCP (inclusief SMTP en FTP), X.400 en FTAM, maar ook voor remote access (Telnet, Triple-X en VTP) naar informatiediensten zoals PICA en RCC. Bij de introductie binnen SURFnet van Internet-IP werd dit protocol gerouteerd over het X.25-netwerk. De belangrijkste reden hiervoor was dat het IP-verkeer toen nog een bescheiden omvang had. Beveili-gings- en beheeraspecten en een zeer sterke groei van het IP-verkeer zijn aanleiding geweest om deze opzet te wijzigen. Er is voor gekozen de protocollen op huurlijnniveau te integreren (zie figuur 2). Hierdoor ontstaan technisch gezien twee gescheiden netwerken, die beide onafhankelijk van elkaar services aanbieden. Door deze opzet kan voor verschillende gebruikersgroepen en toepassingen een verantwoord beveiligingsniveau worden gerealiseerd.

De X.25-service

Voor de X.25-service betekent deze nieuwe opzet dat alle in het netwerk aanwezige beveiligingsvoorzieningen optimaal kunnen worden gebruikt. Hieronder vallen:

- Closed User Group (CUG), voor het kunnen afschermen van oneigenlijke toegang tot host/server-systemen die aan het netwerk zijn gekoppeld.

- Permanent Virtual Circuit (PVC), voor logische directe verbindingen tussen twee access-poorten; vergelijkbaar met een vaste huurlijnverbinding.

- Netwerk User Identification (NUI), voor identificatie van eindgebruikers bij het gebruik van triple-X access-poorten. Deze NUI's voorkomen dat personen anoniem oneigenlijk gebruik maken van het X.25-netwerk. Hier gaat een duidelijk preventieve werking van uit.

- Toegang tot andere (publieke) netwerken kan naar wens van de aangesloten instelling (inclusief accounting en billing) worden geconfigureerd.

Voor specifieke applicaties, zoals administratieve, financiële en bibliotheektoepassingen en voor toegang tot de publieke netwerken en diensten die op basis van connecttijd en/of volume worden doorberekend, is de X.25-service een geschikt Wide Area Netwerk-protocol.

De IP-service

De IP-service biedt de aangesloten instellingen vooral flexibiliteit. Een instelling bepaalt zelf welke services (Telnet, SMTP en FTP) en welke IP-nodes (PC's, minicomputers en mainframes) vanaf een LAN kunnen of mogen communiceren met de buitenwereld. Dit kan in de router die de scheiding vormt tussen het LAN en het WAN, van een instelling worden geconfigureerd. Vanuit SURFnet gezien zijn alle IP-nodes op een LAN van een instelling gelijkwaardig. De beveiligingsproblematiek dient daarom voor een groot deel binnen de aangesloten instelling te worden ingevuld. Sinds 1992 adviseert SURFnet de aangesloten instellingen om hun gebruikers alleen via goed beheerde host/server-systemen toegang te verlenen tot de IP-service. Alleen op deze wijze zijn beter repressieve en correctieve beveiligingsmaatregelen te nemen. Een goede beheerstructuur van het LAN is een belangrijke randvoorwaarde bij een verantwoord gebruik van de IP-service.

De IP-service is bruikbaar voor netwerkapplicaties die een grote bandbreedte nodig hebben, zoals bij het oversturen van bestanden voor grafische ver-

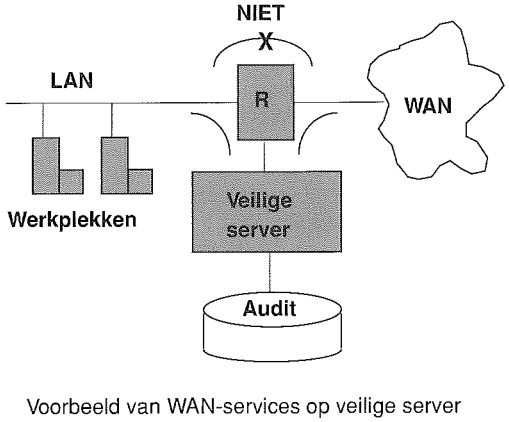
werking (images). Tevens is de IP-service geschikt in omgevingen waarbij de gebruikers een grote mate van flexibiliteit moet worden geboden. De IP-services zijn in technische zin betrouwbaar en voor vele research- en onderwijstoepassingen een goede oplossing.

Zowel de X.25- als de IP-service gaat uit van een relatief open verbinding met het SURFnet. Interne beveiligingsmaatregelen bij de aangesloten instelling zijn nodig om op een verantwoorde wijze gebruik te kunnen maken van de services. Indien een instelling een hoog veiligheidsniveau wenst is het inrichten van een Fire Wall een mogelijke oplossing.

Externe communicatie via een Fire Wall

Indien een organisatie het eigen LAN niet toegankelijk wil maken voor derden en toch behoefte heeft aan elektronische communicatie met de buitenwereld kan het 'Fire Wall'-principe [Ches92] [Smoo92] worden toegepast. Hierbij is de toegang van het WAN naar het LAN met de gebruikers, host en servers, volledig afgesloten.
Voor gebruikers die extern willen communiceren wordt dan een 'veilige server' ingericht die:
- voorzien is van adequate audit-functies;
- via een router aan een WAN is gekoppeld;
- op een gecontroleerde wijze vanaf het LAN toegankelijk is;
- op gecontroleerde wijze een aantal WAN-services beschikbaar stelt;
- op een gecontroleerde wijze communiceert met WAN.

Figuur 3. Fire Wall-concept.



Voorbeeld van WAN-services op veilige server

	WAN-services	
Veilige server	IN	UIT
E-mail	+	+
File transfer	-	+
Remote access	-	+

Nieuwe diensten

SURFnet bv ziet beveiliging niet als een apart onderdeel van de dienstverlening maar als structureel onderdeel van elke service.

SURFnet participeert in diverse (inter)nationale projecten om netwerkdiensten veiliger te maken. Eén van die projecten heeft tot doel veilige elektronische post te introduceren. De implementatie is gebaseerd op Privacy Enhancement for Electronic Mail (PEM) [Priv93], een Internet-standaard. Daarbij wordt gebruik gemaakt van zowel public als secret key-algoritmen. Binnen afzienbare tijd zal Privacy Enhanced Mail kunnen leiden tot een in een operationele omgeving toepasbaar produkt. De implementatie van het OSI-alternatief, X.400 (1988/1992), zal waarschijnlijk langer op zich laten wachten.

Calamiteitenteam

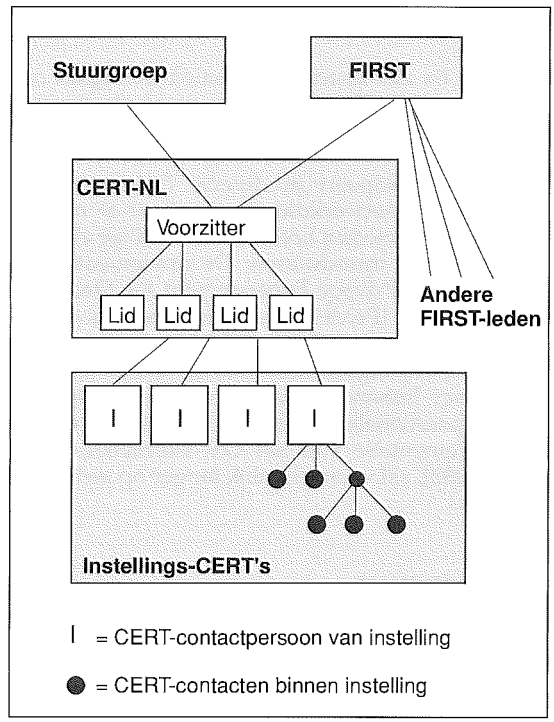
Naar het voorbeeld van het Amerikaanse Internet Computer Emergency Response Team (CERT) heeft SURFnet bv een landelijk opererend beveiligingsteam (CERT-NL) [CERT92] ingericht. De eerste CERT [Harv91] werd eind 1988 door ARPA (Advanced Research Projects Agency van het departement van Defensie van de Verenigde Staten) opgericht. Deze CERT is bij de Carnegie Mellon University in Pittsburgh ondergebracht. Aanleiding voor de oprichting was de Internet-Worm, die op 2 november 1988 duizenden computers in het Internet in de problemen bracht. Momenteel is een twintigtal CERT's wereldwijd actief. Deze CERT's zijn verenigd in het Forum on Incident and Response Security Teams (FIRST). Het doel van FIRST is een platform te bieden aan de CERT's om de onderlinge communicatie te verbeteren.

De CERT-NL is in het leven geroepen om de aangesloten instellingen van SURFnet een platform te kunnen bieden voor (urgente) beveiligingsproblemen. Het is voor een CERT van groot belang om binnen iedere organisatie of doelgroep vaste en goed gedocumenteerde aanspreekpunten te hebben.

De taak van zo'n aanspreekpunt, de instellings-CERT, is tweeledig:
- het bieden van een eenduidige communicatiestructuur (netwerk van personen) ten behoeve van (urgente) beveiligingsproblemen;
- het bieden van een eenduidig aanspreekpunt voor de landelijke CERT (CERT-NL).

De belangrijkste doelstellingen van een CERT zijn:
- centraal meldpunt voor incidenten;
- coördinatie van acties op incidenten;
- het verlenen van technische assistentie;
- het geven van informatie op het gebied van beveiliging;
- het ontwikkelen en verspreiden van hulpmiddelen.

De CERT-NL is met zeven leden gestart en heeft een 24-uurs bereikbaarheid.



Figuur 4. Relatie tussen CERT's en FIRST.

BEVEILIGING BINNEN DE AANGESLOTEN INSTELLINGEN

Beveiliging van een Wide Area Netwerk heeft geen enkele zin als de netwerken van de erop aangesloten instellingen onveilig zijn. Het is daarom van belang dat de gebruikers van Wide Area Netwerkservices ervoor zorgen dat binnen het lokale netwerk adequate maatregelen worden getroffen. In de hierna volgende subparagrafen wordt ingegaan op de aspecten beleid, organisatie en techniek.

Beleid

Het blijkt dat bij veel instellingen een beleid en een daaruit afgeleid plan voor computer- en netwerkbeveiliging ontbreken. Het ontbreken van een beveiligingsplan maakt het moeilijk een evenwichtig pakket van maatregelen samen te stellen op het gebied van het voorkomen van bedreigingen (preventief), het signaleren van bedreigingen (detectief), het ervoor zorgen dat indien een bedreiging zich manifesteert de schade beperkt blijft (repressief) en het ervoor zorgen dat de geleden schade zo snel mogelijk wordt hersteld (correctief). Belangrijke voorwaarde om deze maatregelen ook daadwerkelijk effectief te kunnen laten zijn is een duidelijk en herkenbaar commitment van het management. Enkel het uitspreken van de bezweringsformule 'Beveiliging is noodzakelijk' is absoluut onvoldoende.

Organisatorische aspecten

Voor hoger onderwijs en onderzoek past een pioniersopstelling van een beheerorganisatie omdat juist daar de vraag naar steeds geavanceerdere technische hulpmiddelen continu groot is. Aansluiting van administratieve gebruikers op het lokale net levert echter een geheel andere vraagstelling op. Administratieve gebruikers zijn gebaat bij een zo hoog mogelijke beschikbaarheid en betrouwbaarheid van de gebruikte toepassingen. Goed werkende applicaties en goede ondersteuning van de kant van de beheerders zijn voor deze gebruikers cruciaal. Schade bij uitval van computers en netwerk is voor administratieve gebruikers relatief groter dan voor gebruikers in onderwijs en onderzoek.

Binnen universiteiten en hogescholen heerst momenteel geen cultuur om volgens strakke (controleerbare) procedures te werken. Het is daarom beter eerst te streven naar meer bewustwording en acceptatie van het feit dat men onderling goede afspraken moet maken en zich daaraan ook moet houden om ongestoord en veilig met de beschikbare IT-faciliteiten te kunnen werken. De nadruk moet dus komen te liggen op het verbeteren van deskundigheid en attitude met betrekking tot beveiliging bij gebruikers, beheerders en management. Adequate voorlichting en opleiding over beveiliging wordt daarom door SURFnet gezien als een goede basis.

Technische aspecten

In het project Administratieve Automatisering en Beveiliging wordt bij het beveiligen van lokale netwerken het volgende onderscheid gemaakt: de werkplek, het lokale netwerk en servers/hosts. Voor al deze componenten is het mogelijk beveiligingsvoorzieningen te realiseren. Deels kan dit worden bewerkstelligd door de bestaande voorzieningen anders te gaan gebruiken, deels zullen er aanvullende specifieke voorzieningen dienen te worden gerealiseerd. Uiteraard zal aan de hand van een bedreigings- en kosten/baten-analyse een keuze worden gemaakt.
Ten aanzien van de beschikbaarheid van beveiligingsprodukten kan worden opgemerkt dat er op het ogenblik slechts een beperkt aantal internationale standaarden voor open netwerken toepasbaar is. Daarom zal zeker voorlopig gebruik moeten worden gemaakt van leveranciersafhankelijke oplossingen. Het keuze-aanbod voor bepaalde mechanismen wordt hierdoor aanzienlijk beperkt.

BEVEILIGINGSMAATREGELEN IN HET LAN

In de hierna volgende subparagrafen zal worden aangegeven welke technische maatregelen kunnen worden genomen om het gebruik van een LAN en daarmee indirect ook van een WAN veiliger te maken.

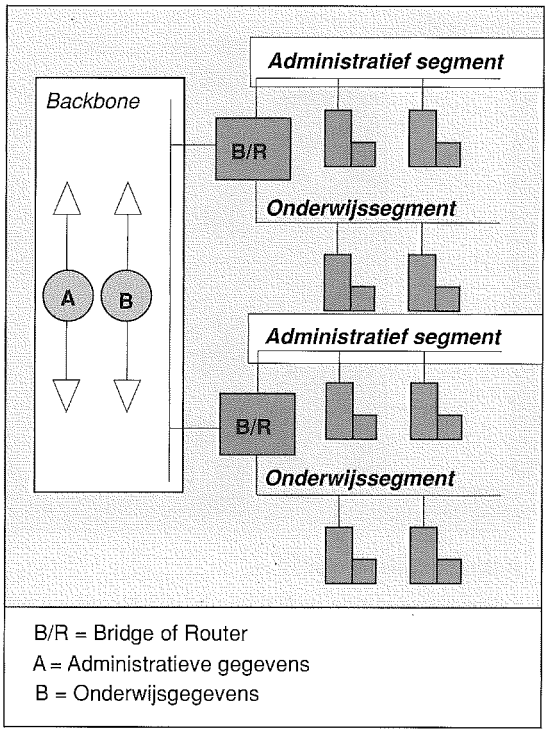
Werkplek

De gebruiker moet als een zwakke schakel in de beveiligingsketen worden gezien. Het ligt dus voor de hand ervoor te zorgen dat de werkplek van deze gebruiker voldoende veilig is. Maatregelen ter beveiliging van werkplekken moeten dan ook betrekking hebben op de beveiliging tegen ongeautoriseerd gebruik, zoals bijvoorbeeld toetsenbordblokkade, maar denk hierbij vooral ook aan fysieke beveiliging (deur of PC op slot na werktijd).
Een andere belangrijke maatregel voor de werkplek betreft bescherming tegen virussen. Het gebruik van anti-virusprogrammatuur kan hierbij een hulpmiddel zijn, het blijft echter vaak achter de feiten aanlopen ('al is een virusscanner nog zo snel, een nieuw virus achterhaalt hem wel'). Toegang tot Wide Area Netwerk-services dient alleen via adequaat beheerde servers te worden aangeboden, zodat oneigenlijk gebruik traceerbaar is. Goede voorlichting aan de bron van potentiële problemen (de gebruiker) is zeker zo belangrijk.

Lokaal netwerk

Zoals eerder al is aangegeven zijn lokale netwerken relatief gemakkelijk af te luisteren. De exclusiviteit en integriteit van de te transporteren gegevens (inclusief wachtwoorden) worden hierdoor bedreigd. Gelukkig zijn er middelen beschikbaar die kans op afluisteren kunnen reduceren. In het kort kunnen deze middelen als volgt worden gerubriceerd:
- segmentering met behulp van routers/ bridges;
- smart HUB's;
- LAN-encryptie;
- Challenge Signed Response-mechanisme.

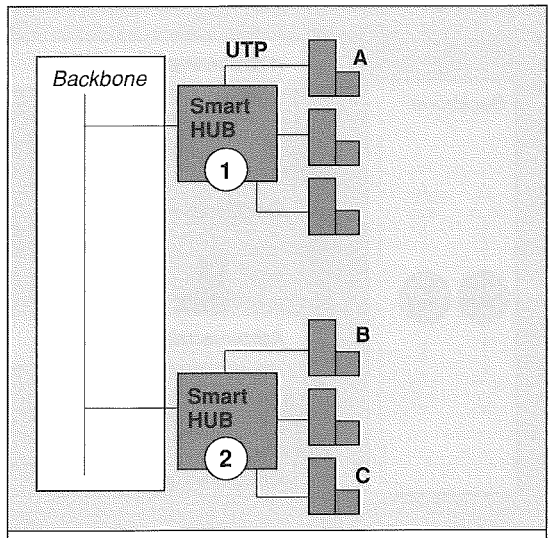
Segmentering
Door middel van bridges en routers kunnen netwerken in logische segmenten worden onderverdeeld. Vooral bij grote lokale netwerken verspreid over meerdere locaties/gebouwen worden deze componenten veelvuldig toegepast. Facultaire netwerken (segmenten) worden op deze wijze vaak gekoppeld aan een backbone van de instelling. Deze backbone dient hierbij niet voor gebruikers toegankelijk te zijn. Voordeel van deze opzet is dat deze segmenten redelijk autonoom kunnen worden gemanaged. Bij een goed ingericht router/ bridge-netwerk heeft een storing op één segment geen negatieve consequenties voor de overige netwerksegmenten. Deze opzet heeft dus een positieve invloed op de performance en beschikbaarheid van het totale netwerk.
Hoewel het geen echte beveiligingsprodukten zijn, biedt de aanwezige filterfunctie mogelijkheden om gegevensstromen te sturen. Indien deze functionaliteit aanwezig is, wordt in de literatuur vaak gesproken over intelligente bridges en routers. Men dient zich echter wel te realiseren dat gebruikers binnen één segment gegevens van elkaar kunnen blijven onderscheppen. Hiermee dient bij de indeling van de segmenten rekening te worden gehouden. Bijvoorbeeld door het inrichten van onderwijs-, onderzoek- en administratieve segmenten die door middel van een veilige backbone onderling worden verbonden (zie figuur 5).



Figuur 5. LAN-segmentering met routers en bridges.

Smart HUB's
Een HUB is een netwerkcomponent waarop meerdere computersystemen via een directe verbinding onderling kunnen worden gekoppeld. Hiermee wordt een stervormige structuur gecreëerd (zie figuur 6). De eigenschap dat elke computer een eigen verbinding heeft met een HUB wordt gebruikt om beveiligingsfuncties te introduceren. In de literatuur worden deze HUB's vaak 'smart HUB's' genoemd. Beveiliging in HUB's is nog nieuw. De nieuwste versies van HUB's bieden twee belangrijke beveiligingsfuncties:
- afluisterbeveiliging;
- indringersbeveiliging, een beveiliging tegen maskerade.

Invoering van beveiliging met smart HUB's kan relatief gemakkelijk gebeuren, vooropgesteld dat er al sprake is van een stervormig gestructureerd bekabelingssysteem. Het smart HUB-concept houdt een grote belofte voor de toekomst in. Met enkele toevoegingen aan de functionaliteit en vooral aan het netwerkmanagement kunnen belangrijke tekortkomingen van een Ethernet-LAN (met een inherent open structuur) worden gecompenseerd. Het concentratiepunt waar de HUB is opgesteld, kan in de toekomst met alle gewenste beveiligings-



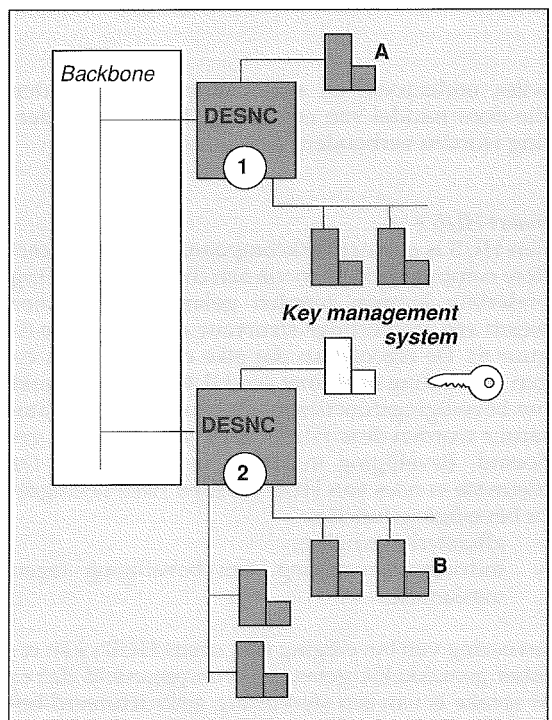
A stuurt gegevens naar C

- HUB 1 zet frame op backbone
- HUB 2 ontvangt frame
- HUB 2 stuurt volledig frame naar C
- HUB 2 stuurt frame met ruis naar B

UTP=Unshielded Twisted Pair

Figuur 6. Toepassing van smart HUB's op een LAN.

Figuur 7. LAN-encryptie met DESNC van Digital.



A stuurt gegevens naar B

- DESNC 1 codeert gegevens
- DESNC 1 plaatst gecodeerde gegevens op backbone
- DESNC 2 ontvangt gecodeerde gegevens
- DESNC 2 decodeert gegevens
- DESNC 2 stuurt gedecodeerde gegevens naar B

functionaliteit worden uitgebreid, zoals filtering en encryptie. Momenteel zijn smart HUB's nog minder breed toepasbaar dan men op het eerste gezicht zou vermoeden. Dit wordt hoofdzakelijk veroorzaakt door de onvoldoende beschikbaarheid van functionaliteit en de beperkte inpasbaarheid in de bestaande technische infrastructuren.

LAN-encryptie

Een ander middel om beveiliging in een LAN te realiseren is encryptie, ook wel vercijfering genoemd. Vercijfering maakt gegevens onleesbaar. Dit wordt bereikt door de gegevens met een vercijferingsalgoritme om te zetten in onleesbare gegevens. Hierbij wordt gebruik gemaakt van een specifieke vercijferingssleutel. De oorspronkelijke gegevens zijn uit de vercijferde vorm slechts weer te herleiden als men kennis van de sleutel voor het ontcijferen heeft (zie figuur 7).
Inmiddels zijn er verscheidene produkten op de markt verkrijgbaar waarmee de informatie die over een LAN wordt verstuurd, kan worden vercijferd. De huidige generatie apparatuur haalt echter de maximale snelheid van bijvoorbeeld Ethernet (10Mb/s) niet. Met name op plaatsen waar grote concentraties vercijferd verkeer voorkomen, zoals bij centrale hosts en servers, moet men rekening houden met performance-problemen. Proefnemingen in dergelijke situaties zijn aan te raden. De hoge kosten die met cryptoboxen gepaard gaan, leiden slechts tot toepassing in situaties met een hoge beveiligingsbehoefte. Met name wanneer de backbone met andere middelen niet voldoende veilig is te maken, is LAN-encryptie aan te bevelen. De combinatie van encryptie, access control en LAN-security audit-functies, zoals deze door cryptoboxen wordt geboden, biedt een sterke beveiliging.

Challenge Signed Response

Challenge Signed Response is een authenticatiemethode voor het verkrijgen van toegang tot computersystemen. Het kan gezien worden als een one-time-password (wachtwoord voor eenmalig gebruik). De eerste ervaringen binnen de SURFnet-doelgroep zijn positief te noemen, zowel uit beheer- als uit beveiligingsoogpunt.

Wanneer een gebruiker een verbinding met een host/server wil opzetten, genereert dit systeem een zogenaamde challenge (zie figuur 8). Deze challenge wordt naar de gebruiker gestuurd en bestaat meestal uit een willekeurig getal. Dit getal moet de gebruiker invoeren in een token. Een token is een soort calculator die aan de gebruiker ter beschikking is gesteld. Het token voert vervolgens een berekening uit, die alleen door dat ene token kan worden uitgevoerd (meestal door middel van een unieke vercijferingssleutel). Het resultaat van de berekening is een respons. Deze respons moet vervolgens door de gebruiker via het toetsenbord worden ingevoerd om zijn identiteit aan de host/server te bewijzen. De identiteit van de gebruiker wordt in dit geval bewezen door de unieke respons van het token. Er zijn diverse CSR-varianten op de markt beschikbaar voor een groot aantal verschillende computersystemen.

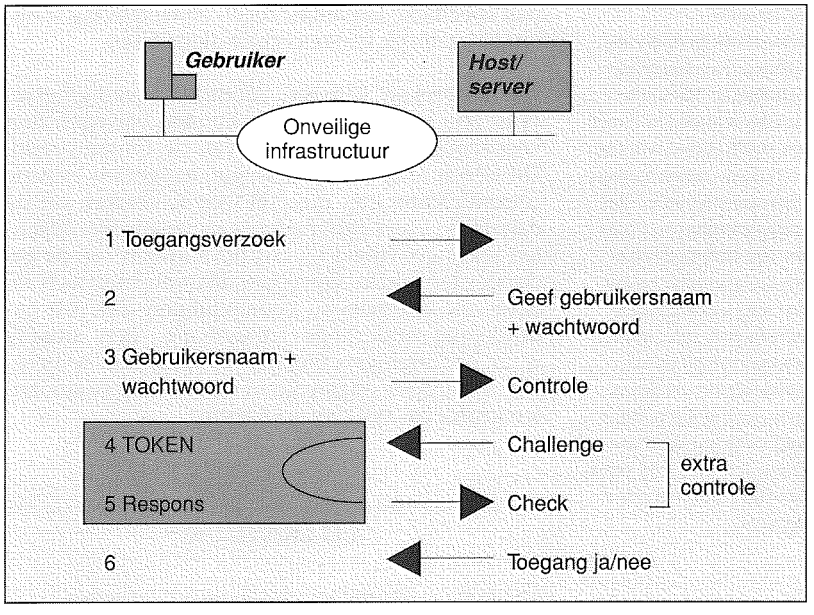
Het gebruik van Challenge Signed Response gaat het afluisteren van wachtwoorden op een LAN tegen. Misbruik is bij correct gebruik praktisch uitgesloten. Het mechanisme biedt echter geen enkele bescherming tegen het afluisteren van al het andere netwerkverkeer.

Als iemand oneigenlijk gebruik wil maken van een host/server dan zal deze persoon bijna altijd ergens in het proces gebruik maken van een interactieve login-sessie. Als het systeem tegen deze bedreiging goed is beschermd, dan is het hele systeem beter beschermd en dus veiliger. Het CSR-mechanisme leent zich voor introductie op grote schaal.

Samenvatting van beveiliging binnen de aangesloten instellingen

Een afluisterdreiging kan op adequate wijze worden vermeden door een goede structurering van het netwerk te zamen met een degelijke beheerorganisatie. Voor veel toepassingen kan worden volstaan met middelen zoals segmentering met behulp van routers en bridges of smart HUB's. Het concept van de smart HUB is goed doordacht en heeft daarom een veelbelovend toekomstperspectief. Een middel als LAN-encryptie blijkt een erg kostbaar mechanisme in verhouding tot performance en beheer. De inzet ervan is alleen zinvol als de beveiligingseisen zeer hoog zijn.

Een voldoende beveiliging tegen het afluisteren van LAN's en maskerade van eindgebruikers kan worden bereikt door de combinatie van Challenge Signed Response en één van de middelen om het LAN zelf te beveiligen.
Beveiliging dicht bij de werkplek moet hierbij niet worden vergeten. Goede voorlichting aan de gebruikers en beheerders van de netwerken blijft ook bij een technisch gezien 'veilig netwerk' noodzakelijk. Uiteraard dienen beleid en daaruit voortvloeiende beveiligingsplannen de basis te vormen voor alle te nemen maatregelen (zowel organisatorisch als technisch).



Figuur 8. Principe van Challenge Signed Response.

TOEKOMSTIGE ONTWIKKELINGEN

Hoewel het moeilijk is voorspellingen te doen over een sterk in beweging zijnde markt, worden hierna enkele oorzaken genoemd waardoor beveiliging de komende jaren een belangrijke rol zal gaan spelen bij het verbreden van het gebruik en de introductie van nieuwe toepassingen.

Wereldwijd heeft in het afgelopen decennium een jaarlijkse verdubbeling plaatsgevonden van het aantal computersystemen dat door middel van netwerken onderling met elkaar is verbonden. Dit heeft onder meer tot gevolg dat er ieder jaar een nieuwe onervaren gebruikersgroep bijkomt die net zo groot is als de groep van bestaande gebruikers (waarvan weer de helft slechts één jaar ervaring heeft). Deze trend zet zich de komende jaren waarschijnlijk door. Binnen enkele jaren zal hierdoor een soort global village ontstaan, waarbij miljoenen mensen over de gehele wereld vanaf hun eigen werkplek onderling gegevens kunnen uitwisselen en delen. Er zijn al schattingen gemaakt van meer dan 200 miljoen gebruikers in 1995.

De gebruikers (raadplegers) zullen vanaf verschillende locaties toegang wensen te krijgen tot gegevens. Denk hierbij aan de trend om medewerkers vaker thuis te laten werken en aan onderwijs op afstand. De fysieke locatie van deze gegevens is voor de eindgebruiker niet relevant. Betrekkelijk anoniem zwerft deze gebruiker via netwerken door de global village. Anonimiteit wordt echter door hackers gezien als het ideale vertrekpunt voor het verrichten van oneigenlijke handelingen. Een vorm van tweezijdige authenticatie zal moeten worden geïntroduceerd om deze toepassing ook bij gebruik op grotere schaal succesvol te laten zijn. Niet alleen de gebruiker, maar ook de informatiedienst moet namelijk authentiek zijn.

Indien deze gegevens worden gebruikt als referentie of als grondstof voor verdere verwerking dan is het van belang dat de integriteit van deze gegevens eenduidig kan worden vastgesteld. Er dient dus gewerkt te gaan worden aan integere opslag en distributie van deze gegevens. Cryptografische technieken kunnen hiervoor een mogelijke oplossing gaan bieden.

Elektronische post zal steeds meer gaan worden gebruikt voor het uitwisselen van formele documenten. Een voorbeeld hiervan zijn EDI-berichten (Electronic Data Interchange) ten behoeve van de uitwisseling van financiële gegevens en voor centrale/decentrale verwerking. Voor het gebruik van beveiligde elektronische post zullen naast technische ook juridische problemen moeten worden opgelost. Uiteraard gaat de rechtsgeldigheid van elektronische documenten een rol spelen, maar daarnaast moet ook rekening worden gehouden

E. Zegwaart
Is werkzaam bij de afdeling Network consultancy van SURFnet bv. Hij is in het verleden betrokken en verantwoordelijk geweest voor een groot aantal automatiseringsprojecten op het gebied van computernetwerken. Op dit moment participeert hij in een Europees project dat tot doel heeft secure E-mail te introduceren. Hij is tevens manager van het project Administratieve Automatisering en Beveiliging. Hij heeft enkele publikaties en diverse lezingen op het gebied van Wide Area Netwerken verzorgd.

met specifieke landelijke regel- en wetgeving rondom het gebruik van encryptie-algoritmen.

Het ontbreken van een adequaat beveiligingsniveau zou instellingen ertoe kunnen bewegen hun voorzieningen af te sluiten van de buitenwereld. Dit is een af te raden strategie, aangezien externe communicatie niet meer is weg te denken uit de dagelijkse werkzaamheden van velen. Het afsluiten zal ongetwijfeld tot creatieve ideeën van de gedupeerden leiden. Gevolgen daarvan laten zich raden; vele alternatieve voorzieningen met een onduidelijke onderlinge samenhang. Een situatie waar bedreigingen moeilijk in kaart zijn te brengen, waardoor ongetwijfeld de kans op calamiteiten groter zal zijn dan voorheen.

LITERATUUR

[Cert92] *CERT-NL Operational Framework* version 2.1 june 1992, SURFnet bv.

[Ches92] B. Cheswick, *The Design of a Secure Internet Gateway*, AT&T Bell Laboratories, Murray Hill, New Jersey 07974.

[Gass88] M. Gasser, *Building a secure computer system*, Van Nostrand Reinhold, New York 1988.

[Harv91] Ch.C. Harvey, *CERT-Computer Emergency Response Team*, Computer Networks and ISDN Systems 23 (1991) 167-170.

[Holb91] P. Holbrook en J. Reynolds, *Site Security Handbook*, Request For Comment 1244, July 1991.

[IS7492] *OSI Security Architecture* (IS7498-2).

[ITSE91] *Information Technology Security Evaluation Criteria (ITSEC)*, versie 1.2 juni 1991.

[Kari91] A.T. Karila, *Open Systems Security, an Architectural Framework*, Telecom Finland, 1991.

[MacM91] *Information Security Handbook*, MacMillan Publishers Ltd, 1991.

[Malk91] G. Malkin en A. Marina, *Answers to Commonly asked 'New Internet User' Questions*, Request for Comment 1325.

[NGI89] *Beveiliging bij datacommunicatie*, Nederlands Genootschap voor Informatica, afdeling Beveiliging, Kluwer Bedrijfswetenschappen, 1989.

[NGI92] *Beveiligingsbeleid en beveiligingsplan*, Nederlands Genootschap voor Informatica, afdeling Beveiliging, Kluwer Bedrijfswetenschappen, 1992.

[NRC92] *Computers at Risk: Safe Computing in the Information Age*, National Research Council.

[Priv93] Privacy Enhancement for Electronic Mail: RFC 1421, 1422,1423 and 1424.

[Quat90] J.S. Quaterman, *The Matrix. Computer Networks and Conferencing Systems Worldwide*, Digital Press 1990.

[Smoo92] C.-M. Smoot en J.S. Quaterman, *Building Internet Firewalls*, UNIXWORLD, februari 1992.

[SRII90] *Improving the security of your Unix system*, SRI International Report.

[SURF85] Rapport *'Samenwerking ... Reken maar!'*, Stichting SURF, september 1985.

[SURF92] Management Rapportage Voorbereidingsfase, Project Administratieve Automatisering en Beveiliging, SURFnet bv, 1992.

[SURF93] Rapport *'Veiliger gebruik van computernetwerken: resultaten van het project Administratieve Automatisering en Beveiliging'*, SURFnet bv, ISBN 90 73749 04 2. Dit rapport is het tweede kwartaal 1993 beschikbaar voor de doelgroep van SURFnet bv.

[Vers92] T. Verschuren, *Lilies that fester smell far worse than weeds*, SURFnet Bulletin 92.3, SURFnet bv.

Beveiliging van digitale kieslijnen

Drs.ing. D. Brouwer

Een kieslijn is al sinds jaar en dag een uitstekend middel om in korte tijd tegen lage kosten een verbinding tussen twee locaties te realiseren. Naast de analoge kieslijn, waarbij met behulp van modems een datacommunicatieverbinding wordt opgezet, raakt ook de digitale kieslijn steeds meer in trek.
Maar hoe zit het met de beveiliging van dergelijke verbindingen? Brouwer voelt de oudste digitale kieslijn in Nederland, de Datanet-1-verbinding, aan de tand.

INLEIDING

Datacommunicatie wordt gebruikt voor het op elektronische wijze uitwisselen van informatie. Voor datacommunicatiedoeleinden kan gebruik worden gemaakt van vaste lijnen of kieslijnen.
Er zijn meerdere redenen om te opteren voor kieslijnen. Met behulp van kieslijnen kan op snelle en flexibele wijze een verbinding worden opgebouwd en is een groot aantal andere aansluitpunten bereikbaar. Omdat de vaste exploitatiekosten laag zijn lenen kieslijnen zich in het bijzonder voor het maken van kortstondige en incidentele verbindingen. Aan datacommunicatieverbindingen in het algemeen en aan kieslijnen in het bijzonder zijn echter risico's verbonden. Het is daarom noodzakelijk beveiligingsmaatregelen te treffen.

Omdat in de meeste literatuur over beveiliging van kieslijnen nagenoeg uitsluitend aandacht wordt besteed aan analoge kieslijnen, is in dit artikel juist gekozen voor de behandeling van digitale kieslijnen. Bovendien neemt het belang van analoge kieslijnen af ten gunste van het gebruik van digitale lijnen.
De probleemstelling die in dit artikel centraal zal staan, is de wijze waarop digitale kieslijnen zijn te beveiligen tegen het tot stand brengen van ongeautoriseerde verbindingen. Tevens zal worden ingegaan op de aan digitale kieslijnen verbonden audit-aspecten.

In dit artikel is als voorbeeld van digitale kieslijnen gekozen voor het door PTT Telecom geëxploiteerde netwerk Datanet-1. Dit is een openbaar netwerk dat werkt op basis van packet-switching-technieken. Een ander voorbeeld van digitale kieslijnen is de momenteel sterk in opkomst zijnde dienst van PTT Telecom IDN (Integrated Digital Network), waarbij een gekozen digitale verbinding van 64 Kbps (IDN1) of van 2 Mbps (IDN30) kan worden opgebouwd. IDN is de voorloper van ISDN, dat de komende jaren in Nederland zal worden ingevoerd. Aangezien de beveiligingsaspecten van de verschillende verschijningsvormen van digitale kieslijnen sterk vergelijkbaar zijn, kunnen de in dit artikel naar voren komende risico's en maatregelen eenvoudig op bijvoorbeeld IDN worden betrokken.
Voor een goed begrip van de aan het gebruik van openbare netwerken verbonden risico's zal allereerst aandacht worden besteed aan het fenomeen digitale kieslijnen, de topologie van Datanet-1 en de tijdens de verbindingsopbouw te onderscheiden fasen. Na een inventarisatie van de risico's zal vervolgens worden ingegaan op de mogelijke beveiligingsmaatregelen en de relevante audit-aspecten.

DIGITALE KIESLIJNEN

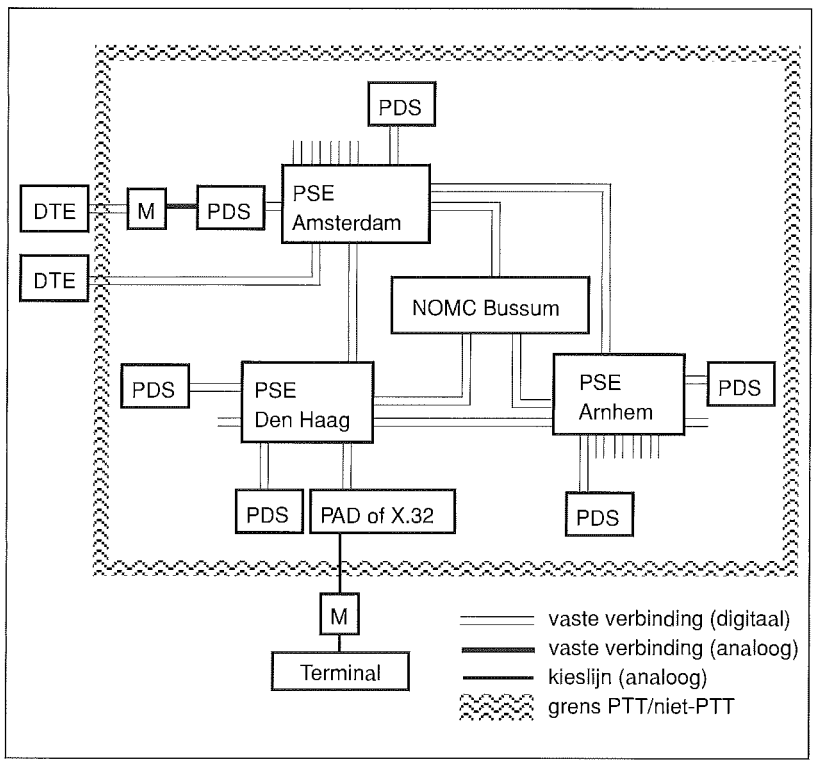
Een kieslijn wordt in de literatuur veelal gedefinieerd als: een datacommunicatieverbinding die tot stand wordt gebracht via het openbare telefoonnet [NGI89]. Bedoeld zijn hier analoge kieslijnen. Het telefoonnetwerk is namelijk ten gevolge van de beperkte bandbreedte niet geschikt voor het transport van digitale signalen. Daarom wordt het digitale signaal van computers door modems omgevormd tot een analoog signaal en bij de ontvanger weer omgezet in een digitaal signaal. Bij digitale lijnen kan de informatie zonder tussenkomst van modems worden aangeboden.

Het begrip digitale kieslijnen

Bij de eerder aangehaalde definitie voor kieslijnen wordt voorbijgegaan aan een essentieel element bij het opbouwen van een kieslijnverbinding, namelijk dat de tot stand gekomen verbinding afhankelijk is van door de oproeper verstuurde kies- c.q. routeringsinformatie. Onder kieslijnen worden in dit artikel verstaan zowel analoge als digitale lijnen die kunnen worden gebruikt voor het tot stand brengen van datacommunicatieverbindingen via een openbaar datacommunicatienetwerk, waarbij de verbindingsopbouw tot stand komt afhankelijk van de door een oproeper naar het netwerk verstuurde kiesinformatie.

Omdat digitale verbindingen via een openbaar netwerk eveneens afhankelijk zijn van de verstuurde kiesinformatie, worden ook deze lijnen beschouwd als kieslijnen en hierna aangeduid met de term 'digitale kieslijn'. Deze term is de schrijver overigens - in tegenstelling tot de term digitale huurlijn - niet in de literatuur tegengekomen. In de volgende subparagrafen zal worden ingegaan op het door PTT Telecom geëxploiteerde openbare pakketgeschakelde netwerk Datanet-1.

Figuur 1. Opbouw van Datanet-1.



Opbouw Datanet-1

De opbouw van Datanet-1 is geschetst in figuur 1. Zoals uit deze figuur blijkt, is Datanet-1 in feite een hybride netwerk: het bestaat uit analoge kieslijnen alsmede analoge en digitale vaste verbindingen. Er kunnen onder andere de volgende componenten worden onderscheiden:

– *Een beheerscentrum, aangeduid met NOMC (Network Operating and Management Centre)*
Het NOMC is gevestigd in Bussum en is het beheers- en onderhoudscentrum van Datanet-1. Alle storingen en onregelmatigheden worden aan het NOMC gemeld.

– *Drie Packet Switching Exchange-centrales (PSE)*
De PSE's zijn geplaatst in Amsterdam, Arnhem en Den Haag, en onderling met elkaar verbonden via een backbone-netwerk van lijnen met een hoge capaciteit. In tegenstelling tot hetgeen wel eens wordt aangenomen, bestaan deze verbindingen niet altijd uit glasvezelkabels. Er kan bij storingen ook gebruik worden gemaakt van draaggolf- en straalverbindingen.
Gebruikers die op Datanet-1 een aansluiting wensen met een capaciteit van 48.000 bps of hoger worden rechtstreeks aangesloten op een PSE.

– *Een vijftigtal PDS-knooppunten (Packet Data Satellite)*
De PDS'en zijn stervormig aangesloten op de PSE's. De verbinding tussen de gebruiker en een PDS is een vaste verbinding met een capaciteit van 2400, 4800 of 9600 bps. Over deze verbinding wordt het signaal nog in analoge vorm getransporteerd. Wel communiceert een PDS met een aangesloten gebruiker via een synchroon protocol, het zogenaamde X.25 protocol. X.25 is alleen een access protocol; onderling communiceren de PDS'en via een speciaal protocol, genaamd netgram protocol [Heij86].

– *Modems, in figuur 1 aangeduid met M*
De modems worden door PTT Telecom opgesteld bij de abonnee maar blijven eigendom van PTT Telecom en zijn dus onderdeel van het netwerk. Ze worden gebruikt voor de omvorming van een digitaal in een analoog signaal voor de vaste verbinding tussen abonnee en PDS.

– *Een twintigtal Packet Assembler Disassemblers (PAD)*
De PAD-faciliteit is in het leven geroepen ten behoeve van gebruikers die niet beschikken over een terminal met X.25-functionaliteit en voor gebruikers die slechts incidenteel gebruik maken van Datanet-1.

– *Een DTE (Data Terminal Equipment)*
Een DTE is de computer van de gebruiker die is aangesloten op het Datanet-1-netwerk.

Soorten Datanet-1-aansluitingen

Een gebruiker kan kiezen uit de volgende aansluitmogelijkheden aan Datanet-1:

a. Netwerkaansluiting
Met de netwerkaansluiting krijgt de gebruiker via één rechtstreeks aansluitpunt op de PDS de beschikking over zeven aansluitingen op Datanet-1, die ieder een eigen aansluitnummer hebben.

b. Normale aansluiting
Een normale aansluiting is leverbaar in snelheden van 2400, 4800, 9600, 48.000 en 64.000 bps. Het is mogelijk op één fysieke aansluiting verscheidene logische kanalen te definiëren. Via elk logisch kanaal is communicatie met een andere abonnee mogelijk.

c. Deelaansluiting
Bij een deelaansluiting heeft men de beschikking over slechts één logisch kanaal met een snelheid van 2400 bps. Men kan dus slechts tegelijkertijd met één andere abonnee communiceren.

d. Transactie-aansluiting
De transactie-aansluiting is een variant op de deelaansluiting en is bedoeld voor communicatie waarbij in één oproep weinig informatie wordt uitgewisseld (bijvoorbeeld bij elektronisch betalingsverkeer). De verbindingsopbouw wordt hierbij beperkt doordat maximaal twintig pakketten mogen worden verzonden. Na overschrijden van deze limiet wordt de verbinding door Datanet-1 verbroken.

e. PAD-aansluiting
Met de PAD-aansluiting krijgt men via het analoge telefoonnetwerk een asynchrone verbinding met Datanet-1. In tegenstelling tot de hierna genoemde X.32-aansluiting is de PAD-aansluiting bedoeld voor gebruikers die niet beschikken over een DTE met X.25-functionaliteit. Om via een PAD verbinding te maken met een willekeurige Datanet-1-abonnee hoeft men slechts te beschikken over een asynchrone terminal, een modem en een toegangscode tot de PAD. De PAD draagt zorg voor de conversie van asynchroon verkeer naar X.25-formaat en vice versa.
Maximale snelheid van de verbinding is momenteel 2400 bps.

f. X.32-aansluiting
De X.32-aansluiting op Datanet-1 is ultimo 1991 geïntroduceerd. Een X.32-aansluiting biedt dezelfde functionaliteit als de PAD-aansluiting. De abonnee heeft echter de beschikking over maximaal drie logische kanalen en kan dus tegelijkertijd met maximaal drie andere abonnees een verbinding opbouwen. Een ander verschil met de PAD-aansluiting is, dat de te verzenden data niet asynchroon maar in pakketvorm moeten worden aangeboden.

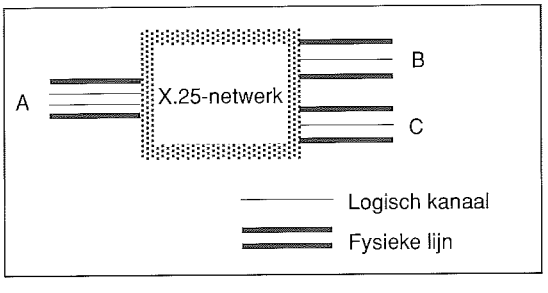
Datacommunicatie via Datanet-1

In tegenstelling tot het openbare telefoonnetwerk functioneren pakketgeschakelde netwerken, zoals Datanet-1, niet volgens de circuit-switching-techniek, maar wordt gebruik gemaakt van packet-switching. Hierbij wordt de te verzenden informatie onderverdeeld in datapakketjes van een vaste lengte. Zoals eerder in deze paragraaf reeds is aangegeven, zijn twee protocollen relevant:

– *Het netgram protocol*
Datanet-1 gebruikt intern het netgram protocol. Dit zorgt ervoor dat ieder ontvangen pakket wordt voorzien van een bestemmingsadres en door het net wordt gerouteerd. Daarbij wordt gebruik gemaakt van de store and forward-faciliteiten in de knooppunten, waarbij de pakketten tijdelijk worden opgeslagen. Vervolgens worden de pakketten afhankelijk van het bestemmingsadres en de beschikbare verbindingen doorgerouteerd. Het voordeel van een dergelijke methode is dat een fysieke lijn tegelijkertijd voor meer dan één communicatieverbinding kan worden gebruikt. Een tweede voordeel is de mogelijkheid tot het automatisch benutten van alternatieve lijnen indien één of meer lijnen zijn uitgevallen.
Het netgram protocol zorgt er tevens voor dat de ontvanger de pakketten krijgt aangeboden in de volgorde waarin de zender deze heeft verstuurd.

– *Het X.25-protocol*
Voor de communicatie tussen Datanet-1 en de abonnees wordt gebruik gemaakt van de CCITT Recommendation X.25 (het 'X.25-protocol') [CCIT]. In dit protocol is gespecificeerd op welke wijze de datapakketten dienen te worden opgebouwd. De fysieke verbinding tussen de abonnee en het netwerk kan bij X.25 worden onderverdeeld in verscheidene zogenaamde 'logische kanalen'. Deze kanalen kunnen tegelijkertijd worden gebruikt en via ieder kanaal kan men communiceren met een afzonderlijke netwerkabonnee.
In figuur 2 is uitgebeeld dat abonnee A over één fysieke verbinding via twee logische kanalen gelijktijdig communiceert met de abonnees B respectievelijk C. In Datanet-1-termen heeft abonnee A een

Figuur 2. De begrippen logisch kanaal en fysieke lijn.



Virtual Call opgebouwd met abonnee B en een Virtual Call met abonnee C. De wijze waarop de verbindingsopbouw plaatsvindt wordt in de volgende subparagraaf toegelicht.

Verbindingsopbouw via Datanet-1

Bij Datanet-1 kan een aantal niveaus in de verbindingsopbouw worden onderscheiden:
- opbouw van de fysieke verbinding;
- opbouw van de modemverbinding;
- opbouw van de Virtual Call.

Vervolgens kan de logische verbinding worden opgebouwd. Dit laatste wordt in dit artikel verder niet behandeld. Volledigheidshalve is deze fase nog wel in tabel 1 opgenomen; voor meer informatie wordt verwezen naar de literatuur [Brou92].

Het opbouwen van de fysieke en de modemverbinding is alleen nodig indien gebruik wordt gemaakt van de PAD- of X.32-faciliteit. Bij de overige aansluitingen is dit niet nodig omdat daar gebruik wordt gemaakt van vaste verbindingen tussen abonnee en PDS.

Bij het opbouwen en afbreken van de Virtual Call wordt een onderscheid gemaakt in de volgende fasen:
- identificatie;
- call setup;
- data transfer;
- call clearing.

Deze fasen worden in de volgende alinea's toegelicht.

- Identificatiefase

Datanet-1 ondersteunt de identificatiefase alleen voor de PAD- en X.32-aansluitingen met behulp van de Network User Identification (NUI)-faciliteit [CCIT]. De gebruiker dient zich hierbij door het versturen van identificatiegegevens bekend te maken aan het netwerk.

- Call setup-fase

Tijdens de call setup-fase wordt de Virtual Call opgebouwd. Het opbouwen van logische verbindingen via Virtual Calls is vergelijkbaar met de verbindingsopbouw via het telefoonnet. Het komt er simpelweg op neer dat de oproeper kiesinformatie aanbiedt aan het netwerk. De kiesinformatie moet worden aangeboden in de vorm van specifieke data-pakketten (zogenaamde Call Request-pakketten, zie figuur 3).

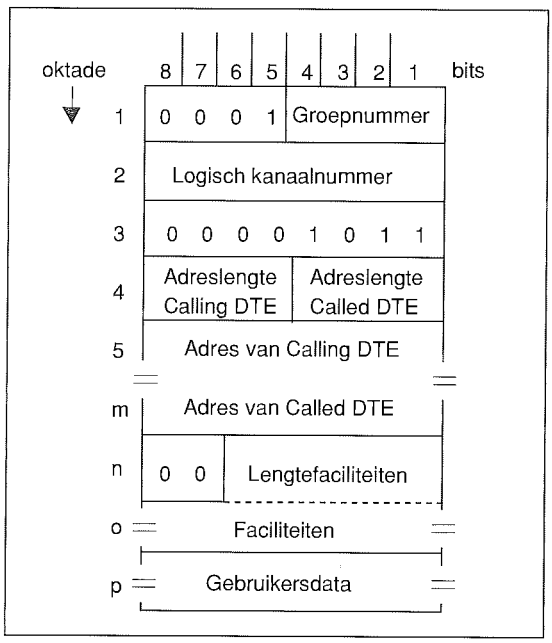
De opgeroepen abonnee wordt door het netwerk op de hoogte gesteld van de oproep en besluit door middel van het verzenden van een bepaald datapakket al dan niet de oproep te honoreren (vergelijkbaar met het al dan niet oppakken van de hoorn van de telefoon). Omdat communicatie over het netwerk plaatsvindt via datapakketten is het proces van verbindingsopbouw technisch echter wel afwijkend van het telefoonnetwerk. Bovendien zijn in het netwerk controles ingebouwd om vast te stellen of de beide abonnees gerechtigd zijn met elkaar te communiceren.

- Data transfer-fase

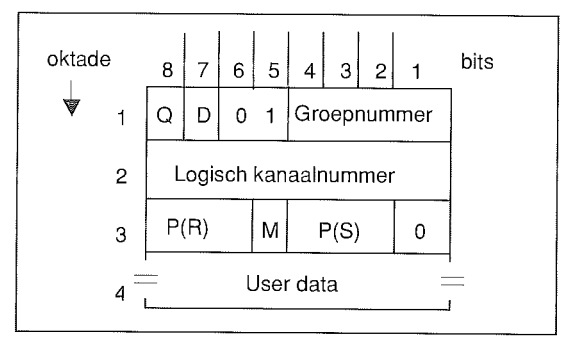
Na het opbouwen van de Virtual Call kan de eigenlijke datacommunicatie plaatsvinden door middel van het uitwisselen van datapakketten. Het formaat van een datapakket is gegeven in figuur 4.

Zoals uit figuur 4 blijkt zijn de netwerkadressen van de oproepende en de opgeroepen abonnee niet meer in het pakket opgenomen. Met behulp van door de PDS opgebouwde administratie tijdens de call setup-fase worden de pakketten op grond van het groepnummer en het logisch kanaalnummer naar hun bestemming gerouteerd. Afhankelijk van onder andere de beschikbaarheid en de belasting van de lijnen zullen de pakketten over de verschillende lijnen van het netwerk worden gerouteerd. De gevolgde route kan daardoor per Datanet-1-pakket verschillend zijn. Alle datapakketten lopen echter wel altijd via de verbindingen tussen de abonnees en bijbehorende PDS'en.

Figuur 3. Call Request-pakket.



Figuur 4. Datapakket.



– Call clearing-fase
In de call clearing-fase wordt de Virtual Call afgebouwd en komen de gebruikte logische kanalen weer vrij.

Verbindingsopbouw bij gebruik van een X.32-aansluiting
Een gebruiker van een X.32-aansluiting kan niet worden door andere abonnees, hij kan alleen zelf het initiatief nemen tot het opbouwen van een verbinding. Hij bouwt hiertoe eerst een normale telefoonverbinding op met een speciale Datanet-1-node. Vervolgens wordt de modemverbinding tot stand gebracht en kunnen X.25-pakketten worden aangeboden. De gebruiker dient zich allereerst te identificeren door een aansluitnummer en een toegangscode. Deze worden opgenomen in het Call Request-pakket. Bij ontvangst van een Call Request-pakket wordt door de Datanet-1-node gecontroleerd of de ontvangen toegangscode correct is. Is dit het geval dan wordt het Call Request-pakket verder gerouteerd. De verdere verbindingsopbouw verloopt dan overeenkomstig de hierboven beschreven situatie.

Is de toegangscode niet correct dan wordt het Call Request-pakket alsnog verder gerouteerd, maar wordt tevens het Reverse Charging-bit aangezet. Hiermee wordt aan de ontvangende partij verzocht of hij ermee akkoord gaat dat de datacommunicatiekosten voor zijn rekening komen. Deze op het eerste gezicht voor EDP-auditors onbegrijpelijke handelwijze is te verklaren door het feit dat de identificatie voor PTT Telecom in de eerste plaats van belang is om vast te kunnen stellen aan wie de datacommunicatiekosten moeten worden toegerekend [PTT91].

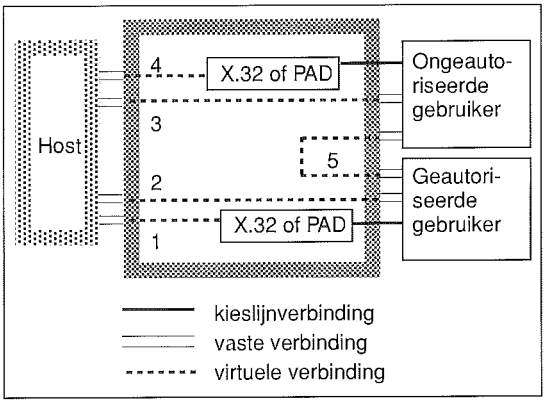
Verbindingsopbouw bij gebruik van een PAD
Ook een PAD-gebruiker kan alleen zelf het initiatief nemen voor het opbouwen van een verbinding. Hij bouwt hiertoe eerst een normale telefoonverbinding op met de PAD. Vervolgens wordt met een standaardmodem een modemverbinding tot stand gebracht (maximale snelheid momenteel 2400 bps). De PAD verstuurt een welkomstscherm en men krijgt de keuze tussen ongeïdentificeerd of geïdentificeerd kiezen.

a. Ongeïdentificeerd kiezen wil zeggen dat men niet rechtstreeks het Datanet-1-nummer kan opgeven van een netwerkabonnee. Men kan alleen de naam opgeven van een door een netwerkabonnee beschikbaar gestelde netwerkdienst. De PAD verstuurt dan de benodigde pakketten naar deze dienst. Identificatie vindt vervolgens plaats door de netwerkdienst. Voorbeelden van dergelijke diensten zijn de door verschillende banken aangeboden 'elektronisch-bankieren'-functies.

b. Geïdentificeerd kiezen houdt in dat men zich kenbaar maakt aan het netwerk door het ingeven van een door de netwerkdienst verstrekt gebruikersnummer en (zelf te wijzigen) password. Is de identificatie toereikend dan verschijnt ter controle een scherm met daarop de datum en het tijdstip van de voorlaatste succesvolle aanlogpoging alsmede het aantal daarna opgetreden niet-succesvolle aanlogpogingen. Men kan nu wel rechtstreeks een verbinding opbouwen met een andere netwerkabonnee door het desbetreffende abonneenummer te verzenden naar de PAD.

RISICO'S VAN DATACOMMUNICATIE VIA DATANET-1

Een situatieschets van de mogelijke verbindingsopbouw via Datanet-1 is gegeven in figuur 5. De cijfers geven de mogelijke verbindingen aan. De verbindingen genummerd 1 en 2 zijn de enig gewenste verbindingen, de verbindingen 3, 4 en 5 dienen te worden voorkomen.



Figuur 5. Mogelijke verbindingsopbouw.

Bij datacommunicatie via een openbaar netwerk worden de volgende risico's gelopen:

– algemene risico's die bij iedere vorm van datacommunicatie worden gelopen:
  a. passieve aanval,
  b. actieve aanval;

– specifieke risico's bij het gebruik van kieslijnen:
  c. onjuiste verbindingsopbouw,
  d. onjuiste verbindingsafbouw.

Ad a. Passieve aanval
Bij een passieve aanval worden de verzonden berichten afgeluisterd, vaak zonder dat de geautoriseerde gebruiker dit opmerkt. Een passieve aanval is het gemakkelijkst op de vaste verbindingen tussen de netwerkabonnees en het Datanet-1 entrypoint (de PDS). De lijnsnelheid van deze verbindingen is relatief laag. Via deze verbindingen worden alleen datapakketten verzonden van/naar de desbetreffende abonnee, waarbij de datapakketten bovendien keurig in de juiste volgorde worden getransporteerd.
Bij een passieve aanval kunnen worden onderscheiden:

a1. Het aftappen van gegevens
Vertrouwelijke informatie kan op deze wijze in handen komen van derden. Hierbij dient te worden bedacht dat men door aftappen van gewone analoge telefoonlijnen in het bezit kan komen van het gebruikersnummer en -password van een PAD- of X.32-gebruiker. Vervolgens kan dan gebruik worden gemaakt van de Datanet-1-autorisaties van de rechtmatige gebruiker.

a2. Een analyse van de berichtenstroom
Hierbij wordt geanalyseerd wie naar welke bestemming gegevens verzendt. Bij het aftappen van Call Request-pakketten kan uit het Calling DTE- en het Called DTE-adres worden herleid wie met wie communiceert.

Een passieve aanval is het gemakkelijkst op de verbinding tussen netwerkabonnee en PDS.

Ad b. Actieve aanval
Ook een actieve aanval is het gemakkelijkst op de vaste verbindingen tussen de netwerkabonnees en het Datanet-1 entry-point. Onder een actieve aanval wordt verstaan [Davi89]:

b1. Wijzigen, verwijderen, toevoegen van berichten
Bij wijziging van berichten zal ook de Frame Check Sequence (een aan het X.25-pakket toegevoegde checksum) moeten worden aangepast. Dit zal voor een aanvaller geen belemmering vormen omdat geen gebruik wordt gemaakt van geheime algoritmen of sleutels.
Bij verwijderen of toevoegen van berichten op de vaste verbinding tussen netwerkabonnee en PDS zal ook de nummering van de navolgende berichten door de aanvaller moeten worden aangepast.

b2. Veranderen van het bronadres.

b3. Veranderen van het bestemmingsadres
Het veranderen van het bron- of bestemmingsadres is alleen mogelijk in pakketten die het Calling respectievelijk Called DTE-adres bevatten (dus niet bij datapakketten).

b4. Veranderen berichtenvolgorde
Bij het veranderen van de berichtenvolgorde zal ook de nummering van de berichten door de aanvaller moeten worden aangepast, anders zal dit worden gedetecteerd.

b5. Herhalen van een reeds verzonden bericht
Herhalen van een reeds verzonden bericht zal door de nummering van de berichten worden bemerkt. Wil de aanvaller dit voorkomen dan zal hij het nummer van het reeds verzonden bericht moeten aanpassen of dit bericht op een zodanig moment versturen dat de nummering van de verzonden en ontvangen pakketten consistent is met de voorgaande berichtenuitwisseling. Tevens zal de nummering van alle navolgende rechtmatig verstuurde pakketten door de aanvaller moeten worden aangepast.

b6. Vervalsen van een bevestiging
Een ontvanger claimt een bericht te hebben ontvangen terwijl dat in werkelijkheid nooit is verzonden.

Ad c. Ongeautoriseerde verbindingsopbouw
Bij gebruik van kieslijnen loopt men het risico dat een ongeautoriseerde verbinding wordt opgebouwd. Onder een ongeautoriseerde verbindingsopbouw wordt in dit verband verstaan het opbouwen van een verbinding door een persoon:

c1. die daartoe niet bevoegd is, dan wel

c2. met ruimere dan de voorbehouden bevoegdheden, dan wel

c3. met behulp van niet voor inkiesdoeleinden beschikbaar gestelde componenten (hard- en/of software), dan wel

c4. vanaf een niet gewenste locatie, dan wel

c5. gedurende niet gewenste tijdstippen.

Uit de hiervoor gegeven definitie volgt dat een geautoriseerde verbinding voldoet aan het begrip 'de vijf juisten' (juiste persoon, juiste bevoegdheden, juiste componenten, juiste locatie, juiste tijdstip). Of men een kiesverbinding daadwerkelijk op alle vijf aspecten wil beveiligen, zal afhangen van het specifieke doel van de verbinding alsmede van de gelopen risico's. In dit artikel wordt verder voornamelijk ingegaan op de juiste locatie. Voor een toelichting op de overige risico's en de hiertegen te nemen maatregelen wordt verwezen naar de literatuur [Brou92]. Overigens is het theoretisch mogelijk dat ook na een juiste verbindingsopbouw datapakketten worden ontvangen van een 'onjuiste' afzender ten gevolge van schakel- c.q. routeringsfouten in de netwerknodes van Datanet-1 (bijvoorbeeld de PDS of de PSE).

Ad d. Onjuiste verbindingsafbouw
Normaal gesproken zal de verbinding als volgt worden afgebouwd: beëindigen van de sessie met de host en vervolgens het afbouwen van de Virtual Call. Stel nu echter dat eerst de Virtual Call wordt afgebouwd. De op de host gestarte applicatie hoeft dit niet te merken. In dat geval zal bij het weer tot stand komen van een Virtual Call met de host (op hetzelfde logische kanaal) tevens de logische verbinding weer worden voortgezet en hoeven geen verdere identificerende gegevens kenbaar te worden gemaakt.

BEVEILIGINGSMAATREGELEN

In deze paragraaf zullen maatregelen worden besproken die voor de beveiliging van datacommunicatie via een openbaar pakketgeschakeld netwerk kunnen worden getroffen. In de volgende subparagrafen wordt een onderverdeling aangebracht naar de verschillende te onderscheiden fasen van verbindingsopbouw, datacommunicatiefase en verbindingsafbouw.

Maatregelen tijdens de opbouw van de fysieke en modemverbinding

In tegenstelling tot het gebruik van analoge kieslijnen zijn nu geen speciale beveiligingsmaatregelen te treffen. De door de netwerkleverancier beschikbaar gestelde PAD- of X.32-aansluiting moet namelijk voor algemeen gebruik toegankelijk zijn. De enige wijze waarop eventueel beveiligingsmaatregelen zijn te implementeren, is door te voorzien in een eigen PAD-faciliteit. In het kader van dit artikel wordt hier verder niet op ingegaan. Volledigheidshalve zijn de mogelijke maatregelen nog wel in tabel 1 opgenomen; voor meer informatie wordt verwezen naar de literatuur [Brou92].

Maatregelen tijdens het opbouwen van een Virtual Call

Tijdens het opbouwen van een Virtual Call zijn de volgende beveiligingsmaatregelen relevant:

a. controle op het Calling DTE-adres door de netwerkdienst;
b. blokkering door de netwerkdienst;
c. Besloten Gebruikers Groepen;
d. identificatie van de X.25-aansluiting;
e. het gebruik van Permanent Virtual Circuits;
f. weigeren van een verzoek tot Reverse Charging;
g. gebruik van een datum/tijdslot;
h. redundante informatie in het Call Request-pakket.

Deze maatregelen zullen achtereenvolgens worden besproken.

Ad a. Controle op het Calling DTE-adres door de netwerkdienst
Zoals behandeld begint het opbouwen van een verbinding met het versturen van een Call Request-pakket. In dit pakket worden de adressen van de Calling en de Called DTE gespecificeerd. Door bewuste manipulatie van het Calling DTE-adres zou men zich kunnen voordoen als een ander aansluitnummer. Een door PTT Telecom geïmplementeerde controle is dan ook dat voor ieder Call Request-pakket wordt vastgesteld dat het gespecificeerde Calling DTE-adres overeenkomt met het toegekende aansluitnummer. Een dergelijke controle is mogelijk omdat de verbinding tussen abonnee en netwerk entry-point een vaste verbinding is. Hierbij geldt een vaste relatie tussen de binnenkomende fysieke kabel en het bijbehorende aansluitnummer (vergelijkbaar met het telefoonnet!). PTT Telecom voorziet in een dergelijke controle bij Datanet-1. Een Datanet-1-abonnee kan zijn aansluitnummer zelf in het Call Request-pakket meegeven, maar dit hoeft niet. Indien zijn aansluitnummer niet in het pakket is ingevuld, zal dit automatisch gebeuren door de PDS van Datanet-1. Indien een adres is ingevuld dat niet correspondeert met de desbetreffende vaste verbinding waar het Call Request-pakket binnenkomt, dan zal dit pakket worden geweigerd en verstuurt het Datanet-1-netwerk een foutmelding naar de Calling DTE.

Controle door de netwerkleverancier op het Calling DTE-adres is een basisvoorwaarde voor een te beveiligen X.25-netwerk.

Controle door de netwerkleverancier op het Calling DTE-adres is een basisvoorwaarde voor een te beveiligen X.25-netwerk. Mits deze maatregel niet door de abonnees is te beïnvloeden wordt een bescherming verkregen tegen risico b2 (het veranderen van het bronadres).

Ad b. Blokkering door de netwerkdienst
Het Datanet-1 ondersteunt een viertal in de X.25-standaard [CCIT] gedefinieerde faciliteiten waarmee blokkering van het berichtenverkeer mogelijk is:

1. Incoming calls barred
Het desbetreffende aansluitnummer kan wel zelf een verbinding opzetten maar is geblokkeerd voor inkomende berichten.

2. Outgoing calls barred
Het aansluitnummer kan nu niet zelf een verbinding initiëren (een door dit nummer verstuurd Call Request-pakket zal door het netwerk worden geweigerd), maar kan wel inkomende berichten accepteren.

3. One-way logical channel outgoing
Deze situatie is dezelfde als 1, maar geldt voor één logisch kanaal.

4. One-way logical channel incoming
Analoog aan 3, maar nu is voor een kanaal alleen inkomend verkeer mogelijk.

Door voor een individuele netwerkaansluiting de faciliteit 'incoming calls barred' aan te vragen wordt een blokkering verkregen tegen Incoming Call-pakketten. Deze methode is dus alleen geschikt voor aansluitnummers die alleen zelf actie nemen om een verbinding op te bouwen. Met de faciliteit 'incoming calls barred' wordt een harde beveiliging verkregen tegen risico c1, het opbou-

wen van een verbinding door een ongeautoriseerde gebruiker.

Ad c. Besloten Gebruikers Groep binnen Datanet-1
Een beveiliging tegen de ontvangst van een door een ongeautoriseerde gebruiker verzonden Call Request vormt het gebruik van de in de X.25-standaard gedefinieerde Closed User Group facility (CUG) of Besloten Gebruikers Groep (BGG). Aansluitnummers die in een BGG zijn opgenomen, kunnen in principe alleen met elkaar communiceren. Indien een Call Request wordt verstuurd door een gebruiker buiten de BGG naar een gebruiker binnen de BGG zal de toegang door Datanet-1 worden geweigerd. De beveiliging van een BGG staat of valt met het gemak waarmee men zich kan voordoen als een ander aansluitnummer. De eerder besproken controle op het Calling DTE-adres door de netwerkleverancier is een vereiste.

Het enkele feit dat nummers zijn opgenomen in een BGG zegt nog niets over de beveiliging.

Het bovenstaande wordt echter gecompliceerd doordat aansluitnummers binnen een BGG individueel faciliteiten kunnen aanvragen die de beveiliging kunnen bedreigen. Het enkele feit dat nummers zijn opgenomen in een BGG zegt dan ook nog niets over de beveiliging! Bij Datanet-1 kunnen de volgende faciliteiten door de beheerder tijdens het verzoek tot opname van een bepaald Datanet-1-aansluitnummer in een BGG worden gespecificeerd:

a. CUG with Incoming Access
Een aansluitnummer binnen de BGG kan door deze faciliteit toch berichten ontvangen van aansluitingen buiten de BGG.

b. CUG with Outgoing Access
Een aansluitnummer binnen de BGG kan door deze faciliteit een Call Request verzenden naar aansluitingen buiten de BGG.

c. Incoming calls barred within CUG
Een aansluitnummer met deze faciliteit is weliswaar opgenomen in de BGG, maar kan geen Incoming Call krijgen van aansluitingen binnen de BGG.

d. Outgoing calls barred within CUG
Een aansluitnummer met deze faciliteit is weliswaar opgenomen in de BGG maar kan geen Call Request verzenden naar aansluitingen binnen de BGG.

Beheer van de BGG
Bij gebruik van de BGG-faciliteit wordt via een speciaal formulier aan de netwerkleverancier bekend gemaakt wie binnen de eigen organisatie als beheerder van de BGG zal optreden. De beheerder is de enige persoon die geautoriseerd is om aansluitnummers in de BGG te laten opnemen. De beheerder kan ook ten behoeve van andere contractanten om toegang tot de BGG verzoeken. (Onder contractant verstaat PTT Telecom degene die het Datanet-1-aansluitnummer heeft aangevraagd en bijgevolg de nota's krijgt toegestuurd.)
Ook de X.32- en de geïdentificeerde PAD-aansluiting kunnen in een BGG worden opgenomen. Het verdient uit veiligheidsoverwegingen echter de voorkeur om deze niet in een BGG op te nemen. Teneinde een BGG zo besloten mogelijk te houden verdient het daarnaast aanbeveling dat de beheerder van de BGG, bij de naar de netwerkleverancier verstuurde aanvraag tot opname van een individuele aansluiting in een BGG, geen gebruik maakt van de faciliteit Incoming Access Allowed en de faciliteit Outgoing Access Allowed. Zelfs dan is er echter nog geen garantie dat de in de BGG opgenomen nummers alleen met elkaar kunnen communiceren! Het staat de contractant van een aansluitnummer namelijk vrij om ook aan een beheerder van een andere BGG een verzoek te richten tot opname in de BGG.
Op deze wijze kan een aansluitnummer zijn opgenomen in meerdere BGG's zonder dat de beheerders van deze BGG's hiervan kennis hebben. Hier kunnen zich merkwaardige situaties voordoen. Zo kan een aansluitnummer zijn opgenomen in BGG X zonder verdere faciliteiten en opname verzoeken in BGG Y met de faciliteiten Incoming Access allowed en Outgoing Access allowed. De netwerkleverancier heeft dan een probleem. Indien de aanvraag wordt gehonoreerd, is het resultaat dat het aansluitnummer kan communiceren met aansluitnummers binnen zowel BGG X als BGG Y als overige aansluitnummers.

PTT Telecom heeft deze situatie procedureel ondervangen. Indien bij de behandeling van een aanvraag tot opname van een aansluitnummer in een BGG blijkt dat het nummer reeds in een andere BGG is opgenomen waarbij andere faciliteiten zijn verleend dan de nu aangevraagde, dan neemt PTT Telecom contact op met de aanvragers (in het voorbeeld de contractant van het aansluitnummer en de beheerder van BGG Y).

Bij een juist gebruik van een BGG (waaronder een juiste definiëring van de BGG-faciliteiten) wordt een bescherming verkregen tegen risico c1, het maken van een call door een ongeautoriseerde gebruiker. Mits geen X.32- of PAD-aansluitingen in de BGG worden opgenomen, wordt daarnaast een bescherming verkregen tegen risico c4 (initiëren van een verbinding vanaf een ongeautoriseerde locatie).
Het is ook mogelijk een eigen equivalent te creëren van de reeds beschreven Besloten Gebruikers Groep. Hierbij wordt door de Called DTE zelf gekeken naar het in dit pakket gespecificeerde Calling DTE-adres. Afhankelijk van dit adres zal een call wel respectievelijk niet worden toegestaan. Een voordeel van deze methode ten opzichte van de BGG-faciliteit die door de netwerkleverancier kan worden geleverd, is dat men de blokkering ge-

heel onder beheer van de eigen organisatie uitvoert.
Controle van het Calling DTE-adres kan plaatsvinden in de hoger gelegen lagen in de host-computer waarna op dit niveau wordt besloten of de call al of niet wordt gehonoreerd. Deze controle kan echter ook geschieden met behulp van speciale apparatuur die tussen de host en de netwerkaansluiting wordt geschakeld. Deze speciale apparatuur (security gate) kan veelal ook voorzien in de volgende functionaliteiten:
- bewaking van een inactiviteitslimiet;
- datum/tijdslot per geautoriseerd aansluitnummer;
- encryptie van de user data in het datapakket;
- audit trail.

Ad d. Identificatie van een netwerkaansluiting
In de X.25-standaard is ook de NUI (Network User Identification)-faciliteit opgenomen. De NUI-informatie wordt meegestuurd met het Call Requestpakket en kan worden gezien als een soort password waarmee de aansluiting zich aan het netwerk bekend moet maken alvorens een call kan worden opgezet. De NUI-informatie wordt gecontroleerd door de leverancier van de netwerkdienst en wordt niet doorgezonden naar de Called DTE. Deze informatie wordt overigens in klaartekst verzonden en zal bij een passieve aanval op het berichtenverkeer dus kunnen worden achterhaald.
De NUI-faciliteit wordt door Datanet-1 alleen voor de X.32- en de PAD-aansluiting toegepast en wordt voor de overige aansluitingen niet ondersteund.

Ad e. Gebruik van een PVC
De term PVC staat voor Permanent Virtual Circuit. Het verschil met een VC (Virtual Call) ligt in het feit dat via een PVC alleen communicatie mogelijk is tussen twee specifiek in het netwerk gedefinieerde netwerkabonnees. Een PVC is enigszins vergelijkbaar met een digitale huurlijn dan wel een Besloten Gebruikers Groep met slechts twee abonnees.
Ter benadrukking van het onderscheid tussen een PVC en een VC wordt een VC ook wel aangeduid met de benaming SVC (Switched Virtual Circuit of soms Switched Virtual Call).

Bedacht dient te worden dat een PVC wordt gedefinieerd per logisch kanaal. Voor een aansluitnummer met meerdere kanalen kan op deze wijze voor één kanaal een PVC gedefinieerd zijn maar kan een ander kanaal beschikken over de mogelijkheid om een SVC op te bouwen. Bij Datanet-1 is het zelfs niet mogelijk alleen een PVC aan te vragen. Er wordt minimaal één SVC meegeleverd ten behoeve van netwerk-interne besturingssignalen. Indien het gebruik van deze SVC niet gewenst is, dient deze uit beveiligingsoverwegingen voor inkomend verkeer te worden geblokkeerd. Op deze wijze wordt dan een bescherming verkregen tegen de risico's c1 (ongeautoriseerde gebruiker) en c4 (ongeautoriseerde locatie).

Ad f. Reverse Charging
Reverse Charging is een in X.25 gedefinieerde faciliteit waarmee de Calling DTE in het Call Requestpakket kan aangeven dat de Called DTE wordt verzocht de verbindingskosten op zich te nemen. Indien de Called DTE bij de netwerkleverancier niet de Reverse Charging Acceptance faciliteit heeft aangevraagd, zal de call echter door het netwerk worden geweigerd.

Indien het gebruik van een SVC niet gewenst is, dient deze uit beveiligingsoverwegingen voor inkomend verkeer te worden geblokkeerd.

Hoewel het niet aanvragen van de Reverse Charging Acceptance-faciliteit niet echt als een beveiligingsmaatregel kan worden beschouwd, is deze maatregel toch niet geheel zonder betekenis. Eerder is reeds aangegeven dat indien bij een X.32-aansluiting (door een ongeautoriseerde persoon) een verkeerde toegangscode is ingegeven een Call Request toch verder wordt gerouteerd, maar dan met het verzoek tot Reverse Charging. Het opnemen van een X.32-aansluiting in een Besloten Gebruikers Groep waarbij voor de overige in de BGG opgenomen nummers de Reverse Charging Acceptance-faciliteit is aangevraagd, zou dus zeer onverstandig zijn!

Ad g. Datum/tijdslot
Met behulp van een datum/tijdslot kan worden bereikt dat gedurende een bepaalde tijd niet wordt gereageerd op een verzoek tot het opbouwen van een Virtual Call. De meest simpele manier om dit te bereiken is het opnemen van een tijdschakelaar in het netsnoer van de modem. De modemverbinding via de vaste verbinding tussen abonnee en PDS-centrale van het netwerk valt dan weg maar de meeste netwerkleveranciers (waaronder PTT Telecom met betrekking tot Datanet-1) hebben daar geen problemen mee. Zodra de modem weer wordt aangezet, wordt de modemverbinding automatisch hersteld en kan weer gebruik worden gemaakt van de netwerkdiensten.
Een datum/tijdslot kan ook individueel worden ingesteld door in een tabel op te nemen naar welke netwerkaansluitnummers gedurende welke tijden een positieve reactie zal worden verzonden als antwoord op een verzoek tot het opbouwen van een Virtual Call. De benodigde gegevens (netwerkaansluitnummers, tijd en datum waarop een verbinding mag worden opgebouwd) kunnen worden gecontroleerd in de applicatieve laag. Er bestaan echter ook afzonderlijke apparaten (zoals de eerder in deze paragraaf onder Ad c besproken security gate) waarin deze functionaliteit kan worden opgenomen.
Een datum/tijdslot geeft een bescherming tegen risico c5 (verbindingsopbouw op ongeautoriseerd tijdstip).

Ad h. Redundante informatie in het Call Request-pakket
In het Call Request-pakket kan op twee manieren redundante informatie worden opgenomen. De eerste manier is het gebruik van subadressering, dit is het toevoegen van extra cijfers aan het Called DTE-adres. Het aantal mogelijk toe te voegen cijfers is netwerk-afhankelijk; bij Datanet-1 heeft men de mogelijkheid om aan het zevencijferige Datanet-1-aansluitnummer maximaal vier cijfers aan het bestemmingsadres toe te voegen. Deze vier cijfers kunnen worden gebruikt om de host-zijde mede te delen met welke applicatie men een verbinding zoekt. Subadressering kan echter ook worden gebruikt als een soort password-beveiliging; de waarde hiervan is beperkt gezien het geringe aantal cijfercombinaties (10^4). Bovendien wordt de informatie onversleuteld door het netwerk getransporteerd.
Bij de tweede manier wordt extra informatie opgenomen in het user data field van het Call Request-pakket. Ook in het Call Request-pakket staat namelijk 1024 bits aan gebruikersdata ter beschikking. Bij volledig gebruik van dit aantal bits is de raadkans nagenoeg nihil (aantal mogelijkheden is 2^{1024}). Aandachtspunt blijft natuurlijk wel dat de afgesproken code bekend raakt indien het bericht wordt afgetapt.
Het toevoegen van redundante informatie als een soort password aan het Call Request-pakket biedt een bescherming tegen risico c1 (het initiëren van een verbinding door een ongeautoriseerde gebruiker). Er wordt alleen een harde bescherming verkregen indien het afgesproken password slechts eenmalig geldig is.

Tabel 1. Relatie maatregelen versus risico's.

Fase / • Maatregel	Beschermt tegen de risico's
Opbouwen fysieke c.q. telefoonverbinding	
• Blokkade inkomend verkeer	c1, c4, c5
• Dial-back apparatuur	c1, c4
• Uitgebreide manuele procedure	c1, c5, d
Opbouwen modemverbinding	
• Deactiveren Automatic Answer	c1, c4, c5
• Speciale modulatietechniek	a1, a2, b1, b2, b3, c1, c3, d
• Speciale datacompressie	a1, a2, b1, b2, b3, c1, c3, d
• Datum/tijdslot	c5
Call setup fase	
• Controle Calling DTE-adres (door netwerkleverancier)	b2
• Blokkering door netwerkdienst	c1
• BGG	c1, c4
• NUI	b2, c1
• PVC	c1, c4
• Weigeren Reverse Charging	(c1)
• Controle Calling DTE-adres (door abonnee zelf)	c1, c5
• Datum/tijdslot	c5
• Redundante informatie in Call Request-pakket	c1
Datatransferfase	
• Encryptietechnieken	a1, a2, b1, b2, b3, c1, c3, d
• Manipulation Detection Code	a1, a2, b1, b2, b3, c1, c3, d
• Message Authentication Code	b1, c1, d
• Digitale handtekening	b1, b6, c1, d
• Nummering van berichten	b1, b4, b5
• Datum/tijdstempel	b4, b5
• Delivery confirmation	b1
Opbouwen logische verbinding	
• Dual challenge response procedure	c1, c3
• User-ID/lijn-combinatie	c2
• Datum/tijdslot	c4
• Encryptietechnieken	a1, a2, b1, b2, b3, c1, c3, d
Afbouwen verbinding	
• Bewaking draaggolf	d
• Bewaking lijnactiviteit	d

De in afgedrukte risico's worden alleen afgedekt bij gebruik van link-encryptie.
Voor de mate van bescherming en de niet-besproken maatregelen wordt verwezen naar de literatuur [Brou92].

Maatregelen tijdens de datacommunicatiefase

De mogelijk te treffen maatregelen tijdens de datacommunicatiefase zijn overeenkomstig dergelijke maatregelen bij het gebruik van vaste lijnen [Brou92]. In dit artikel zal daarom alleen worden ingegaan op een specifieke maatregel bij Datanet-1, namelijk het gebruik van Delivery Confirmation. (In tabel 1 zijn de mogelijke maatregelen wederom weer wel opgenomen.)

De nummering binnen de datapakketten heeft normaal gesproken alleen lokale betekenis (tussen PDS en abonnee) en biedt daardoor geen bescherming tegen het tussenvoegen of verwijderen van berichten op andere plaatsen in het netwerk. Echter, indien in het Call Request-pakket het zogenaamde Delivery bit op één wordt gezet, krijgt de nummering wel een end-to-end-betekenis. Tussenvoeging en verwijdering van berichten zal dan wel worden gedetecteerd! Gebruik van het Delivery bit kan echter wel de snelheid van de gegevensoverdracht verminderen. Er mogen dan namelijk maximaal twee datapakketten voor de desbetreffende verbinding in het netwerk aanwezig zijn. Na het versturen van twee pakketten dient dus eerst op een bevestiging van de andere abonnee te worden gewacht.
Het gebruik van Delivery Confirmation geeft de zend- en ontvangsttellers een end-to-end-betekenis. Indien elders in het netwerk berichten worden toegevoegd of weggelaten (risico b1), zal dit worden gedetecteerd.

Maatregelen tijdens het afbouwen van de verbinding

Er staan twee maatregelen ter beschikking voor de bewaking van de juiste verbindingsafbouw, te weten de bewaking van de draaggolf en de bewaking van de lijnactiviteit.

Bewaking van de draaggolf
Het kortstondig wegvallen van de draaggolf op de vaste verbinding tussen netwerkabonnee en PDS kan betekenen dat de verbinding door een ongeautoriseerde persoon is onderbroken c.q. overgenomen. Het zal dan gewenst zijn de verbinding af te bouwen. Hiertoe dient de opgestarte applicatie te worden beëindigd en de Virtual Call te worden afgebouwd. Na een analyse van de foutoorzaak kan de verbinding opnieuw worden opgebouwd.
Bewaken van de draaggolf geeft een bescherming tegen risico d (onjuiste verbindingsafbouw).

Bewaking van de lijnactiviteit
In de applicatiegerichte lagen kan een bewaking van de lijnactiviteit worden opgenomen. Indien de inactiviteitslimiet wordt overschreden, dient zowel de opgestarte applicatie als de Virtual Call te worden afgebouwd.
Bewaken van de lijnactiviteit geeft een bescherming tegen risico d (onjuiste verbindingsafbouw).

AUDIT-ASPECTEN

a. Beoordeling netwerk(leverancier)

Zoals uit het voorgaande kan worden afgeleid, is het beveiligingsniveau van een netwerk in sterke mate afhankelijk van de door de netwerkdienst gekozen organisatie en technische impletatie. De onderstaande vragen kunnen worden benut bij een beoordeling hiervan.

Continuïteitsaspecten:
- Welke alternatieve paden zijn binnen het netwerk voorhanden?
- Worden bij inschakeling van een alternatief pad de bestaande Calls onderbroken?
- Welke garanties geeft de leverancier ten aanzien van de up-time van het netwerk?
- Wat zijn de actuele cijfers c.q. de bewezen resultaten ten aanzien van de gerealiseerde up-time?
- Denk erom dat alle logische kanalen van een zelfde netwerkaansluiting via dezelfde vaste verbinding lopen. Bij uitval van deze verbinding met verscheidene logische kanalen kan geen enkel logisch kanaal meer worden benut. Een SVC als backup voor een PVC zal dan niet functioneren! Uit continuïteitsoogpunt kan men besluiten meer dan één aansluiting aan te vragen. Welke garanties geeft de leverancier dan ten aanzien van de routering van de fysieke verbinding? (Twee kabels die vlak langs elkaar lopen zullen bij graafwerkzaamheden beide kunnen uitvallen; indien beide aansluitingen op dezelfde PDS zijn aangesloten, leidt uitval van deze PDS tot uitval van beide lijnen, etc.)

Betrouwbaarheidsaspecten:
- Welke foutdetectie en -correctieprocedures worden in het (interne) netwerkprotocol toegepast? Wat is de kans dat een wijziging in een verstuurd pakket niet door het protocol wordt opgemerkt?
- Welke garanties geeft de netwerkleverancier ten aanzien van de integriteit van de verzonden berichten?
- Ondersteunt het netwerk de mogelijkheid van end-to-end-controle?
- Welke maatregelen zijn getroffen ter controle op de identiteit van de gebruiker c.q. aansluiting (bijvoorbeeld test op combinatie Calling DTE-adres ↔ fysieke lijn)?
- Zijn bovenstaande maatregelen niet door gebruikers te beïnvloeden? (De maatregel dient bijvoorbeeld niet te worden vastgelegd in apparatuur die bij klant staat opgesteld!)
- Voor welke typen aansluitingen wordt de NUI-faciliteit ondersteund? Op welke wijze handelt het netwerk een Call Request af indien een verkeerde identificatie wordt meegegeven?
- Welke doorschakelmogelijkheden zijn in het netwerk aanwezig? Wordt de Calling DTE op de hoogte gebracht van het feit dat de door hem verstuurde pakketten worden doorgeschakeld naar een ander adres dan de Called DTE?
- Welke procedures worden door de leverancier gevolgd ten aanzien van Besloten Gebruikers Groepen? Hoe wordt gehandeld indien conflictsituaties ontstaan ten aanzien van de aangevraagde faciliteiten voor aansluitingen die in meer dan één BGG moeten worden opgenomen?
- Geeft de netwerkleverancier security statements ten aanzien van de betrouwbaarheid van het berichtenverkeer? Worden periodiek Third Party Reviews gehouden?

b. Inventarisatie te onderzoeken lijnen

- Maak een plan om een volledig overzicht te verkrijgen van de gebruikte datacommunicatielijnen. Mogelijk te hanteren bronnen zijn:
  - beheerders van computercentra;
  - technische diensten;
  - datacommunicatiefacturen van afdeling financiële zaken;
  - beheerders van de Besloten Gebruikers Groepen;
  - definities in de netwerksoftware (bijvoorbeeld VTAM/NCP-definities in geval van IBM-componenten);
  - de leverancier van de netwerkdienst zelf.
- Stel vast welk gebruik wordt gemaakt van de lijnen (bijvoorbeeld ten behoeve van openbare diensten of juist alleen voor bedrijfsinterne communicatie).
- Stel vast welke lijnen in de audit worden betrokken (bijvoorbeeld alle lijnen met uitsluiting van de lijnen ten behoeve van openbare diensten).

c. Inventarisatie BGG's

- Ga na wie beheerder is van de verschillende

lijnen en BGG's (welk organisatie-onderdeel, welke functie, interne/externe medewerker).
- Vraag een (technisch) overzicht van de lijnen (soort aansluiting, capaciteit, aantal logische kanalen, faciliteiten per nummer en per kanaal).
- Vraag een overzicht van de gebruikte BGG's en de daarin opgenomen nummers (inclusief de geldende faciliteiten). Vergelijk dit overzicht eventueel met bij de netwerkleverancier opgevraagde gegevens.
- Vraag van eventueel 'zelf gecreëerde BGG's' welke maatregelen van interne controle en beveiliging zijn getroffen (bijvoorbeeld ten aanzien van definiëring, implementatie, het voorzien in een controle op een audit trail).

d. Beoordeling in opzet getroffen beveiligingsmaatregelen tijdens de Call Setup-fase

- Zijn blokkeringen voor ingaand/uitgaand verkeer aangebracht op kanaalniveau of aansluitnummerniveau?
- Zijn PAD- of X.32-aansluitingen opgenomen in BGG's? In geval van X.32-aansluitingen: worden verzoeken tot Reverse Charging niet geaccepteerd?
- Zijn in de BGG's nummers opgenomen met toegang buiten de BGG? Wat is hiervan de reden?
- Welke aanvullende beveiligingsmaatregelen zijn getroffen bij gebruik van PVC's?

e. Beoordeling juiste werking beveiligingsmaatregelen tijdens Call Setup-fase

- Leg de te onderzoeken aansluitnummers vast in een bestand.
- Start een programma dat achtereenvolgens een Call Request verstuurt met als Called DTE-adres het te onderzoeken nummer. Het programma dient de respons van het netwerk c.q. de Called DTE vast te leggen in een loggingsbestand.
- Onderzoek het loggingsbestand op nummers waarvoor netwerktechnisch geen/wel beveiligingsmaatregelen zijn getroffen tegen inkiezen en stel vast of dit in overeenstemming is met de in opzet getroffen beveiligingsmaatregelen.

CONCLUSIE

Voor digitale kieslijnen (bijvoorbeeld X.25 of ISDN) is een aantal standaardbeveiligingsfaciliteiten gedefinieerd. Het geboden beveiligingsniveau is echter in sterke mate afhankelijk van de door de netwerkdienst gekozen organisatorische en technische implementatie. Zo kan de netwerkdienst elementen uit de standaarden niet of slechts ten dele implementeren. In deze standaarden zijn bovendien niet alle uit beveiligingsoogpunt essentiële controlemaatregelen beschreven. Controle door de netwerkdienst op de juistheid van het in het Call Request-pakket opgenomen Calling DTE-adres is een basisvoorwaarde voor een te beveiligen X.25-netwerk. Deze controle is echter niet in Recommendation X.25 voorgeschreven. Bovendien zijn in de standaarden alleen technische aspecten opgenomen, organisatorische aspecten worden niet behandeld. Toch zijn ook deze aspecten van wezenlijk belang, bijvoorbeeld bij het opnemen van een aansluiting in meer dan één Besloten Gebruikers Groep.

Gesteld kan dus worden dat men voor de betrouwbaarheid en continuïteit van het berichtenverkeer in eerste instantie in sterke mate afhankelijk is van de netwerkdienst. Voor Datanet-1 is een groot aantal maatregelen getroffen om de betrouwbaarheid en continuïteit te waarborgen. Zo wordt voorzien in essentiële maatregelen als controle op de combinatie Calling DTE/fysieke lijn en controle op consistentie met eerder verstrekte BGG-faciliteiten bij aanvragen tot opname in andere BGG's. Ook ter waarborging van de continuïteit van het berichtenverkeer zijn verscheidene maatregelen getroffen. Men dient er echter alert op te zijn dat de verbinding tussen de abonnee en het entry-point van Datanet-1 bestaat uit een vaste verbinding die relatief gemakkelijk is af te tappen (analoog signaal, relatief lage transmissiesnelheid en alle pakketten in juiste volgorde). Uit beveiligingsoogpunt is het tevens een minder gelukkige keuze dat een verzoek tot het opbouwen van een Virtual Call door een X.32-aansluiting ook bij onjuiste identificatiegegevens wordt doorgestuurd (dan echter met het verzoek tot Reverse Charging).

Voor het uitvoeren van een audit van digitale kieslijnen is een grote mate van materiedeskundigheid noodzakelijk. Zo mag bij gebruik van PVC's of BGG's niet meteen worden aangenomen dat de beslotenheid van de datacommunicatie op adequate wijze is geregeld. Dergelijke constateringen zullen eerder aanleiding geven tot een meer gedetailleerd onderzoek naar de specificaties van de afzonderlijke aansluitingen en daarbinnen van de afzonderlijke logische kanalen.

Tot slot mag niet onvermeld blijven dat nieuw geïntroduceerde mogelijkheden uit beveiligingsoogpunt ook nieuwe risico's met zich mee kunnen brengen. De voor Datanet-1 geïntroduceerde X.32-aansluitmogelijkheid is hiervan een recent voorbeeld. In de toekomst kunnen ten aanzien van deze invalshoek nog gaan meespelen de reeds in Recommendation X.25 gedefinieerde maar nog niet in Datanet-1 geïmplementeerde doorschakel-

mogelijkheden (Call Redirection en Call Deflection). Voor EDP-auditors is het daarom een noodzaak om op de hoogte te blijven van de nieuwste ontwikkelingen.

LITERATUUR

[Brou92] D. Brouwer, *Beveiliging van analoge en digitale kieslijnen*, 1992.

[CCIT88] *Data communication Networks: Services and Facilities, interfaces, Recommendations X1-X32, CCITT*, Volume VIII, Fascicle VIII.2, 1988.

[Davi89] D.W. Davies en W.L. Price, *Security for computer networks*, 1989.

[Heij86] P.C. den Heijer en R. Tolsma, *Datacommunicatie*, 1986.

[NGI89] *Beveiliging bij datacommunicatie*, NGI rapport, 1989.

[PTT91] *Wide Area Networks en Datanet 1*, PTT Telecom, Samsom BedrijfsInformatie, Alphen aan den Rijn 1991.

Drs.ing. D. Brouwer Heeft in Rotterdam de studies HTS-Elektrotechniek en Bedrijfseconomie doorlopen. Na enige jaren te hebben gewerkt in het bedrijfsleven als datacommunicatie- en systeemspecialist is hij sinds 1988 als EDP-auditor werkzaam in het bankwezen.

Secure Cash Management; an audit perspective

M. Kennett BA

In November 1992 Cargill BV went live with a leading edge Financial EDI (FEDI) application. Matthew Kennett of Cargill's Internal Audit Department was closely involved in ensuring adequate security was built into the application.
In this article he describes the audit process used by Cargill during the application development and comments on the lessons for other companies undertaking this kind of audit review.

FOREWORD

Companies all over Europe are developing systems to take them towards the 21st century. As part of this effort they are making increasing use of advanced technologies including Electronic Data Interchange (EDI). A recent article in the Journal of European Business talked of, *'EDI ... changing dramatically the way a company works internally and with other companies'*. [JOEB92] However with the opportunities brought by such technologies comes a major threat to the security of the company employing them. This security threat comes from many directions and has to be addressed in the design, development and implementation of systems. The security of their systems is the responsibility of the senior managers in a company and one weapon in their armoury is often the use of an Internal Audit Department.

This article discusses the use of Internal Audit to review the security of an EDI payment application developed by Cargill BV for use in locations across Europe.

INTRODUCTION

The audit review described in this article was carried out by the Internal Audit Department of Cargill.

Cargill

Cargill is a diversified, multinational company specialising in commodity trading, food ingredient processing and financial markets. Founded in 1865, the company is headquartered in Minneapolis, Minnesota, USA and employs more than 63,000 people in 56 countries.

Cargill's business activities are grouped into five sectors: agriculture, food processing, industrial, meat and trading. More than 40 distinct product groups operate from 800 plants and offices. Worldwide turnover is approximately $ 50 billion annually. Cargill has been active in Europe since 1955 and employs more than 8,000 people in the Western and Eastern Europe and the former Soviet Union.

Cargill Internal Audit

Cargill operates an internal audit staff of 100 serving four major geographies; North America, South America, Pacific Rim and Europe. Each geography is responsible to the International Audit Director, based in the corporate headquarters in Minneapolis, USA.

Cargill's European, CIS (Common wealth of Independent States) and African operations are audited by a staff based in Cobham, UK. The Cobham staff are responsible for the audits of almost 100 different operations/systems.

The internal audit department has four major functions within Cargill;
- Financial Audits;
- I/S Data Facility Audits;
- System Development Reviews;
- Special Projects (Acquisitions, etc.).

The audit process is driven by the relative risks involved in each operation with a risk model being used to determine which operations will be reviewed and the scope of each review.

Corporate auditors with a wide range of business and financial skills perform the majority of the work with a team of I/S specialists, based in Minneapolis, performing the data facility audits.

PROJECT SCOPE

In 1991 Cargill assembled a team from its Swiss and Dutch operations to develop a Cash Management System (CMS). The system was needed to meet the common requirements of Cargill's major European treasury departments. The system was developed principally from the Amsterdam office which is home to the processing, trading and administrative operations of Cargill BV.

CMS was designed to allow for the central processing of payments and receipts that were entered at decentralised or remote locations. The fundamental principle was that remote locations, such as a processing plant, would have full control of their business whilst the central treasury location had full control of all funds.

CMS is an IBM AS/400 based system written using the Synon/2 development language. CMS was developed as four separate subsystems (Standing Data, Cash Management, Settlements and Forex) which could be installed independently or together. Interfaces to accounts payable/receivable and general ledger systems were also planned.
One of the key features of CMS is an automated payment process. This allows for on-line payment request approval followed by an EDI transmission direct to the payment system of the paying bank. This requires the payment request to be entered only once, at the location (either central or remote) requesting the payment.

The implementation of on-line payment approval and the development of a Cargill/Bank EDI link presented several significant security risks.

The implementation of on-line payment approval and the development of a Cargill/Bank EDI link presented several significant security risks (outlined later). Cargill invited several firms of I/T consultants to propose solutions to these risks. The solution proposed by KPMG Klynveld Management Consultants (KPMG), as described by H. Roos and H. Veenman in Compact 92/4, was accepted and KPMG were commissioned to develop the software required for a secured CMS system (SECCMS).

INTERNAL AUDIT REVIEW

The latest Institute of Internal Auditors' report on Systems Auditability and Control (SAC), based on a survey of 400 major organisations worldwide, found; *'Systems that are developed in a structured and organised manner, with controls built into the design, are the systems that most effectively and efficiently support the objectives of the organisation'*. SAC went on to emphasise that *'The Internal Auditor should assess the adequacy of the Electronic Funds Transfer systems' data security and access control features ...'* [SAC91].

The CMS management team were conscious of the

need for an independent review of the proposed system development and requested an early involvement of Cargill's Internal Audit Department.
The Cargill Internal Audit Department became involved in the development of the CMS at its very earliest stages in March 1991. Initial reviews were conducted by an I/S auditor from the US and concentrated on the following objectives:

a. system designed with controls that ensure:
   - accuracy and integrity of data;
   - reliability of system;
   - security against unauthorised access;

b. standard system development lifecycle is followed;

c. development adequately planned and managed;

d. system meets actual user requirements.

At this stage several suggestions were made for controls that could be built into the system during the development lifecycle.

The review described in this article is the specific review of the secured payment function (SECCMS)[1] as developed by KPMG in conjunction with Cargill's CMS team. This review was to cover the key security risks within the CMS system and was centred around the need to prevent misappropriation of funds.
The analysis of SECCMS began in November 1991 with a high level review by the European Internal Audit Manager. This review of the major risks was the basis for developing our SECCMS audit plan. This audit plan was executed between May 1992 and December 1992.

Objectives of SECCMS Review

The overall objective of our review was to ensure SECCMS provided adequate security to protect Cargill from risks arising from the on-line approval and electronic processing of payments.

A 1990 UK Audit Commission survey revealed internal control procedures were only responsible for the detection of 23 percent of computer aided fraud reported, with the majority uncovered by chance [MACS92]. Our aim was to ensure the security within SECCMS was sufficient to prevent all computer aided fraud attempts as well as eliminating costly errors, such as accidental duplicate payments.

Methodology

SECCMS is a technically complex application involving techniques being used for the first time within the Cargill corporation. One of the keys to our review was gaining an understanding of the techniques used that was sufficient to appraise their implications for the overall system security. This is emphasised in the SAC review which says, *'the auditors' greatest challenge is maintaining a full understanding of the latest advances in the technology platform that supports an application'* [SAC91].

Our initial approach to understanding the SECCMS technology was to thoroughly review the system documentation provided by KPMG and the Cargill development team. Time was also spent interviewing the key team members to supplement what was learnt from the documentation. Once a sufficient technical knowledge was acquired the following methods were used during the review:

a Design Stage Review
We reviewed the security implications of all proposals at the pre programming stage. Figure 1 emphasises the increasing costs of making changes as system development progresses. We played a proactive role in developing system security rather than conducting an after the fact review.

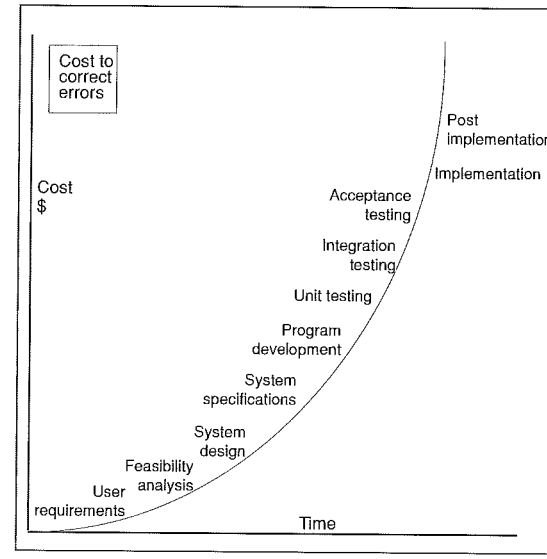


Figure 1. Relative cost to correct errors. Phases of system development life cycle.

b System Testing
We considered it important to examine the security features in a test environment. Even though the emphasis was on ensuring that security features were included in the SECCMS design we also carried out an extensive planned test programme. The purpose of the tests was to ensure the security features worked as planned. The 'hands-on' stage of the review was critical to giving the go ahead to live implementation of the system.

c Operating Procedure Design
Development of secure operating procedures was one of the major roles played by the audit department. The security of the system is dependent upon the procedures used to operate it. In some areas such as the management of cryptographic keys failure to set adequate procedures could completely compromise system security.

1 *In order to maintain the security of SECCMS some aspects of the system security are not discussed in detail or are intentionally omitted.*

We worked with the CMS team to identify areas requiring operating procedures. These areas were then prioritised and procedures were developed in conjunction with the user coordinators. Implementation of the key procedures was a condition to going live with the system.

d Post Implementation Review
One month after the system went live we carried out a review of all areas of SECCMS security including operational procedures. This was important as a control that the proposed security and procedures had actually been implemented in the live environment.

KEY SECURITY CONCERNS

There were several areas of the system that gave rise to significant security concerns. The major risk areas are shown in figure 2.

Payment stage	Risk
Entered by requester onto AS/400	– None
Final approval against supporting documents	– Approval given by an unauthorised person – Unauthorised change to payments details after approval
Treasury acceptance	– Accepting an approved payment that has been changed – Treasury function performed by an unauthorised person
Treasury sent to bank	– Sending a payment instruction that has not been approved
Received by bank	– Receipt of a payment instruction not sent by Cargill – Receipt of a payment instruction changed without authorisation
Confirmed	– Same payment instruction resent to bank

Figure 2. Major risk areas.

The critical risks within SECCMS were:

Alteration of Locally Approved Payments
The risk of an approved payment request being modified, without authorisation, before transfer from the remote to the central AS/400.

Identity of User Logging on to Workstation
The risk that without positive user identification you cannot be sure only authorised persons access the payment system.

AS/400 Security Officer Authority
The risk of the security officer having authority to change approved payments within the AS/400.

Transfer of Payment Instructions to Bank
The risks were interception and alteration of payment instructions, insertion of false payment instructions or sending a payment instruction twice.

SOLUTION ADOPTED

The KPMG security solution (SECCMS) involves the use of a secure PC workstation for approval and treasury functions. The PC is secured by the use of IBM Transaction Security System (TSS) hardware and software.

TSS hardware

TSS, as implemented by Cargill, consists of the following TSS hardware:

Personal Security Card (PSC)
A small plastic card with an embedded microchip. The card holds profile and configuration data containing the security options and SECCMS menus available to the user. Digital recordings of the user's signature are also held on the PSC for use in the user identification process required at the start of a secure session and immediately before performing some critical functions.

Security Interface Unit (SIU)
A card reader that transmits information from the PSC to the secure workstation. An electronic pen is attached to the SIU to compare the user's signature to the signature stored on the PSC.

Cryptographic Adaptor (CA)
This device is installed in the workstation and provides the cryptographic functions necessary to generate and verify a Message Authentication Code (MAC).

The need for MACs

The TSS hardware and software is used to calculate cryptographic codes (MAC) over the payment. The MAC is used as a way of detecting any unauthorised changes made to the payment request between the application of final approval and receipt of payment request by the bank. The application of final approval is a critical moment as it is the last time the payment request details on the AS/400

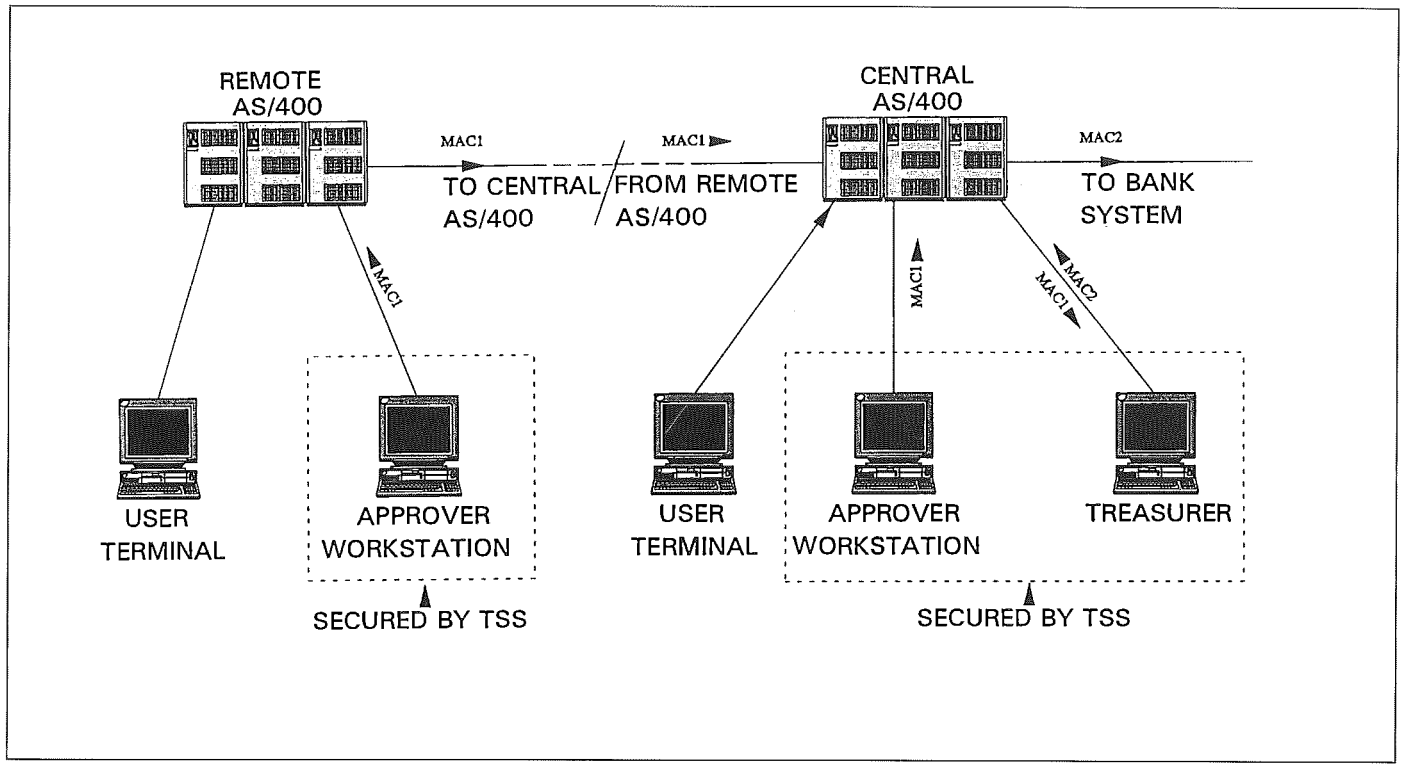


Figure 3. Secured workstation environment.

are vouched to the supporting documents (invoice, goods receipt note, etc.).
The MAC uses details from all critical fields of the payment and will fail if any of these fields are changed in any way. The first code (MAC1) is computed during final approval. The second code (MAC2) is computed when treasury releases the payment to the bank. Any change in the payment between approval and release (MAC1) and release and bank (MAC2) will be detected and the payment will automatically be stopped.

MAC generation

MACs are generated basis keys stored on the PSC of the user. The MAC1 keys (one per approver) are generated internally by Cargill. The MAC2 keys (one per bank) are generated by the banks. One of the critical areas of our review was to ensure adequate procedures are in place to safeguard the confidentiality of the keys. This will be a key concern of audit departments of all organisations, *'The control and review of key management will undoubtedly become of great importance to the organisation's auditors...'* [CFSB92].

Payment flagtable

Whilst the above solution guarded against an unauthorised change to a payment instruction it did not provide protection against the double transmission of a valid payment interchange to the bank. This could occur accidentally, for example during recovery from a system failure. The solution to this problem lay in validating, on the basis of a unique transaction identifier, all payments against a table of payments already sent to the banks. If the payment is validated it is itself added to the table before being sent to the bank. The table is also secured by a MAC.

Audit role in the solution

The role of the Internal Audit function was not in designing the above solutions but in giving an independent opinion as to whether the proposed solutions adequately addressed the risks.

AUDIT FINDINGS

The continual involvement of the audit department in designing and implementing the system security meant that the post implementation review of system security went very smoothly.

Whilst some recommendations were made to management they were all aimed at further enhancing SECCMS security as no significant security weaknesses were identified.

The key areas identified for improvement involved making maximum use of the security facilities offered by TSS, in particular:

a. Restricting use of PSCs (and thereby access to all secured payment functions) to normal working hours/days. This is a function of the profile data loaded on the PSC at initialisation.

b. Utilising the TSS authorised command structure to ensure users are only authorised to commands appropriate to their task. In particular the I/S staff who support the system require some authorised commands that are inappropriate for a treasurer.

FUTURE AUDIT INVOLVEMENT

With the system development completed and the installation programme beginning, the management of the project is entering a new phase. This also means the Internal Audit Department will have to use new techniques to meet its objective for SECCMS.

If we reconsider the original objective of this review; *'to ensure SECCMS provided adequate security to protect Cargill from risks arising from the on-line approval and electronic processing of payments'* we see that it is a long term objective. It is the duty of Cargill's senior management to ensure a high level of security is maintained as SECCMS is installed in other locations.

The key to maintaining future security is producing a set of procedures to be followed when implementing and operating the system in any location. This procedures manual is currently developed and will be completed before the next install of the SECCMS.

Internal Audit will use two main techniques to ensure it is satisfied with the system security:

a. Review the installation and operating procedures developed by the project managers.

b. Conduct field reviews in all offices operating SECCMS. We are developing a standard audit programme to ensure consistency in these reviews.

LESSONS LEARNT

We have learnt many lessons from our review of SECCMS, several of which are applicable to any organisation conducting a similar review:

Start review pre-development

It is essential to be involved from the start for two main reasons:

a. You need time to build your knowledge of the technical concepts involved.

b. It is far more cost effective to build security into the design than to try and impose security onto the system after it has been developed.
The Computer Fraud & Security Bulletin emphasised this saying, *'the management and introduction of new security procedures will benefit greatly from the auditors having been involved from the start'* [CFSB92].

It is far more cost effective to build security into the design than to try and impose security onto the system after it has been developed.

Understand technical concepts

The security of SECCMS relies on techniques, like cryptographic keys, that will not be familiar to most financial/systems auditors. This makes it important that at least one person involved in the system understands these functions to a level where they can effectively appraise their contribution to system security.

Emphasise procedures

The security of a system like SECCMS hinges on the operational procedures implemented around the system. You need to ensure the proposed procedures will provide adequate security and that they are implemented fully when the system goes live. *'A lack of formal procedures specifically designed to combat computer fraud appears to leave many organisations relatively unprepared and unprotected'* [INAD91].

Stay involved

The security of a system is not ensured at the development stage. It depends on how the system is operated after it goes live. The Internal Audit Department has a duty to ensure system security is maintained.

M. Kennett BA
Studied for a BA(Hons) degree in "European Finance and Accountancy" at Leeds Polytechnic and graduated in 1989. One year of the course was spent studying at the Hochschule in Bremen for a Diplom Betriebswirt (Business Management Degree).
Started work for Cargill in September 1989 as an assistant auditor, he has been working as a senior auditor since January 1992.
Main role is as a financial auditor. Specialities are in audit department automation (computerised testing tools) and system development reviews.

LITERATURE

[CFSB92] *Computer Fraud and Security Bulletin*, Elsevier Science Publishers Ltd, England, September 1992.

[INAD91] *Internal Auditor - Emerging Technologies*, Institute of Internal Auditors, Florida, August 1991.

[JOEB92] *Journal of European Business*, Faulkner & Gray Inc., New York, Vol.4, No.2: November/December 1992.

[MACJ92] *Management Accounting*, Chartered Institute of Management Accounting, London, Vol.70, No.7: July/August 1992.

[MACS92] *Management Accounting*, Chartered Institute of Management Accounting, London, Vol.70, No.8: September 1992.

[SAC91] *Systems Auditability and Control Report*, Institute of Internal Auditors Research Foundation, Florida, 1991.

[TSS90] *Transaction Security System Programming Guide and Reference*, International Business Machines Corporation, 1990.

Nieuwe ontwikkelingen in de cryptografie: Kerberos en Digital Signature Standard

Drs. T.P. de Vries

Diefstal van informatie is moeilijk te voorkomen. Het gebrek aan bescherming neemt toe met het aan elkaar koppelen van netwerken. De enige oplossing is uiteindelijk encryptie. In dit artikel nieuwe ontwikkelingen: Kerberos en DSS.

INLEIDING

Cryptografie wordt gezien als de enige efficiënte en effectieve manier om de berichten op communicatieverbindingen te beveiligen. Verwacht wordt dat binnen vijf jaar alle grote software-programma's inclusief PC-besturingssystemen encryptiefaciliteiten zullen bevatten.
De grote gebruikers zullen steeds meer de behoefte voelen om hun kostbare gegevens te beschermen tegen modificatie en aftappen. Bij gebrek aan de geïntegreerde mogelijkheid van encryptie zullen zij dan ook twijfelen om programmatuur aan te schaffen.

Behalve het zorg dragen voor de vertrouwelijkheid van privacy-gevoelige informatie kan met cryptografie ook worden vastgesteld of de authenticiteit van de afzender niet is vervalst en of de integriteit van de inhoud sinds verzending is gehandhaafd.
Encryptie biedt tevens een beschermingsmogelijkheid tegen virussen door programmatuur te voorzien van een digitale handtekening. Dit stelt de gebruiker in staat elke keer als de software wordt gebruikt de integriteit ervan te laten vaststellen.

In de toepassing van informatietechnologie doet zich een verplaatsing voor in het gebruik van stand-alone-systemen naar multi-vendor-systemen die op zich gebruik maken van steeds krachtiger netwerken.
De problemen die optreden bij het bouwen van gedistribueerde applicaties voor dergelijke netwerken zijn onder meer:

- er bestaan geen alles omvattende technieken of standaarden voor gedistribueerde systemen;
- de deeloplossingen die worden geboden door de verschillende leveranciers kunnen niet samenwerken met de oplossingen van andere leveranciers of platforms;
- het niet optimaal gebruik maken van de beschikbare middelen als disks, processors en printers die over de gehele organisatie verspreid staan opgesteld.

Om deze problemen op te lossen verscheen de Open Software Foundation (OSF) met zijn Distributed Computing Environment (DCE). In juni 1989 vroeg OSF aan de verschillende leveranciers of zij technieken beschikbaar wilden stellen om in het DCE te worden opgenomen.
De voor OSF Distributed Computing Environment gekozen authenticatietechniek berust op het door het Massachusetts Institute of Technology (MIT) ontwikkelde Kerberos-schema. In de volgende paragraaf wordt nader op Kerberos ingegaan.

Het commercieel toepassen van cryptografie wordt echter tegengewerkt door overheidsbeperkingen.
De rol die de overheden hierin spelen (met name de Amerikaanse overheid) wordt belicht in de paragraaf 'Encryptie-algoritmen'. Daarin wordt tevens ingegaan op het door het U.S. National Security Agency (NSA) ontwikkelde public key-algoritme voor digitale handtekeningen, de Digital Signature Standard (DSS).

KERBEROS

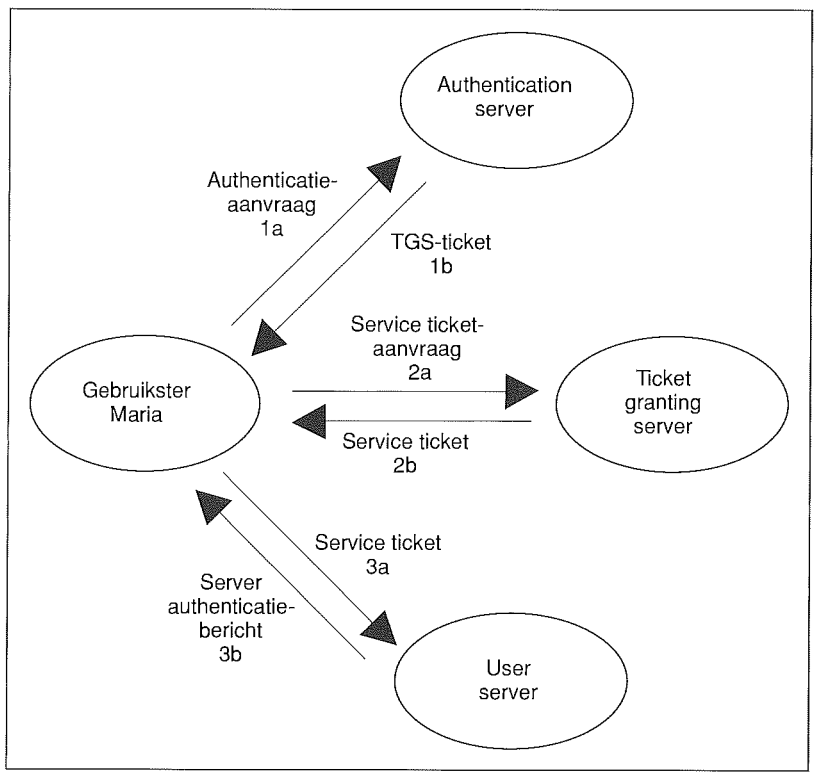
Cerberus is de driekoppige hond die in de Griekse mythologie de toegang tot de onderwereld Hades bewaakt. Niemand is in staat hem te passeren zonder zijn goedkeuring.
De moderne Kerberos [Kerb88] beschermt de toegang tot de gegevens op remote computersystemen. Of deze Kerberos te passeren zal zijn moet nog blijken. Het zal mede afhangen van de sterkte van zijn implementatie.

Het protocol

In een open omgeving hebben wij te maken met indringers die zich als andere personen proberen voor te doen, met namaakservices en met de mogelijkheid om datacommunicatieverbindingen af te tappen.
Het gebrek aan fysieke controle over werkstations en netwerkaansluitingen in een grote open omgeving maakt positieve identificatie van gebruikers, werkstations en netwerkservers noodzakelijk.

Kerberos voorziet in de mogelijkheid van wederzijdse authenticatie van gebruikers en services in een omgeving waar netwerkaansluitingen en werkstations niet kunnen worden vertrouwd. Het schept mogelijkheden om de identiteit van gebruikers en services vast te stellen met behulp van een te vertrouwen derde partij.
Het Kerberos-mechanisme berust op het principe gegevens te vercijferen en te ontcijferen met een unieke sleutel die gemeenschappelijk is tussen de derde partij en de te identificeren gebruiker, bestanden, programmatuur of andere objecten.
De berichten worden vercijferd zodat wijzigen of aftappen wordt opgemerkt of onleesbare gegevens oplevert. De sessiesleutel voor het vercijferen wordt gedistribueerd door middel van het wederzijdse authenticatiemechanisme dat eraan voorafgaat.
De encryptie in Kerberos is gebaseerd op DES. Een aantal encryptiemethoden wordt ondersteund. Het gebruikte algoritme kan desgewenst worden vervangen door een ander.

Figuur 1. Basisfuncties Kerberos.



Om te voorkomen dat een gebruiker zich elke keer als hij gebruik wil maken van een geboden service moet identificeren, wordt er naast een Authentication server gebruik gemaakt van een Ticket granting server (TGS). De TGS verzorgt de toegang tot de verschillende servers.

Het Kerberos-authenticatiemechanisme bestaat uit drie stappen. De werking wordt geïllustreerd aan de hand van de aanvraag van gebruikster Maria om van een bepaalde service gebruik te maken.

In de eerste stap wordt Maria's identiteit geverifieerd met behulp van de Authentication server en wordt zij voorzien van een ticket dat haar in staat stelt de Ticket granting server te benaderen en deze te vragen om toegang tot bepaalde services. Het ticket is slechts bruikbaar gedurende een beperkte tijdsduur.

In de tweede stap krijgt Maria van de Ticket granting server een service ticket voor de verlangde user service.

In de derde stap wordt het service ticket naar de verlangde User server gezonden. Deze maakt de services voor Maria beschikbaar nadat de authenticiteit van Maria is geverifieerd en Maria op haar beurt de authenticiteit van de server heeft vastgesteld.

Hieronder volgt een nadere uitwerking van dit protocol.

Gebruikersauthenticatie
1a Authenticatie-aanvraag
Om haar TGS-ticket te krijgen zendt Maria een verzoek om toegang tot de Ticket granting server (met identificatie tgs) te zamen met haar identificatie (IDm) naar de Authentication server.

1b TGS-ticket
Als antwoord krijgt zij het TGS-ticket encrypt met haar password (PWm) terug.
Op deze wijze kan het antwoord worden gezien als een envelop die alleen kan worden geopend door degene die in het bezit is van het correcte password.
Merk op dat het password niet over het netwerk wordt getransporteerd.

Het TGS-ticket bestaat uit twee delen.
Het eerste deel kan door Maria worden gelezen; het bevat de sessiesleutel (KSt) die gebruikt gaat

worden voor de communicatie tussen Maria en de Ticket granting server.
Het tweede deel kan alleen de Ticket granting server lezen. Dit deel is vercijferd met de sleutel van de Ticket granting server (Ktgs) en bestaat uit de identificatie van de Ticket granting server (tgs), de identificatie van Maria (IDm), het werkstationadres (address), een tijdstempel (time), de geldigheidsduur van het ticket (limit) en de sessiesleutel tussen Maria en de Ticket granting server (KSmt).

Autorisatie aanvraag voor service
2a Service ticket-aanvraag
Maria zendt een aanvraag met de naam van de verlangde service (us), het voor haar niet-leesbare deel van het TGS-ticket en haar eigen envelop met een 'authenticator' naar de Ticket granting server.
De envelop bestaat uit de 'authenticator' encrypt met de van de Authentication server gekregen sessiesleutel (KSmt). De 'authenticator' bestaat uit Maria's identificatie (IDm), het werkstationadres en een tijdstempel.

2b Service ticket
De Ticket granting server ontcijfert het voor hem ontcijferbare deel van het ticket met zijn unieke sleutel Ktgs. De server komt hierdoor in het bezit van de sessiesleutel KSmt en kan hiermee de envelop openen door de 'authenticator' te ontcijferen.
Hierna worden de identiteit van Maria en de geldigheid van het tijdstempel geverifieerd.

De Ticket granting server stelt nu een Service ticket (ST) voor de aangevraagde User server (us) samen. De opbouw is gelijk aan die van het TGS-ticket. Met dit verschil dat nu gebruik wordt gemaakt van de sleutel van de verlangde server (Kus) voor het vercijferen van de identificatie van deze server, de identificatie van Maria (IDm), het werkstationadres (address), een tijdstempel (time), de geldigheidsduur van het ticket (limit) en de sessiesleutel tussen Maria en de verlangde User server (KSmu).

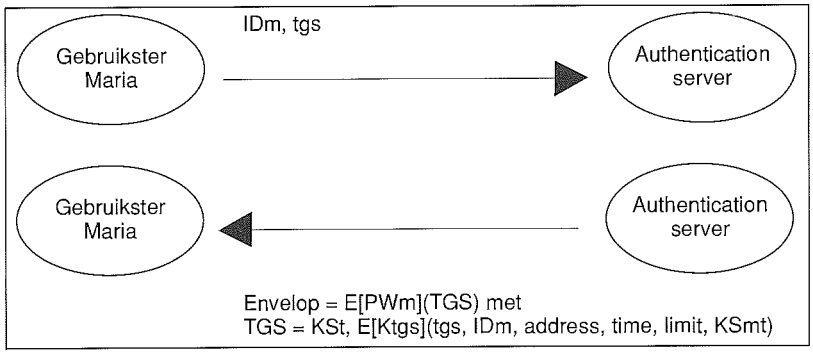
De Service ticket (ST) wordt vercijferd met de sessiesleutel (KSmt) naar Maria gezonden.
Op deze wijze kan het antwoord worden gezien als een envelop die alleen kan worden geopend door degene die in het bezit is van de correcte sessiesleutel, in dit geval Maria.

Beschikbaar stellen verlangde service
3a Service ticket
Maria opent de envelop door het ontcijferen van het Service ticket met KSmt. Maria beschikt nu over de klare sessiesleutel (KSmu). Met de sessiesleutel stelt zij haar eigen envelop samen bestaande uit de vercijferde 'authenticator' De 'authenticator' bestaat uit: Maria's identificatie, het werkstationadres en een tijdstempel.

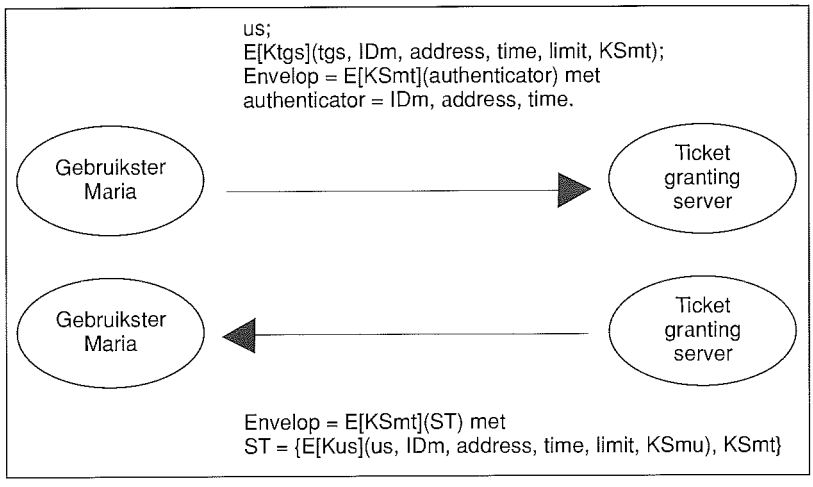
Het voor haar niet-leesbare deel van het Service ticket en de envelop, de vercijferde authenticator, worden door Maria naar de verlangde User server gezonden.

3b Server authenticatiebericht
De User server ontcijfert het voor hem leesbare deel met Kus en gebruikt de sessiesleutel (KSmu) om de envelop te openen, waarna de identiteit van Maria en de geldigheid van het tijdstempel worden geverifieerd.

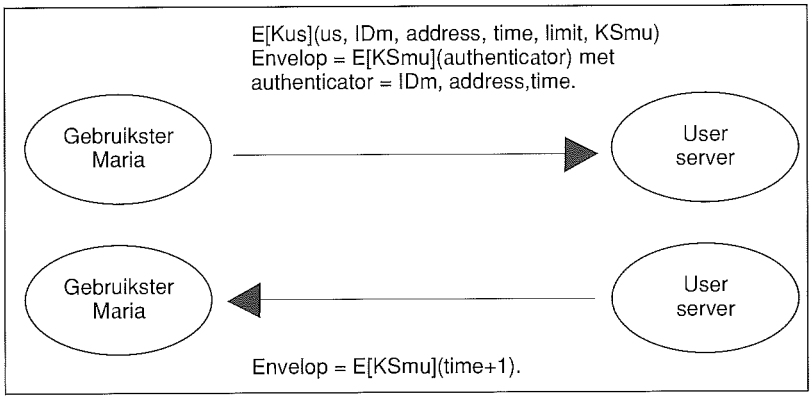
Maria wordt nu door de User server in staat gesteld diens authenticiteit vast te stellen door gebruik te maken van het tijdstempel. Hij verhoogt hiertoe de time stamp met 1 en vercijfert het resultaat met de sessiesleutel KSmu. Deze envelop zendt hij naar Maria.



Figuur 2. De gebruikersauthenticatie.



Figuur 3. Ticket granting server-activiteiten.



Figuur 4. Verzoek om een service.

Maria kan nu de authenticiteit van de server vaststellen, immers alleen de authentieke server is in staat de envelop met het Service ticket te openen, het tijdstempel correct aan te passen en deze in een door Maria te openen envelop aan Maria te zenden.

Zoals uit het bovenstaande blijkt, dient het hier beschreven Kerberos-protocol over een initieel key management voor de generatie en distributie van sleutels over het netwerk te beschikken. Dit is dan ook voorzien, te zamen met additionele faciliteiten voor de administratie van identificatiegegevens en encryptiesleutels.

De voordelen van Kerberos zijn:

- De gebruiker kan overal in het netwerk inloggen op een server mits hij/zij daartoe is geautoriseerd.

- Kerberos kan relatief eenvoudig worden geïmplementeerd op werkstations en PC's.

- Kerberos voorziet in zowel authenticatie als vercijfering. Dezelfde sessiesleutel die is gebruikt voor de gebruikersauthenticatie kan worden toegepast om het berichtenverkeer tussen de gebruiker en de server te vercijferen. Hierdoor is het voor een indringer onmogelijk op de verbinding in te breken tussen de gebruikersauthenticatie en de daadwerkelijke berichtvercijfering.

- Vercijfering kan selectief worden toegepast.

- Kerberos is openbaar zodat iedere fabrikant het kan toepassen in zijn produkten.

De problemen

Enige problemen in relatie tot het Kerberos-authenticatiemechanisme zijn:
- de geldigheidsduur van het ticket;
- het volmachtprobleem;
- de integriteit van de software op het werkstation.

De keuze van de geldigheidsduur van een ticket is een kwestie van een keuze tussen beveiligingsniveau en gebruiksvriendelijkheid.
Indien de geldigheidsduur te lang is kan resterende tijd worden misbruikt als een gebruiker bijvoorbeeld vergeet uit te loggen.
Als de geldigheidsduur kort is zal de gebruiker na het verlopen van de geldigheid opnieuw zijn password moeten invoeren.
Een niet opgelost probleem is hoe een server in staat kan worden gesteld gebruik te maken van andere netwerkservices, zonder daarbij de geauthenticeerde gebruiker dezelfde rechten te verlenen.
Een voorbeeld hiervan is de situatie waarbij een applicatie directe toegang behoeft tot beveiligde bestanden, die voor de gebruiker zelf niet direct benaderbaar dienen te zijn.

Op een vrij toegankelijk werkstation is het mogelijk het login-programma zodanig te wijzigen dat het een vastlegging van een ingevoerd password maakt. Het moet dus onmogelijk zijn de software die draait op het werkstation te modificeren.
Een mogelijke oplossing zou zijn om de Kerberosfuncties en de daarbij betrokken geheime gegevens uit te voeren respectievelijk op te slaan binnen een betrouwbare omgeving. Hiervoor kan bijvoorbeeld gebruik worden gemaakt van een smartcard.

Tevens zal moeten worden voorzien in een betrouwbare derde partij. Indien alle services, inclusief de authenticatie services, worden aangeboden door één en dezelfde organisatie is dit een relatief eenvoudig probleem. Als er meer partijen zijn betrokken die elkaar niet vertrouwen wordt dit probleem gecompliceerder.
De oplossing is een combinatie van afspraken, wettelijke regelingen, organisatorische en technische maatregelen, zoals procedures en key management.

ENCRYPTIE-ALGORITMEN

De introductie van een nieuw encryptie-algoritme voor digitale handtekeningen door het U.S. National Security Agency (NSA) en het U.S. National Institute of Standards and Technology (NIST) heeft de discussie rond het gebruik van encryptie, de import- en exportbeperkingen en de vermeende zwakte en 'trapdoors' in door NSA voorgestelde algoritmen weer doen oplaaien.
De discussie doet sterk denken aan de discussie die enige jaren terug rond DES is gevoerd.
In de volgende subparagrafen wordt ingegaan op DSS en DES. Een vergelijkend overzicht is weergegeven in tabel 1.

DSS

Voor de tweede keer heeft de U.S. Government zich bemoeid met een voorstel voor een encryptie-algoritme.
In 1970 betrof het een symmetrisch encryptie-algoritme, de nu algemeen geaccepteerde en voor commerciële toepassingen veelvuldig gebruikte Data Encryption Standard (DES) [DES], [DEA].
Ditmaal betreft het een public key-algoritme dat alleen geschikt is voor het genereren en verifiëren van een digitale handtekening. Voor het vercijferen van gegevens is het ongeschikt.

Deze Digital Signature Standard (DSS) is ontwikkeld door de NSA en is gebaseerd op de public key-techniek van discrete logaritmen, gepubliceerd door Taher ElGamal in 1985 [ElGam].
Het voorstel is vervolgens door het NIST geëvalueerd en eind 1991 voorgesteld als standaard.

Deze gang van zaken bevreemdde veel insiders. Tot eind 1990 werd het meest bekende public key-algoritme RSA (zo genoemd naar de beginletters van zijn ontwerpers Rivest, Shamir en Adleman) [RSA] nog aanbevolen door het NIST.
Dit heeft er onder meer toe geleid dat RSA reeds veelvuldig wordt toegepast in het bedrijfsleven. Leveranciers zoals IBM, Digital Equipment, Apple,

MicroSoft en Sun Microsystems hebben RSA reeds in hun produkten geïntegreerd.
De elektronische directories-standaard X.500, de standaard voor het Franse bankwezen Etebac-5 en de Australische digitale handtekeningstandaard (AS2805.6.5.3.) berusten bijvoorbeeld op RSA.
RSA is momenteel dan ook de defacto-standaard voor public key-algoritmen.

In tegenstelling tot nieuweling DSS zijn DES en RSA al meer dan twaalf jaar onderhevig geweest aan intensieve analytische kraakpogingen van internationaal vermaarde specialisten. Hierbij stonden hun alle benodigde hulpmiddelen ter beschikking. Desondanks is het tot op heden niet gelukt een structurele en commercieel haalbare aanval te vinden. Dit onderstreept de sterkte van DES en RSA.
De sterkte van DSS daarentegen moet nog worden bewezen. Het is dan ook de vraag of het bedrijfsleven verlegen zit om nog een standaard voor de digitale handtekening.

Hieronder volgt een korte beschrijving van DSS.

DSS is in staat een korte digitale handtekening te genereren over een checksum. Deze checksum moet, bijvoorbeeld met DES, worden berekend over de te tekenen gegevens. DSS voorziet niet in vercijfering van de gegevens. Hiervoor kan bijvoorbeeld DES worden gebruikt.
Een ander zwaar wegend nadeel van DSS is dat hij ongeschikt is voor elektronische sleuteldistributie aangezien hij ongeschikt is voor vercijfering.

DSS is in staat tot het snel genereren van een digitale handtekening. Het verifiëren is langzaam. Het NIST claimt voor zijn prototype smartcard dat deze een digitale handtekening kan genereren in 0.05 seconden, terwijl verificatie 30 seconden duurt.
Voor RSA op dezelfde kaart gelden respectievelijk 28 seconden en 2.5 seconden.

Volgens het NIST zal er over het algemeen meer behoefte bestaan aan het snel genereren van een digitale handtekening dan aan het snel verifiëren. De overweging hierachter is dat de verificatie over het algemeen wordt uitgevoerd door gespecialiseerde hardware gekoppeld aan een mainframe, waardoor voldoende processing-capaciteit aanwezig is. De generatie moet echter kunnen worden uitgevoerd door een smartcard of op een PC.
Deze bewering van het NIST is echter onterecht voor de meeste toepassingen. Zo zal bijvoorbeeld voor het zetten van een enkele handtekening vaak een serie van certificaten moeten worden geverifieerd om de public key te authenticeren. Voor virusdetectie bestaat behoefte aan een snelle verificatiemethode en is de snelheid van de generatie van ondergeschikt belang.

Nadat er door specialisten bezwaar was gemaakt tegen de in hun ogen te korte modulus van 512 bits, is de toegestane lengte door het NIST opgevoerd tot 1024 bits. Natuurlijk zal het opgevoerde beveiligingsniveau ten koste gaan van de snelheid van het algoritme.
Er wordt (onder meer door Claus P. Schnorr, Duitsland [Schno]) aanspraak gemaakt op patenten met betrekking tot de technieken gebruikt in DSS. Tot op heden is deze patentproblematiek echter nog niet opgelost.

Het is de vraag
of het bedrijfsleven zit te wachten
op een tweede standaard
voor de digitale handtekening.

IBM heeft de patentclaims op DES opgezegd. Dit in tegenstelling tot de RSA Data Security Inc., die RSA tot het jaar 2000 heeft gepatenteerd.

DES

Iedere vijf jaar moet de DES-validiteit als Federal Standard worden verlengd. De laatste verlenging in 1988 werd voorafgegaan door een poging van het NSA om de DES-validiteit niet te laten verlengen. In plaats daarvan probeerde NSA andere cryptografische algoritmen door de commerciële sector als standaard te laten aanvaarden.
De commerciële sector was sterk tegen, omdat:
- DES nog steeds veilig was voor de commerciële toepassingen en het niet nodig was deze te vervangen;
- de investeringen in DES-technologie te hoog zijn;
- de NSA-alternatieven niet hetzelfde beveiligingsniveau boden als DES.

In 1992 is gespeculeerd dat DES gebroken zou zijn. Een diepgaande analyse van de beschreven aanvallen maakt echter duidelijk dat deze meer theoretisch dan praktisch zijn.
Afgezien daarvan gaan de aanvallen uit van bepaalde veronderstellingen. Deze veronderstellingen kunnen in commerciële systemen niet eenvoudig worden bewerkstelligd.
In aanvulling hierop kan een frequentere wijziging van de sleutels de aanvallen voorkomen.

We moeten echter onder ogen zien dat de processingsnelheid van de toekomstige computersystemen de sterkte van DES en de huidige effectieve sleutellengte van 56 bits (inclusief paritybits 64 bits) zal achterhalen. Op termijn zal dan ook behoefte bestaan aan een nieuwe standaard. We moeten ervan uitgaan dat het circa tien jaar zal duren alvorens het vertrouwen in de nieuwe standaard hetzelfde niveau heeft bereikt als DES nu geniet en dat zo'n nieuw algoritme op grote schaal voor commerciële toepassingen wordt aanvaard.

Over de hele wereld nemen de commerciële investeringen in DES-beveiliging nog steeds toe. Het geboden beveiligingsniveau rechtvaardigt deze investeringen. Het ontwerp van het DES key management is over het algemeen zodanig dat DES

op zijn minst nog vijf jaar effectief kan worden toegepast. Dit jaar zal de DES-validiteit daarom voor nog eens vijf jaar worden verlengd.
De commerciële sector en de overheden moeten echter nu reeds gaan samenwerken in de ontwikkeling van een opvolger van DES. Deze kan dan in 1998 worden voorgedragen voor validiteit als standaard.
De inspanning voor de ontwikkelingen dient niet te worden gecontroleerd door het NSA of welke overheidsinstantie dan ook.

	DES	**RSA**	**DSS**
Oorsprong	IBM	Rivest Shamir Adleman	ElGamal
Techniek	permutaties en substituties	factorisatie grote getallen	discrete logaritme
Algoritme	symmetrisch	asymmetrisch	asymmetrisch
Sleutellengte	64 bits	n.v.t.	n.v.t.
Modulus lengte	n.v.t.	variabel tussen 512 en 1024 bits	variabel tussen 512 en 1024 bits
Status	gestandaardiseerd in 1977	gepatenteerd in 1978	voorgesteld als standaard
Functies			
Integriteit	ja	ja	ja
Authenticatie	ja	ja	ja
Vertrouwelijkheid	ja	ja	nee
Non-repudiation	nee	ja	ja
Snelheid			
Generatie	snel	langzaam	snel
Verificatie	snel	snel	langzaam
Geschikt voor key management	ja	ja	nee

Tabel 1. Vergelijking tussen DES, RSA en DSS.

Import- en exportbeperkingen

Indien de toepassing van cryptografie beperkt zou zijn tot digitale handtekeningen en het vercijferd uitwisselen van sleutels zouden de overheden niet zoveel beperkingen opleggen aan het gebruik van cryptografie. Maar omdat encryptie ook kan worden gebruikt voor het vercijferen van gegevens wordt het gebruik door de overheden beperkt om redenen van nationale veiligheid.

Het aanvragen van licenties voor het gebruik van cryptografie zal daarom over het algemeen niet tot problemen leiden indien de toepassing alleen voorziet in een authentication code, zoals de Message Authentication Code (MAC). In het geval dat gebruik wordt gemaakt van vercijfering zal alleen een licentie worden verstrekt aan financiële organisaties en aan bedrijven die hun zetel in de Verenigde Staten hebben.

De verspreiding van DSS met alleen de mogelijkheid van digitale handtekening zal niet of minder worden gefrustreerd door deze exportbeperkingen. DSS is er echter nog niet en bovendien heeft het bedrijfsleven meer en meer behoefte aan de mogelijkheid van vercijfering van zijn vertrouwelijke informatie. Bijvoorbeeld als deze bedrijfsspionage-gevoelige gegevens bevat.

Momenteel wordt een groot deel van de encryptieapparatuur gefabriceerd/geproduceerd in de Verenigde Staten.
De daar gehanteerde exportbeperkingen op cryptografische technieken belemmeren Amerikaanse leveranciers sterk in de mogelijkheid om hun produkten aan te bieden in wereldwijde bedrijfstoepassingen.
Maar ook binnen Europa gelden dergelijke beperkingen.

Een reiziger met een laptop-computer met geïntegreerde encryptie-faciliteiten moet dan ook niet vreemd opkijken als hij op een vliegveld wordt gesommeerd zijn computer deze keer maar thuis te laten.

Elk internationaal bedrijf moet alvorens het besluit om encryptie te gaan toepassen nagaan of het hiervoor wel toestemming zal krijgen van overheidswege.
Maar in het Europa van 1993 met de verdwijnende grenzen en steeds sterkere internationale vertakking van grote bedrijven bestaat juist een grote behoefte om de kostbare vertrouwelijke gegevens te beschermen.

De commerciële sector zou graag een meer realistische exportcontrole zien op het gebruik van DES en RSA. De realiteit is dat internationale criminele organisaties gebruik maken of zullen gaan maken van cryptografie, ongeacht of zij deze via legale dan wel illegale weg verkrijgen. De overheden zullen dan ook met deze complicatie rekening dienen te houden. Ontspanning van de huidige exportcontroles zal de commerciële sector zeer zeker helpen in het handhaven of verbeteren van internationale concurrentiepositie.

TOT SLOT

Door de behoefte aan open systemen met mogelijkheden als filesharing en distributed services, zoals deze bijvoorbeeld in DCE worden voorgestaan, is een beveiligingsmechanisme als Kerberos noodzakelijk geworden.
Kerberos beschikt over wederzijdse authenticatie, encryptie en sleuteldistributiemogelijkheden. Hier-bij worden passwords nooit in klare vorm gecommuniceerd.
Als DSS beschikbaar komt kan het vrij worden toegepast doordat er geen beperkingen bestaan op het gebied van patenten en export. Momenteel lijkt dit echter het enige voordeel van DSS.
RSA is een volwaardig encryptie-algoritme, in staat tot zowel het genereren van digitale handtekeningen als vercijfering en hierdoor bruikbaar voor sleuteldistributiedoeleinden.
RSA wordt reeds enige jaren op grote schaal toegepast in commerciële computersystemen over de gehele wereld. RSA is momenteel dan ook de defacto-standaard voor public key-algoritmen waarvan de sterkte en de bruikbaarheid uitvoerig zijn bewezen.
Het is de vraag of het bedrijfsleven zit te wachten op een tweede standaard voor dè digitale handtekening.

Het toepassen van volwaardige en effectieve encryptie-algoritmen als DES en RSA wordt momenteel nog gehinderd door ondoorzichtige import- en exportbeperkingen. De overheden rechtvaardigen zich hiervoor met redenen van nationale veiligheid. Zij verliezen hierbij echter twee belangrijke punten uit het oog.
Het is momenteel reeds mogelijk algoritmen als RSA en DES te kopen in eenvoudige software-versies of deze na te bouwen op grond van de algemeen beschikbare publikaties.
De beperkingen op het gebruik van encryptie belemmeren het bedrijfsleven in de mogelijkheden zijn zakelijke belangen te beschermen.

LITERATUUR

[DEA81] ANSI X 3.92, 1981, *American National Standard for Information Systems - Data Encryption Algorithm (DEA)*, 1981.

[DES77] National Bureau of Standards, *Data Encryption Standard;* Federal Information Processing Standards Publication 46, Government Printing Office, Washington D.C., 1977.

[ElGa85] ElGamal, *T.A public-key cryptosystem and signature scheme based on discrete logarithms,* IEEE Trans. Inf. Theory IT-31, p.p. 469-472, 1985.

[Kerb88] Kerberos: *An Authentication Service for Open Network Systems;* J.G. Steiner, Massachusetts Institute of Technology; C. Neuman, Department of Computer Science; J.I. Schiller, Massachusetts Institute of Technology, 1988.

[RSA78] R.L. Rivest, A. Shamir en L. Adleman: *A method for Obtaining Digital Signatures and Public-Key Cryptosystems,* Communications of the ACM, Vol. 21(2) p.p. 120-126, februari 1978.

[Schn89] C.P. Schnorr, *Efficient identification and signatures for smartcards.* Advances in Cryptology: Proceedings of Crypto '89, G. Brassard Ed., Lecture Notes in Computer Science 435, Springer-Verlag, New York, p.p. 239-251, 1989.

Drs. T.P. de Vries
Is organisatie-adviseur bij KPMG Klynveld Management Consultants. Hij is gespecialiseerd in de beveiligingsmethoden voor het elektronisch berichtenverkeer, smartcard- en magneetstripkaart-toepassingen, PC-beveiliging en de onderliggende mathematische en cryptografische principes. Hij is betrokken bij beveiligingsopdrachten met behulp van cryptografische technieken voor onder meer financiële instellingen, creditcardmaatschappijen, de detailhandel en handelsmaatschappijen.

Beveiligingsperikelen rondom Novell NetWare

J.L. Ramos Najera

Als ervaren netwerk-auditor was Ramos Najera zich, evenals vele collega's, bewust van het feit dat de beveiliging van het PC-netwerkbesturingssysteem Novell NetWare relatief goed, maar niet waterdicht was.
Toch was de plotselinge paniek rond de ontdekking van concrete leemten in het najaar van 1992 ook voor hem verrassend.
Het relaas van een insider.

INLEIDING

De laatste maanden van het jaar 1992 zijn zeer turbulent geweest voor de firma Novell en de gebruikers van het populaire netwerkbesturingssysteem Novell NetWare. Men is terecht opgeschrikt door de kraakprogramma's die binnen een kort tijdsbestek het licht zagen en waarmee de normaliter zeer geavanceerde beveiliging van Novell NetWare plotsklaps als een kaartenhuis in elkaar stortte. Deze kraakprogramma's tonen duidelijk aan dat de huidige beveiligingsmechanismen binnen PC-netwerken nog van onvoldoende niveau zijn en nodig dienen te worden verbeterd.

Het resultaat van dit alles is echter wel dat vele slapende honden zijn wakker gemaakt in netwerkland en dat is een goede zaak. In de eerste plaats zijn er de gebruikers van Novell NetWare die dachten het meest veilige netwerkbesturingssysteem in huis te hebben als PC-platform voor (kritische) applicaties. Ten tweede Novell zelf die niet had bedacht dat de beveiligingsmaatregelen op zo'n manier konden worden omzeild, of dit heimelijk had geaccepteerd ter wille van hogere prestaties. Hals over kop moest Novell de desbetreffende leemten dichten; zij is hier naar mijn mening redelijk goed in geslaagd. De leveranciers zijn uiteindelijk de lachende derde want gebruikers zullen niet gauw hun installed base verlaten, maar zullen aankloppen voor additionele beveiligingsprodukten en -adviezen alsmede voor het updaten van hun oude versies.

Voor degenen die de gebeurtenissen niet hebben gevolgd of door de vele, soms tegenstrijdige en onduidelijke berichten het overzicht hebben verloren, zal in dit artikel een overzicht worden gegeven van de kraakmethoden en, wat belangrijker is, hoe deze door Novell zijn c.q. zullen worden bestreden en wat de gebruiker zelf kan doen.

KRAAKMETHODEN

Er zijn destijds meerdere kraakmethoden ontdekt. Hiervan hebben twee programma's grote publiciteit gekregen welke door Novell, na veel aandringen, serieus zijn genomen. De twee kraakprogramma's zijn:

1. Het programma KNOCK.EXE, dat een grove fout in de login-procedure gebruikte om als supervisor (de beheerder van het systeem) in te loggen.

2. Het programma HACK.EXE, waardoor dezelfde rechten als die van de supervisor verkregen kunnen worden.

Beide programma's zullen in dit artikel nader worden belicht.

In de media worden verscheidene kraakmethoden genoemd, waarbij de maatregelen die door Novell in eerste instantie waren genomen tegen het programma HACK.EXE werden omzeild. Door Vanderaart [Vand92] wordt zelfs beweerd dat de ene na de andere 'hack' zijn compiler verlaat en binnen zestig seconden de door Novell aangebrachte beveiliging kraakt. Dit moet met een korreltje zout worden genomen, maar het geeft wel aan dat de beveiligingsmaatregelen niet waterdicht zijn. Overigens raad ik iedereen die zich om beveiliging zorgen maakt aan de uitgave van LAN Magazine van november 1992 (jaargang 4, nummer 10) aandachtig te lezen.

Een opmerkelijke zaak in het geheel is dat beide kraakprogramma's ontwikkeld zijn in Nederland. Als oorzaken hiervoor kunnen worden aangedragen: de relatief actieve Novell Gebruikersgroep Nederland (NGN) en de mentaliteit van Nederlanders om anderen, en met name grote bedrijven, een ha(c)k te zetten.

KNOCK.EXE

Dit programma is ontwikkeld door de hackersgroep die ook het bekende blad Hack-tic uitgeeft en is vrij verkrijgbaar op diverse bulletin boards. Het programma maakt gebruik van een grove fout in de login-procedure van enkele Novell NetWare-versies die vóór NetWare 286 versie 2.2 en NetWare 386 versie 3.11 zijn verschenen.

De fout ligt in het feit dat de inlog-procedure af en toe niet goed functioneert en een leeg (dus geen) password als juist accepteert terwijl er wel degelijk een password vereist is. Door genoeg keren op een geautomatiseerde wijze een inlog-poging als supervisor met een leeg password te plegen (knock, knock) lukt het op een gegeven moment als supervisor in te loggen. Het effect wordt versterkt doordat een leeg password niet als een inbraakpoging wordt gezien en aldus niet kan worden ondervangen door de *intruder detection* en *lockout*-faciliteit van NetWare.

HACK.EXE

Het HACK.EXE-programma is door een aantal Leidse studenten ontwikkeld en op de jaarlijkse NightWare party van de NGN medio september 1992 gedemonstreerd aan onder anderen vertegenwoordigers van de firma Novell. Het programma maakt het mogelijk dat een gebruiker zich 'supervisor equivalent' kan maken, ofwel dezelfde rechten kan verkrijgen als de beheerder (= supervisor) en hierdoor ongelimiteerd aan het werk kan gaan. De gevolgen kunnen in een operationele omgeving uiteraard desastreus zijn. Om deze reden beloofde de NGN aan Novell het programma niet vrij te geven; Novell stelde daartegenover dat zij zo spoedig mogelijk met een oplossing zou komen. Wat het eerste deel van deze afspraak betreft kunnen we stellen dat deze maatregel zeer zwak is geweest en naar verwachting (en getuige de verschillende artikelen die verschenen zijn) niet heeft gewerkt.

Het programma HACK.EXE maakt gebruik van een zwakte die in de vele datacommunicatie-omgevingen is terug te vinden: authenticatie vindt slechts eenmaal plaats, namelijk tijdens de inlog-procedure.

Het HACK.EXE-programma maakt gebruik van een zwakte die in veel toepassingen in een telecommunicatie-omgeving terug is te vinden: *authenticatie* vindt slechts eenmaal plaats, namelijk tijdens de inlog-procedure. Na authenticatie van de *gebruiker* vindt er later nog slechts *identificatie* en *geen authenticatie* van de *zender van het bericht* plaats. Hierdoor ontstaat het gevaar dat men zich voordoet als een ander, vaak 'masquerading' genaamd.

In het geval van NetWare vindt identificatie en authenticatie plaats door de juiste username/password-combinatie in te geven na het starten van het programma LOGIN.EXE. Het mechanisme dat hierbij wordt gehanteerd, is overigens gedocumenteerd [Lamb92] en werkt als volgt:

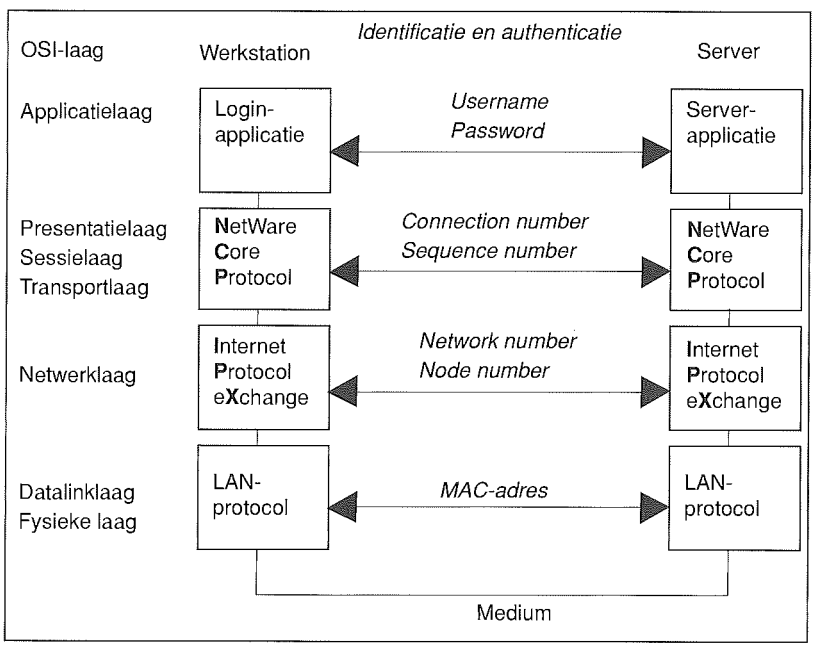
1. het inlog-programma op het werkstation (de cliënt) vraagt de gebruiker om een username;
2. de cliënt voert eerst een logout uit om alle eventueel bestaande connecties af te breken;
3. vervolgens wordt door de cliënt de object ID van de desbetreffende gebruiker opgevraagd;
4. tevens wordt door de cliënt aan de server een zogenaamde *log key* (randomgetal) gevraagd;
5. de server verzendt een random *log key* van acht bytes (octetten);
6. het inlog-programma vraagt vervolgens aan de gebruiker om een password;
7. de gebruiker voert dit in waarna het password in combinatie met de *log key* door middel van een onomkeerbaar encryptie-algoritme wordt

verwerkt tot een getal van zestien bytes, de password value;
8. de 16-byte *password value* en de 8-byte *log key* worden via een éénweg-encryptiemethode verwerkt tot een nieuwe 8-byte *password value*. Deze wordt vervolgens voor authenticatie verzonden naar de server;
9. de server voert, met behulp van het op de server vercijferd opgeslagen password, dezelfde stappen uit als de cliënt om de *password value* te berekenen;
10. indien de *password value* van de cliënt en de server gelijk zijn, wordt de gebruiker positief geauthenticeerd.

Op basis van het bovenstaande kunnen wij concluderen dat, mits het encryptie-algoritme sterk genoeg is, de inlog-procedure zelf zeer adequaat is. Niet alleen wordt hierdoor voorkomen dat het password kan worden afgetapt, maar door het gebruik van een randomgetal (de *log key*) wordt tevens voorkomen dat men de inlog-procedure kan naspelen door de gegevensstroom te herhalen. Een zwakke schakel in het geheel is echter dat, gezien het feit dat de *log key* en de *password value* bekend zijn en de lengte van het password in de praktijk kort is (circa zes karakters), het password door exhaustive search (uitproberen van LOGIN.EXE in een eigen omgeving) vrij snel zou kunnen worden achterhaald. Een maatregel hiertegen is het voldoende frequent wijzigen van het password.

Na het inloggen vindt identificatie (en dus geen authenticatie) van de zender en de ontvanger plaats aan de hand van verschillende velden in de berichten die tussen cliënt en server over en weer worden gezonden (zie figuur 1). Op LAN-protocol-niveau (Ethernet, Token Ring, etc.) vindt identificatie plaats met behulp van de MAC-adressen

Figuur 1. Identificatie en authenticatie-informatie in NetWare-protocollen.



(Medium Access Control) van de zender en de ontvanger. De MAC-adressen zijn normaliter in de hardware (netwerk-interface-kaart) 'gebakken' maar kunnen ook software-matig worden ingesteld (waardoor een algemene bedreiging voor masquerading ontstaat).

Op netwerkniveau vindt identificatie plaats aan de hand van de *network* en *node numbers* van de zendende en de ontvangende partij in een IPX-pakket (Internet Packet eXchange). De *node numbers* zijn overigens gelijk aan de MAC-adressen.

De end-to-end-communicatie vindt plaats op NCP-niveau (NetWare Core Protocol) en identificatie vindt plaats op basis van het *connection number*. Indien een bericht met een bepaalde *connection number* binnen komt, zal de server het hierin gevatte verzoek uitvoeren met de rechten van de gebruiker die aan de desbetreffende connectie is gekoppeld (deze koppeling vindt plaats na de inlog-procedure).

Het bovenstaande heeft tot gevolg dat een ongeautoriseerde partij een connectie van een geautoriseerde gebruiker als het ware kan kapen door een bericht aan te maken met alle juiste identificerende velden op IPX- en NCP-niveau en dat bericht via het netwerk richting server te versturen. Dit is precies de werking van het programma HACK.EXE, waarbij het slachtoffer uiteraard de supervisor is. Opmerkelijk is dat het programma hierbij slechts gebruik maakt van standaardfuncties die door de NetWare Shell (NETx) ter beschikking worden gesteld, waaronder een call om een IPX-pakket geheel zelf in te vullen en dit te verzenden zonder verdere initialisatie en controle. Met andere woorden, Novell heeft zelf de gereedschappen verschaft waarmee de inbraak kon worden gepleegd.

De hack gaat ongeveer als volgt in zijn werk:
1. allereerst wordt gecontroleerd of alle noodzakelijke netwerk-software (IPX-driver, NETx-shell) aanwezig is en in goede status verkeert;
2. met standaard NetWare calls worden gegevens omtrent de eigen connectie verzameld en daarvan wordt onder andere de naam gebruikt voor het later uitvoeren van de SECURITY_EQUALS-opdracht (zie stap 5);
3. in een loop wordt van de bestaande connecties de *username* opgevraagd totdat de supervisor is gevonden of de loop geheel is doorlopen;
4. als de supervisor gevonden is, worden gegevens (zoals de *network node* en *connection number*) omtrent deze connectie verzameld;
5. met de verzamelde gegevens wordt een IPX-pakket aangemaakt met de SECURITY_EQUALS-opdracht die de gebruiker (lees hacker) dezelfde rechten geeft als de supervisor;
6. in een loop waarbij het *sequence number* van het NCP-bericht varieert wordt telkens het IPX-pakket verzonden totdat de cliënt een acknowledge (melding succesvolle verwerking) ontvangt;
7. de gebruiker heeft nu dezelfde rechten als de supervisor.

Het zij hier opgemerkt dat de NCP-berichten van een *sequence number* zijn voorzien. De server zal al-

leen de vervatte opdracht uitvoeren als het *sequence number* gelijk is aan of één hoger is dan de voorgaande. Door alle mogelijke *sequence numbers* uit te proberen kan het juiste *sequence number* worden gevonden.
Door een gelijk *sequence number* als de voorgaande te gebruiken, zal het zelfs niet worden bemerkt door de 'echte' gebruiker als hij/zij zelf iets verzendt. NetWare laat dit gewoon toe, want deze techniek wordt door NetWare 'misbruikt' in de zogenaamde *burst* mode.
Oplettende lezers zullen zich echter afvragen: maar controleert het NCP-protocol dan niet op pakketten die uit volgorde zijn? Het antwoord is: ja, maar deze berichten worden door NCP slechts genegeerd, aangezien men ervan uitgaat dat dit onder normale omstandigheden niet kan voorkomen. Dit vertrouwen is gebaseerd op het feit dat elke NCP-*request* wordt gevolgd door een NCP-*confirmation*, wat ook wel onterecht het IPX-ping-pong-protocol wordt genoemd (het is namelijk NCP en niet IPX die dat doet). Er vindt verder geen enkele actie plaats.

HET ANTWOORD VAN NOVELL

Het antwoord van Novell op KNOCK.EXE was zeer merkwaardig te noemen. Novell bleek namelijk op de hoogte te zijn van dit probleem en had het reeds opgelost in Novell NetWare versie 2.2 en 3.11. Daarnaast waren patches voor oudere versies reeds enige tijd beschikbaar op diverse bulletin boards, maar Novell had bewust of onbewust verzuimd leveranciers en gebruikers hierover te informeren.

Bezitters van NetWare 2.2 en 3.11 behoeven zich dus niet langer druk te maken om dit probleem. Voor gebruikers van de oudere versies van NetWare is het echter zeer aan te bevelen de desbetreffende patches te installeren of een upgrade naar de genoemde versies aan te schaffen. De patches kunnen bij het NGN worden aangevraagd.

Het antwoord op HACK.EXE kwam in de vorm van een VAP (Value Added Process) voor NetWare 286-versies en een NLM (NetWare Loadable Module) voor NetWare 386-versies met de naam SECUREFX, die wel controleerde op de *sequence numbers* van NCP-berichten. Als het nummer niet opvolgend is, wordt een door de gebruiker te bepalen actie ondernomen. Hierbij kan de beheerder kiezen uit drie mogelijkheden: geen actie, een melding verzenden of de connectie verbreken. De eventuele melding wordt naar alle gebruikers verzonden.

De oplossing die door SECUREFX wordt geboden, is echter onvoldoende. Nog steeds bestaat de mogelijkheid dat het juiste *sequence number* wordt achterhaald en de inbraak alsnog succesvol plaatsvindt. Schrijver dezes heeft tijdens een cursus Novell NetWare Security met behulp van een standaard-PC en met een software datascope deze truc uitgehaald. Het is verbazingwekkend om te ervaren dat door het verzenden van slechts één eenvoudig IPX-pakket iemand supervisor-rechten verkrijgt.
De SECUREFX-oplossing kan zelfs nadelig werken. Wat gebeurt er namelijk als het echt een netwerkfout betreft? Ook kan iemand een programma maken dat het hele netwerk in verwarring brengt door voortdurend meldingen of connectieverbrekingen te genereren van allerlei gebruikers. De goeden moeten dan onder de kwaden lijden, zullen we maar zeggen.

Het is verbazingwekkend om te ervaren dat door het verzenden van slechts één eenvoudig IPX-pakket iemand supervisor-rechten verkrijgt.

Novell diende dus met een andere, betere oplossing te komen waarbij de authenticatie van de zender van een bericht kan worden vastgesteld. Op 5 oktober 1992 kwam Novell met de mededeling dat Novell de problemen in breder verband ging aanpakken door 'an agressive two-phase strategy to analyse, develop and verify solutions to the broader issues surrounding this threat'. Deze twee fases hielden het volgende in:
- fase 1: vercijfering van de NCP-protocolinformatie;
- fase 2: vercijfering van alle data in IPX-pakketten.

Al gauw werd het duidelijk dat fase 1 iets anders inhield dan werd gesuggereerd. De protocolinformatie wordt namelijk niet vercijferd, maar de oplossing is gebaseerd op het toevoegen van een *digital signature* per bericht, te vergelijken met een Message Authentication Code (MAC). Deze handtekening bestaat uit een veld van acht bits dat met behulp van een encryptie-algoritme wordt berekend aan de hand van een random 8-bit *session key* en een 16-bit *Message Digest Code* (een soort checksum). Om te voorkomen dat deze maatregel wordt omzeild door het opnieuw inbrengen van berichten is de waarde van de digitale handtekening afhankelijk van het vorige bericht en wordt de vorm van afhankelijkheid tussen de berichten per login at random bepaald.

Beloofd werd dat de fase 1-oplossing binnen twee weken na verschijning van de mededeling beschikbaar zou zijn voor testdoeleinden. Het uiteindelijke produkt zou bestaan uit een 'add-on' die naar keuze wel of niet kon worden geïnstalleerd. Fase 2 zou slechts beschikbaar komen voor klanten met zeer hoge beveiligingseisen. Waarschijnlijk worden hiermee klanten bedoeld die een volledige DES-licentie kunnen verkrijgen (zoals militaire en financiële instellingen).

Ten tijde dat dit artikel werd geschreven (januari 1993), was de fase 1-oplossing nog niet (vrijelijk) verkrijgbaar. De eerste berichten vermelden wel

J.L. Ramos Najera
Is sinds 1981 werkzaam bij KPMG en sinds 1991 Telecommunications Consultant bij KPMG Klynveld Management Consultants. Zijn audit-ervaring ligt met name op het gebied van telecommunicatie in een breed perspectief. Hij is met regelmaat spreker op diverse seminars op het gebied van beveiliging van netwerken in het algemeen en Novell NetWare in het bijzonder.

dat er moet worden betaald en wel in de vorm van netwerkprestatie. Geschat wordt dat de digitale handtekening een prestatiedegradatie van tien procent inhoudt voor 386-machines en van maar liefst veertig procent voor 286-machines. Maar wie heeft gezegd dat beveiliging niets kost?

AANBEVOLEN

Gezien de consequenties van de beveiligingsoplossingen van Novell zullen organisaties zich beraden over het wel of niet implementeren van deze opties.

Naar mijn mening dienen organisaties die bedrijfskritische toepassingen op basis van Novell NetWare hebben geïmplementeerd, minimaal te kiezen voor implementatie van fase 1-beveiliging. De meeste organisaties zullen tegenwoordig 386-werkstations als cliënt gebruiken, waardoor een aanvaardbare prestatiedegradatie van circa tien procent het gevolg zal zijn.

Voor de organisaties die niet kiezen voor deze optie, wat de reden ook mag zijn, beveel ik aan de volgende aanvullende maatregelen te nemen (voor een algemeen inzicht in de beveiligingsmogelijkheden van Novell NetWare wordt verder verwezen naar [Ramo91]):

Op de server:
- installeer de patch tegen KNOCK.EXE voor versies ouder dan NetWare 286 2.2 en NetWare 386 3.11;
- installeer SECUREFX op alle servers en kies minimaal voor melding van mogelijke inbraakpogingen.

Voor de beheerder(s):
- verwijder indien mogelijk de guest account van de servers;
- gebruik de account supervisor nooit, maar geef alle beheerders een eigen beheeraccount met supervisor-rechten (de meeste kraakprogramma's en hackers zullen namelijk de supervisor account zoeken en misbruiken);
- gebruik de beheer-account slechts indien noodzakelijk (dus niet voor het gewone werk);
- laat een connectie met een beheer-account nooit onnodig lang bestaan;
- ontwikkel een geautomatiseerde routine waarmee dagelijks minimaal de File Server Error Log en de uitvoer van het standaard Novell commando SECURITY worden gecontroleerd.

Voor alle gebruikers (dus eventueel ook de beheerder):
- beperk *concurrent connections* (simultane connecties per gebruiker) tot één (hierdoor wordt voorkomen dat een connectie per ongeluk open blijft staan);
- beperk de rechten van gebruikers tot slechts het noodzakelijke voor het uitvoeren van hun functie (least privilege).

TOT SLOT

De moraal van het verhaal is dat wij flink met onze neus op het feit zijn gedrukt dat beveiligingsmaatregelen waarop werd vertrouwd volledig teniet kunnen worden gedaan door manifestatie van bedreigingen die inherent zijn aan het gebruik van telecommunicatie in het algemeen en PC-netwerken in het bijzonder.

Bij de beschreven ontwikkelingen bespeur ik echter een enigszins hypocriete houding van de gebruikers. Waarom maakt iedereen zich druk om deze leemten in de beveiliging van Novell NetWare en laat men bijvoorbeeld wel toe dat wachtwoorden van mainframe- en mini-systemen in klare taal over lokale netwerken worden getransporteerd met legio mogelijkheden om deze zeer eenvoudig af te tappen? De toepassingen die op mainframe- en mini-systemen draaien zijn in het algemeen toch meer kritisch van aard? Netwerkbeveiliging is dus een zaak die aandacht van het management verdient.

De vraag die iedereen bezighoudt is of de beveiligingsproblematiek die door HACK.EXE wordt benadrukt ook van toepassing is op andere PC-netwerkbesturingssystemen, zoals Banyan VINES en MicroSoft LAN Manager. Volgens de leveranciers van Banyan wordt de protocolinformatie vercijferd en heeft Banyan dit probleem niet (ik hoop dat zij hierbij niet dezelfde verwarrende terminologie gebruiken als Novell). Van MicroSoft heb ik niets vernomen maar er bestaat een sterk vermoeden dat LAN Manager wel eens dezelfde problemen zou kunnen hebben als Novell. Wellicht zal ik hier bij een andere gelegenheid op terugkomen.

Tot slot mijn complimenten voor de oplossing die Novell heeft geboden. Ik denk dat Novell hiermee een voorsprong op de concurrentie neemt. Het is echter te hopen dat dit soort oplossingen in nog breder verband zal worden opgepakt en gestandaardiseerd.

LITERATUUR

[Lamb92] J. Lamb, S.R. Jarocki en A.M. Seijas, *NetWare Security: Configuring and Auditing a Trusted Environment,* Novell Systems Research Department.

[Ramo91] J.L. Ramos Najera, *PC-beveiliging in een netwerkstructuur,* in Compact 1991/2.

[Vand92] J. Vanderaart, *Het lek en de hack en Last minute update,* IDG Communications Nederland, LAN Magazine, Jaargang 4 nummer 10, November 1992.

CUMULATIEF

Overzicht van eerder verschenen artikelen in Compact

Een selectie van geactualiseerde artikelen uit de 12 1/2 jaar Compact 1974 - 1986 is opgenomen in het boek *24 over EDP-auditing*. 24 auteurs over EDP-auditing in theorie en praktijk: visies, ontwikkelingen, werkwijzen en oplossingen.
Het boek is verkrijgbaar via de boekhandel onder nummer: ISBN 90 14 03648 5.

2 17e jaargang 90/2 zomer 1990

Kwaliteitsbeheersing bij systeemontwikkeling
ing. L.J.M.W. Gielen RI en drs.ing. G.J.P. Swinkels

Het gebruik van geautomatiseerde hulpmiddelen bij systeemontwikkeling
ir. J.A. Verstelle

Jackson Structured Programming en kwaliteitsbeheersing bij systeemontwikkeling
mw. V. Six

Beoordelen betrouwbaarheid geautomatiseerde informatiesystemen op basis van de risico-analysemethode
drs. R.G.A. Fijneman RA, drs. E.P.R. van Vroenhoven en J.A.W. Winterink RA

3 17e jaargang 90/3 herfst 1990

FunctiePunt Analyse voor de begroting van software-ontwikkeling
ir. B.A.W.M. Bruns

Effect van software-kwaliteit op de kostenbegroting van systeemontwikkeling
drs. M.J. van der Vos

Qualify: beoordeling effectiviteit en efficiëntie van informatiesystemen
drs.ing. G.J.P. Swinkels en P.P.M.G.G. Brouwers

An approach to Data Centre Efficiency Auditing
D. Hall

4 17e jaargang 90/4 winter 1990

Informaticarecht en EDP-auditing in perspectief
prof. A.W. Neisingh RA en
mw. mr. A.M. Ch. Kemna MBA

Software-bescherming: tien jaar theorie en praktijk
mr. V.A. de Pous

Software-ontwikkelingscontracten
prof.mr. J.M.A. Berkvens

Escrow. Het depot van de broncode: fopspeen of panacee?
mw. mr. A.M.Ch. Kemna MBA

Strafbaarstelling van computermisbruik
R.A. s'Jacob

1 18e jaargang 91/1 lente 1991

Geschillenbeslechting in de automatiseringsbranche
mr. F.V.B.M. Mutsaerts

De bewijskracht van computermateriaal in de civiele procedure
mw. mr. I.M.A. de Graaf-Hinfelaar en
mw. mr. A.M.Ch. Kemna MBA

Praktische problemen van organisaties bij de implementatie van de Wet Persoonsregistraties
ir. B.A.W.M. Bruns

Een invulling van de beveiligingseis uit de Wet Persoonsregistraties
P.A.J. van der Knaap

Computercriminaliteit in Nederland
mr. V.A. de Pous

2 18e jaargang 91/2 zomer 1991

Beheerst PC-gebruik
ing. A. van der Vlist RI

De relatieve veiligheid van PC-besturingssystemen
drs.ing. J.C. van Winkel RI

PC-beveiliging in een netwerkstructuur
J.L. Ramos Najera

Detectie en bestrijding van computervirussen
J. Brinkman

The PC as a secure network workstation
dr. I.G. Graham en S.H. Wieten

The implementation of TSS
drs. T.P. de Vries

3 18e jaargang 91/3 herfst 1991

Beveiligingsbeleid geautomatiseerde informatievoorziening
mw. D. Jansen Heijtmajer

Geautomatiseerde produktiebesturing
E.J.M. Ridderbeekx

Audit van CA-SEVEN
E.J.M. Ridderbeekx

Registratie en analyse van produktieproblemen
ing. J.R. Hendriks en drs. J. Kuipers RA

SAP en de beheersing van geautomatiseerde controles
A.A.J. Breed RI, M. Groesz RI en drs. M.A. Weverink

4 18e jaargang 91/4 winter 1991

Systemen voor logische toegangsbeveiliging
drs. P. Veltman RA

Toepassing van CA-ACF2 in de praktijk
ing. D.J. Huis

Access control op Unisys A Serie computers
drs. M.A. Bongers RA en J-M. van Leerdam

Beveiliging van Tandem-systemen
K.E.A. van Dijk en M.M.J.A. van Dijk

RACF als access control software voor MVS-omgevingen
ing. G.H.M. Meijer

Implementatie van een beveiligingspakket
J.H. Diekema

1 19e jaargang 92/1 lente 1992

Fysieke beveiliging, een overzicht
J.F.C. van Epen CISA

Water en vuur. Effectiviteit van brandbeveiligingsmaatregelen in en om rekencentra
ing. J.F. Kuperus en ing. G.H.M. Meijer

Netconditionering
R. van de Wouw

Fysieke beveiliging en de chipcard-technologie
drs. Th.H. van Hesteren, ing. J.A.M. van Schaik en drs. T.P. de Vries

Beveiligingsbeleid gegevens en gegevensverwerking, een praktisch voorbeeld
ir. B.J.M. van Wely

Forensische EDP-auditing
R.A. s'Jacob RA

2 19e jaargang 92/2 zomer 1992

Investeren in informatietechnologie: take IT or leave IT
drs.ing. G.J.P. Swinkels en drs. H.G.P. van Irsel

Managing with Information Technology - a decade of wasted money?
ir. M.C.A. van Nievelt

Informatietechnologie in een kantooromgeving: produktiviteitsmanagement van kantoorarbeid en kantoorautomatisering
drs. F.R.E. Lekanne Deprez

Het plannen en rechtvaardigen van infrastructurele IT-investeringen
drs. H.G.P. van Irsel en P. Fluitsma

Uitbesteding van automatisering: more than make or buy
mw. drs. H.W.A. van den Heuvel en mw. mr. A.M.Ch. Kemna MBA

3 19e jaargang 92/3 herfst 1992

De EDI-infrastructuur bij de Kas-Associatie
P. van Berge

Beheersbaarheid van het EDI-verkeer in de praktijk
G.J. Endenburg RI

EDI bij de Rijksdienst voor het Wegverkeer
J.W.J. Laan

EDI, een strategisch perspectief voor het bankwezen
drs. M.A. Bongers RE en mw.drs. M. Steeman

Beheersing van inzet en gebruik IT: van kopzorg tot hoofdzaak
drs. G.C.M. Mol en drs. J.F.H. Vrins

4 19e jaargang 92/4 winter 1992

De veiligheid van betaalautomaten
E.R. Fekkes

S.W.I.F.T. and Security
This article was produced by S.W.I.F.T. s.c. Marketing and the Chief Inspector's Office

Het binnenlandse traject van SWIFT-posten; het SWIFT-8007-circuit
drs. F.G. Knaack

Betrouwbaarheid van het FA-systeem
drs. R. Oudega

Een Nederlandse standaard voor de elektronische handtekening
mw.drs. M.C. van Lith

De beveiliging van elektronisch bankieren
mw.drs. M.C. van Lith

Secure Cash Management; a case study
H. Roos RA and H. Veenman MBT

Beveiligingsaspecten en juridische aspecten als communicerende vaten
ir. G.J. Schuringa en mr. R.E. van Esch