KWARTAALBLAD EDP-AUDITING

1994/2

ZOMER COMPACT

Compact ®
Jaargang 21, nummer 2
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
(hoofdredacteur)
drs. R.G.A. Fijneman
prof. A.W. Neisingh
drs. P. Veltman

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
M.M. Buijs
mw.drs. M.C. van Lith
E.J.M. Ridderbeekx
drs. D.J.P. Witte

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

NOTU
VAKTIJDSCHRIFTEN

Lid van de Nederlandse organisatie van tijdschriftuitgevers NOTU

ISSN 0920 - 1645

INHOUDSOPGAVE

2
Redactioneel

3
Audit van een SNA-netwerk
M.M. Buijs RI en E.J.M. Ridderbeekx RE RI
Datacommunicatie is van vitaal belang voor de hedendaagse geautomatiseerde informatievoorziening en dient daarom te voldoen aan hoge kwaliteitseisen. De consequentie hiervan is dat periodiek moet worden vastgesteld dat de werkelijke situatie beantwoordt aan die eisen. In dit artikel wordt na een korte beschrijving van de concepten en terminologie, aan de hand van een risicomatrix een werkprogramma beschreven voor de audit van datacommunicatienetwerken gebaseerd op IBM's Systems Network Architecture.

18
Beveiliging van analoge kieslijnen
Drs. ing. D. Brouwer RE
Analoge kieslijnen zijn al sinds jaar en dag een uitstekend middel om op flexibele wijze tegen lage kosten een verbinding tussen twee locaties te realiseren. Door technische verbeteringen in modems kunnen inmiddels aanzienlijke overdrachtssnelheden worden bereikt. Doordat analoge kieslijnen een verbinding verzorgen op de onderste laag van het OSI-model (de fysieke laag) staat voor de beveiliging van deze lijnen een groot aantal maatregelen ter beschikking. Dit artikel geeft een overzicht van de beschikbare beveiligingsmaatregelen en de risico's welke hiermee worden afgeschermd.

36
Beveiliging van UNIX
Mw. drs. M.C. van Lith RE
Het besturingssysteem UNIX wordt inmiddels op grote schaal in het bedrijfsleven toegepast. De moderne versies bieden adequate mogelijkheden tot beveiliging, maar de systeembeheerder moet bij het inrichten hiervan zorgvuldig te werk gaan. In dit artikel wordt ingegaan op de beveiliging van UNIX en de mogelijkheden om het geïmplementeerde beveiligingsniveau met behulp van geautomatiseerde functies te controleren.

45
Typologie van workflow-managementsystemen
Drs. D.J.P.Witte
Een workflow-managementsysteem biedt de mogelijkheid een substantiële produktiviteitsverbetering in de kantooromgeving te realiseren. Implementatie van een dergelijk systeem wordt vaak voorafgegaan door herontwerp van de processen. Het workflow-managementsysteem kan worden beschouwd als de faciliterende technologie van een herontworpen werkproces. In dit artikel wordt aan de hand van een beschrijving van verschillende typen van workflow-managementsystemen inzicht gegeven in de wijze waarop werkprocessen in de kantooromgeving geautomatiseerd kunnen worden ondersteund.

53
EDP Auditorium

54
Cumulatief

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.

Het voor u liggende nummer van Compact is het laatste dat onder de bezielende leiding van hoofdredacteur Dick Steeman tot stand is gekomen. Ruim twintig jaar geleden nam hij het initiatief te komen tot een regelmatige voorlichting aan accountants over zaken met betrekking tot automatisering die hun belangstelling zouden moeten hebben. Vandaar ook de naam Compact (Computer en Accountant). Het terrein waarop Steeman actief is heeft zich in de loop der jaren ontwikkeld tot EDP-auditing.

Eind zestiger en begin zeventiger jaren werden accountants bij de controle van de jaarrekening voor het eerst geconfronteerd met het fenomeen automatisering. Kennis op dit terrein ontbrak en zo ontstond een gespecialiseerde groep die vaststelde wat de invloed van automatisering op het stelsel van maatregelen van interne controle en op de accountantscontrole zou zijn. Bij deze activiteiten is het niet gebleven. Het gebruik van informatietechnologie in organisaties werd omvangrijker en complexer; de invloed op de uitvoering van de accountantscontrole werd in vele gevallen niet groter. Het management van de organisaties daarentegen realiseerde zich al snel dat specifieke expertise noodzakelijk was om vast te stellen dat het gebruik van IT adequaat kon worden beheerst. Op die wijze ontwikkelde de professie zich naar EDP-auditing: beoordeling en advisering omtrent kwaliteitsaspecten van het gebruik van informatietechnologie in organisaties. Een terrein dat zich in de loop der jaren verder heeft ontwikkeld doordat naast accountants ingenieurs – op de gebieden van informatica, elektronica, telecommunicatie en telefonie –, wiskundigen en anderen deze organisaties gingen bevolken.
Deze ontwikkeling heeft Steeman mede vorm gegeven door publikaties over deze onderwerpen in Compact te entameren. Lange tijd heeft Steeman kunnen volharden in het gebruik van Nederlandse woorden in het vakgebied, dat werd overheerst door het Engels/Amerikaans. In publikaties heeft hij daarvan blijk gegeven en in het bijzonder in de oratie die hij ter gelegenheid van zijn benoeming tot hoogleraar aan de Erasmus Universiteit te Rotterdam hield. Daarin werd de EIV-accountant geïntroduceerd, waarbij EIV staat voor Elektronische Informatieverwerking. Deze accountant heeft het in de terminologie niet gehaald. Toen de slag om het Nederlands gestreden was heeft Steeman nog een warm pleidooi gevoerd het begrip audit trail te vervangen door reference trail. Reference trail is immers een juistere weergave van hetgeen wordt bedoeld.

Onder het niet aflatend enthousiasme van Steeman heeft Compact zich vervolgens van een intern huisorgaan ontwikkeld tot een kwartaaltijdschrift op het gebied van EDP-auditing dat een hoog vaktechnisch gehalte heeft bereikt. De redactie is Dick Steeman veel dank verschuldigd.

Ter gelegenheid van het uittreden van Steeman uit de maatschap KPMG Klynveld EDP Auditors is op 16 juni jongstleden een symposium gehouden met als titel 'Evolutie in Informatiebeveiliging: het toenemend belang van EDP Auditing'.
Onder voorzitterschap van collega Bronts voerde een zestal sprekers het woord over dit onderwerp, waarbij de problematiek van gebruikerszijde en door vakgenoten werd belicht. De proceedings van dit symposium zullen binnenkort in boekvorm verschijnen.

Prof. A.W. Neisingh RE RA

Audit van een SNA-netwerk

M.M. Buijs RI en
E.J.M. Ridderbeekx RE RI

Datacommunicatie in het algemeen en SNA in het bijzonder is veelomvattend en complex, en kan vanuit verschillende invalshoeken worden benaderd. Van belang bij een SNA-audit is daarom vooral de afbakening van het onderzoeksobject.
De auteurs beschrijven een werkprogramma voor de uitvoering van een goed begrensde audit van de VTAM- en NCP-definities, die tot zinvolle resultaten leidt.

INLEIDING

Op een bekende autotentoonstelling te Amsterdam hoorden wij een branchevertegenwoordiger eens verkondigen dat auto's niet meer weg te denken zijn uit het verkeersbeeld. Als we dit artikel openen met de stelling dat datacommunicatie van vitaal belang is in de hedendaagse geautomatiseerde informatievoorziening, doen we eigenlijk hetzelfde: het publiek is het er volkomen mee eens, maar nieuw inzicht levert het niet op.

Erkenning van het belang van datacommunicatie heeft echter consequenties. Zoals de automobilist eisen zal stellen aan het comfort, de veiligheid, de snelheid en de prijs waarmee hij zich kan verplaatsen, zo zal een organisatie eisen stellen aan de manier waarop aan datacommunicatie vorm is gegeven. Er is in dat geval geen fundamenteel onderscheid: zowel de automobilist als de datacommunicatie-organisatie heeft een bepaalde visie op kwaliteit, en onderkent dat zonder een aanvaardbare kwaliteit het middel mogelijk erger is dan de kwaal.

Ook dit - al dan niet expliciet - stellen van kwaliteitseisen heeft een consequentie: periodiek zal men zich op de hoogte moeten stellen van de mate waarin de werkelijke situatie aan de gestelde eisen tegemoet komt. Dit vraagt om een meting. Waar de automobilist voor een veiligheidskeuring naar de APK gaat, zal de organisatie in veel gevallen een beroep doen op de diensten van een EDP-auditor. Toegegeven, deze vergelijking gaat op een groot aantal punten mank. Essentieel is echter dat het in beide gevallen gaat om een onafhankelijk en deskundig oordeel; in het eerste geval over de veiligheid van een vervoermiddel, in het tweede over de kwaliteit van de datacommunicatie.

Dit artikel gaat in op een dergelijke meting. Niet van datacommunicatie in zijn algemeenheid, maar van IBM's Systems Network Architecture (SNA) in het bijzonder. Niet van SNA in al zijn facetten, maar rondom de centrale betekenis van de netwerkdefinities. Om te voorkomen dat de uitvoerbaarheid van een audit in gevaar komt doordat het onderzoeksgebied te ruim wordt of de grenzen van dat gebied in het geheel niet aan te geven zijn, kan men zich in eerste instantie richten op dat (deel)facet waarmee de kwaliteit van (een gedeelte van) de datacommunicatie-infrastructuur met name gestalte krijgt: de netwerkdefinities in een SNA-omgeving.

In het vervolg van dit artikel zal allereerst kort worden ingegaan op SNA-concepten en -terminologie, waarbij bijzondere aandacht uitgaat naar de structuur van de definities in VTAM en NCP. Vervolgens zal, op basis van onderkende risico's, worden uiteengezet hoe de uitvoering van een audit kan plaatsvinden. Hierbij is een tweedeling gehanteerd: in de eerste plaats komen de netwerkdefinities aan bod, ten tweede zal kort worden ingegaan op de auditaspecten ten aanzien van netwerkbesturing. Bij dit laatste neemt het produkt NetView een centrale plaats in.

SNA: CONCEPTEN EN TERMINOLOGIE

De overgang van batch-georiënteerde naar online-toepassingen in het begin van de zeventiger jaren veroorzaakte in eerste instantie een toename van op zichzelf staande, inflexibele datacommunicatie-produkten.

De in 1974 door IBM geïntroduceerde Systems Network Architecture (SNA) bood een 'overall' architectuur die het scala van losse produkten kon vervangen. SNA evolueerde in de loop der jaren van een netwerkconcept rond één centrale host-computer tot een netwerkconcept met meerdere host-computers, al dan niet verspreid over verschillende netwerken. De dominantie van de hosts zal naar verwachting in de toekomst afnemen, mede als gevolg van de ontwikkelingen met betrekking tot Advanced Program to Program Communication (APPC) en Advanced Peer to Peer Networking (APPN).

Terminologie

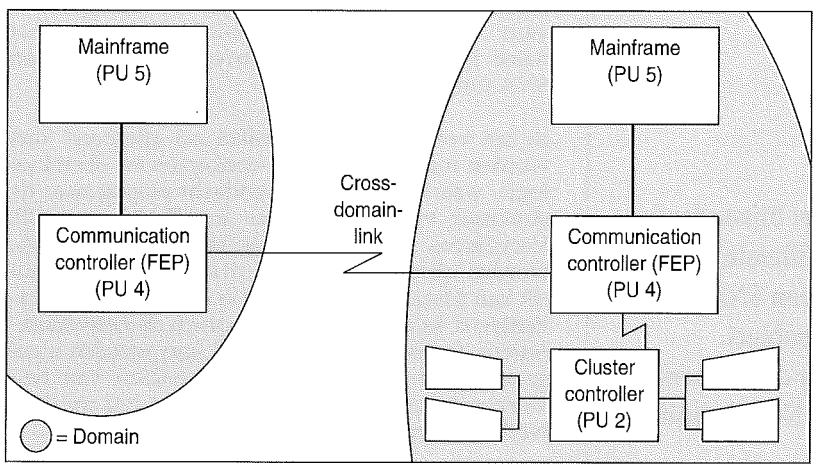
In een SNA-omgeving worden naast de centrale host-computers (kortweg hosts) en terminals twee andere belangrijke netwerkcomponenten onderscheiden:

- de cluster controller; deze bundelt het transmissieverkeer van maximaal 32 terminals. De cluster controller fungeert als een multiplexer die het gedeelde gebruik van een verbinding door de verschillende terminals mogelijk maakt;

- de communication controller of Front End Processor (FEP); deze neemt bepaalde netwerktaken van de host over, en is de schakel tussen host en cluster controller.

Een ander onderscheid dat wordt gemaakt binnen de SNA-architectuur betreft enerzijds de door de apparatuur uit te voeren *taken* en anderzijds de *deelnemers* aan het netwerk.

Figuur 1. Voorbeeld van een eenvoudig SNA-netwerk.



De *taken* worden verdeeld in een aantal klassen, de Physical Units (PU). Met een physical unit van een bepaalde klasse wordt primair aangeduid wat de taak van die PU is in het netwerk; een specifieke hardware-component kan dus strikt genomen niet gelijk worden gesteld aan een PU van een bepaalde klasse. Voorbeelden van PU-definities zijn:
- PU 5: de host(computer)-functie;
- PU 4: de communication controller-functie;
- PU 2: de cluster controller-functie;
- PU 1: 'intelligente' terminals, de overige terminaltypen worden door SNA niet als PU herkend.

De *deelnemers* aan het netwerk worden aangeduid met Logical Units (LU); een LU kan een terminalpoort zijn, maar ook een applicatieprogramma.

De netwerk-resources die verbonden zijn met een host worden beheerd door het System Services Control Point (SSCP). Deze taak wordt verzorgd door de, op de host actieve, netwerkprogrammatuur Virtual Telecommunications Access Method (VTAM). Evenals een PU en een LU wordt de SSCP aangeduid als een Network Addressable Unit (NAU).

Het gedeelte van een netwerk dat onder beheer van een SSCP valt wordt een domain genoemd; bij meerdere hosts in een netwerk (en derhalve meerdere VTAM's en evenzovele SSCP's) zijn er meerdere domains te onderscheiden. Bij een sessie tussen LU's uit verschillende domains spreekt men van een cross-domain-sessie.
In figuur 1 is een eenvoudig voorbeeld van een netwerk afgebeeld.

De grens tussen netwerken kan dwars door een PU 4 of PU 2 lopen; het gevolg hiervan is dat één fysieke FEP meerdere, bij verschillende domains behorende, PU 4's kan bevatten. Op soortgelijke wijze kan één fysieke cluster controller meerdere PU 2's bevatten.

Software in een SNA-omgeving

Ten aanzien van de software in een SNA-omgeving kan globaal onderscheid worden gemaakt in twee categorieën, te weten *basissoftware* voor SNA-netwerken en *applicatiesoftware* voor gebruikersapplicaties.

De *basissoftware* wordt gebruikt om het SNA-netwerk te definiëren en in stand te houden. Men kan niet om het gebruik van deze programmatuur heen. In IBM's SNA-netwerken wordt de basissoftware gevormd door:
- ACF/VTAM (kortweg VTAM), draait op de host-computer, en
- ACF/NCP (Network Control Program, kortweg aangeduid als NCP), draait op de communications controller.

De *applicatiesoftware* maakt gebruik van de diensten van de basissoftware om een omgeving te creëren die geschikt is voor gebruikersapplicaties. Voorbeelden van dergelijke programmatuur zijn CICS, IMS/DC, IDMS/DC en TSO. Deze program-

matuur legt de 'transactieverwerkende' basis voor 'echte' gebruikersapplicaties, zoals financiële, logistieke en personele informatiesystemen.

VTAM- EN NCP-STRUCTUUR

VTAM is de meest gangbare netwerkprogrammatuur van IBM. Het draait onder regime van diverse besturingssystemen, zoals MVS/XA, MVS/ESA, DOS/VSE en VM. De diverse componenten van het netwerk dienen binnen VTAM gedefinieerd te worden door middel van VTAM-definitie-statements.
De belangrijkste functie van VTAM is het ter beschikking stellen van de netwerkdiensten van de SSCP. Er is slechts één SSCP per VTAM. Veelal bestaat een netwerk uit meerdere hosts en meerdere VTAM's. VTAM maakt het dan mogelijk communicatie tussen diverse SSCP's te bewerkstelligen.
Niet alle netwerkbeheersingstaken worden door VTAM uitgevoerd. Enkele taken, met name de taken die betrekking hebben op de definitie van en de communicatie binnen het remote gedeelte van het netwerk, zijn 'gedelegeerd' aan de communication en cluster controllers.

De VTAM-definities worden gevormd door een verzameling parameters en gegevens, waarvan de source code gewoonlijk is opgenomen in de dataset SYS1.VTAMLST. Tijdens de periodieke initialisatie van VTAM wordt, uitgaande van deze gegevens, het netwerk tot stand gebracht.
De netwerkdefinitie in de SYS1.VTAMLST vindt plaats op het niveau van major nodes. Een major node bestaat uit een verzameling resources (de minor nodes) die, als een groep, aan VTAM bekend is, en derhalve door VTAM als een groep geactiveerd en gedeactiveerd kan worden.

De volgende major nodes kunnen voorkomen:

Application major nodes
Application major nodes vormen de definitie van de applicatiesoftware die aan VTAM bekend gemaakt wordt (bijvoorbeeld CICS, TSO, JES2, etc.). Deze major node-definities zijn herkenbaar aan de macro VBUILD, TYPE=APPL.

Local SNA device major nodes
Deze major nodes, herkenbaar aan de macro VBUILD, TYPE=LOCAL, definiëren PU's en daaraan gekoppelde LU's, die channel-gekoppeld zijn en gebruik maken van het SDLC-protocol.

Local non-SNA device major nodes
De devices die als non-SNA door middel van de LBUILD-macro gedefinieerd worden, zijn weliswaar channel-gekoppeld, maar maken geen gebruik van het SDLC-protocol.

CDRM major nodes
Een Cross-Domain Resource Manager (CDRM) is een functie van de SSCP die zorg draagt voor de behandeling van sessies tussen verschillende domains. Een CDRM wordt gedefinieerd met behulp van de macro VBUILD, TYPE=CDRM.

CDRSC major nodes
Cross-Domain Resources (CDRSC) die via de functies van de CDRM sessies over domain-grenzen heen met elkaar kunnen aangaan, dienen in sommige situaties expliciet gedefinieerd te worden. De definitiemacro luidt VBUILD, TYPE=CDRSC.

Adjacent SSCP major nodes
In een multi-domain- en multinetwerkomgeving moeten aangrenzende SSCP's waarmee een sessie tot stand moet kunnen worden gebracht, gedefinieerd worden. Dit gebeurt met behulp van de macro VBUILD, TYPE=ADJSSCP.

Channel Attached major nodes
De Channel Attached (CA) major nodes worden met name gebruikt voor de definitie van Channel To Channel Attachment (CTCA); dit is een directe verbinding tussen twee hosts, zonder tussenkomst van een front-end processor, hetgeen snelle communicatie garandeert. De gebruikte macro luidt VBUILD, TYPE=CA.

Dynamic Reconfiguration major nodes
Het is in VTAM en NCP mogelijk het netwerk dynamisch te herconfigureren zonder de noodzaak van NCP-generatie. Dit dient bewerkstelligd te worden door opname van Dynamic Reconfiguration major nodes, met behulp van het statement VBUILD, TYPE=DR.

Switched Communications Resource major nodes
Switched Communications Resource major nodes worden gebruikt om resources te defmiëren die toegang tot het netwerk kunnen krijgen door het gebruik van geschakelde lijnverbindingen. Het type van de VBUILD-macro is SWNET.

Door het activeren van bovengenoemde major nodes wordt het 'local' gedeelte van het netwerk tot stand gebracht, dat wil zeggen dat gedeelte van het netwerk dat onder beheer van VTAM op de hostcomputer valt.

Naast de genoemde major node-definities zijn er in de SYS1.VTAMLST nog drie andere onderdelen van belang, te weten:

Start Options List (SOL)
Bij initialisatie van VTAM wordt de SOL gebruikt om de initiële parametrisering van de SSCP uit te voeren. De standaardnaam van het SOL-member is ATCSTR00; tijdens de start van VTAM is het echter mogelijk door middel van een operator-ingreep naar een ander member te verwijzen.

Door middel van de CONFIG-optie in de SOL wordt verwezen naar een member met de naam ATCCONxx (waarbij de waarde van xx door de CONFIG-optie wordt gespecificeerd). Dit member bevat de Configuration List.

Configuration List
De Configuration List is een opsomming van membernamen in de SYS1.VTAMLST die de major nodes bevatten die door VTAM actief gemaakt moeten worden.

NCP-definities
Het laatste onderdeel van de SYS1.VTAMLST zijn de definities van het 'remote' netwerk, dat tot stand wordt gebracht door NCP. NCP kan worden beschouwd als het besturingssysteem van de communication controller (FEP). NCP wordt gegenereerd op de host, en vervolgens gedistribueerd naar en geladen in de FEP's.

Tijdens de start van VTAM is het mogelijk door middel van een operator-ingreep af te wijken van het standaard-member.

NCP communiceert met VTAM; dit komt voort uit de functie van NCP, namelijk het overnemen van een aantal netwerktaken van de host (onder andere communicatie met andere NCP's, 'polling' van werkstations en 'dialing' van switched lines) en het uitvoeren van deze taken in de FEP. Vanwege die noodzakelijke communicatie tussen VTAM en NCP zijn de NCP-definities terug te vinden in de SYS1.VTAMLST.

AUDIT-UITGANGSPUNTEN

In de inleiding is al aangegeven dat bij een audit van een SNA-omgeving vanuit verschillende invalshoeken vele facetten onderscheiden kunnen worden. Uit oogpunt van begrenzing en uitvoerbaarheid van het onderzoek gaan we uit van twee centrale aandachtsgebieden, te weten *netwerkdefinitie* en *netwerkbesturing*. Bij netwerkdefinitie gaat het om de vertaling van geformuleerde netwerkcriteria naar een daadwerkelijk functionerend netwerk. Is een operationeel netwerk door middel van de definities eenmaal tot stand gebracht, dan zal moeten worden gezorgd voor de instandhouding van dat netwerk conform de gestelde eisen; dit laatste duiden we aan met netwerkbesturing.

In de bijlage is een risicomatrix gepresenteerd die kan dienen als een goed hulpmiddel bij een SNA-audit die op het bovengenoemde uitgangspunt gebaseerd is. Hierin is een onderverdeling gehanteerd die aansluit bij de aandachtsgebieden netwerkdefinitie en netwerkbesturing. Rijgewijs zijn in de matrix risico's gespecificeerd die mogelijk een rol spelen in een SNA-situatie. Kolomsgewijs is aangegeven op welke kwaliteitsaspecten de risico's met name van invloed zijn. Bij de matrix dienen enkele opmerkingen te worden gemaakt.

De in de bijlage gepresenteerde matrix vormt een globaal basismodel. Echter, hoewel SNA een gemeenschappelijke noemer kan zijn, is het ene netwerk het andere niet. Het is vanzelfsprekend dat bij een kwaliteitsbeoordeling eerst aandacht moet uitgaan naar de specifieke situatie en de daaraan inherente specifieke bedreigingen en risico's. Specifieke onderzoeksdoelstellingen, de netwerktopologie (in termen van 'closed', 'open' of 'trusted' [Paan91]), het gebruik van bepaalde netwerkprodukten, de aard van de informatie die via het netwerk getransporteerd wordt, en de karakteristieke werkwijzen en procedures binnen de betrokken datacommunicatie-organisatie zullen in het algemeen kunnen leiden tot een aanzienlijk aantal uitbreidingen op en verfijningen van het hier gepresenteerde basismodel. Evident is dan ook dat deze specifieke kenmerken invloed hebben op de normen die de auditor bij een kritische beschouwing van SNA hanteert. Er dient derhalve voor gewaakt te worden deze matrix als limitatief en universeel toepasbaar te zien.

De in de matrix opgenomen risico's zijn gegroepeerd. Naast een globale groepering naar netwerkdefinitie en netwerkbesturing is daarbinnen een verdere verbijzondering toegepast. Deze verbijzondering sluit aan op de indeling van het vervolg van het artikel.

NETWERKDEFINITIE

Op het moment dat de in de bijlage beschreven risicomatrix is gecompleteerd met in de onderzoekssituatie onderkende specifieke risico's, heeft men een goed uitgangspunt ter beschikking voor het beoordelen van de kwaliteit van het desbetreffende SNA-netwerk.
Voor de uitvoering van de beoordeling zelf is het noodzakelijk, als afgeleide van elk onderkend aandachtsgebied, eerst de controledoelstelling te formuleren en vervolgens na te gaan welke maatregelen door de organisatie zijn genomen om de desbetreffende risico's tot aanvaardbare proporties terug te brengen.
Per aandachtsgebied zal worden ingegaan op relevante aspecten en maatregelen om de kwaliteit van de netwerkdefinities te waarborgen. Eveneens zal worden aangegeven op welke wijze inzicht verkregen kan worden in de actuele stand van zaken.

In dit artikel worden de volgende risicogebieden met betrekking tot de SNA-netwerkdefinitie onderkend:

1. functionele configuratie van het SNA-netwerk;
2. netwerktoegang;
3. cross-domain-verkeer;
4. SNA Network Interconnect (SNI);
5. single-points-of-failure;
6. switched lines;
7. dynamic reconfiguration;
8. dataset-beveiliging;
9. beheer van VTAM en NCP;
10. VTAM- en NCP-definitieprocedures;
11. uitwijkprocedures.

De aandachtsgebieden 1 tot en met 8 zijn direct te relateren aan relevante gebieden van de VTAM-definities; de aspecten 9 tot en met 11 zijn, ten aanzien van die definities, procedureel van aard.

1. Functionele configuratie van het SNA-netwerk

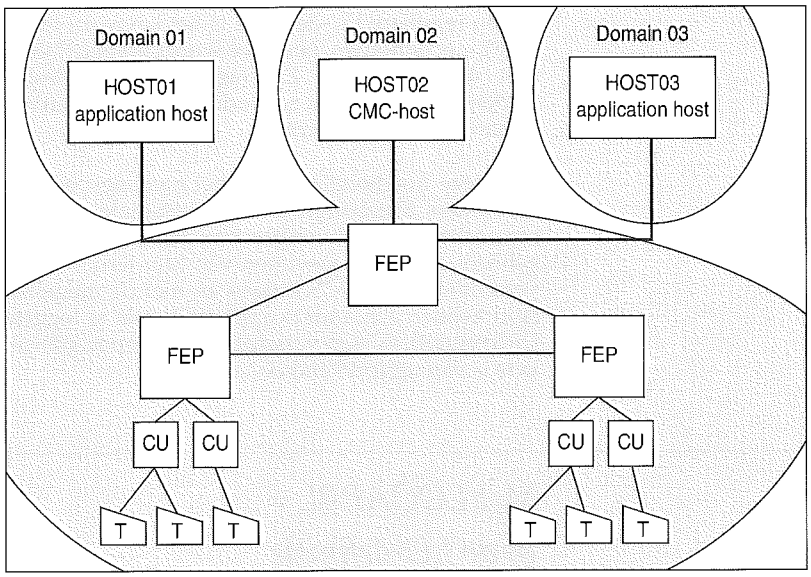
Controledoelstelling:
Stel vast dat de functionele configuratie is afgestemd op de eisen van de organisatie in termen van beheersbaarheid van het netwerk.

De eerste stappen die een auditor zal nemen bij de audit van een SNA-netwerk zullen met name gericht zijn op het verkrijgen van een goed beeld van aard, omvang en specifieke kenmerken van het te beoordelen netwerk. Maar er komt een moment dat men de fraai-ogende kleurenplot, die iedere zichzelf respecterende netwerkorganisatie met gepaste trots zal presenteren, achter zich moet laten. Tijd om eens een kijkje te nemen in VTAM, om te zien hoe dat netwerk nu feitelijk tot stand komt.

Een goed startpunt - op de grens van oriënteren en onderzoeken - is dan het beoordelen van een aantal factoren die wij samenvatten onder de naam 'functionele configuratie', onder de veronderstelling van een multi-domain-situatie. Met betrekking tot de VTAM-definities gaat het dan met name om de verdeling van de VTAM-structuur over de aanwezige domains en de daarmee bepaalde functionaliteit per VTAM.

Dit is van belang omdat hiermee de beheersbaarheid van het netwerk mede bepaald kan worden. Als voorbeeld noemen we het zogenaamde Communication Management Configuration (CMC)-concept. Hiervan is sprake als in een multi-domain-omgeving één host-VTAM eigenaar is van alle remote network resources. Deze host-VTAM wordt aangeduid als de CMC-host of network-host. Het remote gedeelte van het netwerk valt derhalve in zijn geheel binnen het domain van de CMC-host. Het grote voordeel van een dergelijke configuratie ligt op het vlak van netwerkbeheer; activiteiten op het gebied van probleem- en storingsafhandeling kunnen worden geconcentreerd rondom één VTAM. De overige hosts worden aangeduid als data-hosts, daar zij grotendeels ontlast zijn van het vervullen van netwerktaken, en zich met name kunnen richten op het beschikbaar stellen van applicaties en het verwerken van daartoe behorende gegevens. Een CMC-concept is geïllustreerd in figuur 2.

Een beeld van de bedoelde structuur wordt verkregen door na te gaan welke major nodes en welke NCP-definities iedere afzonderlijke VTAM activeert. In een CMC-situatie zal de CMC-host alle NCP-definities activeren. Voor de beeldvorming over de VTAM-structuur is ook de SOL van belang, omdat die iedere specifieke VTAM identificeert. Ook geeft de SOL aan tot welk netwerk de desbetreffende VTAM behoort.
Bij de audit kan tevens worden nagegaan of en zo ja, welke overwegingen de datacommunicatie-organisatie heeft gehanteerd bij het maken van een keuze met betrekking tot de structuur.



Figuur 2. CMC-structuur.
CU = Cluster controller
T = Terminal
FEP = Front End Processor

2. Netwerktoegang

Controledoelstelling:
Stel vast dat de relevante VTAM-definities een adequate bijdrage leveren aan de kwaliteit van het toegangspad van gebruikers tot onderliggende resources.

Naast de algemene functie die het SNA-netwerk ten behoeve van de datacommunicatie heeft, kan dit netwerk ook gezien worden als de eerste laag in het toegangspad van een gebruiker op weg naar de onderliggende opgeslagen gegevens; immers, de netwerktoegangswijze is medebepalend voor de toegang tot TP-software als IDMS/DC en CICS, editors als TSO, gebruikersapplicaties, en file access-software als VSAM en IDMS/DB.

In het navolgende wordt ingegaan op een viertal factoren die van invloed zijn op de wijze waarop gebruikers toegang tot het netwerk kunnen krijgen. Hier is onmiskenbaar het kwaliteitsaspect exclusiviteit aan de orde. Achtereenvolgens zullen worden besproken:
- de LOGAPPL-parameter;
- de USSTAB;
- de VTAM Session Management Exit (SME);
- de invloed van aanvullende netwerk(toegangs)produkten.

LOGAPPL

Een eerste vereiste voor een gebruiker die toegang wil verkrijgen tot het netwerk is dat deze de beschikking heeft over een terminal. Deze terminal moet binnen VTAM zijn gedefinieerd. Dit gebeurt door middel van een LU-definitie in het NCP-member van de communication controller waaraan de terminal (via cluster controller en links) fysiek is verbonden. Is de definitie niet opgenomen, dan is datacommunicatieverkeer niet mogelijk.

In een reguliere LU-definitie is het keyword LOGAPPL= opgenomen. Hiermee wordt gespecificeerd met welke primary LU (applicatie) de desbetreffende terminal, na activering, standaard en automatisch een sessie krijgt.

Met deze functionaliteit kan het toegangspad van gebruikers aanzienlijk worden versmald. Zo kan bijvoorbeeld afgedwongen worden dat bepaalde gebruikers na het aanzetten van hun terminal een verbinding met CICS krijgen en niet de mogelijkheid hebben aan andere applicaties aan te loggen. Differentiatie tussen verschillende groepen gebruikers is vanzelfsprekend ook mogelijk.

Met LOGAPPL = in de LU-definitie kan het toegangspad van gebruikers aanzienlijk worden versmald.

De auditor zal moeten nagaan op welke wijze van het LOGAPPL-keyword gebruik wordt gemaakt, en hoe dit het toegangspad van de gebruiker beïnvloedt. De specificatie van LOGAPPL zal altijd moeten worden bezien in relatie tot eventueel gebruikte netwerk(toegangs)produkten. De LU-definities in NCP geven de waarden van het LOGAPPL-keyword; de applicaties waaraan hiermee wordt gerefereerd, zijn als major nodes opgenomen in de SYS1.VTAMLST.

Unformatted System Services Table (USSTAB)
Unformatted System Services (USS) is een faciliteit die door VTAM aan terminals wordt geboden om 'unformatted' commando's om te zetten in 'formatted' (dat wil zeggen door VTAM interpreteerbare) commando's. Met name de wijze waarop wordt omgegaan met het LOGON-commando (het 'aanloggen' aan applicaties) wordt hierdoor bepaald. Tevens wordt USS gebruikt voor boodschapafhandeling. VTAM levert deze vorm van service met behulp van de USSTAB's, en wel op twee niveaus:

- *Session level-service;* deze service zorgt voor de commando- en boodschapafhandeling voor LU's. Commando-afhandeling wordt gebruikt als de eindgebruiker een logon- of logoff-request aan een applicatie doet. Boodschapafhandeling wordt gebruikt als VTAM boodschappen naar een LU stuurt.

- *Operation level-service;* deze service wordt gebruikt voor het afhandelen van operator-requests en de daaruit voortvloeiende berichtenstroom. Hiertoe dient in de member SYS1.VTAMLST (ATCSTRxx) de optie 'USSTAB=' te zijn opgenomen.

Voor beide soorten services levert IBM een default table mee: ISTINCDT voor session level en ISTINCNO voor operation level. Iedere LU is aan een USSTAB gekoppeld, waarbij het zonder meer mogelijk is in één netwerkomgeving meerdere USSTAB's te gebruiken, specifiek afgestemd op een bepaalde groep LU's.

De auditor zal in beschouwing moeten nemen welke functie de USSTAB in de netwerktoegang vervult. De inhoud van de USSTAB, die bestaat uit diverse mogelijke macro's, bepaalt of een gebruiker in staat wordt gesteld het VTAM-commando 'LOGON' uit te voeren, waarmee een sessie met een applicatie kan worden bewerkstelligd. De functie van de USSTAB zal altijd moeten worden bezien in relatie tot eventueel gebruikte netwerk-(toegangs)produkten.

Het risico dat een USSTAB in beginsel met zich meebrengt betekent tevens dat het beheer van de tabellen de toets der kritiek moet kunnen doorstaan. Er zal sprake moeten zijn van een adequate wijzigings- en toekenningsprocedure, waarbij wijzigingen van USSTAB's slechts door geautoriseerd personeel kunnen worden doorgevoerd. Tevens is een goede documentatie van de USSTAB's van belang.
De plaats van de load-module van de USSTAB is de SYS1.VTAMLIB. De wijze waarop een USSTAB is gekoppeld aan de terminal van een gebruiker kan worden nagegaan in de LU-definitie van de desbetreffende terminal in de NCP-definities.

VTAM Session Management Exit (SME)
De Session Management Exit (SME) is een exit-routine in VTAM die gebruikt kan worden ten behoeve van sessie-autorisatie en sessie-doorberekening. IBM levert met VTAM geen SME mee; de exit, indien wenselijk, moet expliciet gecodeerd worden.

Indien de exit gecodeerd is, geeft VTAM op diverse momenten tijdens de levensduur van een sessie gegevens door aan de exit-routine. Zo wordt tijdens het opzetten van een sessie informatie doorgegeven over de betrokken LU's. De exit kan zodanig worden gebouwd dat deze informatie wordt vergeleken met vooraf gedefinieerde LU-paren. Op basis van deze vergelijking kan vanuit de exit de opdracht aan VTAM gegeven worden om de sessie niet toe te staan.
Het is van belang dat de auditor nagaat of van de SME gebruik wordt gemaakt. De verplichte naam van de exit is ISTEXCAA. Indien gebruikt, is de module geplaatst in de SYS1.VTAMLIB. Als de vraag ten aanzien van het gebruik van de exit bevestigend kan worden beantwoord, moet een analyse plaatsvinden van de functionaliteit, en zal, waar nodig in overleg met systeemprogrammeurs, moeten worden nagegaan of de exit deze functionaliteit inderdaad levert. Aandacht zal tevens moeten uitgaan naar de wijze waarop de exit wordt beheerd: documentatie, testprocedures en wijzigingsbeheer moeten adequaat zijn.

Naast de SME biedt VTAM mogelijkheden voor gebruik van een separate Session Authorization Exit en een Session Accounting Exit. De (verplich-

te) namen voor deze exits zijn respectievelijk ISTAUCAT en ISTAUCAG. In de SME zijn de functies van deze exits gecombineerd en uitgebreid, en derhalve ligt het voor de hand slechts van de SME gebruik te maken. Mocht een situatie worden aangetroffen waarin de genoemde Session Authorization Exit en Session Accounting Exit toch worden gebruikt, dan gelden daarvoor uiteraard dezelfde controle-overwegingen.

De invloed van aanvullende netwerk(toegangs)-produkten
De wijze van initiële toegang tot het netwerk kan mede worden bepaald door aanvullende programmatuur, al dan niet met een primaire functie gericht op toegangscontrole. Ter illustratie gaan we kort in op twee voorbeelden van dergelijke software: SAMON en NetView/AS.

SAMON
SNA Application Monitor (SAMON) is een standaard IBM-produkt gericht op het ondersteunen van applicatietoegang en het 'monitoren' van de status van applicaties.
Voor wat betreft het koppelen van terminals aan applicaties fungeert SAMON als een gebruikersvriendelijk doorgeefluik. Op het moment dat een terminal wordt aangezet, verschijnen applicatiestatus-panels, waarin is weergegeven welke applicaties voorhanden zijn en wat hun status (actief/inactief) is. De gebruiker kan opgeven aan welke applicatie hij wil aanloggen; SAMON geeft deze informatie door aan de desbetreffende applicatie.
SAMON kan bijdragen aan beveiliging van de netwerktoegang door:
a. het gebruik van een network-password;
b. het gebruik van een terminal-password;
c. het gebruik van een user exit die wordt aangeroepen bij het aanloggen aan SAMON, waardoor een security-check kan plaatsvinden door een softwarematig beveiligingspakket.

SAMON heeft invloed op de manier waarop van LOGAPPL en USSTAB gebruik wordt gemaakt. Het neemt als het ware (een gedeelte van) de functies van de USSTAB over. Wil men bewerkstelligen dat iedere terminal meteen met SAMON wordt verbonden bij het aanzetten van het apparaat, dan moeten de LOGAPPL-keywords van terminal-LU's verwijzen naar SAMON.

NetView/AS
NetView/Access Services, lid van de uitgebreide IBM NetView-familie, biedt onder andere functionaliteiten op het gebied van netwerktoegang. Een eindgebruiker kan, op het moment van aanzetten van zijn of haar terminal, worden gevraagd zich te identificeren. Na validatie van deze identificatie in NetView/AS en eventueel een softwarematig beveiligingsprodukt als RACF of ACF2, worden de gebruiker, op basis van een gebruikersprofiel, die applicaties ter beschikking gesteld waartoe hij daadwerkelijk gerechtigd is.

Ook NetView/AS zal invloed hebben op de wijze waarop van USSTAB's en het LOGAPPL-keyword gebruik wordt gemaakt. Door een entry in de USSTAB kan worden bewerkstelligd dat een terminal te allen tijde eerst in NetView/AS terecht komt voordat een 'logon' aan andere applicaties kan plaatsvinden; door opname van een verwijzing naar NetView/AS in de LOGAPPL-keywords wordt de terminal direct na het aanzetten al met NetView/AS verbonden.

Door een entry in de USSTAB kan worden bewerkstelligd dat een terminal eerst in NetView/AS terecht komt.

3. Cross-domain-verkeer

Controledoelstelling:
Stel vast dat de manier waarop van cross-domain-verkeer gebruik wordt gemaakt in overeenstemming is met de eisen die - met name ten aanzien van exclusiviteit - aan het datacommunicatieverkeer gesteld (moeten) worden.

In een multi-domain-omgeving dient iedere VTAM te beschikken over een definitie van alle andere VTAM's in het netwerk waarmee gecommuniceerd moet worden. Dit wordt bewerkstelligd door het opnemen van Cross-Domain Resource Managers (CDRM's) in CDRM major nodes. De CDRM is dat gedeelte van VTAM dat functioneel zorg draagt voor cross-domain-communicatie. De CDRM is ook de eigenaar van de resources uit zijn domain. Iedere VTAM wordt in de CDRM major node(s) op de hoogte gesteld van het bestaan van elke andere CDRM waarmee communicatie mogelijk moet zijn. Bovendien bevat de CDRM major node een definitie van de eigen CDRM (host-CDRM).

Cross-Domain Resources (kortweg CDRSC's) zijn LU's (bijvoorbeeld applicaties en terminals) die zich in het domain van een andere VTAM bevinden. Om communicatie mogelijk te maken tussen resources in verschillende domains is het noodzakelijk dat, naast de definitie van het andere domain, ook de resources die tot dat domain behoren bekend worden gesteld aan de respectievelijke VTAM's. Grofweg kan dat op twee verschillende manieren gebeuren:

a. *Statische definitie* van CDRSC's, waarbij de resources uit een ander domain waarmee communicatie mogelijk moet zijn expliciet worden gedefinieerd (in CDRSC major nodes).

b. *Dynamische definitie* van CDRSC's, waarbij de resources uit een ander domain waarmee communicatie mogelijk moet zijn dynamisch gecreëerd worden op het moment dat die communicatie tot stand wordt gebracht.

Statische definities hebben als voordeel dat alleen die LU's die expliciet als CDRSC's gedefinieerd zijn, daadwerkelijk een SNA-sessie kunnen opbouwen. Het nadeel van deze opzet is de grotere inspanning die wordt gevergd zodra deze definities moeten worden opgebouwd en onderhouden. Dit nadeel ontbreekt bij dynamische definitie, en duidt dan ook op het voordeel van *dynamische definities*: een eenvoudiger beheer. Dit geldt met name bij grote, complexe netwerken met veel gebruikers. Het risico van onbeperkte dynamische definities is gelegen in het feit dat om het even welke LU een sessie kan aangaan met elke andere LU. Voorwaarde is wel dat de desbetreffende VTAM, als eigenaar van de LU, bekend is bij de host die het verzoek ontvangt.

Of dynamische definities mogelijk zijn wordt bepaald door parametersetting in de CDRM major nodes. Hierin komt, per CDRM, een tweetal parameters voor, te weten CDRDYN en CDRSC. CDRDYN (YES/NO), dat alleen relevant is voor de host-CDRM, geeft aan of de host-CDRM dynamische definities voor CDRSC's mag creëren. Dit geldt zowel voor een inkomend verzoek van een onbekende LU, als voor een uitgaand verzoek naar een onbekende LU. CDRSC (OPT/REQ), dat alleen relevant is voor een externe CDRM, geeft aan of die externe CDRM toestaat dat voor onder zijn beheer vallende CDRSC's dynamische entries worden gecreëerd.

De auditor zal moeten nagaan hoe op bovenstaande wijze aan cross-domain-verkeer vorm is gegeven. Het is niet goed mogelijk aan te geven in welke gevallen duidelijk wel, en in welke gevallen duidelijk niet voor statische definitie gekozen moet worden. Wel zal moeten blijken dat de netwerkorganisatie hier overwogen keuzen heeft gemaakt, en dat gelijksoortig cross-domain-verkeer op een gelijksoortige manier wordt geparametriseerd: een pleidooi voor het opstellen van standaarden is hier op zijn plaats. In geval van statische definities zal goede documentatie moeten worden aangelegd die inzicht geeft in de betekenis van gedefinieerde LU-namen.

4. SNA Network Interconnect (SNI)

Controledoelstelling:
Stel vast dat de manier waarop van SNI gebruik gemaakt wordt in overeenstemming is met de eisen die - met name ten aanzien van exclusiviteit - aan het datacommunicatieverkeer gesteld (moeten) worden.

Door middel van SNA Network Interconnect kunnen SNA-netwerken worden gekoppeld aan andere SNA- of non-SNA-netwerken. Waar het in de vorige paragraaf ging om inter-domain-datacommunicatie binnen hetzelfde netwerk, gaat het bij SNI om inter-netwerk-datacommunicatie. Een koppeling tussen twee netwerken wordt aangeduid met de term gateway. Hierbij is het mogelijk dat het beheer van het andere netwerk binnen dezelfde organisatie ligt, maar er kan uiteraard ook een verbinding zijn met een netwerk dat tot een andere organisatie behoort.

Hierin schuilt het risico met betrekking tot SNI: in het geval van een gateway naar een extern netwerk worden er verbindingen tot stand gebracht tussen 'eigen' LU's en 'vreemde' LU's, waarbij men overtuigd zal moeten zijn van de goede bedoelingen van de laatste categorie LU's.

In termen van VTAM- en NCP-definities wordt een gateway gecreëerd door het opnemen van de definities van:
a. een gateway-SSCP;
b. een gateway-NCP;
c. CDRM major nodes.

De gateway-SSCP, die zorg draagt voor initiëring, beëindiging en routering van SNI-sessies, is herkenbaar aan de parameterwaarde GWSSCP=YES in de SOL van de desbetreffende VTAM. De gateway-NCP assisteert de gateway-SSCP in sessie-afhandeling en vormt in feite de koppeling tussen de twee verbonden netwerken. Gateway-NCP's zijn herkenbaar aan de aanwezigheid van de GWNAU-macro, en de operands GWCTL en NETID in de NCP-definities (om precies te zijn: in de PCCU-macro). We willen hier wijzen op de mogelijkheid van een zogenaamde 'back to back'-gateway: hiervan is sprake als gateway-NCP's in verschillende netwerken van elkaar gescheiden worden door een tussenliggend netwerk dat geen SSCP's bevat (vaak aangeduid met de term 'dummy network' of 'null-network'). Deze constructie zorgt voor een grote mate van onafhankelijkheid tussen de verbonden netwerken, een eenvoudiger beheer, en een betere beheersbaarheid (bijvoorbeeld de controle op operator-activiteiten). Figuur 3 laat een schematische voorstelling zien van een 'back to back'-gateway.

Ook in een SNI-situatie dient VTAM te beschikken over een definitie van VTAM's in andere netwerken waarmee gecommuniceerd moet worden. Dit wordt, net als bij cross-domain-verkeer, gerealiseerd door definitie van cross-domain resource managers. Gezien het karakter van SNI als een bijzondere vorm van cross-domain-verkeer, verschilt de werking van de CDRDYN- en de CDRSC-parameter niet van de situatie beschreven in de vorige subparagraaf.

De auditor zal zich moeten richten op een inventarisatie van aard en omvang van SNI in het onderzochte netwerk. Functionaliteit van gateways zal beschreven moeten zijn, evenals implementatie- en parametrisatiestandaarden die gehanteerd moeten worden bij creatie van een gateway. Voor de CDRM- en CDRSC-definitie gelden dezelfde overwegingen als bij cross-domain-verkeer, met dien verstande echter dat het zeer wel mogelijk is dat bij een SNI-koppeling met een extern netwerk stringentere eisen worden gesteld aan het cross-domain-verkeer. Immers, men kan hier geconfronteerd worden met een gekoppeld netwerk dat buiten het eigen beheersgebied valt, en op de kenmerken waarop men slechts (zeer) beperkt zicht heeft. Mogelijkerwijs kent het gekoppelde netwerk meerdere SNI-verbindingen, die van invloed (zouden moeten) zijn op de eisen die aan de SNI-koppeling gesteld worden.

5. Single-points-of-failure

Controledoelstelling:
Stel vast dat het netwerk voldoende waarborgen biedt ten aanzien van de beschikbaarheid van het datacommunicatieverkeer bij het uitvallen van kritische knooppunten.

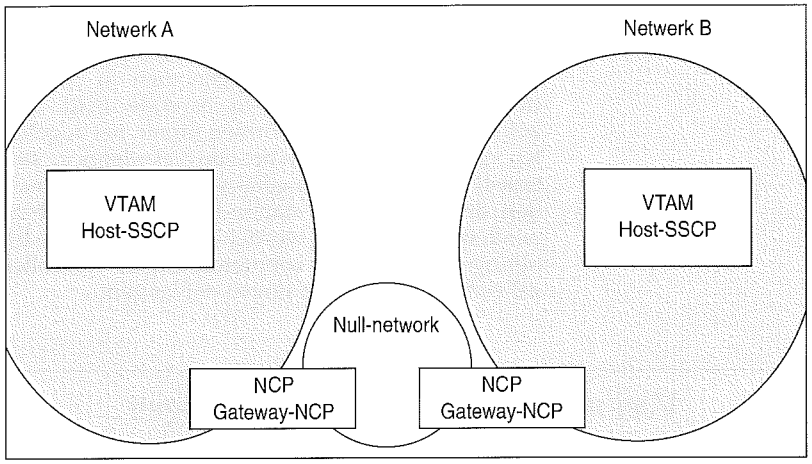
Met het oog op de netwerkbeschikbaarheid zal tijdens het ontwerpen van een netwerk rekening moeten worden gehouden met het voorkómen van kritische single-points-of-failure. Dit zijn plaatsen in het netwerk (bijvoorbeeld FEP's) waar convergentie van het lijnverkeer optreedt, waardoor het uitvallen van dat netwerkknooppunt voor zeer grote problemen kan zorgen.
In de praktijk zal het vermijden van dergelijke single-points-of-failure veelal neerkomen op de mogelijkheid om het dataverkeer binnen het netwerk alternatieve routes aan te bieden. Binnen een SNA-netwerk is dit bijvoorbeeld mogelijk door middel van een netwerktopologie waarbij de FEP's onderling meervoudig zijn verbonden. Hiermee wordt bedoeld dat elke FEP door middel van ten minste twee aparte fysieke lijnen verbonden is met ten minste twee andere fysiek en geografisch gescheiden FEP's. Daarnaast is het een kwestie van definities om te zorgen dat elke FEP in staat is te communiceren via de alternatieve routes.

Om te kunnen beoordelen in welke mate het optreden van single-points-of-failure in de netwerktopologie wordt vermeden, zal de auditor zich aanvankelijk kunnen richten op de al eerder genoemde fraaie kleurenplot van het netwerk; dit moet echter gebeuren in combinatie met een beschouwing van de hoeveelheid en aard van de gegevens die bepaalde knooppunten in het netwerk passeren. Dit laatste bepaalt immers hoe kritisch een knooppunt werkelijk is.

Om in de definities te kunnen verifiëren dat de single-points-of-failure tot een aanvaardbare hoeveelheid teruggebracht zijn, moet de aandacht uitgaan naar PATH-statements in VTAM en NCP. Hierbinnen worden onder meer zowel de fysieke verbindingen (explicit routes) als logische verbindingen (virtual routes) aangegeven. Hoewel een meervoudige verbinding hier gedefinieerd wordt, zegt de aanwezigheid van meerdere explicit routes niets over de aanwezigheid van fysieke lijnverbindingen. De aanwezigheid daarvan kan de auditor vaststellen door overzichten uit netwerkbesturingssoftware (zoals NetView), die informatie kunnen geven waaruit het daadwerkelijk gebruik van een lijn blijkt.

In de SYS1.VTAMLST-members met NCP-code zijn van elke FEP-subarea de overige subarea's opgenomen die door de desbetreffende FEP bereikt kunnen worden; door middel van een cross-reference kan worden vastgesteld dat de desbetreffende subarea's elkaar kunnen benaderen.

Overigens dient men zich te realiseren dat separate fysieke verbindingen tussen FEP's op verschillende locaties niet hoeft te betekenen dat deze verschillende lijnen niet (deels) door dezelfde kabelgoot lopen. PTT Telecom geeft over de mate van fysieke scheiding in het algemeen geen garanties af; verdere afspraken hieromtrent zijn echter niet onmogelijk. Ook dit aspect kan zeer wel een aandachtspunt voor de auditor zijn.



Figuur 3. Back to back-gateway, null-network.

6. Switched lines

Controledoelstelling:
Stel vast dat de definitie van switched lines binnen het SNA-netwerk adequaat is in relatie tot de eisen op het gebied van exclusiviteit en doelmatigheid.

Bij datacommunicatie binnen een netwerk kan gebruik worden gemaakt van vaste huurlijnen of switched lijnen. Bij een switched (geschakelde) verbinding kan het circuit dat wordt gebruikt om de verbinding tot stand te brengen, bij elke nieuwe verbinding variëren. Deze switched lijnen zijn doelmatig bij verbindingen waarbij aantal, tijdsduur en frequentie van sessies moeilijk op voorhand voorspelbaar zijn of grote fluctuaties vertonen. Worden eenmaal geschakelde verbindingen gebruikt, dan moet het netwerk per definitie als 'open' worden beschouwd en ontstaat het risico dat onbevoegden zich toegang verschaffen tot het netwerk c.q. tot geautomatiseerde informatiesystemen.

Gedurende het onderzoek moet de auditor aandacht schenken aan de mate waarin gebruik wordt gemaakt van switched lijnen. Ten behoeve van elke afzonderlijke switched lijn dient een major node-definitie (VBUILD TYPE=SWNET) te worden opgenomen in de NCP-definities in de SYS1.VTAMLST. Binnen deze major nodes worden de minor nodes gedefinieerd. Elke fysieke unit (bijvoorbeeld een cluster controller) wordt geïdentificeerd door middel van een PU-statement; het kiesnummer waarover het contact tot stand kan worden gebracht moet worden beschreven met behulp van PATH-definities. Terminals en applicaties worden gedefinieerd door middel van LU-statements.

Veel meer dan bij vaste verbindingen moet bij switched lines aandacht worden besteed aan identificatie en authenticatie. Binnen SNA wordt hier-

toe een mogelijkheid geboden door twee eXchange-ID (XID)-parameters. Deze parameters, IDBLK en IDNUM, zijn opgenomen in de PU-definitie van een SWNET-major node. Beide zijn hexadecimale codes en vormen samen het zogeheten station-ID. Komen in het netwerk identieke station-ID's voor die zich gelijktijdig bij VTAM melden, dan zal alleen de station-ID die als eerste binnenkomt door VTAM worden geaccepteerd. De bij het tweede station-ID behorende cluster controller zal vervolgens foutmeldingen ontvangen.

Veel meer dan bij vaste verbindingen moet bij switched lines aandacht worden besteed aan identificatie en authenticatie.

De door de netwerkbeheerder gehanteerde procedure voor het toekennen van de station-ID's zal object van onderzoek moeten zijn, waarbij de nadruk moet worden gelegd op de waarborgen met betrekking tot de uniciteit van de station-ID's.

Daarnaast zal erop moeten worden toegezien dat eenmaal geschakelde verbindingen na het beëindigen van een sessie niet onnodig actief blijven, en dat sessies niet in stand blijven na het verbreken van een verbinding. Het in stand blijven van een sessie houdt een risico in ten aanzien van de exclusiviteit, terwijl door het actief blijven van de verbinding onnodige lijnkosten worden veroorzaakt. De (optionele) parameter in een SWNET-major node die bepaalt of een geschakelde verbinding wordt verbroken na het beëindigen van een sessie is DISCNT= (default: NO). Afhankelijk van de gebruikersomgeving zal moeten worden overwogen of de verbinding na de laatste LULU-sessie in stand moet blijven en weer opnieuw kan worden gebruikt of moet worden verbroken (DISCNT= YES). Of een sessie wordt afgesloten nadat een verbinding verbroken is, hangt af van het karakter van de LU's die aan de sessie deelnemen. Sommige applicaties beëindigen een sessie op het moment dat de verbinding verbroken wordt, andere houden de sessie in stand.

Speciale aandacht zal moeten uitgaan naar de maatregelen die door de datacommunicatie-organisatie zijn getroffen op het gebied van (aanvullende) inkiesbeveiliging. Hierbij kan gedacht worden aan voorzieningen (bijvoorbeeld *dial-back modems* en gespecialiseerde inkiesbeveiligingsapparatuur/programmatuur), waarmee zekerheid kan worden verkregen over de locatie en identiteit van een inkiezende gebruiker. De auditor zal moeten vaststellen of en zo ja, in welke mate hiervan gebruik wordt gemaakt. Vervolgens zal de toereikendheid van de procedures rondom die aanvullende voorzieningen moeten worden beoordeeld: met name de autorisatieprocedure van functionarissen voor het gebruik van inkiesverbindingen en het beheer van de identificatiegegevens en telefoonnummers zijn hier van belang.

7. Dynamic reconfiguration

Controledoelstelling:
Stel vast dat dynamic reconfigurations uitsluitend door daartoe bevoegde functionarissen, en op een juiste en controleerbare wijze, kunnen worden uitgevoerd.

De VTAM- en NCP-definities zijn in beginsel statisch. Aangebrachte wijzigingen worden pas tijdens de periodieke initialisatie van VTAM en generatie van NCP actief. Toch zijn er mogelijkheden om dynamisch veranderingen aan te brengen in het - conform de netwerkdefinitie opgebouwde - netwerk. Dynamic reconfiguration (DR) biedt onder andere de gelegenheid dynamisch PU's en LU's te verwijderen of toe te voegen.

Er zijn twee manieren om DR uit te voeren. De eerste is die waarbij de aan te brengen wijzigingen in een DR-major node in de SYS1.VTAMLST worden geplaatst, en door middel van een VTAM-commando (VARY NET, DRDS) worden geactiveerd. Indien de tweede manier wordt gehanteerd, is die expliciete opname van de DR in een major node niet noodzakelijk; door middel van het VTAM-commando MODIFY DR wordt de wijziging direct doorgevoerd.

Door het ad hoc-karakter van deze faciliteit en het feit dat dergelijke wijzigingen vaak tijdens probleemsituaties en onder tijdsdruk worden uitgevoerd, bestaat het risico dat er onjuiste dan wel ongeautoriseerde wijzigingen op de VTAM/NCP-definities plaatsvinden. Bovendien kan de controleerbaarheid van uitgevoerde DR beperkt zijn; dynamische wijzigingen worden teniet gedaan door een nieuwe VTAM-initialisatie en NCP-generatie.

De auditor moet zich richten op de geldende voorwaarden om DR te mogen en kunnen doorvoeren. Dit betekent, naast aandacht voor toegang tot de SYS1. VTAMLST (zie de volgende subparagraaf), tevens een analyse en beoordeling van autorisaties om de activerende VTAM-commando's te gebruiken. Hierbij is het zeer wel denkbaar dat ook gebruikte netwerkbeheersoftware zoals NetView in de beschouwing moet worden betrokken. De procedure rondom het doorvoeren van DR moet beschreven zijn, en waarborgen dat toepassing van DR controleerbaar blijft. Bovendien moet ervoor worden gezorgd dat DR-wijzigingen die een permanent karakter hebben, hun weg vinden naar een permanente wijziging in de VTAM- en NCP-definities.

8. Dataset-beveiliging

Controledoelstelling:
Stel vast dat de exclusiviteit van de VTAM- en NCP-definities gewaarborgd is.

In voorgaande subparagrafen is ingegaan op enkele aspecten van de netwerkdefinitie in VTAM en NCP. Duidelijk is dat deze definities bepalend zijn

voor de functionaliteiten van het netwerk. Het is dan ook van het grootste belang dat voorkomen wordt dat ongeautoriseerden wijzigingen in de definities - en daarmee in de netwerkfunctionaliteiten - aanbrengen.

De auditor zal moeten vaststellen dat toegangsmogelijkheden op de libraries en datasets waarin de definities zijn vervat, beperkt zijn tot geautoriseerd personeel. Om dit te realiseren zal in de meeste gevallen gebruik worden gemaakt van de diensten van een pakket voor logische toegangsbeveiliging, zoals RACF, ACF2 of TOP SECRET. Tijdens een SNA-audit is een zijstapje naar deze programmatuur dan ook noodzakelijk om de daar gedefinieerde toegangsregels aan een kritische blik te onderwerpen. De meest kritische datasets zijn de SYS1.VTAMLST en de SYS1.VTAMLIB. Toegang tot deze datasets zal voorbehouden moeten zijn aan die functionarissen van de datacommunicatieorganisatie die het technisch beheer voeren over VTAM (zie hierna) en die volgens de VTAM- en NCP-definitieprocedure zijn aangewezen om wijzigingen daadwerkelijk aan te brengen.

9. Beheer van VTAM en NCP

Controledoelstelling:
Stel vast dat het beheer van VTAM en NCP in het geheel van netwerkbeheeractiviteiten een plaats heeft, en dat binnen dat beheer voldoende aandacht is besteed aan functiescheiding.

Over de beheeraspecten van een netwerk zijn vele artikelen geschreven. We willen dat werk hier niet nog eens overdoen, maar volstaan met een opsomming van de ons inziens belangrijkste taken op het gebied van netwerkbeheer:

a. Het, binnen het kader aangegeven door datacommunicatiebeleid, formuleren en vaststellen van functionaliteits-, kwaliteits- en prestatiecriteria[1] waaraan het netwerk dient te voldoen.

b. Het (technisch optimaal) realiseren van een netwerk dat voldoet aan de geformuleerde criteria.

c. Het structureel bewaken van de functionaliteit, de kwaliteit en de prestatie van het netwerk, en het doorvoeren van verbeteringen als aan de geformuleerde criteria niet wordt voldaan.

Het beheer van VTAM en NCP, als onderdeel van netwerkbeheer, ligt met name op het gebied van de ad b. genoemde taak. Ten aanzien van het VTAM- en NCP-beheer moet een onderscheid worden gemaakt in *functioneel beheer* en *technisch beheer*.

Bij *functioneel beheer* gaat het met name om de uitvoering van taken die waarborgen dat hantering van VTAM en NCP geschieden op een wijze die in het verlengde ligt van de geformuleerde criteria.

Gedacht kan worden aan:
- het opstellen van definitieprocedures;
- het initiëren van wijzigingen in de definities;
- het formuleren van standaarden met betrekking tot bepaalde definities (zoals netwerktoegang, gateways, cross-domain-verkeer, cross-network-verkeer, etc.);
- het toezien op een juiste wijze van VTAM- en NCP-gebruik.

Bij *technisch beheer* gaat het met name om het daadwerkelijk hanteren van VTAM en NCP ter realisatie van de geformuleerde criteria.

Gedacht kan worden aan:
- het aanbrengen van wijzigingen in VTAM en NCP;
- het geven van technische adviezen;
- het zorg dragen voor de technische beschikbaarheid van VTAM en NCP;
- het installeren en testen van nieuwe versies/releases;
- het bij voortduring bewaken van het functioneren van het netwerk en het opheffen van storingen.

Het is ons inziens van belang dat een dergelijke functiescheiding, al dan niet met gebruik van de termen technisch en functioneel beheer, duidelijk herkenbaar en operationeel is. Hiermee kan namelijk in belangrijke mate worden gerealiseerd dat de technische realisatie van het netwerk aansluit op de wensen en eisen van de organisatie. Ontbreekt een dergelijke structuur, dan bestaat het risico dat technisch-operationeel personeel functionele zeggenschap over het netwerk heeft, waarbij de gewenste scheiding tussen beschikkende en uitvoerende functie verloren gaat.

Inzicht in beheerstructuren zal moeten worden verkregen uit interviews met functionarissen uit de datacommunicatie-organisatie, en het inventariseren en beoordelen van organisatie- en taak/functie-beschrijvingen, procedures en handboeken.

10. VTAM- en NCP-definitieprocedures

Controledoelstelling:
Stel vast dat de procedures met betrekking tot VTAM- en NCP-definitie adequaat zijn, waardoor de integriteit van de definities gewaarborgd is en blijft.

De definities in VTAM en NCP zullen aan veranderingen onderhevig zijn. De redenen hiervoor zijn talrijk en kunnen variëren van de realisatie van een nieuwe gateway met een netwerk van een andere organisatie, tot het koppelen van een terminal aan een nieuwe medewerker. In het algemeen zullen de wijzigingen in het 'remote' gedeelte van het netwerk (veel) talrijker zijn dan wijzigingen in het 'local' gedeelte.

Belangrijk is dat de organisatie heeft voorzien in een goede procedure, die de integriteit en autorisatie van deze wijzigingen waarborgt. Een wijziging in de definities mag slechts voortvloeien uit technische en/of functionele noodzakelijkheid, en deze aansluiting moet uit een registratie blijken. Daarnaast is het belangrijk dat de functioneel beheerder autorisatie geeft voor het aanbrengen van wijzigingen, en dat deze autorisatieverlening achteraf zichtbaar gemaakt kan worden. Vanuit zijn functionele verantwoordelijkheid zal de functioneel be-

1 Wellicht wekt deze formulering verbazing; immers, ook 'functionaliteit' en 'prestatie' kunnen worden gezien als onderdeel van een ruim kwaliteitsbegrip. Het is echter onze ervaring dat in een netwerkomgeving vaak specifiek aandacht wordt besteed aan functionaliteitseisen ('X.25-verkeer moet ondersteund worden') en prestatie-eisen ('de beschikbaarheid van het netwerk moet 99,9% bedragen'), maar dat kwaliteitsaspecten als 'exclusiviteit' en 'integriteit' weinig expliciete aandacht krijgen of als onuitgesproken randvoorwaarden aanwezig worden verondersteld. De gehanteerde formulering is een pleidooi voor het tot uitdrukking brengen van criteria naar deze kwaliteitsinvalshoek.

heerder moeten toezien op een juiste handelwijze met betrekking tot de VTAM- en NCP-definities.

Het activeren van (gewijzigde) definities vindt veelal plaats door netwerk-operators. Ook de procedures in deze operationele beheeromgeving moeten door de auditor in beschouwing worden genomen. De aanwezigheid en het gebruik van instructies met een juiste inhoud en een goede mate van detail moeten waarborgen dat VTAM en NCP op een correcte wijze en met een goede periodiciteit geactiveerd worden. Voor een goede gang van zaken is het vereist dat de netwerk-operators tijdig op de hoogte worden gesteld van relevante wijzigingen. Zo zal duidelijk moeten zijn welke NCP's, vanwege aangebrachte wijzigingen, opnieuw geactiveerd moeten worden.

Om de aanwezigheid en toereikendheid van deze procedures te kunnen beoordelen is de auditor met name aangewezen op interviews met het betrokken personeel, en op handboeken, procedures en instructies in schriftelijke vorm.

11. Uitwijkprocedures

Controledoelstelling:
Stel vast dat is voorzien in procedures, scenario's en instructies die waarborgen dat de beschikbaarheid van de netwerkdefinities gewaarborgd is.

Binnen de procedures die een organisatie hanteert om de beschikbaarheid van de geautomatiseerde informatievoorziening conform gestelde eisen te garanderen, zullen uitwijkprocedures een voorname rol spelen. Dat hierbij ook aandacht moet uitgaan naar beschikbaarheidsaspecten van datacommunicatie is vanzelfsprekend.

Specifiek met het oog op netwerkdefinities zou een calamiteit kunnen betekenen dat het netwerk geheel of gedeeltelijk verlamd is omdat VTAM niet beschikbaar is. De gevolgen hiervan kunnen variëren van het niet beschikbaar zijn van een aantal applicaties tot het uitvallen van het gehele netwerk. Zeker in een CMC-configuratie is de beschikbaarheid van de CMC-host een zeer kritische factor voor het functioneren van het 'remote' netwerkgedeelte.

In termen van netwerkdefmitie zal de organisatie moeten zorg dragen voor maatregelen waardoor de functies van een niet-beschikbare VTAM kunnen worden overgenomen door een andere VTAM. Dit kan voor een belangrijk deel worden gerealiseerd door te zorgen voor de aanwezigheid van 'slapende' definities; in het geval van CMC kan men denken aan de aanwezigheid van een kopie van de VTAM- en NCP-definities van de CMC-host op een andere host. Gaat de CMC-host onverhoopt 'down', dan kan de netwerkfunctie worden overgenomen door de 'uitwijk'-host door het activeren van de tot dan toe 'slapende' definities.

De auditor zal moeten nagaan welke maatregelen geformuleerd zijn om bij calamiteiten de totstandbrenging en instandhouding van het netwerk te waarborgen. Dit betekent een inventarisatie en beoordeling van calamiteiten- en uitwijkprocedures, met name waar het gaat om netwerkuitwijkscenario's. De aanwezigheid van 'slapende' definities kan eenvoudig worden bepaald aan de hand van de inhoud van de SYS1.VTAMLST. Ook zal vastgesteld moeten worden dat netwerk-operations de beschikking heeft over duidelijke instructies die in het geval van netwerkuitwijk moeten worden gevolgd. Testverslagen moeten antwoord geven op de vraag of de toereikendheid van netwerkuitwijk is beproefd.

NETWERKBESTURING: DE ROL VAN NETVIEW

Controledoelstelling:
Stel vast dat de toegang tot NetView en de toekenning van NetView-bevoegdheden aan functionarissen adequaat zijn.

In de vorige paragraaf is uitgebreid aandacht besteed aan de netwerkdefinitie met behulp van VTAM en NCP, op basis van de gedachte dat hiermee de basis wordt gelegd voor de functionaliteit - en daarmee de kwaliteit - van het SNA-netwerk. Heeft men eenmaal de beschikking over een operationeel netwerk, dan zal moeten worden gezorgd voor de *instandhouding* van dat netwerk conform geformuleerde criteria. Dit kan worden aangeduid met de term netwerkbesturing, en richt zich met name op:
- het voortdurend bewaken van de werking van datacommunicatieprogrammatuur en -apparatuur ('monitoring');
- het nemen van correctieve maatregelen in geval van storingen en knelpuntsituaties.

NetView

In de begindagen van SNA was de situatie dat de netwerkbesturing voor het belangrijkste deel werd uitgevoerd door middel van VTAM. VTAM-consolemeldingen gaven de netwerk-operators een beeld van de status van het netwerk, en met behulp van VTAM-commando's kon worden ingegrepen in die status. De plaats waar die netwerkbesturing plaatsvond lag in het hart van het rekencentrum, waardoor fysieke beveiliging een belangrijke rol speelde.

De groeiende complexiteit van SNA-netwerken bracht echter gaandeweg de noodzaak aan het licht van een krachtige centrale faciliteit waarmee netwerkbesturing ook in zeer uitgebreide en complexe netwerkomgevingen doelmatig en doeltreffend kon worden uitgevoerd. Halverwege de jaren tachtig introduceerde IBM het produkt NetView, als een geïntegreerd geheel van netwerkbesturingsprodukten. Het biedt zowel monitorfaciliteiten als zeer krachtige functies om in het netwerk in te grijpen. Aandacht voor de beveiliging van een dergelijk produkt is dan ook van belang.

Twee zaken zullen in de beschouwing van

NetView-beveiliging zeker een rol moeten spelen [Frin93]:
- de toegang tot NetView zelf;
- de wijze waarop van de interne autorisatiestructuren van NetView gebruik is gemaakt voor het afschermen van kritische commando's en functies.

In het navolgende zal op deze aspecten worden ingegaan.

Toegang tot NetView

Toegangsmogelijkheden tot NetView dienen in de eerste plaats binnen het pakket zelf gedefinieerd te worden. Iedere gebruiker - in NetView-termen een 'operator' - moet bekend gemaakt worden met een operator-identifier en een operator-password. De passwords zijn opgeslagen in leesbare vorm; geen ideale situatie. Derhalve dient te worden gezorgd voor een toegangsvalidatie, die voor het belangrijkste deel plaatsvindt in toegangsbeveiligingsprogrammatuur. Gebruikt men RACF (en is dit aan NetView bekend gemaakt) dan zal toegangsvalidatie plaatsvinden op basis van de passwords vastgelegd in dat produkt. Bij het gebruik van andere toegangsbeveiligingsprogrammatuur is men aangewezen op het hanteren van NetView-exits om een zelfde validatie te realiseren; een beoordeling van die exits is dan noodzakelijk.

De plaats waar de NetView-operator-definities, inclusief de passwords, geplaatst zijn, is de dataset met de naam DSIOPF.

NetView-autorisatiestructuur

In DSIOPF worden aan iedere NetView-operator een of meer profielen (profiles) toegekend. Een profiel kan worden gezien als een verzameling autorisaties, waarbij die autorisaties op twee aspecten betrekking hebben:
- bevoegdheden voor het gebruik van commando's (scope classes);
- bevoegdheden ten aanzien van resources (span of control).

Profielen
Ieder profiel staat in een separaat profielbestand. Ter illustratie een voorbeeld van de definitie van een profiel met de naam PROFIELA:

```
PROFIELA   PROFILE
           AUTH       CTL=SPECIFIC
           DOMAINS    CNM01
           SPAN       SPAN1,SPAN2
           OPCLASS    3,4
```

Het AUTH-definitie-statement geeft aan voor welke netwerk-resources operators aan wie dit profiel is toegekend, commando's kunnen geven. CTL= SPECIFIC, in combinatie met DOMAINS CNM01, geeft aan dat dit beperkt is tot resources in het domain met de naam CNM01. De andere mogelijke waarde, CTL=GLOBAL, geeft aan dat commando's gegeven kunnen worden voor alle resources.

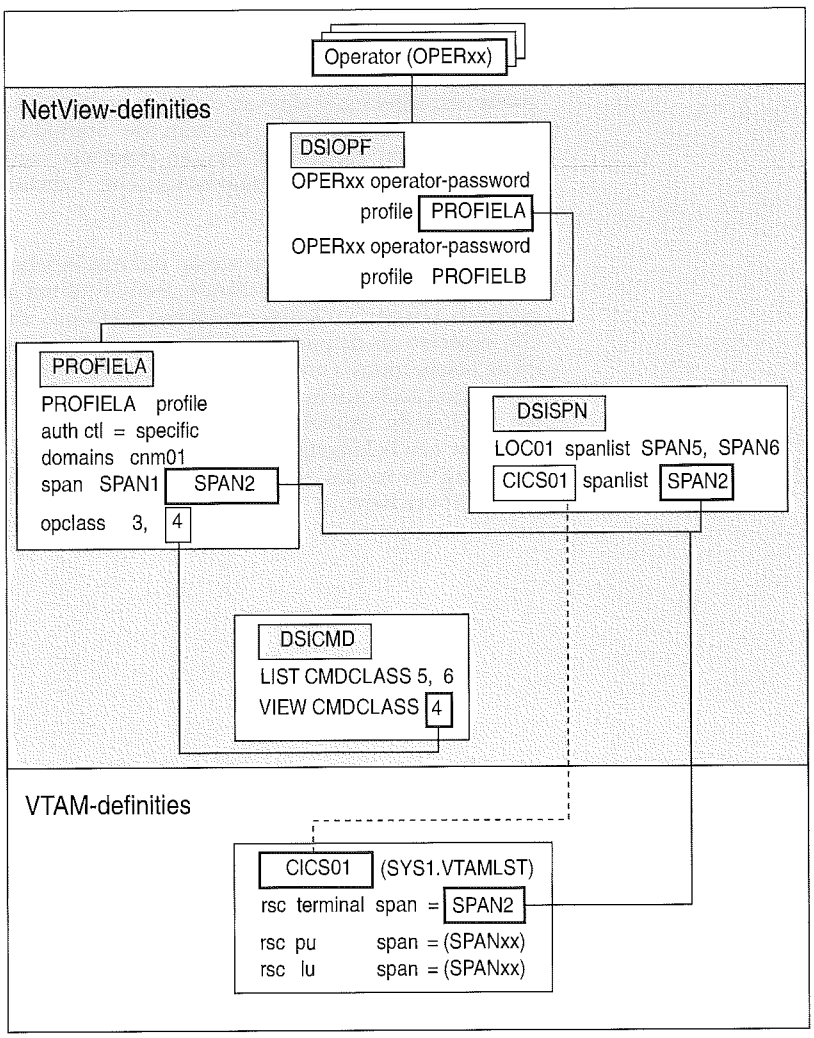
Het SPAN-statement geeft in bovenstaand voorbeeld aan dat operators met dit profiel de beschikking hebben over de spans of control met namen SPAN1 en SPAN2. Aan deze spans kunnen bepaalde specifieke resources worden gekoppeld. OPCLASS geeft aan dat een operator met dit profiel de beschikking heeft over de scope classes 3 en 4. Aan deze scope classes kunnen bepaalde commando's worden gekoppeld.

Span of control
We zullen nu, aan de hand van het bovenstaande profielvoorbeeld, aangeven hoe aan de spans SPAN1 en SPAN2 resources kunnen worden gekoppeld. Dit gebeurt in de SPANLIST-statements in de dataset DSISPN. Hierin staat bijvoorbeeld:

```
LOC01      SPANLIST    SPAN5,SPAN6
CICS01     SPANLIST    SPAN2
```

Hier wordt de major node met naam CICS01 gekoppeld aan SPAN2. CICS01 valt nu binnen de span of control van het profiel PROFIELA, en daarmee binnen de span of control van de gebruiker

Figuur 4. NetView-autorisatiestructuur.



M.M. Buijs RI en E.J.M. Ridderbeekx RE RI zijn werkzaam als EDP-auditor bij het Ministerie van Defensie.

aan wie dit profiel wordt toegekend. De application major node LOC01 valt buiten de span of control. Overigens betekent het feit dat een major node binnen de span of control van een gebruiker valt, niet dat tevens de onderliggende minor nodes dat ook doen. Hiervoor zal een SPAN=-statement moeten worden opgenomen bij de definitie van de major nodes zelf.

Scope class
Ten slotte: de koppeling van commando's aan scope classes. Dit gebeurt door CMDCLASS-statements in de dataset DSICMD. Bijvoorbeeld:

```
LIST      CMDCLASS   5,6
VIEW      CMDCLASS   4
```

Dit statement geeft aan dat het NetView LIST-commando is gekoppeld aan de scope classes 5 en 6. Vanwege OPCLASS 4 is een gebruiker met het profiel PROFIELA gerechtigd om het VIEW-commando uit te voeren; het commando LIST mag door diezelfde operator niet worden gebruikt.

De NetView-autorisatiestructuur zoals die hierboven uiteengezet is, is in figuur 4 nogmaals schematisch weergegeven.

Beschikkend over kennis van de werking van NetView-autorisatiestructuren zal de auditor moeten nagaan welke autorisaties aan welke functionarissen zijn toegekend. De koppeling van scope classes en spans of control aan operators dient een goede afspiegeling te zijn van de verantwoordelijkheden en bevoegdheden die aan de betrokken functionarissen toegekend zijn, en moet een verlengstuk vormen van organisatorische functiescheidingen.

Volledigheidshalve merken we op dat met een beschouwing van het bovenstaande geen invulling is gegeven aan een volledige audit van NetView. Zo zijn aspecten als de parametrisering van het pakket en de afscherming van kritische datasets niet expliciet in de beschouwing betrokken. We hopen echter voldoende duidelijk te hebben gemaakt dat NetView een belangrijk hulpmiddel is bij netwerkbesturing en in die zin bij een SNA-audit zeker aandacht verdient.

SLOTOPMERKINGEN

In de inleiding van dit artikel gaven we aan dat niet alle mogelijke facetten van een SNA-audit zouden worden besproken. Gezien de toch niet geringe omvang van het artikel kan men zich ongeveer voorstellen wat een allesomvattende audit aan aandachtspunten zou opleveren. Dit is illustratief voor datacommunicatie in het algemeen en SNA in het bijzonder: het is uitgebreid, complex, en naar zeer veel verschillende gezichtspunten benaderbaar. Een audit die zich in eerste instantie richt op de VTAM- en NCP-definities kan ons inziens valkuilen voorkomen; zo'n audit is afgebakend, uitvoerbaar, maar vooral ook zinvol.

LITERATUUR

[Paan91] R. Paans en H. de Lange, *Auditing the SNA/SNI Environment*, Computers & Security, vol. 10 (3), mei 1991.

[Frin93] H. Frints, *The MVS Environment*, in: Ernst & Young, *A Practical Approach to Logical Access Control*, McGraw-Hill, 1993.

[Rana89] J. Ranade en G. Sackett, *Introduction to SNA Networking using VTAM/NCP*, McGraw-Hill, 1989.

[Rana91] J. Ranade en G. Sackett, *Advanced SNA Networking*, McGraw-Hill, 1991.

Risicomatrix SNA-netwerkdefinitie en-besturing

(B=beschikbaarheid, I=integriteit, E=exclusiviteit, C=controleerbaarheid, DM=doelmatigheid, DT=doeltreffendheid)

risico	kwaliteitsaspect						getroffen maatregelen
	B	I	E	C	DM	DT	
FUNCTIONELE CONFIGURATIE							
Beheersbaarheid van het netwerk laat te wensen over					*	*	
NETWERKTOEGANG							
LOGAPPL laat toegangspad te ruim			*				
USSTAB laat toegangspad te ruim			*				
Beheer en toekenning USSTAB voldoen niet			*		*		
Functionaliteit SME voldoet niet			*				
Beheer SME voldoet niet			*		*		
Aanvullende produkten beïnvloeden toegangspad negatief			*				
CROSS-DOMAIN-VERKEER							
Ongeautoriseerde sessie-opzet tussen cross-domain LU's			*				
Geen standaarden voor parameter-settings		*	*	*			
Integriteit statische definities niet vaststelbaar		*		*			
SNA NETWORK INTERCONNECT (SNI)							
Ongeautoriseerde sessie-opzet tussen cross-netwerk LU's			*				
Functionaliteit gateways niet gedocumenteerd			*	*			
Geen implementatie- en parametrisatiestandaarden voorhanden		*	*	*			
Integriteit statische definities niet vaststelbaar		*		*			
SINGLE-POINTS-OF-FAILURE							
Kritische knooppunten niet logisch en fysiek meervoudig onderling verbonden	*						
SWITCHED LINES							
Ongeautoriseerd netwerkverkeer via geschakelde verbindingen			*				
Uniciteit station-ID's niet gegarandeerd			*				
Sessie blijft in stand na verbreken verbinding			*				
Verbinding blijft in stand na beëindigen sessie					*		
DYNAMIC RECONFIGURATION							
Ongeautoriseerde aanpassingen in het netwerk			*				
Onjuiste aanpassingen in het netwerk		*					
Aanpassingen in het netwerk niet controleerbaar				*			
Aanpassingen met blijvend karakter worden niet overgenomen in definities	*	*					
DATASET-BEVEILIGING							
Ongeautoriseerde benaderingen van definitiegegevens			*				
BEHEER VAN VTAM EN NCP							
Beheer VTAM en NCP sluit niet aan op overkoepelend netwerkbeheer						*	
Onduidelijkheid in verantwoordelijkheidstelling t.a.v. beheer					*	*	
Technisch beheer bepaalt de functionaliteit van het netwerk		*	*		*	*	
VTAM- EN NCP-DEFINITIEPROCEDURES							
Definitiewijzigingen niet integer		*					
Integriteit definitiewijzigingen niet vaststelbaar		*		*			
Ongeautoriseerde wijzigingen in de definities			*				
Autorisatie van definitiewijzigingen niet vaststelbaar		*		*			
Activering VTAM/NCP niet adequaat	*					*	
UITWIJKPROCEDURES							
Geen uitwijk/calamiteitenprocedure en bijbehorende instructies voorhanden	*						
Toereikendheid procedures niet getest	*						
`Slapende' definities niet aanwezig	*						
NETWERKBESTURING MET NETVIEW							
Ongeautoriseerde netwerkbesturingsactiviteiten	*	*	*				

BIJLAGE

In de cellen van de matrix is door middel van een asterisk aangegeven op welk kwaliteitsaspect een risico met name van invloed is.

Beveiliging van analoge kieslijnen

Drs.ing. D. Brouwer RE

Analoge kieslijnen bieden op beveiligingsgebied een groot aantal mogelijkheden. Deze lijnen verzorgen een verbinding op de fysieke laag, waarvoor een groot aantal relatief goedkope beveiligingshulpmiddelen beschikbaar is, zoals modems met encryptiefaciliteit en dial-back-apparaten.
De auteur, datacommunicatiespecialist en thans werkzaam als EDP-auditor, behandelt op systematische wijze de risico's van analoge kieslijnverbindingen en de te treffen maatregelen, en presenteert een uitgewerkte auditaanpak.

INLEIDING

In Compact 1993/1 is stilgestaan bij de beveiliging van digitale kieslijnen. Zoals daar reeds is gesignaleerd, zal het belang van analoge kieslijnen afnemen ten gunste van het gebruik van digitale kieslijnen. Bij de tegenwoordige stand van de techniek wordt het begrip kieslijnen nog in eerste instantie geassocieerd met telefoonlijnen die met gebruikmaking van modems worden toegepast voor datacommunicatiedoeleinden. Hoewel digitale lijnen zonder twijfel de toekomst hebben zal voor kieslijnen toch nog geruime tijd gebruik worden gemaakt van 'gewone' analoge lijnen. Bij veel 'nieuwe' ontwikkelingen, zoals telewerken, het verlenen van stand-by hulp vanaf de thuislocatie en remote access tot LAN-omgevingen, wordt dan ook gebruik gemaakt van telefoonlijnen. Redenen hiervoor zijn onder meer dat een zeer groot aantal telefoonaansluitingen voorhanden is en dat ook over telefoonlijnen door het beschikbaar komen van nieuwe modulerings- en datacompressietechnieken aanzienlijke overdrachtssnelheden kunnen worden gehaald.

Dit artikel behandelt de risico's die verbonden zijn aan het gebruik van telefoonlijnen voor datacommunicatiedoeleinden en de daartegen te treffen beveiligingsmaatregelen. Voor een goed begrip van de aan het gebruik van openbare telefoonnetwerken verbonden risico's zal allereerst aandacht worden besteed aan de topologie van het openbare telefoonnetwerk en de tijdens de verbindingsopbouw te onderscheiden fasen. Na een inventarisatie van de risico's zal vervolgens worden ingegaan op de mogelijke beveiligingsmaatregelen. Hierbij zal ook worden stilgestaan bij de beveiligingsmaatregelen die getroffen kunnen worden tijdens het proces van datacommunicatie. Tot slot zullen de relevante auditaspecten worden behandeld.

ANALOGE KIESLIJNEN

Oorspronkelijk is het telefoonnetwerk een circuit-switching netwerk, dat wil zeggen dat een apart circuit wordt gereserveerd voor de opgebouwde verbinding. Dit circuit staat niet ter beschikking voor andere verbindingen. Voor de duur van het gesprek blijft het circuit onveranderd. Voor een goed begrip van de opbouw van een dergelijk circuit is het noodzakelijk een globale beschrijving te geven van het openbare telefoonnetwerk.

Opbouw van het openbare telefoonnetwerk

De globale opbouw van het openbare telefoonnetwerk is weergegeven in figuur 1 [Dirk86, Heij86].

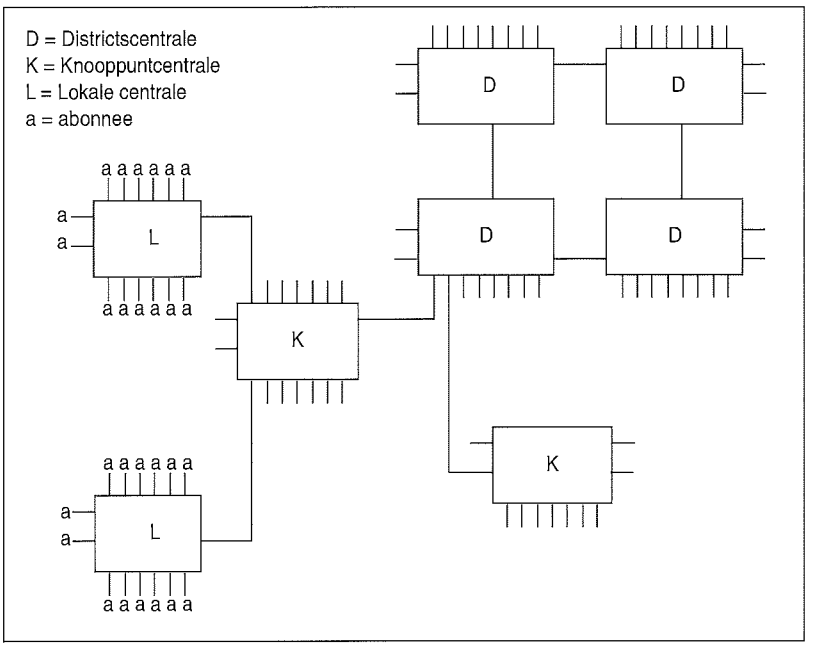
Zoals uit figuur 1 blijkt is het openbare telefoonnetwerk hiërarchisch opgebouwd; het hart wordt gevormd door de districtscentrales. Deze centrales zijn maasvormig met elkaar verbonden, alle overige verbindingen zijn stervormig. Ieder district is opgedeeld in maximaal tien sectoren. Elke sector heeft een zogenaamde knooppuntcentrale. Voor één van de sectoren is de knooppuntcentrale opgesteld ter plaatse van de districtscentrale. Op een knooppuntcentrale kunnen maximaal tien lokale centrales worden aangesloten, waarvan wederom één ter plaatse van de knooppuntcentrale. Iedere abonnee is door middel van een vaste verbinding verbonden met een lokale telefooncentrale.
Voorgaande beschrijving is een vereenvoudigde weergave. Zo komen in werkelijkheid ook dwarsverbindingen voor tussen districts- en knooppuntcentrales en knooppuntcentrales onderling. Daarnaast bestaan er ook eindcentrales, wijkcentrales en hoofdwijkcentrales. Bovendien bestaat het openbare telefoonnetwerk niet meer als een afzonderlijke c.q. geïsoleerde infrastructuur maar wordt op onderdelen gebruik gemaakt van de infrastructuur van digitale netwerken. Dit is onder meer mogelijk gemaakt door de toepassing van digitale telefooncentrales.

De oorspronkelijke opbouw van het telefoonnet is nog steeds terug te vinden in het netnummer. Bijvoorbeeld Zelhem heeft als netnummer 08342. Dat houdt in dat vanuit een ander district eerst een 0 wordt gekozen. Met 83 wordt het district Arnhem gekozen. De 4 geeft de vierde knooppuntcentrale in dat district aan, namelijk in de sector Doetinchem. De 2 geeft de tweede lokale centrale aan, te weten die in Zelhem.

Verbindingsopbouw

Bij het opbouwen van een telefoonverbinding voor datacommunicatiedoeleinden kunnen de volgende fasen worden onderscheiden:

– *Opbouw van de fysieke verbinding*
Hiermee wordt bedoeld de opbouw van de verbinding via het fysieke medium; in feite is dit de opbouw van de telefoonverbinding.



Figuur 1. Globale opbouw van het openbare telefoonnetwerk.

– *Opbouw van de modemverbinding*
Hiermee wordt bedoeld de opbouw van de verbinding tussen de modems van de host-computer en de gebruiker via het verzenden van de door de modems gehanteerde draaggolf.

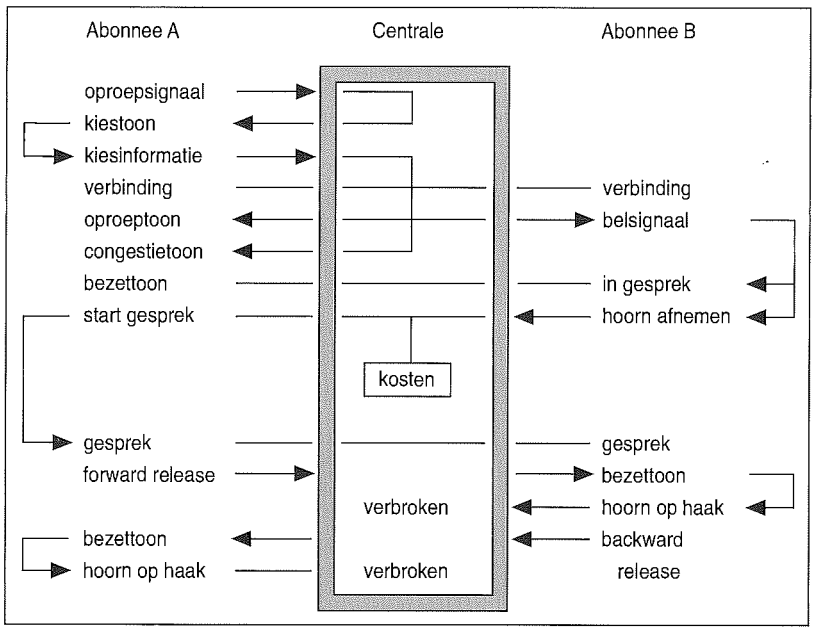
– *Opbouw van de logische verbinding*
Hieronder wordt verstaan het opbouwen van de eigenlijke sessie met de host-computer. Deze start in de meeste gevallen met de uitwisseling van identificatiegegevens (user-id/password).

Na beëindiging van het eigenlijke datacommunicatieproces dient de verbinding in omgekeerde volgorde te worden afgebouwd.

De fasen van de verbindingsopbouw zullen hierna nader worden toegelicht.

Opbouw van de fysieke verbinding
Bij het opbouwen van de fysieke verbinding wordt de eigenlijke telefoonverbinding tot stand gebracht. Het netwerk dat hiervoor wordt gebruikt, wordt het spreekwegennetwerk genoemd. Dit netwerk wordt bestuurd door het besturingsnetwerk bestaande uit apparatuur en programmatuur. Het besturingsnetwerk verzorgt de volgende acties:
- het activeren van een oproep;
- het zenden van kiesinformatie;
- het kiezen van de gewenste abonnee;
- het genereren van een belsignaal;
- het reageren op de 'in gesprek'-toon;
- registratie van de kosten.

De besturing bij een telefoonverbinding kent een aantal signalen. Deze worden hierna behandeld aan de hand van een gesprek tussen twee abonnees die zijn aangesloten op dezelfde centrale (zie figuur 2) [Dirk86].



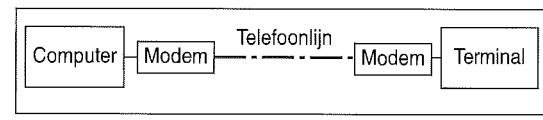
Figuur 2. Verbindingsopbouw.

Stel abonnee A wenst een gesprek met abonnee B. A neemt de hoorn van de haak. Hiermee geeft hij aan de centrale te kennen dat hij een gesprek met een andere abonnee wenst. Het toestel van A verzendt het *oproepsignaal*. De centrale antwoordt met het zenden van de *kiestoon* naar A. A kan hierna aan de centrale het nummer van abonnee B kenbaar maken. Als abonnee B is aangesloten op een andere centrale moet eerst het netnummer kenbaar worden gemaakt. De kiesinformatie (het nummer van de gewenste abonnee) wordt in de centrale verwerkt en een geschakelde verbinding wordt tussen de twee abonnees opgebouwd. Door middel van het *belsignaal* wordt abonnee B geactiveerd. Tegelijkertijd ontvangt A de *oproeptoon*. Hierdoor weet A dat B wordt opgeroepen.
Indien B al in gesprek is ontvangt A de *bezettoon*. Als de centrale de verbinding met B niet tot stand kan brengen ontvangt A de *congestietoon*. Als B de hoorn van de haak neemt is de telefoonverbinding tot stand gekomen en zal de registratie van de kosten starten ten laste van A. Het gesprek kan worden beëindigd door de hoorn op de haak te leggen. Als dit door A gebeurt, wordt dit de forward release genoemd. B ontvangt dan de bezettoon. Indien B de verbinding beëindigt wordt dat de backward release genoemd en ontvangt A de bezettoon. Bij bepaalde typen oude telefooncentrales is de verbinding pas geheel verbroken als beide abonnees de hoorn op de haak hebben gelegd!

Opbouw van de modemverbinding

Het openbare telefoonnetwerk is aangelegd voor de overdracht van analoge signalen met een frequentie tussen 400 en 3400 Hz. Deze bandbreedte is voldoende voor een herkenbare overdracht van spraakverkeer. Voor de overdracht van digitale signalen is zij echter ongeschikt omdat hierbij sprake is van blokvormige pulsen. Deze blokvorm kan door het telefoonnetwerk niet onvervormd worden verwerkt. Om toch overdracht van digitale signalen mogelijk te maken wordt gebruik gemaakt van modulators en demodulators. Een modulator zet een digitaal signaal om in een analoog signaal volgens een bepaalde modulatietechniek. In geval van frequentiemodulatie kan gebruik worden gemaakt van twee frequenties waarbij bijvoorbeeld een sinusvormig signaal van 1300 Hertz een binair '0' signaal representeert en een sinusvormig signaal van 2100 Hertz een binair '1' signaal.
De demodulator zet het analoge signaal weer om in het oorspronkelijke digitale signaal. Hierbij is het dus wel noodzakelijk dat modulator en demodulator gebruik maken van dezelfde (de)modulatietechniek. De modulatie- en demodulatiefunctie zijn ondergebracht in één apparaat: de modem. Deze modem wordt aangesloten op de telefoonlijn. In het meest eenvoudige geval gebeurt dat door de steker van de telefoon uit de contactdoos te trekken en de speciale telefoonsteker/contrasteker van de modem hiertussen te plaatsen. De digitale uitgang van de modem wordt verbonden met een computer of terminal.

Teneinde communicatie tussen een terminal en een computer via het openbare telefoonnetwerk mogelijk te maken is dan minimaal de configuratie nodig van figuur 3.



Figuur 3. Minimaal benodigde configuratie voor datacommunicatie tussen terminal en computer.

Intern is de modem via een zogenaamde line-coupler met de telefoonlijn verbonden. Een in de modem ingebouwd relais bepaalt of deze line-coupler is doorverbonden met het telefoontoestel of de computer respectievelijk de terminal. Een handmatige opbouw van de verbinding kan plaatsvinden doordat de gebruiker van terminal A met zijn telefoon het nummer kiest van de telefoon opgesteld bij de computer. Nadat de telefoonverbinding tot stand is gekomen zoals beschreven in de voorgaande subparagraaf, geeft de gebruiker aan de modem de opdracht om de telefoonlijn door te schakelen naar de termimal door een knop in te drukken die veelal is aangeduid met de term 'data'. De modem van de terminal reageert door een draaggolf op de telefoonlijn te zetten. De opgeroepen abonnee hoort nu een constante fluittoon en kan handmatig de computermodem in de stand 'data' zetten. De modems zullen vervolgens de 'trainingsfase' doorlopen. Hierbij wordt automatisch uitgeprobeerd wat de hoogst mogelijke lijnsnelheid is die kan worden gehaald, welke datacompressietechniek kan worden gebruikt, etc. Een en ander is afhankelijk van de gebruikte modems en de lijnkwaliteit. Indien de computermodem een zelfde modulatietechniek ondersteunt als de terminalmodem kunnen beide modems met elkaar com-

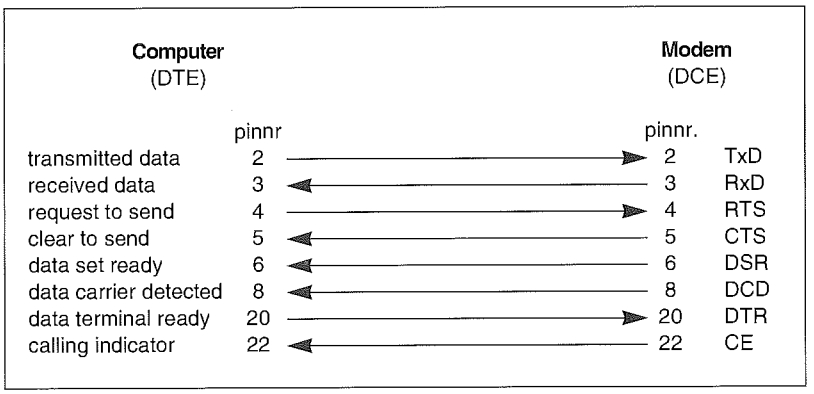
municeren en wordt de modemverbinding tot stand gebracht. Data welke wordt ingebracht op de terminal zal nu via de telefoonlijn worden aangeboden aan de computer.

Bovenstaand is een zeer eenvoudige methode van verbindingsopbouw beschreven. In de praktijk wordt meestal geautomatiseerd een verbinding opgebouwd. De modem van de terminal kan over een dusdanige intelligentie beschikken, dat vanaf de terminal naar de modem een commando kan worden gestuurd, gevolgd door een telefoonnummer. Hierna zal de modem volautomatisch de handelingen uitvoeren voor het 'opnemen van de hoorn' (de modem gaat off-hook) en het verzenden van de kiesinformatie. Ook kan de modem aan de computerzijde zodanig worden geïnstalleerd dat bij detectie van een belsignaal een draaggolf op de lijn wordt gezet (Automatic Answer-faciliteit) en geprobeerd wordt een verbinding op te bouwen. Natuurlijk moeten de zendende en de ontvangende modem wel een zelfde modulatietechniek hanteren anders kan geen modemverbinding worden opgebouwd. Voor het geautomatiseerd opbouwen van een verbinding kan de modem hardwarematig en softwarematig worden aangestuurd. Veelal geschiedt dit met behulp van de V.24-interface respectievelijk besturingscommando's volgens de Hayes-commandoset. Dit wordt hieronder nader toegelicht.

De V.24-interface
De V.24-interface is door CCITT (Comité Consultatif International Télégraphique et Téléphonique) ontworpen voor de communicatie tussen een DTE en een DCE. Deze afkortingen staan voor respectievelijk Data Terminal Equipment (computer, PC of terminal) en Data Circuit terminating Equipment (modem).

De V.24-interface maakt gebruik van 25 lijnen welke onder andere worden gebruikt voor de verzending van data-, besturings- en statussignalen. De lijnen worden wel aangeduid met de term 'circuits'. De uit het oogpunt van controle en beveiliging relevante circuits zijn weergegeven in figuur 4. Deze circuits kunnen alleen juist werken indien tussen DTE en DCE de juiste bekabeling wordt gebruikt (dat wil zeggen geen zogenaamde doorlussingen toepassen!).
De pijlen geven de richting van het signaal aan, een → betekent een signaal van DTE naar modem, een ← van modem naar DTE.

Aan de rechterzijde in figuur 4 zijn de afkortingen van de interface-signalen vermeld zoals die worden gehanteerd in de RS232C-norm van de EIA (Electronic Industries Association). De normen RS232C en V.24 zijn nagenoeg identiek. In figuur 5 wordt de betekenis van de interface-signalen kort omschreven.
De V.24-interface biedt mogelijkheden tot automatisch beantwoorden van een oproep. Indien de modem via het activeren van het CE-signaal aan de DTE te kennen geeft dat een belsignaal wordt ontvangen, kan de DTE het DTR-signaal actief maken. De modem zal dan off-hook gaan zodat de modemverbinding kan worden opgebouwd.



Figuur 4. Relevante circuits van de V.24-interface.

TxD = **Transmitted data**
de te verzenden (dat wil zeggen aan de modem aangeboden) data

RxD = **Received data**
de ontvangen data (dat wil zeggen de data die van de modem naar de DTE gaat)

RTS = **Request To Send**
de DTE geeft hiermee aan de modem te kennen data te willen verzenden

CTS = **Clear To Send**
de modem geeft hiermee aan de DTE te kennen dat hij gereed is de data te ontvangen

DSR = **Data Set Ready**
de modem geeft hiermee aan dat hij gereed is om aan het data-communicatieproces deel te nemen

DCD = **Data Carrier Detected**
de modem geeft hiermee aan dat van een remote modem een draaggolf wordt ontvangen van voldoende kwaliteit

DTR = **Data Terminal Ready**
de DTE geeft hiermee aan dat hij gereed is om aan het datacommunicatieproces deel te nemen

Figuur 5. Korte omschrijving relevante V.24-signalen.

Voor het automatisch versturen van de kiesinformatie is een apart apparaat benodigd, de zogenaamde ACU (Automatic Calling Unit). In de praktijk wordt echter gebruik gemaakt van modems met ingebouwde dial-mogelijkheid. Deze dial-mogelijkheid wordt veelal aangestuurd via de Hayes-commandoset.

Hayes-commandoset
De facto-standaard voor besturing van de modem vanaf de DTE is die van de fabrikant Hayes [B1]. Hayes-compatible modems beschikken over faciliteiten om het gehele proces van verbindingsopbouw onder besturing van DTE-commando's te laten plaatsvinden. De functionaliteit van deze modems is namelijk niet alleen beïnvloedbaar door middel van de V.24-besturingssignalen maar ook door middel van het versturen van commandostrings. De volledige Hayes-set bestaat uit een

Commando's van DTE naar modem:

AT C0	Signaal DCD is altijd actief
AT C1	Signaal DCD werkt volgens V.24-standaard
AT DTxxx	Kies telefoonnummer xxx met tooncode
AT DPxxx	Kies telefoonnummer xxx met pulscode
AT H0	Ga on-hook
AT H1	Ga off-hook
AT A	Activeer Automatic Answer mode
AT \Txx	Verbreek automatisch de verbinding indien gedurende xx minuten geen lijnactiviteit wordt waargenomen

Meldingen van modem naar DTE:

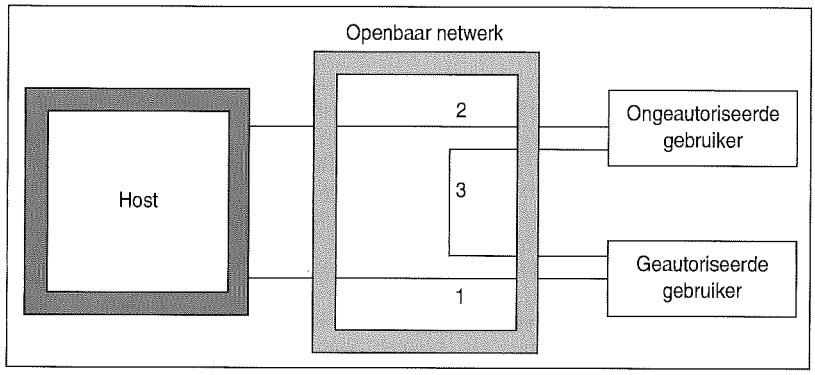
OK	Opdracht is succesvol uitgevoerd
CONNECTxxxx	Verbinding is tot stand gebracht op een snelheid van xxxx bps
RING	Er wordt een belsignaal ontvangen
BUSY	Gekozen telefoonnummer is bezet
NO ANSWER	Remote modem neemt de lijn niet op

Figuur 6. Relevante Hayes-commando's en -meldingen.

veertigtal commando's van DTE naar modem en een twintigtal terugmeldingen van modem naar DTE. Voor ons doel zijn relevant de commando's waarmee de line-coupler kan worden bestuurd en ingesteld. Deze commando's alsmede de meldingen welke betrekking hebben op de verbindingsopbouw staan vermeld in figuur 6.

Automatische opbouw van een modemverbinding tussen twee Hayes-compatible modems is mogelijk door de modems met behulp van een programma aan te sturen. Indien zich bijvoorbeeld een bepaalde gebeurtenis voordoet of een bepaald tijdstip is bereikt, kan het programma de modem opdracht geven het telefoonnummer xxx te kiezen door middel van het commando AT DTxxx. Indien de remote modem in Automatic Answer mode staat zal de modemverbinding zonder tussenkomst van de remote DTE worden opgebouwd. Staat de remote modem niet in Automatic Answer mode dan kan de remote DTE na ontvangst van de string RING opdracht geven om off-hook te schakelen (commando ATH1). Nadat de modemverbinding tot stand is gebracht, versturen de modems naar hun DTE's de string CONNECTxxxx.

Figuur 7. Mogelijke verbindingsopbouw.



Opbouw van de logische verbinding
Na het tot stand komen van de telefoonverbinding met de opgeroepen abonnee en de modemverbinding dient nog de logische verbinding tot stand te worden gebracht. Hiermee wordt bedoeld dat toegang wordt verkregen tot een host via een identificatieprocedure. Hiervoor is het onder andere noodzakelijk dat door de terminal verzonden karakters door de computer juist worden geïnterpreteerd. Dit betekent dat dezelfde protocolinstellingen moeten worden gebruikt (ASCII/EBCDIC, synchroon/asynchroon, aantal databits, aantal stopbits, pariteitbit, etc.).

RISICO'S DATACOMMUNICATIE VIA HET OPENBARE TELEFOONNETWERK

Een situatieschets van de mogelijke verbindingsopbouw via het openbare telefoonnetwerk is gegeven in figuur 7. De cijfers geven de mogelijke verbindingen aan. De verbinding genummerd 1 is de enig gewenste verbinding, verbindingen 2 en 3 dienen te worden voorkomen.

Bij datacommunicatie via kieslijnen worden de volgende risico's gelopen:

a. *Passieve aanval*
   - a1 aftappen van gegevens
   - a2 analyseren van de berichtenstroom
     Hierbij wordt geanalyseerd wie naar welke bestemming gegevens verzendt. Overigens kan bij bijvoorbeeld militaire toepassingen het enkele feit dat berichtenverkeer plaatsvindt, al van betekenis zijn.

b. *Actieve aanval*
   - b1 wijzigen, verwijderen, toevoegen van berichten
   - b2 veranderen van het bronadres
   - b3 veranderen van het bestemmingsadres
   - b4 veranderen van de berichtenvolgorde
   - b5 herhalen van reeds verzonden berichten ('replay')
   - b6 repudiation

c. *Onjuiste verbindingsopbouw*
   - c1 onjuiste persoon
   - c2 onjuiste bevoegdheden
   - c3 onjuiste componenten
   - c4 onjuiste locatie
   - c5 onjuist tijdstip

d. *Onjuiste verbindingsafbouw*

Voor een nadere toelichting op de hier geschetste risico's wordt verwezen naar het reeds eerder ge-

noemde artikel over digitale kieslijnen in Compact 1993/1 en de literatuur [Brou92]. Op deze plaats wordt volstaan met de vermelding van een drietal kanttekeningen die specifiek gelden bij het gebruik van analoge kieslijnen.

Passieve en actieve aanval
Ten aanzien van de risico's a2 (analyseren van de berichtenstroom), b2 (veranderen van het bronadres) en b3 (veranderen van het bestemmingsadres) valt op te merken dat analoge kieslijnen in de meeste gevallen worden gebruikt voor point-to-point-verbindimgen waarbij de verbinding slechts voor één sessie wordt gebruikt. Het heeft dan geen zin om op dataniveau te zoeken naar eventuele bron- en bestemmingsadressen. Alleen in het geval de lijn wordt gebruikt voor meerdere parallelle sessies waarbij op dataniveau wordt aangegeven wat de bron en de bestemming zijn, heeft het voor een 'hacker' zin de adressering in de data te analyseren.

Onjuiste verbindingsopbouw
Ten aanzien van dit risico zijn twee aspecten specifiek het vermelden waard: de doorschakelfunctie en de 'perpetual dial-attack'.

– *Doorschakelfunctie:* Bij de nieuwere digitale centrales heeft de abonnee de mogelijkheid een telefoonnummer 'over te zetten'. Dat wil zeggen indien een nummer gebeld wordt en dit nummer is geprogrammeerd om een ander nummer te bellen, dan wordt automatisch dit andere nummer gebeld. Het overzetten van het telefoonnummer is voor de abonnee mogelijk voor zijn eigen toestel via de in juni 1991 landelijk geïntroduceerde Sterdienst Direkt Doorschakelen (de zogenaamde *21 dienst). Denkbaar is ook dat een ongeautoriseerd persoon voor korte tijd op de telefoonlijn inbreekt en de doorschakelfunctie activeert. Daarnaast wordt wel beweerd dat het doorschakelen voor de nieuwere digitale PTT-centrales ook mogelijk is met behulp van een speciale code die PTT Telecom niet naar buiten vrij geeft maar toch in sommige kringen bekend zou zijn! [Anch88]. Hiermee kan *elke willekeurige* aansluiting op de desbetreffende centrale worden overgezet. Deze functie is toegankelijk voor elke gebruiker van de desbetreffende centrale indien de code bekend is.

– *Perpetual dial-attack:* Indien bij het uitbellen niet eerst wordt gecontroleerd op de aanwezigheid van de kiestoon loopt men het risico dat de eigen uitbelactie nagenoeg samenvalt met een inbelactie van een ander. Dit is te vergelijken met het door de lezer wellicht ooit ervaren praktijkgeval waarbij u met het voornemen een bepaalde persoon te bellen de hoorn van de haak neemt en gelijk verbinding heeft met een persoon die even tevoren uw nummer heeft gedraaid. De verbinding is dan onmiddellijk tot stand gebracht. De hierboven geschetste situatie is niet geheel hypothetisch! Indien de telefoonnummers van de uitgaande lijnen bekend zijn kan een hacker via een computerprogramma constant deze nummers aankiezen net zolang totdat het door hem veroorzaakte belsignaal samenvalt met het off-hook gaan van de modem van de uitkieslijn [Corn87, Jaco85]. Deze methode wordt aangeduid met 'perpetual dial-attack'.

Onjuiste verbindingsafbouw
Normaal gesproken zal de verbinding als volgt worden afgebouwd: afbouw logische verbinding, afbouw modemverbinding en ten slotte afbouw telefoonverbinding. Stel nu echter dat de verbinding onjuist wordt afgebouwd (risico d), bijvoorbeeld omdat eerst de telefoonverbinding wordt afgebouwd. Ten aanzien van de modemverbinding levert dit in de meeste gevallen geen problemen op. Modem- en telefoonverbinding zijn bij de meeste typen modems inherent aan elkaar verbonden. Wegvallen van de telefoonverbinding heeft tot gevolg dat de modem geen draaggolf van de remote modem meer detecteert en daardoor off-line schakelt. De op de host gestarte applicatie hoeft echter niets te merken. In dat geval zal bij het weer tot stand komen van de modemverbinding tevens de logische verbinding worden opgebouwd 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 telefoonnetwerk kunnen worden getroffen. In de volgende paragrafen wordt een onderverdeling aangebracht naar de verschillende te onderscheiden fasen van verbindingsopbouw, datacommunicatiefase en verbindingsafbouw.

MAATREGELEN TIJDENS DE OPBOUW VAN DE FYSIEKE VERBINDING

In deze paragraaf zal een viertal beveiligingsmaatregelen worden besproken die toegepast kunnen worden tijdens de fase van het opbouwen van de fysieke verbinding.

Blokkering inkomend verkeer

Een methode om binnenkomend verkeer te weren is inschakeling van een externe organisatie, namelijk door aan PTT Telecom te vragen de desbetreffende lijn te blokkeren voor inkomend verkeer. Iemand die een dergelijk nummer probeert op te bellen zal geen verbinding krijgen maar ontvangt in dat geval een toon die aangeeft dat een niet bestaand nummer is gekozen.
Deze methode is alleen te gebruiken indien de lijn slechts voor uitgaand verkeer wordt gebruikt. Indien op het desbetreffende nummer ook moet kunnen worden ingebeld, is deze methode ongeschikt.

Blokkering voor inkomend verkeer geeft dus een

bescherming tegen het ongeautoriseerd opbouwen van een verbinding (risico c) ten gevolge van inbelacties. Overigens moet men, zoals reeds in de paragraaf over de risico's is aangegeven, tijdens de uitbelactie van de host bedacht zijn op eventuele doorschakelfuncties.

Bedrijfstelefooncentrale

Een tweede beveiligingsmethode is het gebruik van een bedrijfstelefooncentrale zoals een PABX (Private Automatic Branche eXchange). Indien een lijn alleen gebruikt wordt voor uitbellen, kan een PABX namelijk een soort inbelbeveiliging bieden. Maakt men gebruik van een PABX dan betaalt men aan PTT Telecom voor ieder duizendtal telefoonnummers, bijvoorbeeld voor de nummers 010 - 408 1000 tot en met 010 - 408 1999.
Intern in de PABX kunnen echter ook nummers buiten deze reeks worden geconfigureerd, bijvoorbeeld toestelnummer 3010. Een dergelijk toestel kan men niet rechtstreeks van buiten de PABX bellen, het nummer 010 - 408 3010 zal door PTT Telecom aan een andere abonnee zijn uitgegeven. Op het nummer kan dus niet worden ingebeld. Men kan echter vanaf een dergelijk toestel wel naar 'buiten' bellen.

PABX'en zijn gevoelig gebleken voor hack-praktijken.

Toch is een PABX niet aan te raden voor gebruik als intermediair voor datacommunicatielijnen. Zo is het voor de telefoniste mogelijk op een gesprek 'in te breken', zijn er interne mogelijkheden tot doorschakelen van de verbinding (onder andere follow-me-schakeling), etc. Bovendien zijn PABX'en zelf gevoelig gebleken voor hack-praktijken.

Dial-back-apparatuur

Een derde maatregel wordt aangereikt in de vorm van zogenaamde 'dial-back'-apparaten. Bij de meest eenvoudige vorm van een dial-back-apparaat wordt het belsignaal beantwoord door off-hook te gaan waarna onmiddellijk een backward release plaatsvindt. Vervolgens wordt weer off-hook gegaan en wordt de kiesinformatie op de lijn gezet van een vast geprogrammeerd telefoonnummer. Indien gebruik wordt gemaakt van dial-back-apparatuur resulteert een inbelpoging door een ongeautoriseerd persoon in een oproep van het vast geprogrammeerde telefoonnummer van de persoon die hiertoe wel is geautoriseerd.

Er zijn echter dial-back-apparaten geproduceerd die na de backward release en het weer off-hook gaan niet eerst controleren op de aanwezigheid van de kiestoon. De hacker tracht hiervan gebruik te maken door te proberen om door middel van de perpetual dial-attack de uitbelactie van de computer nagenoeg te laten samenvallen met zijn eigen inbelactie.

Ook kan de hacker het geluk hebben het nummer van de computerlijn te kunnen bellen via een oude centrale welke de verbinding pas definitief afbouwt indien aan beide zijden een release heeft plaatsgevonden [Corn87, Doug86, Jaco85]. Het simpelweg niet verbreken van de telefoonverbinding door de ongeautoriseerde beller resulteert dan eerst in de ontvangst van de door de computermodem verzonden kiesinformatie waarna vervolgens verbinding wordt verkregen met de computer!

Om dit probleem te ondervangen werden dial-back-apparaten aangeboden die na de backward release en het off-hook gaan eerst controleren of de kiestoon wordt ontvangen. Is dit laatste niet het geval dan wordt de dial-back-procedure afgebroken. Ook dit bracht geen afdoende beveiliging, aangezien slimme hackers ervoor zorgden om via een toongenerator de kiestoon te simuleren waarmee dus het dial-back-apparaat werd misleid [Corn87, Doug86, Jaco85].

De volgende beveiligingsstap was het gebruik van twee lijnen: een inkomende en een uitgaande lijn. Na detectie van het belsignaal op de inkomende lijn geeft het dial-back-apparaat een backward release en vervolgens wordt een vast nummer gekozen via een aparte uitgaande lijn.

Inmiddels is de functionaliteit van de dial-back-apparaten sterk uitgebreid en werkt de meest gebruikte dial-back-procedure volgens het volgende principe:

1. De gebruiker kiest het telefoonnummer waarmee men toegang krijgt tot het dial-back-apparaat.
2. Het dial-back-apparaat neemt op.
3. Het dial-back-apparaat vraagt de gebruiker om het unieke identificatie-nummer. Dit kan gebeuren door middel van een digitaal opgenomen en opgeslagen menselijke stem of met behulp van een auto-answer modem waardoor de dialoog door middel van een PC of asynchrone terminal kan plaatsvinden.
4. Wanneer het id-nummer in het dial-back-apparaat bekend is zoekt dit de bij het nummer behorende gegevens op.
5. Afhankelijk van de opgezochte gegevens, de beschikbaarheid van het computersysteem, terugbellijnen en modems, meldt het dial-back-apparaat aan de gebruiker dat hij wordt teruggebeld, in de wachtrij is geplaatst of wordt geweigerd.
6. Het dial-back-apparaat en de gebruiker verbreken nu de verbinding.
7. Indien de gebruiker geautoriseerd is tot toegang tot het computersysteem, belt het dial-back-apparaat de gebruiker terug en verbindt hem met de computer.

In de meer uitgebreide dial-back-systemen worden door de leveranciers drie soorten beveiliging onderscheiden [Geve90]: de primaire, secundaire en tertiaire beveiliging.

De primaire beveiliging is het feitelijke terugbelmechanisme zoals hiervoor beschreven. Dit biedt een bescherming tegen verbindingsopbouw door een ongeautoriseerde gebruiker (risico c1) en verbindingsopbouw vanaf een ongeautoriseerde locatie (risico c4). Overigens wordt geen harde bescherming verkregen omdat nog steeds de reeds aangegeven risico's worden gelopen ten gevolge van doorschakelen en de perpetual dial-attack.

De secundaire beveiliging is een authenticiteitscontrole waarbij gebruik wordt gemaakt van een challenge/response-systeem. Indien het dial-back-systeem op grond van de gebruikers-id ziet dat een challenge/response-procedure dient te worden uitgevoerd, zal het dial-back-apparaat een random getal genereren. Dit door de gebruiker ontvangen getal (de challenge) wordt als input gebruikt voor het berekenen van de response. Deze response wordt berekend met behulp van een algoritme waarbij de uitkomst mede wordt bepaald door een per gebruiker unieke en geheime sleutel. De response wordt vervolgens naar het dial-back-apparaat gestuurd en daar vergeleken met het resultaat zoals dat met behulp van de in het dial-back-apparaat opgeslagen gegevens is berekend. Komen beide uitkomsten overeen dan wordt de gebruiker geautoriseerd.
De secundaire beveiliging biedt een bescherming tegen het opbouwen van een verbinding met een ongeautoriseerde persoon tijdens het uitbellen (risico c1). Zeer belangrijk is dan wel dat de gebruiker na ingave van zijn gebruikersidentificatie eerst door het dial-back-apparaat wordt teruggebeld en dat pas daarna de challenge/response-procedure plaatsvindt (dit is *niet* bij elke dial-back-apparatuur het geval!). Indien eerst de challenge/response-procedure wordt doorlopen, bestaat namelijk toch nog het risico dat tijdens het terugbellen verbinding wordt gelegd met een ongeautoriseerde gebruiker.

Als tertiaire beveiliging wordt gebruik gemaakt van data-encryptie. Dit wordt nader toegelicht in de paragraaf over de beveiligingsmaatregelen tijdens de datacommunicatiefase.

Procedurele maatregelen

Een mogelijke maatregel die gerelateerd aan de huidige stand van de techniek primitief is maar zeer doeltreffend kan zijn, is een zuiver procedurele maatregel, waarbij een interne beheerder van de datacommunicatielijnen en -apparatuur een centrale uitvoerende rol speelt.

Indien de Automatic Answer-faciliteit van de modem niet is geactiveerd en de modem zodanig is ingesteld dat wegvallen van de draaggolf direct leidt tot het 'on-hook' gaan van de modem, is altijd interventie door de beheerder noodzakelijk. Er kan dan de volgende procedure worden toegepast:

1. Een gebruiker die een verbinding wil opbouwen, belt op naar de beheerder van de host-computer.
2. De beheerder vraagt de persoon om zijn gebruikersnummer en verbreekt de telefoonverbinding.
3. De beheerder controleert of het desbetreffende gebruikersnummer op het gevraagde tijdstip actief mag zijn (indien niet => einde procedure).
4. De beheerder zoekt het bij het gebruikersnummer behorende telefoonnummer en twee (eenmalig te gebruiken) wachtwoorden op.
5. De beheerder belt het gevonden telefoonnummer via een (apart) telefoontoestel.
6. De gebruiker neemt de telefoon op. De beheerder vraagt naar het eerste wachtwoord en verbreekt de verbinding indien dit niet correct wordt opgegeven (=> einde procedure).
7. De gebruiker vraagt op zijn beurt aan de beheerder het tweede wachtwoord en verbreekt de verbinding indien dit niet correct wordt opgegeven (=> einde procedure).
8. Gebruiker en beheerder schakelen handmatig de modems off-hook. De modemverbinding wordt tot stand gebracht.
9. De beheerder activeert de computerpoort zodat een logische verbinding kan worden opgebouwd. Indien men tevens het risico wil uitsluiten dat op de desbetreffende poort nog een sessie actief is, kan nog worden voorgeschreven dat hierop eerst wordt gecontroleerd en zo nodig de betrokken sessie wordt afgebroken voordat de computerpoort wordt geactiveerd.

Zeer belangrijk is dat de gebruiker na identificatie eerst wordt teruggebeld en dat pas daarna de challenge/response-procedure plaatsvindt.

Deze methode is in feite een manuele versie van de dial-back-procedure. Ook daar wordt immers gebruik gemaakt van gebruikersnummer, password en een vaststaand terug te bellen telefoonnummer. Het terug te bellen nummer is de primaire beveiliging, de wachtwoorduitwisseling de secundaire beveiliging. Deze methode is nogal omslachtig en zal daarom niet vaak worden toegepast. Groot voordeel van deze methode is wel dat er geen extra investering in apparatuur nodig is terwijl toch bescherming wordt verkregen tegen het opbouwen van een verbinding met een ongeautoriseerde gebruiker (risico c1), verbindingsopbouw vanaf een ongeautoriseerde locatie (risico c4), het opbouwen van een verbinding op een ongeautoriseerd tijdstip (risico c5) en de gevolgen van het niet compleet afbouwen van een logische verbinding (risico d). Ten

aanzien van risico c4 wordt overigens geen harde bescherming verkregen omdat nog steeds de reeds aangegeven risico's worden gelopen ten gevolge van doorschakelen en de perpetual dial-attack.

MAATREGELEN TIJDENS DE OPBOUW VAN EEN MODEMVERBINDING

In deze paragraaf zal een viertal beveiligingsmaatregelen worden besproken die toegepast kunnen worden tijdens de fase van het opbouwen van de modemverbinding.

Automatic Answer-faciliteit

Een beveiliging tegen ongeautoriseerd inbellen is mogelijk door de Automatic Answer-faciliteit van de computermodem te deactiveren. De maatregel verhindert het opbouwen van een modemverbinding. Net als bij de blokkering voor inkomende telefoongesprekken is deze methode alleen te gebruiken indien de computerlijn slechts voor uitgaand verkeer wordt gebruikt waarbij de computer de actie initieert. Indien het initiatief (ook) van gebruikerszijde moet kunnen uitgaan, is deze methode dus ongeschikt. Ook biedt deze methode geen beveiliging tegen de perpetual dial-attack en tegen het ongeautoriseerd activeren van de doorschakelfunctie.

Niet-standaard modulatietechnieken

Een andere beveiligingsmethode tegen ongeautoriseerd inbellen is het gebruik van modems met afwijkende modulatietechnieken die niet commercieel verhandeld worden. Ook deze maatregel verhindert het opbouwen van een modemverbinding. IBM heeft hier in het verleden bijvoorbeeld gebruik van gemaakt voor remote support-lijnen aan door haar geleverde computersystemen. Door gebruik te maken van speciale modulatietechnieken wordt een bescherming verkregen tegen de volgende risico's:

- Passieve aanval (risico a) omdat het ontvangen signaal zonder hulp van een speciale demodulator niet interpreteerbaar is.

- Actieve aanval: risico b1: toevoegen van berichten is niet mogelijk indien men niet de beschikking heeft over de speciale modulatietechniek; wijzigen van berichten is mogelijk maar de aanvaller weet dan niet wat hij wijzigt; verwijderen van berichten blijft mogelijk;
risico b2 en b3: veranderen van het bron- respectievelijk bestemmingsadres is mogelijk als toevalstreffer, want de aanvaller weet niet welke informatie hij vervangt.

- Opbouwen modemverbinding door een ongeautoriseerde gebruiker (risico c1), omdat alleen een modemverbinding zal worden opgebouwd indien beide modems elkaars signalen 'herkennen', dat wil zeggen van dezelfde modulatietechniek gebruik maken.

- Initiëren verbinding met behulp van ongeautoriseerde apparatuur (risico c3). Dit kan worden bereikt door de modem in de DTE in te bouwen en fysieke maatregelen te treffen waarmee wordt voorkomen dat de modem is te verwijderen.

- Niet afbouwen van de logische verbinding (risico d) omdat zonder de beschikking over de speciale modulatietechniek niet met de modem kan worden gecommuniceerd. Indien de sessie niet was beëindigd, wordt door de modem dus niets aan de applicatie doorgegeven.

Het gebruik van speciale modulatietechnieken schermt dus een veelheid aan risico's af (ook de perpetual dial-attack) maar biedt geenszins een waterdichte beveiliging. Het is altijd mogelijk dat iemand in het bezit komt van de speciale modulatietechniek door diefstal van een compleet apparaat, het ontwerp of met behulp van de trial-and-error-methode.

Niet-standaard datacompressietechnieken

Datacompressie is een techniek waarbij gegevens eerst worden bewerkt voordat zij door de modem worden verzonden. De bewerking heeft tot doel het aantal te verzenden bits te beperken zonder dat informatieverlies optreedt. Door de gegevens te comprimeren kan de informatie in een kortere tijd worden uitgewisseld, hetgeen een besparing betekent aan tijd en datacommunicatiekosten. Het eigenlijke comprimeren kan plaatsvinden voordat de gegevens worden aangeboden aan de modem maar kan ook door de modem zelf worden verzorgd. Aan de remote zijde moeten de gegevens natuurlijk weer worden gedecomprimeerd. Van belang is dus dat beide partijen een zelfde compressietechniek hanteren, anders zal de verstuurde informatie niet of onjuist worden geïnterpreteerd. Hoewel datacompressie in eerste instantie voor efficiency-doeleinden wordt toegepast, biedt zij ook een zekere mate van beveiliging.

In feite kan men datacompressie zien als een soort versleuteling waarbij tevens de hoeveelheid te verzenden bits wordt beperkt. Ten aanzien van het bestand zijn tegen 'kraken' van de code kan datacompressie natuurlijk niet dezelfde mogelijkheden bieden als encryptietechnieken!

Er bestaan inmiddels meerdere protocollen voor datacompressie. De facto-standaard voor automatische foutcorrectie door de modem zelf is het MNP (Microcom Networking Protocol). Hiervan is inmiddels een tiental sublevels gedefinieerd. Modems met MNP level 3 of hoger verzorgen naast foutdetectie tevens datacompressie. Foutdetectie wordt bereikt door de te verzenden data te verdelen in genummerde datablokken en per datablok een 16-bits CRC (Cyclic Redundancy Check) toe te voegen. Als de ontvangende modem een fout detecteert in de CRC zal hij om een hertransmissie vragen vanaf het foutief ontvangen blok.

Indien men datacompressie wil toepassen als een beveiligingsmaatregel zal men gebruik moeten maken van niet op de markt verkrijgbare compressietechnieken. Tijdens het 'trainen' van de modems zal de modemverbinding dan alleen worden opgebouwd indien beide partijen over een zelfde type modem beschikken. De afgedekte risico's zijn geheel overeenkomstig de toepassing van speciale modulatietechnieken. Bovendien wordt ten gevolge van de berichtennummering een bescherming verkregen tegen het verwijderen van berichten (risico b1).
Ook het gebruik van speciale datacompressietechnieken is geen waterdichte maatregel, maar er wordt wel degelijk een extra drempel opgeworpen voor het tot stand brengen van een modemverbinding.

Datum/tijdslot

Door gebruik van een datum/tijdslot wordt een bescherming verkregen tegen het opbouwen van een verbinding op een ongeautoriseerd tijdstip (risico c5). Een mogelijke implementatie van een datum/tijdslot is ervoor te zorgen dat een inkomend belsignaal niet automatisch wordt beantwoord. Een dergelijk datum/tijdslot is een vrij rigoreuze methode omdat het de toegang voor alle gebruikers uitsluit. Het uitschakelen kan worden bereikt door ervoor te zorgen dat de inkiesmodem niet reageert op het belsignaal. De meest simpele oplossing hiervoor is een tijdschakelaar tussen het netsnoer van de modem. Hiervan bestaan inmiddels exemplaren die digitaal programmeerbaar zijn tot op de minuut nauwkeurig met per dag verschillende in- en uitschakeltijden. Overigens hoeft men niet bang te zijn dat de modeminstellingen bij uitschakelen van de netspanning verloren raken, omdat deze na het instellen veelal in EEPROM (Electrically Erasable Programmable Read Only Memory) kunnen worden opgeslagen.
Aansturing kan ook applicatief vanuit de hostcomputer gebeuren door middel van het DTR-signaal van de V.24-interface of door middel van de Hayes-commando's ATH en ATA. Een andere methode bij Hayes-compatible modems is om blijvend geen gebruik te maken van de Automatic Answer-faciliteit, maar te controleren op ontvangst van de string RING. Indien de oproep dient te worden gehonoreerd kan dan met het commando ATO de modem off-hook worden geschakeld. Valt de oproep binnen het datum/tijdslot, dan zal de oproep niet worden gehonoreerd.

MAATREGELEN TIJDENS HET OPBOUWEN VAN DE LOGISCHE VERBINDING

In deze paragraaf zal een viertal beveiligingsmaatregelen worden besproken die toegepast kunnen worden tijdens de fase van het opbouwen van de logische verbinding.

Challenge/response-procedure

De identificatie van een gebruiker geschiedt veelal slechts door middel van zijn gebruikers-id en password. Nadeel hiervan is dat deze identificatiegegevens door een hacker kunnen worden afgetapt en vervolgens kunnen worden gebruikt om in te loggen. Een andere identificatiemethode is het gebruik van een challenge/response-procedure welke per gebruiker maar ook per sessie uniek is [Davi89].
Veelal wordt de challenge/response-procedure verzorgd door speciale applicaties. Een challenge/response-systeem is echter ook los verkrijgbaar, de functionaliteit is dan ondergebracht in speciale hardware.
Vaak wordt aan gebruikerszijde niet alleen gebruik gemaakt van softwarematig opgeslagen gegevens, maar is ook speciale hardware nodig (bijvoorbeeld een chipcard die met behulp van een chipcardlezer wordt uitgelezen of speciale hardware die wordt aangesloten op de parallelle poort van een PC). Voordeel van de chipcard is dat deze op eenvoudige wijze na afloop van de sessie uit de chipcardlezer te verwijderen is en op een veilige plaats kan worden opgeborgen.

Het gebruik van speciale modulatietechnieken biedt geenszins een waterdichte beveiliging.

Het berekenen van de response door de gebruiker kan automatisch plaatsvinden indien het apparaat waarmee wordt ingebeld over voldoende intelligentie beschikt. Door de challenge/response-component (hardware of software) in de DTE in te bouwen en (fysieke respectievelijk logische) maatregelen te treffen waarmee wordt voorkomen dat de component is te verwijderen respectievelijk te kopiëren, kan een bescherming worden verkregen tegen het opbouwen van een verbinding met ongeautoriseerde apparatuur (risico c3).
Er kan echter ook gebruik worden gemaakt van apparaatjes ter grootte van een zakrekenmachine die na ingave van de challenge de response berekenen en zichtbaar maken op een display. Behalve van het gebruikte algoritme is het resultaat mede afhankelijk van de geheime opgeslagen sleutel en van een PIN-code die door de gebruiker moet worden ingegeven om het apparaat te activeren. In plaats van controle op de juiste componenten (hard- en/of software) wordt dan primair gecontroleerd op de juiste gebruiker en wordt dus een bescherming verkregen tegen het opbouwen van een verbinding door een ongeautoriseerde gebruiker (risico c1). Indien geen overige (locatiegebonden) beveiligingsmaatregelen zijn getroffen, is de gebruiker flexibel met betrekking tot de plaats van verbindingsopbouw, de speciale challenge/res-

ponse-calculator is immers gemakkelijk mee te nemen.
Overigens kan het voor veel toepassingen net zo belangrijk zijn voor de gebruiker om te weten dat hij met de juiste host en het juiste dial-back-apparaat is verbonden als omgekeerd. Hiertoe kan een tweede challenge/response-procedure worden gevolgd waarbij nu de gebruiker de challenge verstuurt naar de host (dual challenge/response-procedure).

Controle op gebruikersnaam/lijn-combinatie

Vaak zal de inkiesverbinding slechts worden gebruikt voor een beperkte functionaliteit, zoals het raadplegen van gegevens ten behoeve van een storingsanalyse. Nadat een modemverbinding tot stand is gekomen, terwijl er geen bijzondere verdere controlemaatregelen zijn getroffen, is het denkbaar dat ten onrechte niet wordt ingelogd met een user-id dat is gereserveerd voor remote gebruik. In plaats daarvan zou een geautoriseerde gebruiker kunnen inloggen met een geldige gebruikersnaam/password-combinatie zoals die hem ter beschikking is gesteld voor de werkzaamheden die hij overdag vanaf zijn werkplek moet verrichten. Het is natuurlijk ook denkbaar dat een ongeautoriseerde gebruiker hiertoe kans ziet. Mogelijk kan dan gebruik worden gemaakt van user-id's met vergaande autorisatie op systeem-, bestands- en/of applicatieniveau.

Link-encryptie heeft als voordeel dat de totale berichtinhoud wordt versleuteld.

Belangrijk is dat via de kieslijn alleen kan worden ingelogd met de daarvoor gereserveerde user-id's. Teneinde dit te bewerkstelligen kan door middel van een beveiligingsapplicatie worden afgedwongen dat alleen met bepaalde user-id's via de kieslijn kan worden ingelogd. Deze user-id's dienen dan door de access control software op de host-computer alleen te worden geautoriseerd voor beperkte taken. Op deze wijze wordt een bescherming verkregen tegen het inloggen door een geautoriseerde gebruiker onder een gebruikerscode die hem niet is toegewezen voor gebruik via kieslijnen (risico c2).

Datum/tijdslot

Indien een kieslijn slechts gedurende een beperkt aantal uren ter beschikking moet worden gesteld, is het mogelijk de functionaliteit gedurende de overige uren uit te schakelen. Dit kan geschieden per gebruiker door in een applicatie (bijvoorbeeld de access control software) op de host-computer op te nemen gedurende welke dagen/uren een bepaalde gebruiker actief mag zijn.

In tegenstelling tot de methode waarbij de Automatic Answer-faciliteit gedurende bepaalde dagen/uren wordt uitgeschakeld, kan met deze methode per gebruiker een apart datum/tijdslot worden ingesteld.

Encryptietechnieken

Indien onversleutelde of met de verkeerde sleutel vercijferde berichten worden ontvangen, zal de computer de data niet juist interpreteren en zal niet succesvol kunnen worden ingelogd. Deze methode kan zowel in de communicatie- als applicatiegerichte lagen van het OSI-model worden gerealiseerd. Ook een combinatie van beide is mogelijk en zelfs een aansturing van de communicatiegerichte laag door de applicatiegerichte laag.
Indien de encryptietechnieken worden verzorgd door de applicatiegerichte laag zal de DTE over voldoende intelligentie dienen te beschikken om dit te ondersteunen. Encryptie verzorgd door de applicatiegerichte laag wordt aangeduid met de term sessie-encryptie en werkt end-to-end. Dat wil zeggen dat het bericht bij de verzender wordt versleuteld en pas bij de ontvanger wordt ontsleuteld. In eventueel tussengelegen knooppunten of tussengeschakelde componenten vindt geen ontsleuteling plaats. Bij toepassing van sessie-encryptie wordt alleen het dataveld versleuteld. De informatie die door de communicatiegerichte lagen aan het informatiepakket wordt toegevoegd, wordt niet versleuteld.

Encryptie door de communicatiegerichte laag wordt wel aangeduid met link-encryptie. Hierbij wordt de data versleuteld met behulp van aparte encryptor devices, welke worden geplaatst tussen de computermodem en de host-computer of door middel van modems met ingebouwde encryptietechnieken.
Het voordeel van link-encryptie ten opzichte van sessie-encryptie is dan ook dat bij link-encryptie de totale berichtinhoud wordt versleuteld, zodat ook een afscherming wordt verkregen tegen het risico van analyse van het berichtenverkeer (risico a2). Regelmatig verschijnen publikaties over de snelheid waarmee algoritmes zoals DES kunnen worden gekraakt indien behalve de ciphertext ook de plaintext bekend is. Aandachtspunt bij link-encryptie vormt daarom wel de kraakbestendigheid indien over de lijn frequent dezelfde berichten worden verzonden waarvan de inhoud of nagenoeg de gehele inhoud in klaartekst bekend is. Te denken valt hierbij aan het frequent versturen van bepaalde datapakketten (zoals Receive Ready) bij gebruik van synchrone protocollen (zoals SDLC of HDLC). Om het risico van het achterhalen van de encryptiesleutel tot een minimum te reduceren dient deze sleutel regelmatig te worden veranderd. Er bestaan reeds encryptor boxen en modems met encryptiefaciliteiten welke automatisch voorzien in een frequente wijziging van de encryptiesleutel.

Encryptietechnieken (van bewezen sterkte zoals DES) geven een bescherming tegen:

- Passieve aanval (risico a1) omdat het ontvangen signaal zonder kennis van de geheime encryptiesleutel en de encryptietechniek niet interpreteer-

baar is. Bij link-encryptie is hierbij ook risico a2 (analyseren van de berichtenstroom) afgedekt, bij encryptie door de applicatiegerichte lagen is dit risico niet afgedekt.

– Een actieve aanval op het berichtenverkeer (risico b): risico b1: toevoegen van berichten is niet mogelijk indien men niet de beschikking heeft over de geheime sleutel; wijzigen van berichten is mogelijk maar de aanvaller weet dan niet wat hij wijzigt; verwijderen van berichten blijft mogelijk;
risico b2 en b3: bij gebruik van link-encryptie is het veranderen van het bron- respectievelijk bestemmingsadres (indien van toepassing) slechts mogelijk als toevalstreffer, want de aanvaller weet niet welke informatie hij vervangt.

– Onjuiste verbindingsopbouw (risico c). De gevolgen van de risico's van het opbouwen van een verbinding door of met een ongeautoriseerde gebruiker (risico c1), omdat beide partijen over de geheime sleutel dienen te beschikken.
Het opbouwen van een verbinding met ongeautoriseerde apparatuur (risico c3). Dit kan worden bereikt door de encryptiecomponent (hardware of software) in de DTE in te bouwen en (fysieke respectievelijk logische) maatregelen te treffen waarmee wordt voorkomen dat de component is te verwijderen respectievelijk te kopiëren. Onbevoegde kennisname van de encryptiesleutel dient vanzelfsprekend ook te worden voorkomen.

– Niet afbouwen van de logische verbinding (risico d). Zonder kennis van de geheime encryptiesleutel en de encryptietechniek kan geen juist interpreteerbare data worden verzonden.

Niet-standaard datacompressietechnieken

Datacompressie kan ook worden verzorgd door de applicatiegerichte lagen. In tegenstelling tot door modems verzorgde datacompressie wordt dan alleen de gebruikersdata gecomprimeerd.

MAATREGELEN TIJDENS DE DATACOMMUNICATIEFASE

De reeds behandelde niet-standaard modulatie- en datacompressietechnieken alsmede link- en sessie-encryptietechnieken zijn ook tijdens het proces van datacommunicatie toepasbaar. Voorts kunnen de vijf in deze paragraaf behandelde technieken worden gehanteerd.

Manipulation Detection Code

Bij een zogenaamde actieve aanval kunnen berichten worden gemodificeerd. Dit is ook mogelijk voor versleutelde berichten. Hoewel een ongeautoriseerde persoon dan niet precies weet wat hij in de bitstroom verandert, zal dit bij de ontvanger van het bericht toch tot ongewenste gevolgen leiden met wellicht vergaande consequenties.

Primair doel van een MDC (Manipulation Detection Code of ook wel Modification Detection Code) is om de ontvanger van een bericht in staat te stellen wijzigingen te detecteren in een door een andere partij verzonden bericht [Davi89]. Het gebruik van de term code is hier eigenlijk misplaatst. In feite gaat het om een checksum welke via een bepaald algoritme wordt berekend over de data in klaartekst. Omdat de checksum niet volgens een geheim algoritme of met gebruikmaking van een geheime sleutel wordt berekend, moet de checksum worden beschermd. Hiertoe kan over de checksum een digitale handtekening worden berekend. Ook kan de checksum aan de eigenlijke data worden toegevoegd waarna het geheel wordt encrypt en via de lijn verzonden [Davi89]. De ontvanger dient het bericht te decrypten en opnieuw de MDC te berekenen over het ontvangen dataveld. Vervolgens wordt de berekende MDC vergeleken met de ontvangen MDC. De beschikbare technieken zijn zodanig dat nagenoeg iedere verandering in het verzonden bericht leidt tot een afwijking tussen beide MDC's en daardoor kan worden gedetecteerd. Alleen indien de door de ontvanger opnieuw berekende MDC gelijk is aan de ontvangen MDC kan worden gesteld dat het bericht foutloos is ontvangen. Sommige technieken zijn zelfs in staat veranderingen (ten gevolge van transmissiefouten of bewuste manipulatie) van één of enkele bits te lokaliseren en te herstellen.

Omdat bij het hier gehanteerde begrip van de MDC gebruik wordt gemaakt van encryptie van het gehele bericht, wordt een bescherming verkregen tegen de risico's zoals die reeds zijn aangegeven bij de behandeling van encryptie tijdens het opbouwen van de modemverbinding. Bovendien geldt bij een actieve aanval op het berichtenverkeer ten aanzien van risico b1 dat wijzigen van berichten door de ontvanger zal worden gedetecteerd.

Message Authentication Code

Primair doel van de Message Authentication Code (MAC) is om de authenticiteit van (de verzender van) het bericht vast te stellen [Davi89]. Hiertoe wordt door de verzender met behulp van een algoritme en een geheime sleutel over de te verzenden data een controlegetal berekend, dat samen met de eigenlijke data in klaartekst wordt verzonden. De ontvanger van het bericht dient te beschikken over de geheime sleutel zodat over de data opnieuw het controlegetal kan worden berekend. Indien dit overeenkomt met het ontvangen controlegetal wordt geconcludeerd dat de data afkomstig is van een geautoriseerde gebruiker. Omdat een MAC over de berichtinhoud wordt berekend, zal een wijziging in de data tijdens transport tot gevolg hebben dat het bericht als niet authentiek door de ontvanger zal worden gekenmerkt.

Indien het controlegetal wordt berekend met behulp van encryptietechnieken van bewezen sterkte (zoals DES) geven MACcing-technieken een bescherming tegen:

– Een actieve aanval op het berichtenverkeer (risico b): risico b1: toevoegen en wijzigen van berich-

ten is wel mogelijk maar indien men niet de beschikking heeft over de geheime sleutel om de MAC te berekenen zal de host de berichten weigeren; verwijderen van berichten blijft mogelijk.
De risico's b2 tot en met b6 worden niet afgedekt.

– De gevolgen van de risico's van het opbouwen van een verbinding met of door een ongeautoriseerde gebruiker (risico c1), omdat een ongeautoriseerde gebruiker niet beschikt over de geheime sleutel nodig voor het berekenen van de MAC.

– Niet compleet afbouwen van de verbinding (risico d) omdat zonder kennis van de geheime encryptiesleutel en de encryptietechniek de juiste MAC-waarden niet kunnen worden berekend en de host de ontvangen berichten zal weigeren.

Digitale handtekening

Het begrip digitale handtekening wordt in meerdere betekenissen gebruikt. Bij de toepassing van een digitale handtekening die de meeste analogie vertoont met de menselijke handtekening voegt de afzender een code toe aan het te verzenden bericht waarna het geheel in klaartekst wordt verstuurd. Het verschil met MACcing ligt in het feit dat voor de controle op de authenticiteit van het bericht een andere techniek wordt gebruikt. Controle gebeurt namelijk niet op basis van het zelf berekenen van de digitale handtekening over de berichtinhoud en het vervolgens vergelijken met de ontvangen handtekening. De ontvanger is zelfs niet eens in staat zelf de handtekening te berekenen. Hij is alleen in staat te controleren of de digitale handtekening hoort bij het verzonden bericht.

De toepassing van berichtennummering sec heeft weinig zin als bescherming tegen een actieve aanval.

Het genereren van een digitale handtekening is onder andere mogelijk via het gebruik van asymmetrische (public key) algoritmen. Hierbij wordt vooraf een sleutelpaar gegenereerd bestaande uit twee speciale bij elkaar horende sleutels. De essentie hierbij is dat decryptie van een bericht met de andere helft van het sleutelpaar moet worden uitgevoerd dan de helft waarmee de encryptie is uitgevoerd. Van het sleutelpaar komt één (secret) key alleen in het bezit van de zender en blijft dus onbekend voor de ontvanger. De andere (public) key is openbaar. Met behulp van de public key kan de juistheid van de digitale handtekening worden vastgesteld. De handtekening zelf kan echter alleen worden berekend met behulp van de secret key.

Het gebruik van digitale handtekeningen in de hierboven gehanteerde betekenis geeft indien encryptietechnieken van bewezen sterkte worden toegepast een bescherming tegen de risico's zoals die hiervoor reeds zijn gegeven bij de toepassing van MACcing-technieken. Bovendien wordt een bescherming verkregen tegen het risico van repudiation (risico b6) omdat de ontvanger alleen in staat is de juistheid van de digitale handtekening te controleren en niet in staat is deze zelf te berekenen.

Nummering van de berichten

Door de berichten over en weer te nummeren kan verlies en invoegen van berichten worden gedetecteerd. De toepassing van berichtennummering sec heeft weinig zin als bescherming tegen een actieve aanval omdat een eventuele aanvaller ook de berichtennummering zodanig kan manipuleren dat dit niet door de ontvanger zal worden ontdekt. Daarom wordt nummering van berichten vaak gecombineerd met encryptie of MACcing-technieken [Davi89]. Indien het volgnummer deel uitmaakt van de met encryptie of MAC-techniek te bewerken data, wordt bereikt dat het resultaat niet alleen afhankelijk is van de berichtinhoud zelf, maar ook van het volgnummer.

Door berichtennummering in combinatie met MACcing of encryptie toe te passen wordt naast de door de MAC respectievelijk encryptie afgedekte risico's tevens een bescherming verkregen tegen de volgende risico's:

– Risico b1: toevoegen en wijzigen van berichten zal al bij toepassing van MACcing/encryptie worden gedetecteerd. Het verwijderen van berichten zal worden gedetecteerd aan de hand van de berichtennummers.

– Risico b4: veranderen van de berichtenvolgorde is mogelijk maar de ontvanger zal ze bij ontvangst weer in de juiste volgorde terugplaatsen dan wel bij ontvangst vragen om hertransmissie van de nog niet ontvangen nummers.

– Risico b5: replay van berichten is niet mogelijk omdat de ontvanger een reeds ontvangen berichtnummer verder zal negeren. Indien slechts een beperkte nummerreeks wordt gebruikt, is het replaygevaar wel gereduceerd maar niet volledig weggenomen.

Date and time stamp

Een andere methode om een replay van eerder verzonden berichten te voorkomen is het gebruik van een 'date and time stamp' [Davi89]. De verzender voorziet bij deze methode ieder bericht van een datum/tijd-stempel. De toepassing van date and time stamps sec heeft weinig zin als bescherming tegen een actieve aanval omdat een eventuele aanvaller ook de date and time stamps zodanig kan manipuleren dat dit niet door de ontvanger zal worden ontdekt. Daarom wordt over het gehele bericht (inclusief datum/tijd-stempel) een MAC-waarde berekend of wordt het gehele bericht versleuteld. De ontvanger herleidt uit het ontvangen bericht het

datum/tijd-stempel, dat slechts enkele tienden van seconden mag afwijken van de op dat moment geldende datum/tijd.
Om deze methode succesvol te kunnen toepassen is het noodzakelijk dat de 'klokken' van zender en ontvanger worden gesynchroniseerd. De applicatiegerichte laag zal het datum/tijd-stempel aan het bericht moeten toevoegen. Hierbij zal de 'resolutie' voldoende groot moeten worden gekozen. Over het algemeen volstaat het de tijd tot in honderdsten van seconden nauwkeurig aan het bericht toe te voegen.

Door het gebruik van date and time stamps in combinatie met MACcing of encryptie wordt naast de door de MAC respectievelijk encryptietechniek afgedekte risico's tevens een bescherming verkregen tegen risico b4 (verandering van de berichtenvolgorde) en risico b5 (replay van berichten). De ontvanger zal in deze gevallen de ontvangen berichten weigeren omdat de discrepantie tussen de date and time stamp en zijn eigen interne klok te groot is geworden.

MAATREGELEN VOOR BEWAKING VAN DE VERBINDING

In deze paragraaf zal een tweetal beveiligingsmaatregelen worden besproken die toegepast kunnen worden bij de bewaking van de verbinding.

Bewaking van de draaggolf

Een abnormale wijze van beëindiging van de fysieke verbinding voordat de sessie is beëindigd, bijvoorbeeld door een draadbreuk of storing aan de remote zijde, brengt risico's met zich mee. Het gevaar bestaat namelijk dat bij wegvallen van de fysieke verbinding (en daardoor ook de modemverbinding) de opgebouwde sessie desondanks niet wordt afgebroken. Indien een ongeautoriseerd persoon vervolgens inbelt op een lijn waarop nog een sessie actief is, wordt direct een logische verbinding opgebouwd zonder dat een verdere controleprocedure wordt doorlopen. Het is daarom zeer belangrijk de continuïteit van de verbinding te bewaken. Een onderbreking van de verbinding dient onmiddellijk te worden gedetecteerd en te resulteren in het resetten van de lijn naar haar oorspronkelijke staat. Dit kan bijvoorbeeld worden bereikt door de modem de ontvangst van de draaggolf van de remote modem te laten bewaken.
Bij wegvallen van de draaggolf dienen de modem en de overige aangesloten apparatuur voor de desbetreffende lijn terug te keren naar de uitgangspositie. Tevens dient een melding te worden gegenereerd voor de bovenliggende applicatie, die op haar beurt de desbetreffende sessie zal moeten resetten.

Bij gebruik van de V.24-interface is bewaking van de continuïteit van de verbinding alleen mogelijk indien een adequaat gebruik wordt gemaakt van de beschikbare interface-signalen. Problemen met de fysieke verbinding betekenen het wegvallen van de draaggolf; het DCD-signaal (pin 8) zal dit melden aan de computer. Deze dient daarop zelfstandig de logische verbinding af te bouwen en de modem in de uitgangspositie te resetten.

Ook bij gebruik van Hayes-compatible modems is bewaking van de continuïteit van de verbinding alleen mogelijk indien een adequaat gebruik wordt gemaakt van de beschikbare mogelijkheden. Indien wegvallen van de modemverbinding door de DTE moet worden gedetecteerd aan de hand van de status van het DCD-signaal, dient de modem dusdanig te zijn ingesteld dat het DCD-signaal werkt volgens de V.24-standaard. Een andere methode van bewaking door de DTE is controle op ontvangst van de string NO CARRIER. Ook hier dient de DTE zelfstandig de logische verbinding af te bouwen en de modem in de uitgangspositie te resetten.

Bewaking van de draaggolf in combinatie met door de applicatiegerichte lagen te nemen acties bij wegvallen van de draaggolf geeft een bescherming tegen het afbouwen van een fysieke verbinding zonder dat tevens de logische verbinding wordt afgebouwd (risico d).

Bewaking van de lijnactiviteit

Het voordeel van de hiervoor besproken bewaking van de draaggolf is dat onmiddellijk na het wegvallen van de modemverbinding de benodigde acties kunnen worden gestart. Toch is naast een bewaking van de draaggolf ook een bewaking van de lijnactiviteit gewenst. Een logische verbinding kan namelijk door de remote zijde worden afgebroken op een wijze waarbij de modemverbinding blijft bestaan.

Daarom dient een bewaking van de lijnactiviteit plaats te vinden. Hierbij wordt de desbetreffende datacommunicatieapparatuur aan host-zijde door de DTE gereset indien via de verbinding gedurende een langere periode (de 'inactiviteitslimiet') geen activiteit wordt waargenomen. De bewaking dient door de applicatiegerichte lagen plaats te vinden. Deze dienen dan tevens zorg te dragen voor het beëindigen van de logische verbinding.

Bij gebruik van Hayes-compatible modems kan de bewaking van de inactiviteitslimiet eventueel worden gelegd bij de modem (via het commando AT\Tn) zelf. De modem verbreekt dan alleen de modem- en fysieke verbinding, de applicatiegerichte laag dient ook hier de logische verbinding af te bouwen.

Bewaking van de inactiviteitslimiet in combinatie met acties om de fysieke en logische verbinding te beëindigen geeft een bescherming tegen het afbouwen van een logische verbinding zonder dat tevens de fysieke verbinding wordt afgebouwd (risico d). Tussen oorzaak en gevolg verstrijkt echter wel een zekere periode (namelijk de gekozen inactiviteitslimiet).

AUDITASPECTEN

In deze paragraaf wordt ingegaan op aspecten die van belang zijn bij het toetsen van het door de te controleren organisatie gevoerde beheer over analoge kieslijnen (betrokken op zowel de organisatorische als de technische implementatie).

Organisatorische implementatie

Voor de beoordeling van de organisatorische implementatie dient onder meer een antwoord te worden verkregen op de volgende vragen:

- Wat is het beleid dat wordt gevolgd ten aanzien van kieslijnen?
- Is vastgelegd wie verantwoordelijk is voor het opstellen van een risico-analyse, het vaststellen van de beveiligingsmaatregelen, het autoriseren van de kieslijn, het implementeren van de kieslijn, het registreren van de kieslijn?
- Bestaan ten aanzien van de toewijzing van deze verantwoordelijkheden voldoende controletechnische functiescheidingen? Hierbij is met name van belang dat de risico-analyse en de beveiligingsmaatregelen worden beoordeeld door een onafhankelijke instantie.
- Wordt een centrale registratie bijgehouden van de voor datacommunicatie gebruikte kieslijnen (inclusief opgestelde risico-analyses, voorgeschreven beveiligingsmaatregelen, uitslag onafhankelijke toetsing en autorisatie, fysieke locatie, telefoonnummer)?
- Zijn alle kieslijnen in de centrale registratie opgenomen?
  Mogelijke bronnen ter toetsing zijn: de beheerders van computercentra, technische diensten, datacommunicatiefacturen van de afdeling financiële administratie, definities in de netwerksoftware (bijvoorbeeld bij IBM de definities van switched major nodes of de DIAL-parameter in de NCP-definities).
- Is de registratie van de individuele kieslijnen volledig? (risico-analyse, voorgeschreven beveiligingsmaatregelen, etc.)
- Zijn de kieslijnen op de juiste wijze en door de juiste persoon geautoriseerd?
- Zijn de risico-analyses juist uitgevoerd?
- Bieden de voorgeschreven beveiligingsmaatregelen een adequate afscherming tegen de gesignaleerde risico's?
- Heeft een adequate onafhankelijke toetsing plaatsgevonden van de risico-analyse en beveiligingsmaatregelen? Hierbij dient onder andere ook te worden getoetst op consistentie met het beleid.

Technische implementatie

Voor de beoordeling van de technische implementatie van een individuele kieslijn kunnen de volgende stappen worden gevolgd:

Stap 1.
Vraag de specificaties op van de te onderzoeken kieslijn (telefoonnummer, beveiligingsmaatregelen).

Stap 2.
Probeer een telefoon- en modemverbinding op te bouwen.
Afhankelijk van de getroffen maatregelen wordt één van onderstaande resultaten verkregen (zie figuur 8):

Getroffen maatregel	Resultaat
Geen	CONNECTxxxx of NO CARRIER
Blokkering inkomend verkeer	NO ANSWER
Gebruik van dial-back apparatuur	CONNECTxxxx
Procedurele maatregelen	NO ANSWER
Uitschakelen Automatic Answer	NO ANSWER
Niet-standaard modulatietechnieken	NO CARRIER
Speciale datacompressie	NO CARRIER
Datum/tijdslot	NO ANSWER

Figuur 8. Mogelijke resultaten afhankelijk van de getroffen beveiligingsmaatregelen.

Interessant zijn de resultaten CONNECTxxxx en NO CARRIER. Voor een verdere controle zijn de volgende gegevens benodigd:

- het type modem en de instelling ervan;
- het gebruikte protocol (synchroon, asynchroon, ASCII/EBCDIC, pariteit, etc.);
- indien gebruik wordt gemaakt van dial-back-apparatuur dient tevens te worden gevraagd naar het nummer van de aparte terugbellijn en een toegangscode/testgebruiker voor de uit te voeren testactiviteiten.

Na bemachtiging van het juiste modemtype kunnen de volgende aanvullende controles worden uitgevoerd:

a. Algemeen:
   Stel vast dat de modem is afgeschermd tegen remote configureren (sommige modems kunnen na opbouwen van een modemverbinding vanaf de remote zijde worden geconfigureerd).

b. Voor dial-back-apparatuur:
   - Voer de juiste modem- en protocolinstellingen in, bel het nummer van de te controleren lijn en toets de gegevens van de testgebruiker in. De verbinding dient vervolgens door het dial-back-apparaat te worden verbroken.
   - Stel vast of het dial-back-apparaat gebruik maakt van een aparte uitgaande lijn door wederom het nummer van de ingaande lijn te bellen (met behulp van een lijn waarnaar niet door het dial-back-apparaat zal worden uitgebeld!). Met dit nummer

moet weer onmiddellijk een verbinding kunnen worden opgebouwd. Is het nummer in gesprek dan wordt waarschijnlijk geen aparte uitgaande lijn gebruikt (of een andere gebruiker heeft net de ingaande lijn gebeld).
- Stel vast dat de uitgaande lijn geblokkeerd is voor inkomend verkeer door handmatig het nummer te bellen. Hierbij dient men een 'afgesloten' toon te horen.

c. Voor speciale modulatie- of datacompressietechnieken:
- Voer de juiste modem- en protocolinstellingen in en bel het nummer van de te controleren lijn.
- Schakel na de fluittoon de modem op de stand DATA. De modems zullen vervolgens proberen of ze met elkaar kunnen communiceren. Dit noemt men het 'trainen' van de modems. Dit is te horen aan de in de modem ingebouwde luidspreker, want hieruit komt een ruis of fluittoon van wisselende frequentie.
- Ten gevolge van de speciale technieken aan de zijde van het onderzochte nummer zal het trainen niet succesvol verlopen. De verbinding wordt verbroken en de modem meldt dit met de code NO CARRIER.
- Deze controle dient te worden herhaald met verschillende typen modems.

d. Indien geen nadere gegevens over de datacommunicatielijn bekend zijn zal naar bevind van zaken moeten worden gehandeld:
- Wordt de verbinding door de remote zijde verbroken dan is waarschijnlijk een beveiligingsmaatregel getroffen zoals dial-back of uitwisseling van een code (bijvoorbeeld voor de te hanteren datacompressietechnieken) binnen een bepaald tijdsbestek.
- Wordt een onbegrijpelijke tekst ontvangen dan kan het zijn dat het aantal databits, stopbits, de pariteit of de karakterrepresentatie (ASCII, EBCDIC) verkeerd is ingesteld. Een datascoop kan eventueel uitkomst bieden.
- Is op geen enkele wijze een zinvolle tekst op het scherm te krijgen dan wordt wellicht gebruik gemaakt van encryptietechnieken.
- Worden constant karakters ontvangen dan wordt waarschijnlijk van een synchrone verbinding gebruik gemaakt.
- etc.

Stap 3.
Probeer een logische verbinding op te bouwen en onderzoek de in de datacommunicatiefase getroffen maatregelen.
Hierbij zal naar bevind van zaken dienen te worden gehandeld. Het gebruik van een datascope voor het analyseren van het berichtenverkeer zal zeker bij een controle op technieken als een challenge/response-procedure, digitale handtekening, encryptie, MACcing, MDC, etc. onmisbaar zijn. In het kader van dit artikel zal hier niet verder op worden ingegaan. Wel wordt er nog op gewezen dat in een IBM-omgeving de toepassing van zogenaamde 'switched major nodes' speciale aandacht verdient. Deze definities zijn specifiek bedoeld voor kiesverbindingen omdat hierbij niet op voorhand bekend is welke terminal (een zogenaamde LU of Logical Unit) een verbinding opbouwt. Na het tot stand komen van een modemverbinding maakt de opbeller zijn terminal daarom aan de IBM-host bekend door het versturen van een XID (eXtended IDentification). Op basis van de ontvangen XID wijst de IBM-host een terminalnaam (LU-naam) toe. Veelal zijn de geïmplementeerde beveiligingsmaatregelen (zoals toepassing van sessieencryptie, een session management exit, logon-id/source-combinaties) gedefinieerd op het niveau van de LU-naam. Het is daarom noodzakelijk dat aanvullende controles worden uitgevoerd zodat een koppeling wordt gelegd tussen telefoonlijn en de XID's die via deze lijn mogen worden ontvangen.

Er moet een koppeling worden gelegd tussen de telefoonlijn en de XID's die via deze lijn mogen worden ontvangen.

Stap 4.
Test de juiste afbouw van de verbinding.
Hierbij dient men in staat te zijn (eventueel met behulp van de beheerder) een logische verbinding op te bouwen. In de meeste gevallen zal men hiertoe de beschikking dienen te krijgen over een user-id/password. Na het opbouwen van de logische verbinding worden de volgende controles uitgevoerd:

a. De fysieke en de modemverbinding worden verbroken. Deze worden onmiddellijk daarna weer opgebouwd. Vervolgens dient te worden vastgesteld dat ook de logische verbinding is verbroken zodat men opnieuw het identificatieproces moet doorlopen.

b. Er wordt in het geheel geen actie ondernomen. Na overschrijden van de inactiviteitslimiet dient de verbinding door acties vanuit de host-zijde te worden verbroken. Vervolgens wordt onmiddellijk weer een modemverbinding opgebouwd. Hierna dient te worden vastgesteld dat ook de logische verbinding is verbroken zodat men opnieuw het identificatieproces moet doorlopen.

Stap 5.
Koppel de bevindingen terug met de beheerder van de onderzochte kieslijn.

CONCLUSIE

In figuur 9 is een overzicht gegeven van de besproken beveiligingsmaatregelen en de risico's waartegen een bescherming wordt verkregen. Daarbij is geen onderscheid gemaakt of de maatregel het initiële risico afdekt of juist het afgeleide risico. Ter verduidelijking: encryptie vormt (anders dan bijvoorbeeld het gebruik van glasvezelkabel) geen drempel tegen het aftappen van een datacommunicatielijn als zodanig maar wel tegen het ongeautoriseerd gebruik van de afgetapte berichten. Zoals blijkt is een groot aantal beveiligingsmaatregelen mogelijk.

Het gebruik van analoge kieslijnen moge bij de huidige stand van de datacommunicatietechnieken verouderd lijken, op beveiligingsgebied bieden deze lijnen een groot aantal mogelijkheden. Dit wordt veroorzaakt doordat analoge kieslijnen een verbinding verzorgen op de onderste laag van het OSI-model, namelijk de fysieke laag. De gebruiker is hierdoor vrij om de bovengelegen lagen op eigen wijze in te vullen. Sommige risico's zijn alleen af te schermen door maatregelen in de applicatiegerichte lagen van het OSI-model (bijvoorbeeld de controle op de combinatie user-id/lijn). Voor de invulling van de beveiligingsmaatregelen in de onderste lagen van het OSI-model kan echter uit een groot aantal relatief goedkope beveiligingshulpmiddelen worden gekozen. Om enkele voorbeelden te noemen:

- Bij gebruik van Hayes-compatible modems kan de bewaking van de draaggolf en van de lijnactiviteit worden gelegd bij de modem zelf. De modem verbreekt dan overigens alleen de modem- en fysieke verbinding, de applicatiegerichte laag dient de logische verbinding af te bouwen.

- Door toepassing van een modem met ingebouwde data-encryptie volgens de DES-standaard wordt voorzien in linkencryptie.

- Door toepassing van een modem die zowel MNP-5 als DES-encryptie ondersteunt wordt een combinatie verkregen die is te beschouwen als een MDC waarbij tevens in een berichtennummering is voorzien.

- De meer uitgebreide dial-back-apparatuur verzorgt de volgende functies: vaststellen identiteit gebruiker, bewaking toegestane verbindingstijden per gebruiker door individuele datum/tijd-sloten, terugbellen van de gebruiker, vaststellen authenticiteit van de gebruiker door middel van de challenge/response-procedure, versleuteling van berichten door middel van data-encryptie, logging van het moment van verbindingsopbouw en -afbouw alsmede van security violations.

Beveiligingsmaatregelen in de communicatiegerichte lagen van het OSI-model schermen in een eerder stadium van de verbindingsopbouw af dan maatregelen in de applicatiegerichte lagen. Wat betreft de risico's die men loopt door ongeautoriseerd handelen van de eigen medewerkers geldt echter veelal dat juist de maatregelen in de applicatiegerichte lagen een sterkere beveiliging bieden. Met name indien de maatregelen zijn getroffen met behulp van specifieke hardware is fysiek benaderen van de apparatuur in de meeste gevallen voldoende om de maatregelen te omzeilen. Het is daarom van belang om in een risico-analyse vast te stellen of men een bescherming wil tegen alleen ongeautoriseerde derden of ook tegen mogelijk misbruik door de eigen medewerkers. In het eerste geval zal veelal met de verkrijgbare standaardhulpmiddelen reeds een afdoende bescherming kunnen worden verkregen.

Ten slotte wil ik aanmoedigen om onderzoek te starten in hoeverre het mogelijk is een adequate beveiliging te bereiken door middel van het vanuit de applicatiegerichte lagen aansturen van de in de standaard verkrijgbare (datacommunicatie)apparatuur geïmplementeerde beveiligingsmaatregelen. Te denken valt hierbij aan het door de applicatiegerichte laag aangestuurde laden van een encryptiesleutel in datacommunicatie-ondersteunende apparatuur (bijvoorbeeld een daartoe geschikte modem).

Een mogelijke procedure is:
1. De gebruiker belt in op de kieslijn van de host waarna een nog niet encrypte verbinding tot stand wordt gebracht.

Figuur 9. Relatie maatregelen versus risico's.

Maatregel	Beschermt tegen de risico's:
Opbouwen telefoonverbinding	
– Blokkade inkomend verkeer	c1, c4, c5
– 'Kaal' dial-back-apparaat	c1, c4
– Uitgebreide manuele procedure	c1, c4, c5, d
Opbouwen modemverbinding	
– Deactiveren Automatic Answer	c1, c4, c5
– Speciale modulatietechniek	a1, a2, b1, b2, b3, c1, c3, d
– Speciale datacompressietechniek	a1, a2, b1, b2, b3, c1, c3, d
– Datum/tijdslot	c5
Opbouwen logische verbinding	
– (Dual) challenge/response-procedure	c1, c3
– User-id/lijn-combinatie	c2
– Datum/tijdslot	c5
– Encryptietechnieken	a1, a2, b1, b2, b3, c1, c3, d
Datacommunicatiefase	
– 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
Afbouwen verbinding	
– Bewaking draaggolf	d
– Bewaking lijnactiviteit	d

* De onderstreepte risico's worden alleen afgedekt bij gebruik van link-encryptie.

2. De gebruiker verstuurt zijn user-id en laadt zijn encryptiesleutel in de modem.
3. Een tussengeschakeld beveiligingssysteem (of eventueel de host zelf) controleert de user-id (op bestaan en eventueel datum/tijdslot).
4. De bij de user behorende encryptiesleutel wordt uitgelezen en in de modem geladen.
5. Na een synchronisatiesignaal wordt zowel aan gebruikers- als aan host-zijde de encryptiefaciliteit ingeschakeld.
6. Eventueel wordt nu een encryptiesleutel uitgewisseld die na een synchronisatiesignaal in de modems wordt geladen en voor de duur van de sessie als actieve sleutel wordt gebruikt.
7. De gebruiker verstuurt zijn user-id en password naar de host.

Een dergelijke methode is ook toepasbaar voor inkieslijnen die door een groot aantal gebruikers moeten kunnen worden benaderd (bijvoorbeeld Electronic Banking-toepassingen). Een alternatief is natuurlijk het gebruik van sessie-encryptie. Deze vorm biedt weliswaar een beveiliging op end-to-end-basis, maar is niet apparatuur-onafhankelijk en vereist momenteel nog bij beide communicatiepartners aanzienlijke investeringen.

LITERATUUR

[Anch88] Anchor Datacomm, *DES encryptie*, 1988.

[Brou92] D. Brouwer, *Beveiliging van analoge en digitale kieslijnen*, Nieuwerkerk a/d IJssel 1992.

[Corn87] H. Cornwall en W. Hendrikse, *Handboek voor Computer Kraken & Beveiligen*, 1987.

[Davi89] D.W. Davies and W.L. Price, *Security for computer networks*, John Wiley & Sons, New York 1989.

[Dirk86] Dirksen, *Basiskennis Datacommunicatie*, 1986.

[Doug86] I.J. Douglas and P.J. Olson, *Audit and Control of Computer Networks*, 1986.

[Geve90] Geveke Electronics, *Defender II users manual: dial-back device*, 1990.

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

[Jaco85] J. Jacobs, *Kraken en computers*, Veen, Utrecht 1985.

[Matt88] R.L. Matthijssen en J. Truijens, *Computers, datacommunicatie en netwerken*, 1988.

Tijdschriftartikelen

[EDPA89] *Computer Hacking*, The EDP Auditor Journal, volume IV, 1989.

[Info87] *Managing dial-up networks: the critical problems*, Information age, volume 9 no. 4, october 1987.

[Cana89] *How to control Dial-up Access*, Canadian Systems, february 1989.

[Gerb90] D.A. Gerberick, *Strong network security management*, SIGSAC Review, summer 1990.

[Spap88] H.A.J.M. Spape, *Een introductie tot beveiliging bij datatransmissie*, Compact 1988/1.

[Duin88] I.M. van Duin, *Electronic Funds Transfer*, Compact 1988/1.

[Samo85] M. Samociuk, *Hacking, or the Art of Armchair Espionage*, Computer Fraud & Security bulletin, 1985.

[Brod90] I. Brodsky, *Securing private data on insecure public networks*, Edpacs, june 1990.

[Murr89] M. Murray, *Auditing an IBM data communications network*, Edpacs, march 1989.

[Rutl86] L.S. Rutledge, *A Survey of issues in computer network security*, Computers & Security, 1986 nr. 5.

[PC+90] *MNP-modem neemt foutcontrole over / Datacompressie verhoogt de snelheid*, PC+, juli 1990.

[Knuv90] P.M. Knuvers, *SWIFT en controle*, Compact 1990/1.

Drs.ing. D. Brouwer RE
Is zijn loopbaan in 1984 gestart in het bedrijfsleven als datacommunicatie- en systeemspecialist. In 1988 is hij in dienst getreden bij de Postbank N.V. als EDP-auditor. Momenteel is hij werkzaam als controleleider bij de afdeling EDP-audit van de Interne Accountants Dienst van de ING-Bank.

Beveiliging van UNIX

Mw.drs. M.C. van Lith RE

De beveiliging van UNIX is weliswaar eenvoudig van opzet, maar door het grote aantal mogelijkheden ontstaat in de praktijk al snel een complexe implementatie, waarbij een fout die een beveiligingslek tot gevolg heeft niet denkbeeldig is.
Vanuit haar ervaringen als systeembeheerder gaat de auteur aan de hand van voorbeelden in op de beveiligingsmogelijkheden van UNIX, de risico's van een onjuiste implementatie en de wijze waarop een audit met behulp van geprogrammeerde controlefuncties kan worden uitgevoerd.

INLEIDING

In dit artikel wordt een inleiding gegeven op het besturingssysteem UNIX. Aan de hand van voorbeelden wordt uitgelegd hoe UNIX en met name de toegangs- en resource-beveiliging binnen UNIX is opgebouwd. Dit artikel kan voor de EDP-auditor als eerste kennismaking met UNIX dienen en bevat handreikingen voor het uitvoeren van een audit.

UNIX is een relatief oud besturingssysteem. De eerste ontwikkelingen zijn aan het eind van de zestiger jaren gestart en het systeem heeft zich in de zeventiger jaren ontwikkeld tot een volwassen besturingssysteem. Pas in de tachtiger jaren won UNIX in het bedrijfsleven aan populariteit. Een reden van het toenemend gebruik van UNIX is dat de ontwikkelaar, Bell Laboratories van AT&T, het besturingssysteem kosteloos aan universiteiten ter beschikking stelde, waardoor vele studenten ermee opgroeiden en het later in hun carrière toepasten. Hoewel UNIX beschikbaar is voor computers van PC tot mainframe, wordt het voornamelijk gebruikt op minicomputers, vaak in de rol van communicatie-server.

In dit artikel wordt eerst ingegaan op de geschiedenis en ontwikkeling van UNIX en de daaruit voortgevloeide UNIX-varianten en opgerichte organisaties ter bevordering van de standaardisatie. Aansluitend worden de opbouw en werking van UNIX behandeld, alsmede de beveiligings- en controlemogelijkheden. Vanwege de complexiteit en de veelomvattendheid blijven de beveiligingsaspecten van communicatieprogrammatuur buiten beschouwing.

GESCHIEDENIS EN ONTWIKKELING VAN UNIX

UNIX is ontwikkeld met het oogmerk voor ontwikkelaars een omgeving te creëren waarbinnen de samenwerking en communicatie tussen de programmeurs en de ontwerpers is geoptimaliseerd. Dit leidde tot het ontwerp van een multi-user-, multi-tasking-besturingssysteem. MIT, Bell Labs en General Electric startten hiertoe in de zestiger jaren een gezamenlijk project om honderden gebruikers gelijktijdig (time-sharing) te laten werken. Het project bleek niet levensvatbaar te zijn en Bell Labs en General Electric trokken zich terug, zodat MIT alleen het uiteindelijke resultaat MULTICS in produktie bracht. De naam MULTICS is een afkorting van MULTiplexed Information and Computing Service. MULTICS heeft slechts weinig toepassing gevonden.
MULTICS was een multi-level-besturingssysteem, wat inhoudt dat verschillende niveaus bestonden voor zowel gebruikers als beheerders. Tijdens de ontwikkeling kregen enkele medewerkers van het MULTICS-project de behoefte aan een eenvoudiger besturingssysteem en bouwde Ken Thompson, werknemer van Bell Laboratories, de eerste versie van UNICS (UNiplexed Information and Computing Service). De spelling veranderde al spoedig in UNIX. UNIX heeft slechts één niveau van gebruikers, met uitzondering van de super user, die vrijwel altijd alles mag.
In 1973 herschreef Thompson het grootste deel van UNIX in de programmeertaal 'C' samen met Dennis Ritchie, eveneens medewerker van Bell Labs. Omdat 'C' een hogere machine-onafhankelijke programmeertaal is, resulteerde dit in een portable besturingssysteem. Een bijkomend voordeel is dat ook de onder UNIX draaiende applicaties portable zijn.

De UNIX-broncode werd door Bell Labs tegen geringe vergoeding ter beschikking gesteld. Dit leidde tot een diversiteit van UNIX-versies, omdat een ieder vrij was de broncode te wijzigen. De bekendste zijn:
- System V van AT&T;
- XENIX van Microsoft;
- BSD 4.3 van Berkeley University in Californië.

Het uiteenlopen van deze UNIX-versies heeft nadelige gevolgen voor de portabiliteit van voor UNIX geschreven software. Om deze reden werd besloten tot convergentie in de vorm van standaardisatie. De eerste stap in de goede richting was dat XENIX geheel compatible met System V werd gemaakt. Daarnaast is door ICL, Nixdorf, Philips en Olivetti de X/OPEN-groep opgericht, die zich bezighoudt met het ontwikkelen van een UNIX-standaard uitgaande van System V. Een tweede groep van voornamelijk gebruikers, POSIX, houdt zich bezig met het ontwikkelen van een universele standaard voor besturingssystemen, gebaseerd op UNIX.

Als reactie op de macht van AT&T werd door een aantal fabrikanten, waaronder DEC, HP, Nixdorf, Bull en IBM, de Open Software Foundation (OSF) opgericht. De UNIX-gebruikers van AT&T hebben hierop gereageerd met de oprichting van de UNIX International-groep. Beide groepen ontwikkelden een UNIX-implementatie die zowel aan de X/OPEN als aan de POSIX-standaard voldeed. Er blijken echter fundamentele verschillen tussen de OSF- en de AT&T-implementatie te bestaan. De interface met applicaties is gelukkig wel gelijk, zodat dit geen invloed heeft op de portabiliteit van applicaties.

Zeer recentelijk, in september 1993, heeft een aantal grote leveranciers, waaronder IBM, DEC en HP, besloten tot Unified UNIX. Unified UNIX is het grootste gemene veelvoud van de bestaande UNIX-versies van deze leveranciers.

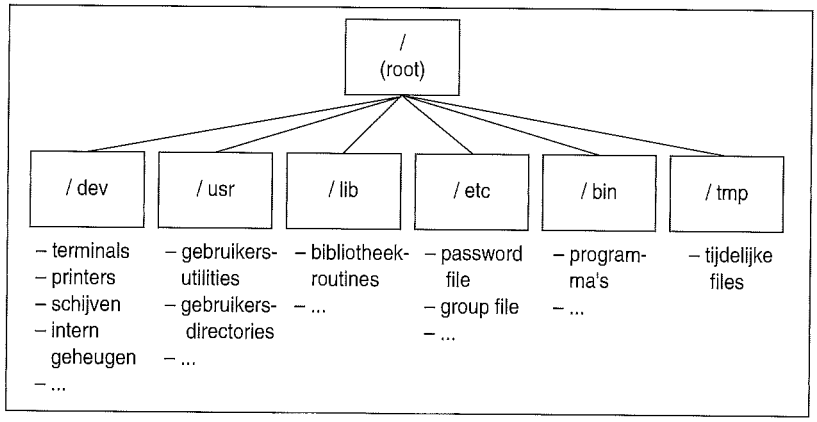
Het uiteenlopen van de diverse UNIX-versies heeft nadelige gevolgen voor de portabiliteit van voor UNIX geschreven software.

In het nu volgende deel van dit artikel wordt achtereenvolgens ingegaan op de opbouw, de beveiligingsaspecten en de controlefuncties van de hedendaagse UNIX-versies. Tenzij anders vermeld zijn de beschrijvingen algemeen voor UNIX-varianten geldig.

OPBOUW EN WERKING VAN UNIX

UNIX is opgebouwd rond een kern, de 'kernel'. Dit is het hart van de besturingsprogrammatuur en zorgt onder meer voor het toewijzen van interne geheugenruimte en het verdelen van de processortijd over de processen.
Rond de kernel is een schil gelegd, de 'shell'. Dit is hetgeen de gebruiker ziet als wordt aangelogd. De shell nodigt met zijn prompt de gebruiker uit om een commando in te toetsen. De shell draagt vervolgens zorg voor de interpretatie van het commando en start eventueel hiertoe programma's op. Zo'n opgestart programma heet een proces. De shell is een gewoon UNIX-programma en is te vergelijken met 'command.com' van MS-DOS. Er bestaan verschillende shells, die variëren in gebruiksvriendelijkheid en/of in toepassingsmogelijkheden. De zogenaamde 'restricted shell' zorgt ervoor dat de gebruiker slechts een beperkt aantal UNIX-commando's kan uitvoeren. Zo kan bijvoorbeeld het commando cd (change directory) niet worden uitgevoerd, zodat de gebruiker niet van directory kan wisselen.

UNIX is eenvoudig van opzet; elk object wordt gerepresenteerd door een file. Objecten zijn terminals, printers, disks, tape-units, intern geheugen,



Figuur 1. Opbouw file-systeem.

directories, maar natuurlijk ook bestanden en programma's. De files (en dus alle objecten) zijn vastgelegd in het file-systeem.

De gebruikers worden gerepresenteerd door middel van een user-id. De objectbeveiliging bestaat uit het toekennen van files aan gebruikers of groepen van gebruikers op een manier dat ongeautoriseerde toegang tot files niet mogelijk is.

Indeling file-systeem

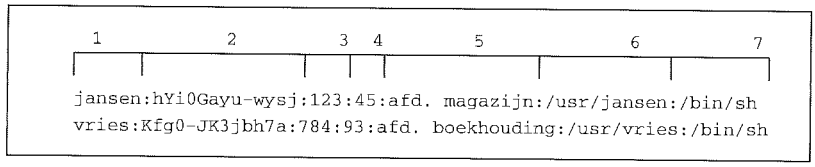
Het file-systeem is hiërarchisch opgebouwd, waarbij de root directory (de topdirectory) bovenaan is geplaatst. Onder de root directory hangt een omgekeerde boomstructuur van sub-directories, waarin de bestanden, programma's en diverse randapparaten zijn ondergebracht. De root directory wordt aangeduid met '/'.

Onder de root directory hangt een aantal standaard-directories, zoals /dev, /usr, /etc, /bin en /tmp. In de directory /dev worden alle devices, zoals terminals, printers, schijven en intern geheugen, vastgelegd (zie figuur 1).

Gebruikers

In de password file /etc/passwd zijn de gegevens van de gebruikers vastgelegd. De password file is een belangrijk bestand omdat de beveiliging van de toegang tot het systeem en de files hierop is gebaseerd. Naast user-id en password zijn per gebruiker enkele andere gegevens vastgelegd.

Figuur 2. Twee regels van een password file.



De password file bevat de volgende gegevens:
1 gebruikersnaam;
2 vercijferd password;
3 user-id;
4 group-id;
5 commentaar;
6 login-directory;
7 shell.

1 *Gebruikersnaam*

De gebruikersnaam is de naam waarmee de gebruiker inlogt op het UNIX-systeem. De gebruikersnaam dient uniek te zijn. Indien in de password file gelijke gebruikersnamen voorkomen, kan slechts worden ingelogd volgens de gegevens (waaronder password) van de eerst voorkomende.

2 *Vercijferd password*

Het password wordt vercijferd opgeslagen met behulp van een one-way function gebaseerd op DES, waarbij datum en tijd van de eerste invoering van het password in de berekening worden meegenomen. Het vercijferingsmechanisme is opzettelijk vertraagd (het wordt 25 maal uitgevoerd) om een geprogrammeerde poging om de beveiliging te doorbreken zeer langzaam te maken. Daarnaast wordt gebruik gemaakt van een gemodificeerde DES-functie, zodat een aanval met het oorspronkelijke DES-algoritme zinloos is.

Er zijn tegenwoordig ook mogelijkheden om de vercijferde passwords in een aparte file op te slaan, de 'shadow password file'. Op de oorspronkelijke plaats in de password file staat dan een 'x' of een '!'. Deze shadow password file is alleen benaderbaar door root. Vanaf release 3.2 van System V is de shadow password file geïmplementeerd. Het is één van de voorwaarden om het C2-beveiligingsniveau te verkrijgen. Het C2-beveiligingsniveau is gedefinieerd in het Orange Book.

3 *User-id*

De user-id is een nummer en is belangrijker dan de gebruikersnaam. Bevoegdheden ten aanzien van files zijn gebaseerd op de user-id en niet op de gebruikersnaam.

Het is belangrijk dat een eenduidige nummering wordt gehanteerd binnen het systeem. Als aan twee gebruikers hetzelfde nummer wordt toegekend, dan kunnen zij elkaars files benaderen en manipuleren, omdat het systeem de twee personen beschouwt als één gebruiker.

4 *Group-id*

Een gebruiker kan in meerdere groepen zijn geplaatst. Bij de meeste UNIX-versies is slechts één group tegelijk actief. In de password file is de group-id vastgelegd die de gebruiker bij het inloggen initieel krijgt toegewezen. Vervolgens kan hij switchen naar een andere groep waarin hij eveneens is ingedeeld. Bij AIX, de UNIX-versie van IBM, zijn altijd alle toegekende groepen actief. AIX voorziet bovendien in een group password. De beveiliging van de opgeslagen passwords is echter

minder goed geïmplementeerd dan die van de persoonlijke passwords. Om deze reden en ten behoeve van de traceerbaarheid van persoonlijke acties is het beter de beveiliging op persoonlijke passwords te baseren.

5 Commentaar
In de rubriek commentaar kan een tekst worden geplaatst ter ondersteuning van het systeembeheer. De omschrijving heeft geen functie anders dan verduidelijking voor de beheerder.

6 Login-directory
Tijdens de aanlogprocedure zal het systeem in de login-directory zoeken naar de profiles (mits onder de sh- of de ksh-shell wordt gewerkt). Eerst wordt de algemene file /etc/.profile uitgevoerd en vervolgens de persoonlijke file homedir/.profile. Deze files zijn te vergelijken met de AUTOEXEC.BAT van MS-DOS. Langs deze weg wordt voor de gebruiker aan systeemparameters een waarde toegekend, zoals *umask* (zie File-beveiliging). Ook kan vanuit de .profile een gebruikersmenu worden opgestart.

7 Shell
In het laatste veld van de password file wordt aangegeven welke shell de gebruiker ter beschikking staat. De meest gebruikte shell is het programma /bin/sh; voor AIX is dat /bin/ksh. Voor elke ingelogde gebruiker wordt een apart shell-proces opgestart.

In aanvulling op de password file kan per user-id in configuratie-files een aantal parameters worden vastgelegd waarbij onder meer het volgende kan worden aangegeven:
- tot wanneer de user-id geldig is;
- of met de gebruikersnaam mag worden ingelogd;
- of remote met de gebruikersnaam mag worden ingelogd;
- of de user-id met behulp van het *su*-commando (set user) mag worden opgestart. Het is met dit commando mogelijk de user-id na het inloggen te wijzigen. Er wordt dan wel om het password behorende bij het nieuwe user-id gevraagd.

Groepen

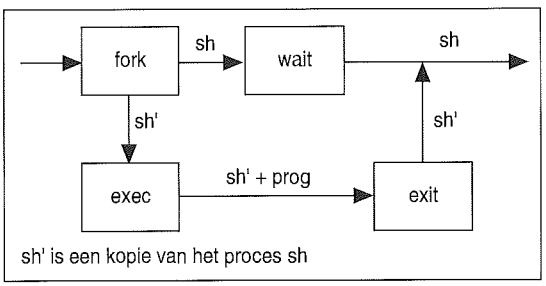
Gebruikers kunnen in meerdere groepen zijn ingedeeld. In de group file /etc/group wordt per groep aangegeven welke gebruikers erin zijn opgenomen. Het muteren van de password file en de group file met een editor wordt afgeraden, omdat op deze manier inconsistenties kunnen ontstaan ten aanzien van de groepindeling. Een voorbeeld hiervan is dat in de password file is vastgelegd dat de gebruiker initieel een bepaalde group-id krijgt, maar volgens de group file is de gebruiker geen lid van de groep. Bovendien is het op deze manier mogelijk gebruikersnummers en groepsnummers dubbel uit te geven.

Het verdient aanbeveling om voor het wijzigen van gebruikersgegevens en groepsgegevens gebruik te maken van beheerprogrammatuur, zoals SAM (HP-UX van Hewlett Packard) of SMIT (AIX van IBM). Deze programmatuur draagt zorg voor consistentie.

Processen

Een programma dat wordt opgestart, resulteert in een proces dat in het interne geheugen draait. Een proces wordt ook wel een 'subject' genoemd, in tegenstelling tot een file, die in deze terminologie 'object' wordt genoemd. Processen kunnen in verschillende 'omstandigheden' voorkomen. Zo kan een proces vanaf de command-line worden opgestart of vanuit een ander proces worden geactiveerd. Ook kan een proces op de achtergrond draaien, terwijl de gebruiker de terminal tot zijn beschikking houdt.

Het opstarten van een programma *prog* wordt in UNIX-termen een 'fork' genoemd; door middel van de system call 'fork' wordt het shell-proces gedupliceerd. Vanuit dit gedupliceerde proces wordt het nieuwe proces opgestart (system call 'exec'). Vanuit dit nieuwe proces kan eveneens door middel van een fork een nieuw proces worden opgestart. Het oorspronkelijke shell-proces wacht (system call 'wait') tot het nieuwe proces is afgelopen, alvorens een nieuw commando te accepteren en een nieuw proces op te starten. Als het proces is afgerond, wordt dit aan het oorspronkelijke proces gemeld met een system call 'exit'.



Figuur 3. Het fork-proces.

Een proces kan worden opgestart als een achtergrondproces door na de programmanaam een '&' in te toetsen. Voorbeeld:

Commando: *prog &*

De shell wacht nu niet tot het proces is afgelopen, maar accepteert meteen een nieuw commando, omdat de system call 'wait' niet wordt uitgevoerd. Op deze manier kan bijvoorbeeld een batch worden gedraaid zonder dat de terminal wordt geblokkeerd. Een bijkomend beveiligingsvoordeel is dat na het intoetsen van het commando de terminal kan worden afgelogd, zodat deze niet voor een onbevoegde beschikbaar kan komen.

BEVEILIGINGSASPECTEN

In dit artikel wordt voornamelijk ingegaan op de logische-beveiligingsaspecten. Wat het fysieke element betreft wordt hier alleen benadrukt, dat het mogelijk is een UNIX-systeem vanaf een systeemtape of systeem-diskette op te starten. Nadat het systeem is geboot en in single user mode is gebracht, is het vrij eenvoudig om de gegevens op de harde schijven te lezen of te manipuleren. Het verdient dus aanbeveling de computer in een afgesloten ruimte te plaatsen.
Een aantal systemen heeft aanvullende beveiliging in de vorm van een slot, waarmee het onmogelijk wordt gemaakt het systeem op te starten zonder de bijbehorende sleutel.

File-beveiliging

De file-beveiliging van UNIX maakt onderscheid in lees-, schrijf- en executierecht. De rechten worden als volgt weergegeven:
r leesrecht: het recht om de file te bekijken;
w schrijfrecht: het recht om de file te muteren of te verwijderen;
x executierecht: het recht om de file (het programma) op te starten.

Voor elke file in het file-systeem is vastgelegd *wie* deze rechten heeft. Hierbij wordt onderscheid gemaakt naar permissies van de eigenaar, permissies van gebruikers behorende tot dezelfde groep als de eigenaar en permissies van de andere gebruikers van het systeem. Aldus worden de volgende categorieën van gebruikers onderkend:
- owner: eigenaar van de file;
- group: de gebruikers die tot deze groep behoren;
- other ('the world'): alle anderen die toegang tot het systeem kunnen verkrijgen.

Als met het ls-commando de directory-inhoud wordt opgevraagd, ziet deze er als volgt uit:

```
bestands-   aant.  eige-          groot-
permissies  links  naar   groep   te      datum     tijd     filenaam
-rw-rw-r--   1     vries   bkh     4657   Sep  3    16:03    brief
-rw-------   1     jansen  mgz      231   Sep 23    13:45    voorraad
```

Figuur 4. Representatie rechten in de directory.

Eerste regel: Het eerste streepje geeft aan dat het een normale file betreft (geen directory, device of ander soort file). Het tweede tot en met het vierde karakter 'rw-' geeft aan dat de eigenaar lees- en schrijfrechten heeft, maar geen executierechten. De volgende drie karakters 'rw-' geven aan dat de groep 'bkh' ook lees- en schrijfrechten heeft. De categorie 'other' heeft slechts leesrechten. Het aantal links staat bij beide files op 1, wat betekent dat er geen andere verwijzingen (aliases) naar dit bestand zijn. De overige rubrieken spreken voor zich.

Tweede regel: Alleen de eigenaar heeft lees- en schrijfrechten op de file 'voorraad'.

Als een file wordt gecreëerd, dan worden standaard de actieve user-id en group-id ingevuld van de gebruiker die de file creëert. De permissiebits worden ingesteld volgens het *umask*-commando dat in de .profile dient te worden opgenomen. Aldus kan worden voorkomen dat een gebruiker ongewild files creëert die door iedereen kunnen worden gelezen en geschreven. Het *umask*-commando geeft aan welke rechten *niet* zullen worden toegekend.

Bijvoorbeeld:

commando:	resultaat:
`umask 077`	`-rwx------`
`umask 022`	`-rwxr-xr-x`

De systeembeheerder dient erop toe te zien dat het *umask*-commando op de juiste manier wordt toegepast.

Met de commando's *chown*, *chgrp* en *chmod* kunnen respectievelijk de eigenaar, de groep en de permissiebits worden gewijzigd.

Bijvoorbeeld :

```
-rw-rw-r-- 1 vries bkh 4657 Sep 3 16:03  brief
```

commando's:
```
chown jansen brief
chgrp mgz brief
chmod 746 brief
```

resultaat:
```
-rwxr--rw- 1 jansen mgz 4657 Sep 3 16:03  brief
```

Met het *chown*-commando kan een gebruiker een file dus weggeven aan een andere gebruiker.
De enige aan wie geen beperkingen ten aanzien van de toegangsbeveiliging kunnen worden opgelegd, is de super user. De super user heeft veelal de gebruikersnaam 'root' met de user-id 0 en heeft alle rechten op alle files. Het is dus niet mogelijk programma's of gegevens voor root af te schermen. Aan de hand van de logging kan worden vastgesteld welke handelingen root heeft uitgevoerd, maar men dient hierbij te bedenken dat root in staat is ook de logging te manipuleren.

Het toekennen van schrijfrechten aan een bestand of programma voor 'the world' brengt een risico met zich mee, daar iedereen, ook eventuele indringers, deze files kan wijzigen.

Naast de rwx-beveiliging leveren veel UNIX-besturingssystemen tegenwoordig de Access Control List (ACL). De ACL is een lijst van uitzonderingen op de rwx-beveiliging. Per gebruiker of groep wordt aangegeven welke rechten zijn toegekend. Op deze manier kan bijvoorbeeld aan één gebruiker (niet de eigenaar) een recht worden toegekend zonder dit aan een hele groep te geven. Ook is het langs deze weg mogelijk een gebruiker van een

groep uit te sluiten. In een ACL worden de volgende commando's gebruikt:
- *permit*: het toestaan van rechten aan gebruikers en/of groepen;
- *deny*: het uitsluiten van rechten voor gebruikers en/of groepen;
- *specify*: het expliciet toestaan van rechten aan gebruikers en/of groepen. Een *specify* gaat voor een *permit*, zodat hiermee uitzonderingen op de *permit* kunnen worden aangegeven.

Voorbeeld van een Access Control List (ACL) :

```
standaard
permissie-bits:          rwx rwx ---
eigenaar:      jansen
groep:         bkh

permit         r--       g:mgz
deny           rw-       g:bkh
specify        rwx       u:jansen
specify        r-x       u:vries
```

In dit voorbeeld is jansen een lid van de groep bkh en vries een lid van de groep mgz. De effectieve rechten zijn als volgt:
groep mgz: leesrecht
groep bkh: executierecht
user jansen: alle rechten
user vries: lees- en executierecht
overigen: geen rechten

Het is niet verstandig in een heterogene omgeving de beveiliging uitsluitend op ACL's te baseren, daar niet alle UNIX-besturingssystemen over de ACL-faciliteit beschikken en de ACL's dan zullen negeren, waardoor een deel van de beveiliging vervalt. Bij het gebruik van bepaalde UNIX-commando's voor het kopiëren van files gaan ACL's verloren, zodat een beveiligingslek kan ontstaan. Er dient dan ook zo min mogelijk van het *deny*-commando gebruik te worden gemaakt. Deze uitsluitingen vervallen als de ACL's worden genegeerd of verloren gaan.

Directory-beveiliging

Ook voor directories zijn voor de drie categorieën (owner, group en other) toegangsrechten vastgelegd. Indien een directory voor iedereen is opengesteld, dat wil zeggen als er lees-, schrijf- en executierechten zijn toegekend aan de eigenaar, de groep en alle anderen, dan kan niet zonder meer worden vertrouwd op de beveiliging geboden door de toegangsrechten van de files in de directory. Als de files in deze directory zijn afgeschermd tegen een bepaalde groep gebruikers, dan kunnen deze toch in staat zijn files te verwijderen, hoewel zij de inhoud van de file niet kunnen benaderen. Dit is een gevolg van de voor UNIX gekozen structuur; de directory is immers een file die mag worden beschreven. Er mag een regel in deze file worden verwijderd of toegevoegd. Het executierecht op een directory houdt in dat de directory mag worden doorzocht. Als een gebruiker geen executierechten heeft op een directory, betekent dit dat voor die gebruiker onder meer de commando's *cat*, *ls* en *find* in de desbetreffende directory niet werken.

Device-beveiliging

Omdat elk object in UNIX gerepresenteerd wordt als een file, zijn randapparatuur en intern geheugen net als bestanden, programma's en directories in het file-systeem (directory-structuur) opgenomen. Een logisch gevolg hiervan is dat de lees- en schrijfrechten voor devices op een zelfde manier worden afgeschermd als voor bestanden en programma's. Leesrechten op een tape-unit dienen te worden geïnterpreteerd als het vermogen om te lezen van tape, waarmee dus gegevens in het systeem kunnen worden geïmporteerd. Met deze rechten kan ook een eventueel aanwezige vertrouwelijke tape worden gelezen.
Als een terminal niet goed beveiligd en bijvoorbeeld leesbaar is, dan kan de toegangsbeveiliging worden doorbroken door het achterhalen van passwords, omdat de inhoud van het scherm ook de inhoud van de file is.

Setuid-bit en setgid-bit

Naast normale programma's bestaan er programma's met een setuid-bit (set user identification) of met een setgid-bit (set group identification) aan. Deze programma's zijn te herkennen aan een 's' op de plaats waar normaal een 'x' staat bij de bestandspermissies (zie figuur5).
Programma's met een setuid-bit aan hebben de eigenschap dat het programma wordt geëxecuteerd met de bevoegdheden van de eigenaar van het programma in plaats van de bevoegdheden van de gebruiker die het programma aanroept. Als de eigenaar van het programma super user is, betekent dit dat het programma wordt uitgevoerd met super user-bevoegdheden, hetgeen een potentieel gevaar met zich meebrengt.

Setuid-programma's kunnen bijvoorbeeld worden gebruikt om taken uit te voeren waarvoor super user-bevoegdheden benodigd zijn. Een gebruiker krijgt dan de mogelijkheid om een specifieke taak uit te voeren, terwijl de rest van het systeem waarvoor super user-bevoegdheden nodig zijn voor hem ontoegankelijk blijft. Een dergelijk programma dient niet door onbevoegden te kunnen worden gewijzigd (geen schrijfrechten). Het programma kan anders worden gebruikt om het file-systeem te manipuleren. Tevens mag het niet mogelijk zijn dat een setuid-programma voortijdig door de gebruiker wordt beëindigd, want dan bestaat het gevaar dat de gebruiker de super user-bevoegdheden behoudt.

Naast setuid-programma's bestaan er programma's met een setgid-bit aan. De werking van deze programma's is analoog, maar heeft nu betrekking op de groep in plaats van één enkele gebruiker. In het file-systeem worden de setuid-bit en de setgid-bit als in figuur 5 weergegeven.

De eerste regel van het voorbeeld geeft de setuid-bit weer; het programma kan door de leden van de groep bkh worden opgestart en het programma zal worden uitgevoerd met de user-id van 'vries' en dus met zijn bevoegdheden. De tweede regel geeft

bestands-permissies	aant. links	eige-naar	groep	groot-te	datum	tijd	filenaam
-rwsr-xr--	1	vries	bkh	7395	Sep 8	15:12	kilometerreg
-rwxr-sr-x	1	jansen	mgz	1284	Sep 11	10:43	voorraadbeheer

Figuur 5. Representatie setuid- en setgid-bit in de directory.

de setgid-bit weer; dit programma kan worden opgestart door iedereen die toegang tot het systeem kan krijgen. Het programma draait met de group-id van 'mgz' en met de bevoegdheden van 'mgz'.

Setuid-bits worden onder meer toegepast bij beheerprogrammatuur voor gebruikers- en groepsgegevens. Alleen met super user-bevoegdheid kunnen de password en de group file worden gemuteerd. Toepassing van super user-bevoegdheid dient echter zoveel mogelijk te worden beperkt om te voorkomen dat onherstelbare fouten worden gemaakt of dat de password file en de group file 'handmatig' worden gemuteerd. Door gebruik te maken van een beheerprogramma voor het aanmaken van gebruikers, waarbij de setuid-bit is aangezet, kan dit probleem adequaat worden opgelost. Voorts maken vele applicaties van het setuid-mechanisme gebruik.

Path

Schrijfbaarheid van directories door onbevoegden vormt een potentieel gevaar, zeker als deze directories in een 'path' zijn opgenomen. Het path is een verzameling directories vastgelegd in een variabele $PATH. Als een gebruiker een programma probeert aan te roepen, doorzoekt het besturingssysteem de directories in het path naar dit programma. Zonder een path wordt het bedoelde programma niet gevonden. Als er meer programma's zijn met dezelfde naam, dan wordt het eerst gevonden programma (dat het eerst voorkomt in het path) opgestart. De waarde van $PATH wordt vaak in de persoonlijke .profile van de gebruiker vastgelegd.

Een gebruiker kan een eigen path definiëren door het *path*-commando in te toetsen in de .profile of door dit commando op de command-line in te toetsen. Als bijvoorbeeld het commando *path / /etc /bin* wordt ingetoetst, worden achtereenvolgens de directories /, /etc en /bin doorzocht als een programma wordt aangeroepen.

Als een directory die voorkomt in het path beschreven kan worden door onbevoegden, dan kan een kwaadwillende gebruiker in zo'n directory een 'trojan horse' plaatsen. Een bestaand programma wordt hierbij vervangen door een programma dat bijvoorbeeld in enkele ogenblikken alle bestanden wist. De kwaadwillende gebruiker heeft misschien zelf niet de bevoegdheden om de commando's in het programma uit te voeren, maar een niets vermoedende beheerder met super user-bevoegdheden wel. In het standaard path en het path dat gebruikt wordt door beheerders dienen geen directories te zijn opgenomen die schrijfbaar zijn voor derden. Het opnemen van de directory '.' (de actuele directory) in het path is eveneens uit den boze, omdat dan programma's in de (willekeurige) actuele directory kunnen worden geactiveerd.

Logging

Logging speelt een belangrijke rol in de controle van de beveiliging. Met behulp van de logging kan worden nagegaan of iemand het systeem onbevoegd heeft kunnen benaderen. Dit is voor AIX vastgelegd in de file /usr/adm/login.log. Tevens kan worden gecontroleerd of processen door ongeautoriseerden zijn aangeroepen.

Naast deze logging kan aanvullende rapportage worden vervaardigd afkomstig uit geautomatiseerde controles gericht op de ingestelde beveiliging.

UNIX-CONTROLEFUNCTIES

Voor het uitvoeren van controle op de beveiliging van het systeem kan gebruik worden gemaakt van de controlefuncties van de UNIX-programmatuur. De controlefuncties zijn echter niet gestandaardiseerd, zodat UNIX-versies van verschillende leveranciers verschillende controlefuncties bieden.

De meeste UNIX-versies beschikken over een controlefunctie waarmee de password file kan worden gecontroleerd op volledige invulling per gebruiker, een functie waarmee consistentie met de group file wordt aangetoond en een functie waarmee kan worden vastgesteld of een verzameling programma's en bestanden zich in een goed beveiligde toestand bevindt. Hierbij kan worden gedacht aan ingestelde lees- en schrijfrechten en een checksum berekend over de files. Om deze controles te kunnen uitvoeren dient voordat het UNIX-systeem in produktie wordt genomen, een beveiligde toestand te worden gecreëerd. Tijdens de geautomatiseerde controles wordt aan deze toestand gerefereerd.

Met deze basishulpmiddelen kan een geautomatiseerd controleprogramma worden samengesteld. Om tot een compleet security audit-programma te komen waarbij handmatig intoetsen niet meer nodig is, is enig programmeerwerk zeker vereist. Om gebreken in de beveiliging op te sporen kunnen onder meer de zes hierna genoemde geautomatiseerde controles worden uitgevoerd.

Controle op de devices

Via een device kunnen gegevens worden geïmporteerd of geëxporteerd. Het is dus belangrijk de devices te beschermen. Voor de devices in de /dev directory kan door middel van een programma worden nagegaan welke rechten zijn toegekend. Vervolgens kan een melding worden afgedrukt als

de instelling van de permissiebits niet voldoet aan het vereiste beveiligingsniveau.

Tevens dient te worden gecontroleerd of een aantal specifieke programma's en bestanden ten behoeve van communicatie met andere systemen aanwezig is en of de permissiebits hiervoor juist zijn ingesteld. Zoals in de inleiding aangegeven, wordt hierop niet nader ingegaan.

Controle op wereldschrijfbaarheid van directories

De schrijfbaarheid van directories en bestanden vormt een potentieel gevaar. Wereldschrijfbaarheid houdt in dat zowel de eigenaar, als de groep, als alle anderen de file of directory mogen beschrijven. Het verdient aanbeveling om de directories te controleren op wereldschrijfbaarheid.

Controle op gebruikers en groepen

Voor zowel de password file als de group file wordt gecontroleerd of per regel alle velden zijn ingevuld. Hierbij kan onder meer worden gecontroleerd of alle gebruikers een password hebben en of user-ids en group-ids dubbel voorkomen. Indien het password niet is ingevuld, is de gebruikersnaam voldoende om toegang tot het systeem te verkrijgen.

De consistentie kan worden vastgesteld door aan te tonen dat gebruikers die in de group file opgenomen zijn, ook in de password file voorkomen en dat gebruikers die in de password file voorkomen ook in de group file zijn vastgelegd.

Controle op batch-programma's

Op UNIX-systemen is een aantal belangrijke batchprogramma's aanwezig, zoals at, cron en rc. Deze programma's zijn kritisch, omdat het setuid-programma's betreft met root als eigenaar. Met at kan op een opgegeven tijdstip een UNIX-commando worden uitgevoerd. Een rancuneuze ontslagen medewerker kan met behulp van at het gehele filesysteem een maand na zijn vertrek laten verdwijnen. Een automatische dagelijkse backup kan met cron-programmatuur worden uitgevoerd. De hiervoor benodigde commando's worden door cron in de directory crontabs vastgelegd. De rc-programma's worden uitgevoerd bij het opstarten van het systeem. Voor files en directories gerelateerd aan at-, cron- en rc-programma's kan worden gecontroleerd of de toegangsrechten te ruim zijn toegekend.
Voor rc-, cron- en at-files dienen geen schrijfrechten aan derden te zijn toegekend. Deze files dienen slechts door een systeembeheerder te kunnen worden aangepast. Ook leesrechten kunnen een risico met zich meebrengen. Een eventuele aanvaller kan in deze files lezen wanneer de backup en de batch met beveiligingscontroles worden gedraaid. Op deze manier kan hij zijn aanvalsmoment optimaal kiezen.

Controle op de integriteit van het file-systeem

Het dient mogelijk te zijn een controle uit te voeren waarbij wordt vastgesteld dat de oorspronkelijke instellingen van de files onveranderd zijn. Hiertoe is een referentiebestand, waarin de gegevens van de files zijn vastgelegd, noodzakelijk. In dit referentiebestand kunnen de volgende eigenschappen ter controle zijn opgenomen: toegangsrechten, grootte, datum en tijd, eigenaar, groep en een checksum. Voor muterende bestanden is het meestal niet zinnig om de lengte en de checksum te controleren. Naast het vaststellen van uitgevoerde mutaties dient tevens te kunnen worden aangetoond dat files zijn verwijderd of toegevoegd. De controle op het muteren of toevoegen van files is om eerder genoemde redenen vooral van belang voor programma's met een setuid-bit en setgid-bit.

Indien het password niet is ingevuld, is de gebruikersnaam voldoende om toegang tot het systeem te verkrijgen.

Een verzameling files die op deze wijze op integriteit worden gecontroleerd, wordt wel de Trusted Computing Base (TCB) genoemd. In de TCB kunnen behalve het besturingssysteem ook belangrijke applicaties of bestanden worden opgenomen.

AIX, het UNIX-besturingssysteem van IBM, biedt naast de TCB het Trusted Communication Path. TCP zorgt ervoor dat alle op de terminal draaiende processen die niet van de gebruiker zijn, worden beëindigd en dat vervolgens alleen programma's die in de TCB zijn opgenomen, kunnen worden opgestart. Door het beëindigen van de draaiende processen wordt voorkomen dat op de terminal ingetoetste passwords kunnen worden afgetapt.

Deze functie kan door de gebruiker worden geactiveerd met de toetscombinatie Ctrl-X, Ctrl-R of kan automatisch worden geactiveerd door in de configuratie-file /etc/security/user voor de gebruiker de parameter tpath=always op te nemen.

Controle op de security audit-programmatuur

Ten slotte dient ook de security audit-programmatuur te worden beschermd tegen het onopgemerkt aanbrengen van wijzigingen. De controles dienen dus ook voor de auditprogrammatuur, de referentiebestanden en de auditrapportage te worden uitgevoerd. Het verdient aanbeveling een kopie van de referentiebestanden op tape in een kluis te bewaren.

Mw.drs. M.C. van Lith RE Is in 1983 in dienst getreden bij KPMG Klynveld EDP Auditors en heeft thans de functie van supervisor. Zij heeft zich onder meer gespecialiseerd in de beveiliging van UNIX, en is enige tijd werkzaam geweest als systeembeheerder van een UNIX-omgeving. In deze functie was zij onder andere verantwoordelijk voor de inrichting van de beveiliging.

SAMENVATTING

Het besturingssysteem UNIX is ontwikkeld door AT&T. Doordat AT&T de source tegen geringe vergoeding beschikbaar stelde, ontstonden vele versies van UNIX. Gelukkig zijn er standaardisatiecommissies in het leven geroepen zoals OSF, X/OPEN en POSIX, waardoor de huidige UNIX-versies grote overeenkomsten vertonen. Dit komt ten goede aan de portabiliteit van zowel systeemsoftware als applicatiesoftware.

Elk object in de UNIX-omgeving wordt gerepresenteerd als een file die ergens in het file-systeem is geplaatst. Hierdoor is de toegangsbeveiliging voor een zeer groot deel terug te brengen tot objectbeveiliging.

Door de veelheid aan beveiligingsaspecten en files die van invloed hierop zijn, is het niet denkbeeldig dat een beheerder iets over het hoofd ziet. De beheerder dient over uitgebreide UNIX-kennis te beschikken en voortdurend alert te blijven.

Hoewel in dit artikel slechts de belangrijkste logische beveiligingsmaatregelen en programmeerbare controlefuncties zijn beschreven, kan worden geconcludeerd dat UNIX ook voor de administratieve wereld voldoende handvatten biedt om een goed te beveiligen, te beheren en te controleren omgeving te creëren.

LITERATUUR

[Dete93] Reinhard Detering, *Het complete UNIX boek*, 1993.

[Aust86] G.J.M. Austen en H.J. Thomassen, *UNIX, het standaard operating system*, 1986.

[Sobe84] M.G. Sobell, *A practical Guide to the UNIX System*, 1984.

[Blan92] A.J.A.R. Blankensteyn, *Basiscursus UNIX*, 1992.

[Hewl91] Hewlett Packard, *HP-UX System Security, Handboek bij het besturingssysteem HP-UX*, 1991.

[IBM91] IBM, *Elements of AIX Security: R3.1, Handboek bij het besturingssysteem AIX*, 1991.

Typologie van workflow-management-systemen

Drs. D.J.P. Witte

De 'flow of work' in een kantooromgeving moet bewust worden aangestuurd. Door sturing en beheersing op een centrale plaats te concentreren, krijgt de organisatie een instrument in handen waarmee de uitvoering van taken en de voortgang van de produktie kunnen worden ondersteund.
Het in kaart brengen van de vaak gecompliceerde werkstromen in relatie tot de geautomatiseerde voortgangsbewaking behoeft een gestructureerde aanpak.

INLEIDING

Uit cijfers van MIT Sloan School of Management blijkt dat in de periode van 1978 tot 1985 in de Verenigde Staten de produktiviteit in de industrie jaarlijks met 2,8 procent is gestegen. In diezelfde periode echter is de produktiviteit in de kantooromgeving jaarlijks met 0,9 procent gedaald. Deze tendens heeft zich nadien doorgezet. Tevens wordt vastgesteld dat de investering op IT-gebied binnen de kantooromgeving vele malen hoger lag dan in de industrie. Wat gaat er dan fout, vraag je je af. Zou er iets mis kunnen zijn met de wijze waarop werkprocessen in de kantooromgeving zijn geautomatiseerd? Veelal worden slechts enkele taken geautomatiseerd door middel van zogeheten verticale maatwerktoepassingen of met behulp van standaardapplicaties die meestal stand alone worden geïmplementeerd. Het automatiseren van een taak binnen het werkproces verhoogt weliswaar de kwaliteit van die handeling, maar draagt meestal niet noemenswaardig bij tot de produktiviteit. Een workflow-managementsysteem biedt wel de mogelijkheid om een substantiële verbetering van de produktiviteit te bereiken. Gedacht moet worden aan vijftig procent tot enkele honderden procenten produktiviteitstoename.

Implementatie van een workflow-managementsysteem binnen een organisatie wordt dikwijls voorafgegaan door een procesherontwerptraject. Het workflow-managementsysteem kan dan ook worden beschouwd als de faciliterende technologie van een herontworpen werkproces. Als voorwaarde geldt wel dat informatietechnologie in het werkproces is geïntegreerd.

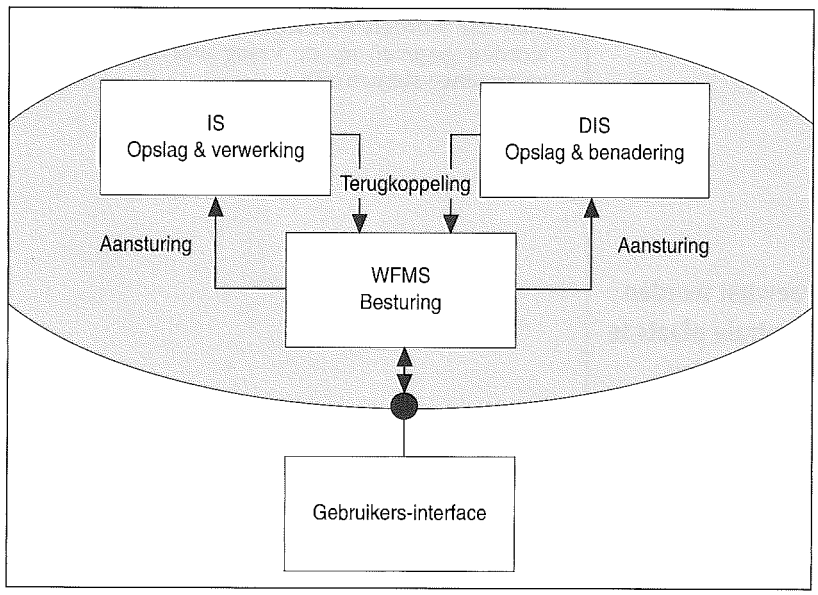
In dit artikel wordt een visie op workflow-managementsystemen gepresenteerd. Dit wordt gedaan aan de hand van een typologie waarin de verdeling van taken en werkprocessen binnen de gewenste IT-infrastructuur wordt beschreven. Door systemen te rubriceren op basis van werkproces- en taakautomatisering worden vijf typen workflow-managementsystemen onderscheiden. Voordat de typologie van workflow-managementsystemen zal worden beschreven, zal eerst antwoord worden gegeven op de vraag wat workflow-managementsystemen zijn.

BEGRIPSVERDUIDELIJKING

Wanneer wordt er gesproken van een informatiesysteem (IS) of van een documentair informatiesysteem (DIS)? En wanneer wordt een systeem tot een workflow-managementsysteem (WFMS) gerekend? Vanuit het oogpunt van een computer is een workflow-managementsysteem niets anders dan een computertoepassing. Het verschil is een onderscheid naar systeemfunctionaliteit. Het WFMS acteert op een hoger abstractieniveau dan informatiesystemen. Een traditioneel informatiesysteem automatiseert de opslag en benadering van bedrijfsgegevens waarop bepaalde bewerkingen (transformaties) kunnen worden uitgevoerd. Een DIS voegt hieraan een extra gegevenstype toe: gedigitaliseerde documenten (images). In het geval dat een systeem zich niet alleen beperkt tot deze functie, maar tevens voorziet in enige vorm van procesbesturing, is er sprake van een informatiesysteem met workflow-managementaspecten. Een workflow-managementsysteem pur sang richt zich uitsluitend op de automatisering van de procesbesturing en de ondersteuning van de werkuitvoering. Een workflow-managementsysteem is dan ook volledig onafhankelijk van image-technologie. In figuur 1 wordt een schematische voorstelling gegeven van de onderlinge verhoudingen tussen IS, DIS en WFMS. De wijze waarop het WFMS communiceert met de gebruiker wordt niet alleen bepaald door de geselecteerde WFMS-implementatie, maar ook door de manier waarop het workflow-systeem is ingericht. Een mogelijk scenario waarop de communicatie tussen gebruiker en WFMS zou kunnen plaatsvinden, luidt als volgt:

- Een gebruiker die aan het werkproces wil deelnemen maakt dit kenbaar aan het WFMS via een inlog-procedure.
- Het WFMS reageert hierop door na te gaan of er nog werk ligt dat door deze gebruiker moet worden afgehandeld.
- Een lijst met te verrichten werk - eventueel op volgorde van prioriteit - wordt aan de gebruiker getoond.
- De gebruiker kiest een stuk werk uit de lijst.
- Het WFMS haalt de gegevens op waaruit het stuk werk bestaat en laadt dit in de applicatie waarmee de gebruiker zijn bewerking moet uitvoeren.
- Na afhandeling geeft de gebruiker het stuk werk terug aan het WFMS. Hierna zal het WFMS het werk begeleiden naar een vervolgactiviteit.

Figuur 1. Functionele relatie tussen IS, DIS en WFMS.



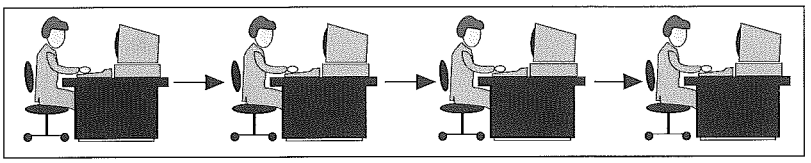
WORKFLOW IS HET ROUTEREN VAN EEN HOEVEELHEID WERK

Bedrijven die produkten leveren die volgens een vast stramien worden gefabriceerd, lenen zich bij uitstek voor automatisering van procesbesturing. Uit deze generieke bedrijfstypering valt op te maken dat niet alleen ondernemingen uit de produktie-omgeving, maar ook de zogenaamde administratiefabrieken in aanmerking komen om logistiek te worden geautomatiseerd. Administratieve omgevingen waar transactiegeoriënteerde werkstromen zijn te onderkennen, zijn kandidaat om workflow-management op toe te passen. Denk hierbij bijvoorbeeld aan een verzekeringsmaatschappij waar schadeclaims en verzekeringspolissen worden behandeld, en ook aan de administratieve afhandeling van patiënten binnen een ziekenhuis. Deze omgevingen worden gekenmerkt door een aaneenschakeling van handelingen die serieel, conditioneel of parallel moeten worden uitgevoerd. De figuren 2, 3 en 4 laten van elk een voorbeeld zien.

Seriële routering
Elke taak, gesymboliseerd door een werknemer achter een computer, moet steeds zijn voltooid voordat men kan overgaan tot de volgende activiteit. Hiermee wordt niet gesuggereerd dat iedere taak door een werknemer moet worden uitgevoerd. Er zijn ook taken die zonder menselijke tussenkomst door de computer worden uitgevoerd. Denk bijvoorbeeld aan het uitvoeren van calculaties of het uitsturen van digitale faxen.

Conditionele routering
De route die door een hoeveelheid werk wordt afgelegd, is afhankelijk van de uitkomst van beslissingsactiviteiten. In figuur 3 zou de tweede activiteit een controle op kredietwaardigheid van een persoon of instelling kunnen zijn. Afhankelijk van de kredietwaardigheid zal een route worden ingeslagen. Dit besliscriterium is binnen het WFMS vastgelegd. Hierdoor zal het WFMS bepalen naar welke van de twee vervolgactiviteiten een stuk werk wordt verstuurd, en niet de gebruiker die de kredietwaardigheid heeft vastgesteld.

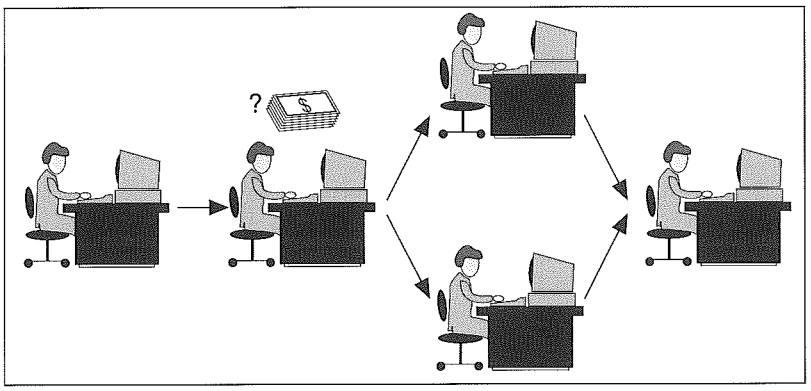
Parallelle routering
Het belangrijkste verschil tussen parallelle routering en conditionele routering van werk is dat bij parallelle distributie meerdere taken gelijktijdig een portie werk mogen afhandelen, terwijl in de conditionele situatie slechts één van de taken op basis van een beslissing een hoeveelheid werk krijgt toebedeeld. Parallelle routering van werk kan alleen worden toegepast indien de simultaan uit te voeren werkzaamheden onafhankelijk van elkaar kunnen worden verricht.



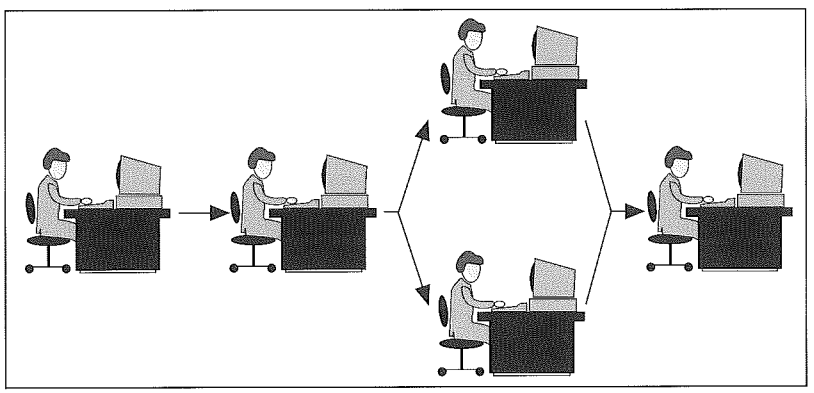
Figuur 2. Seriële routering.

WERKPROCESSTURING MET WORKFLOW-MANAGEMENT

In antwoord op de vraag 'Wat is het verantwoordelijkheidsgebied van de gebruiker?' kan een workflow-managementsysteem op twee manieren worden ingericht. Als twee uitersten worden de verantwoordelijkheid voor een activiteit en de verantwoordelijkheid voor een volledig produkt beschouwd.
In het eerste geval zal het WFMS als taak hebben een hoeveelheid werk (produkt) op het juiste moment bij de juiste gebruiker af te leveren. Het stadium waarin het produkt zich zal bevinden op het moment dat een bepaalde gebruiker dit moet gaan bewerken, is steeds hetzelfde. De gebruiker is als het ware één tandwiel in een groot stelsel van tandraderen.
In de tweede situatie zal de gebruiker aan alle stadia van het produkt een bijdrage leveren. Het WFMS zal, afhankelijk van het stadium waarin het produkt zich bevindt, de juiste bewerkingsgereedschappen (applicaties) aan de gebruiker moeten aanbieden. De gebruiker overziet de gehele ontwikkelingsloop van een bepaald produkt. Afhankelijk van de inrichting kan het WFMS sturing verrichten op activiteitniveau dan wel op produktniveau.
Het merendeel van de huidige generatie workflow-managementsystemen kan op beide manieren worden ingericht.



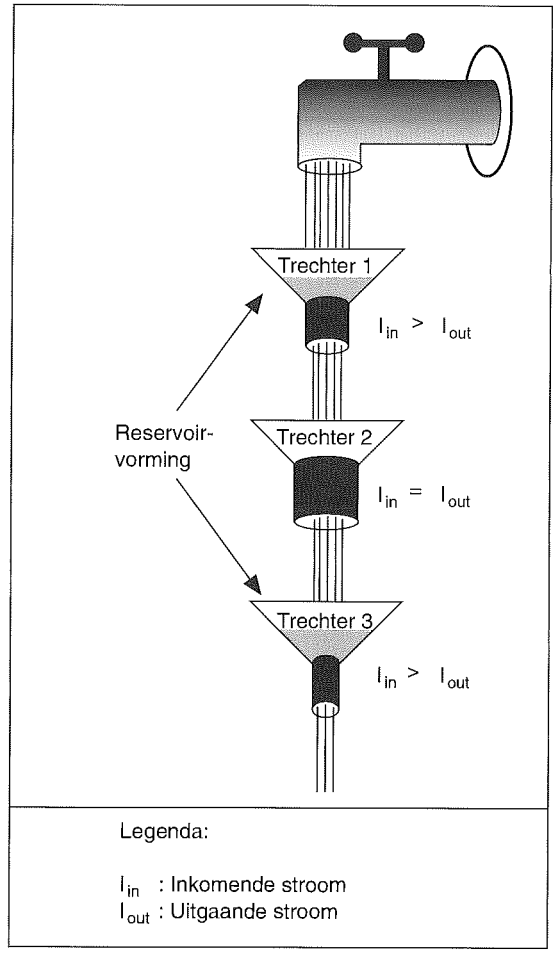
Figuur 3. Conditionele routering.



Figuur 4. Parallelle routering.

WERKPROCESAUTOMATISERING

In de praktijk wordt workflow-management al aangetroffen. Het is dan ook niet vreemd dat dit onderwerp vaak reacties oproept als: 'Oh, maar dat doen wij al jaren!' Wat is dan het nieuwe dat door workflow-management wordt gebracht? Workflow-management bestaat inderdaad al jaren, maar het bewustzijn dát men het reeds (gefragmenteerd) toepaste ontbrak vaak. Alleen een integrale aanpak waarbij alle werkprocessen worden betrokken die een bijdrage leveren aan het primaire bedrijfsproces, kan leiden tot produktiviteitsverbeteringen in de orde van honderd of meer procent. Aan de basis van dit succes staat aan de ene kant een duidelijke bedrijfsstrategie en aan de andere kant een heldere visie op de manier waarop bedrijfsprocessen beheerst moeten worden. De bewustwording en het inzicht om bedrijfsprocessen te beheersen en te controleren maakte tientallen jaren geleden al opgang in de procesindustrie. Een tot de verbeelding sprekend voorbeeld hiervan is het assemblageproces van auto's waarbij robots onderdelen van een auto in de fabricagelijn bevestigen. Maar ook het geautomatiseerd vullen, etiketteren en verpakken van frisdrankflesjes behoort tot dezelfde categorie van procesautomatisering. Neem nu het voorbeeld van de frisdrankenleverancier. Indien de leverancier alleen was overgegaan tot het automatiseren van het vullen van flesjes, ontstaat er stagnatie in het proces op de plaats waar de doppen op de flessen moeten worden be-



Figuur 5. Ontstaan van bottlenecks.

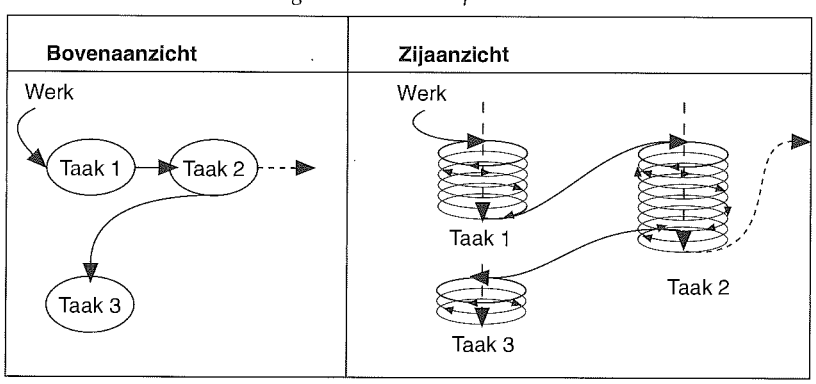
vestigd. Tevens ziet de leverancier zich geplaatst voor het probleem de vulmachine te voorzien van voldoende flesjes. De efficiëntie van het bedrijfsproces wordt bepaald door de verwerkingssnelheid van de traagste activiteit op het kritieke pad. Deze bewering wordt in figuur 5 met behulp van een systeem van drie trechters aanschouwelijk gemaakt.

In de trechters 1 en 3 ontstaat een voorraad omdat de doorvoersnelheid in beide gevallen kleiner is dan de ingaande stroom ($I_{in} > I_{out}$). De doorvoersnelheid van het totale systeem kan worden vergroot door de bottlenecks op te heffen. In tegenstelling tot die van trechter 1 zal een uitstroomvergroting van trechter 3 direct bijdragen tot een verhoging van de doorvoercapaciteit van dit systeem. Met dit voorbeeld wordt aangegeven dat naast taakautomatisering (trechterinstelling) ook gestreefd moet worden naar een stroomlijning tussen de taken onderling. Een workflow-managementsysteem is bij uitstek geschikt deze rol te vervullen.

TYPOLOGIE VAN WORKFLOW-MANAGEMENTSYSTEMEN

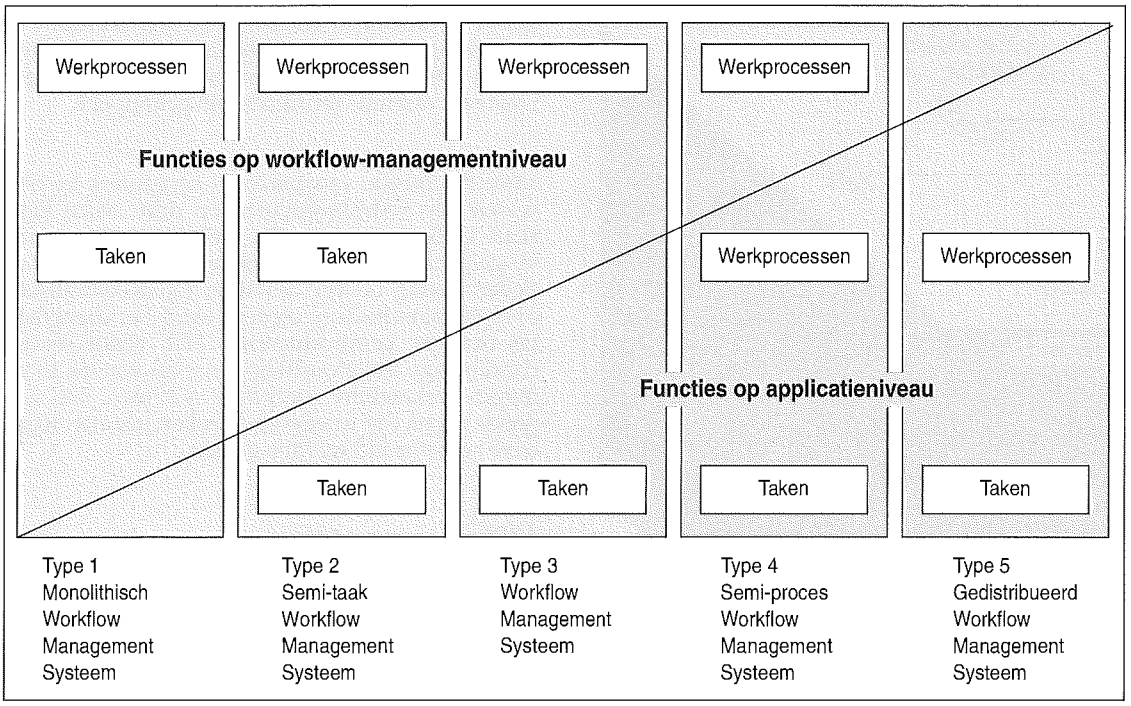
Om workflow-managementsystemen te typeren wordt onderscheid gemaakt in twee niveaus waarin bedrijfsregels worden vastgelegd: *taken* en *werkprocessen*. Een taak voert transformaties uit op een hoeveelheid werk. Nadat een taak is uitgevoerd, betekent dit dat het werk een stap dichter bij het eindprodukt is gekomen. Vervolgens wordt het werk naar een volgende taak verstuurd. De volgorde en de samenhang van de taken wordt in het werkproces vastgelegd. Neem als voorbeeld de afhandeling van een schadeclaim bij een verzekeringsmaatschappij. De eerste taak zou het invoeren van de schadegegevens in een informatiesysteem kunnen zijn. De tweede taak is bijvoorbeeld een controle op eerder geleden schaden. Op basis van de hoogte van de schadeclaim en eerder ingediende claims kunnen verschillende vervolgtrajecten worden ingeslagen. In figuur 6 worden de twee stromingsrichtingen van een hoeveelheid werk aangegeven.

Figuur 6. Taken en processen.



Het bovenaanzicht geeft de horizontale processgang weer en het zijaanzicht de transformaties die de taken op het werk verrichten (verticale applicaties). In de mate waarin processen en taken van elkaar zijn gescheiden, valt een overgangsgebied waar te nemen. In de praktijk worden zowel applicaties aangetroffen die een stuk van het proces automatiseren als managementsystemen die een onderdeel van een taak uitvoeren.

In figuur 7 wordt de typologie van workflow-managementsystemen gepresenteerd. Zij geeft een verdeling weer van processen en taken op applicatie- en workflow-managementniveau. De glijdende schaal zoals die in deze figuur is aangebracht, wordt aanschouwelijk gemaakt met behulp van het workflow-model (figuur 8).

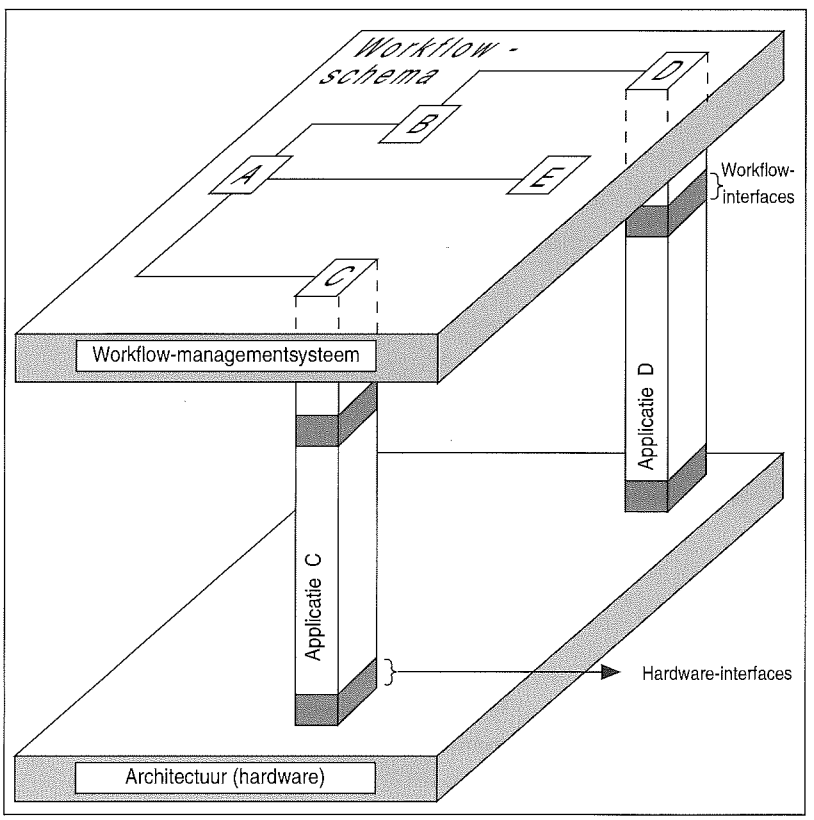


Figuur 7. Typologie van workflow-managementsystemen.

HET WORKFLOW-MODEL

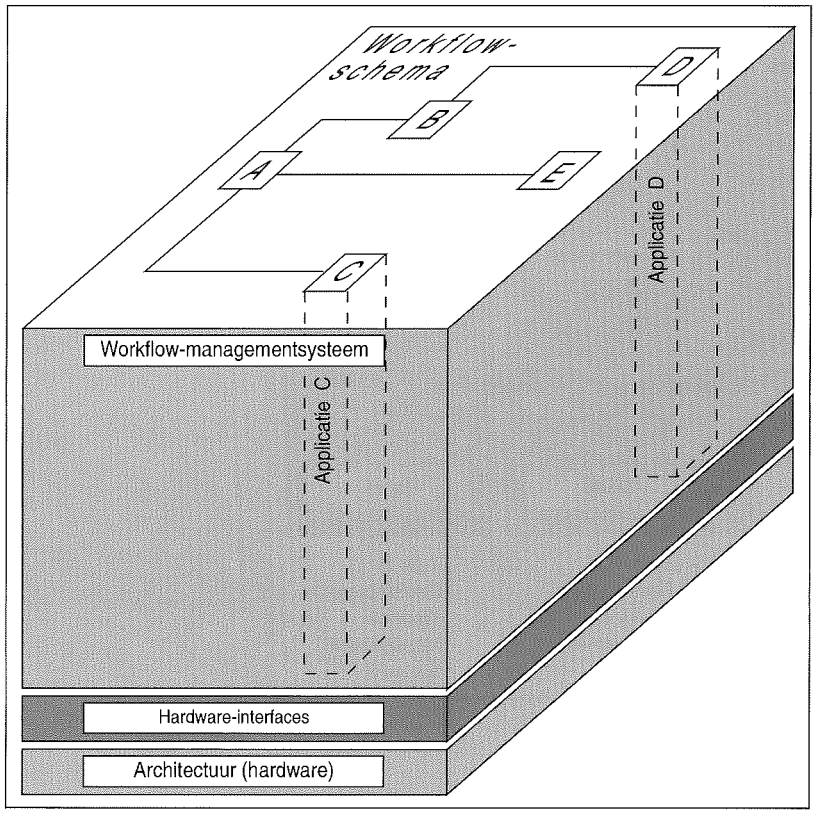
In deze paragraaf wordt het model van een workflow-systeem gebruikt ter verduidelijking van de typologie van workflow-managementsystemen. In het bovenste plateau van het basismodel (figuur 8) wordt het werkproces gedacht. De taken worden in dit voorbeeld aangegeven met de letters A tot en met E. Het geheel van taken en routering van taak naar taak vormt het workflow-schema. Het workflow-schema brengt één geautomatiseerd werkproces in kaart. Orthogonaal op dit vlak bevinden zich (denkbeeldig) de applicaties die elk een taak binnen het werkproces vervullen. Met het onderste plateau wordt de architectuur aangegeven waarop de diverse applicaties operationeel zijn. Concreet kan een tekstverwerker op een PC draaien en, bijvoorbeeld, een salarisadministratiesysteem op een mainframe.

Figuur 8. Basismodel van een workflow-(management)-systeem.



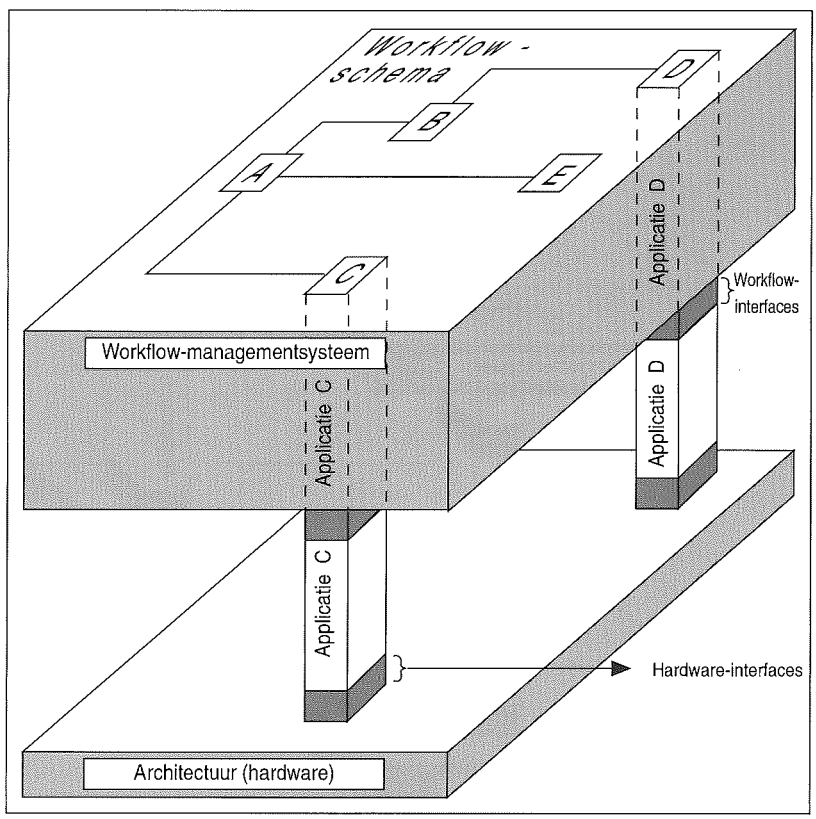
Type 1: Monolithisch workflow-managementsysteem

In het monolithisch workflow-managementsysteem worden zowel processen als taken afgehandeld. De volgorde van de handelingen is 'hard-coded' binnen het systeem opgenomen. In het workflow-model in figuur 9 wordt dit aangegeven door alle (verticale) taken volledig binnen het workflow-systeem onder te brengen. Snel en flexibel inspelen op veranderingen in de markt waardoor een nieuwe aanpak wordt vereist, is niet of moeilijk realiseerbaar. Dergelijke systemen zijn geschikt om in massaproduktie-omgevingen te worden in-



Figuur 9. Traditionele master/slave-verhouding.

Figuur 10. Een deel van de afhandeling van de business logic wordt binnen het WFMS getrokken.



gezet. Voorbeelden waarin deze architectuur van toepassing is, zijn de zogeheten master/slave-systemen. Denk hierbij aan mainframe-toepassingen waaraan 'domme' terminals zijn gekoppeld.

Vóór de intrede van personal computers in 1982 waren alle bedrijfssystemen op deze wijze ingericht. De komst van de PC met zijn eigen verwerkingscapaciteit en de ontwikkeling van netwerken deden menig bedrijf besluiten tot decentralisatie over te gaan. In deze context werd het client/server-concept geïntroduceerd. Het client/server-concept ligt ten grondslag aan veel van de in de markt verkrijgbare workflow-systemen. De volgende typen die worden besproken, moeten tegen deze achtergrond worden gezien.

Type 2:
Semi-taak workflow-managementsysteem

In een semi-taak workflow-managementsysteem wordt een deel van de taken naar de applicatie gedelegeerd. Het andere deel van de taken wordt nog steeds door het managementsysteem afgehandeld. In het workflow-model in figuur 10 wordt dit aangegeven door de verticale pootjes uit te laten steken buiten het workflow-managementsysteem. Binnen dit type heeft het WFMS nog steeds een dominante rol. Door logica van de uit te voeren taak op te nemen binnen het WFMS ontstaat een zogeheten proprietary workflow-systeem dat als oplossing voor het probleemgebied op maat is geschreven. Echter ook nu geldt, zij het in mindere mate, dat de flexibiliteit te wensen overlaat. Anders geformuleerd, zonder herprogrammering kan dit type workflow-systeem niet op andere toepassingsgebieden worden ingezet.

Type 3:
Workflow-managementsysteem

Er is sprake van een zuiver workflow-managementsysteem als een apart systeem de sturing en beheersing van het werkproces volledig verzorgt. Dit type systeem, dat is weergegeven in het basismodel van figuur 8 (zie hiervoor), transformeert geen informatie maar transporteert deze alleen. Een zuiver workflow-managementsysteem bevat dan ook geen kennis van *informatie*structuren maar van *werkproces*structuren. Door de processen los te koppelen van de taken wordt expliciet het managementsysteem ontheven van kennis van bedrijfsinformatie en is het daardoor data-onafhankelijk. In het model in figuur 8 wordt dit aangegeven door de applicaties die taken automatiseren, volledig buiten de horizontale procesbesturingslaag te tekenen. Deze splitsing introduceert een grote mate van flexibiliteit. Immers, een verandering in het werkproces heeft geen consequenties meer voor de wijze waarop een portie werk wordt getransformeerd. Hierdoor blijven de specifieke maatwerktoepassingen ongemoeid. Leveranciers van de huidige generatie workflow-managementsystemen die commercieel de markt op gaan, zullen bij voorkeur hun systeem op dit type baseren. Deze systemen bieden voorzieningen om bestaan-

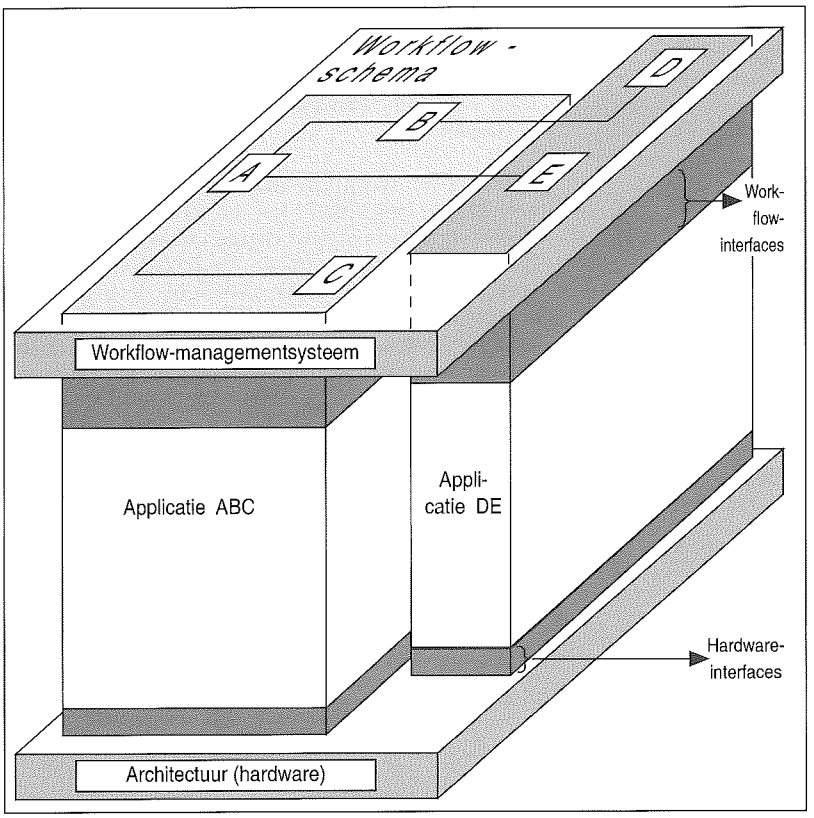
de applicaties te koppelen - workflow-aware te maken - met het WFMS. In figuur 8 wordt dit aangegeven door de gearceerde bandjes tussen de applicatie en het WFMS (workflow interfaces).

Type 4:
Semi-proces workflow-managementsysteem

Bij een semi-proces workflow-managementsysteem wordt een deel van de procesautomatisering getrokken binnen de applicatie die voor de taakautomatisering zorgt. In het workflow-model in figuur 11 wordt dit aangegeven door het samentrekken van een aantal taken binnen één verticale poot. De wijze waarop de activiteiten worden aangestuurd - de gang van het bedrijfsproces - ligt daarmee voor een deel besloten binnen de applicatie. Het WFMS kan geen invloed uitoefenen op de aansturing van de activiteiten die binnen de applicatie zijn opgenomen. Immers, als een hoeveelheid werk eenmaal binnen een applicatie is opgenomen, valt het buiten de invloedssfeer van het workflow-managementsysteem. In de praktijk worden regelmatig systemen aangetroffen die aan dit beeld voldoen. In de tijd dat de automatiseringsinspanning vooral werd ingezet om taken te automatiseren, probeerde men juist taken te clusteren binnen één computertoepassing (eiland-automatisering). We zien nu dat bedrijven de systemen waaraan men gehecht is geraakt, niet willen vervangen, maar juist willen opnemen binnen een workflow-omgeving. De mogelijkheid om een stuk werk te managen wordt hierdoor wel gefragmenteerd. Om de samenhang van de werkuitvoering te kunnen bewaken is de introductie van een workflow-managementsysteem daarom wenselijk.

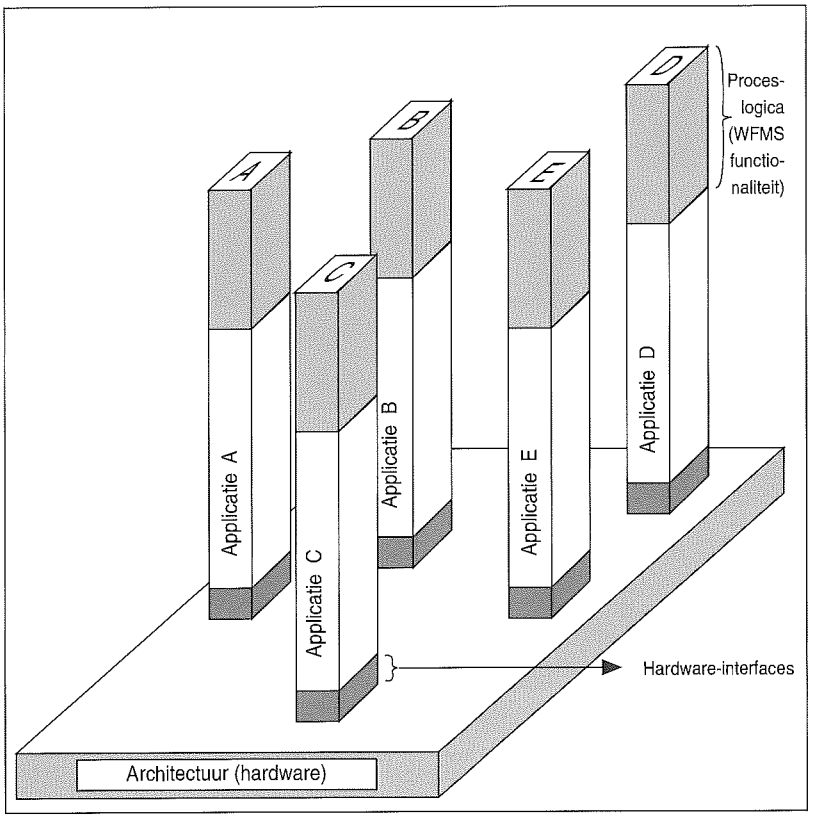
Type 5:
Gedistribueerd workflow-managementsysteem

Bij gedistribueerde workflow-managementsystemen is de procesbesturing verdeeld over de applicaties die met elkaar communiceren via het uitwisselen van gegevens die een hoeveelheid werk representeren. De criteria waarop de applicaties elkaar werk toesturen zijn binnen de applicatie vastgelegd. Omdat er geen 'centrale regelkamer' in dit scenario aanwezig is, is het onmogelijk het integrale werkproces te sturen en te beheersen. In het workflow-model in figuur 12 is het overkoepelende horizontale vlak weggelaten. De verticale applicaties zijn volledig van elkaar geïsoleerd. Een situatie waarin van deze architectuur sprake is, is bijvoorbeeld die waarbij door de organisatie een document rouleert waarop een aantal specifieke handelingen moeten worden verricht. Na het uitvoeren van een bewerkingsslag wordt het document naar een volgende activiteit gestuurd door het bijvoorbeeld als 'attachment' op te nemen binnen een E-mail-pakket. In dit voorbeeld wordt de logica van het werkproces uit de applicatie gehaald. Een mail-pakket verzorgt de distributie en de gebruiker kent zijn positie in het proces (weet waar het naar toe moet). In zijn algemeenheid kan worden gezegd dat in omgevingen die gekenmerkt worden door een ad hoc-karakter, deze werkvorm vaak wordt aangetroffen.



Figuur 11. De gearceerde activiteiten worden door één applicatie afgehandeld.

Figuur 12. Applicaties sturen elkaar werk toe.



Drs. D.J.P. Witte
Is organisatie-adviseur bij KPMG Klynveld Management Consultants en is werkzaam op het gebied van workflow-managementsystemen en documentaire informatiesystemen. Zijn aandachtsgebieden zijn onder meer systeemmodellering, objectoriëntatie en client/servertechnologie. Hij is docent van de cursus Workflow Management die door de PAO Informatica wordt georganiseerd.

Daarnaast bestaat de mogelijkheid om applicaties direct met elkaar gegevens te laten uitwisselen - al dan niet via een netwerk - door verschillende vormen van 'Inter Process Communication' (IPC) toe te passen.

Alle typen workflow-managementsystemen die zojuist zijn besproken, komen in de praktijk voor. Vaak worden meerdere vormen naast elkaar toegepast. Afhankelijk van de bedrijfsdoelstellingen, werkwijze en produkten die door de organisatie stromen zal het ene type beter renderen dan het andere. Anders gezegd: de typologie doet geen uitspraak omtrent de kwaliteit van de kantoorautomatisering in de organisatie. Wat wel door de typen wordt aangegeven, is de mate van flexibiliteit en de mogelijkheden om een stuk werk te managen.

WELK SYSTEEMTYPE GEBRUIKT U?

De boodschap die in dit artikel wordt uitgedragen, is dat de 'flow of work' bewust moet worden aangestuurd. Door de sturing en beheersing op een centrale plaats te concentreren, krijgt de organisatie een instrument in handen waarmee zowel de uitvoering van taken als de voortgang van de produktie kan worden ondersteund. Naast de vraag *wat* er stroomt zal ook inzicht moeten worden verkregen over *hoe* de stroom moet lopen. Dat het in kaart brengen van vaak gecompliceerde werkstromen in relatie met geautomatiseerde voortgangsbewaking behoefte heeft aan een gestructureerde aanpak mag duidelijk zijn. Drastische produktiviteitsverbeteringen kunnen pas worden behaald als bedrijfsprocessen worden ingericht op basis van het produkt dat door de organisatie stroomt met inachtneming van workflow-managementtechnologie. De opmerking 'Het management moet opnieuw met de voeten in de klei' is hier wellicht niet misplaatst.

EDP AUDITORIUM

BOEKBESPREKING

D.S.J. Remenyi, A. Money en A. Twite,
A guide to measuring and managing IT benefits

Drs. E.W. Berghout

Inleiding

Veel EDP-auditors worden momenteel geconfronteerd met de vraag of zij de informatievoorziening van een organisatie willen waarderen; het liefst in geld, eventueel met een rapportcijfer. Het toepassen van economische theorieën in de informatievoorziening mag zich dan ook verheugen in een grote belangstelling. Men spreekt over de economische aspecten van de informatievoorziening, economisch informatiemanagement of kortweg informatie-economie. Vraagstukken die hierbij aan de orde komen zijn: hoeveel geld moet ik aan mijn informatievoorziening uitgeven, aan welke projecten moet ik de hoogste prioriteit geven, hoe moet ik baten en lasten tijdens het realiseren en exploiteren van informatiesystemen in de hand houden, en wanneer moet ik bepaalde informatiesystemen gaan stopzetten? Over deze vragen bestaat al veel literatuur, maar de auteurs van het hier besproken boek hebben gelijk als zij stellen dat er nog geen boek is geschreven dat de gehele levenscyclus van informatiesystemen bestrijkt. In dit boek wordt een poging gedaan om de economische aspecten van alle fasen af te dekken. Daarbij hanteren de auteurs de definitie dat met economische aspecten van informatiesystemen wordt bedoeld: 'een systematische verzameling van concepten en theorieën die de rol van informatie verklaart in het ondersteunen van de onderneming bij het concipiëren, produceren en distribueren van produkten en diensten ter bevordering van de maatschappelijke welvaart'.

Onderwerpen

Het boek begint met de veranderende rol van de informatievoorziening in organisaties. In het verleden heeft het accent vooral gelegen op het verhogen van de efficiëntie en de effectiviteit van bestaande bedrijfsprocessen, tegenwoordig gaat de aandacht veelal uit naar het transformeren van bedrijfsprocessen. M. Porters modellen van 'competitive forces' en 'value chain analysis' worden hierbij gebruikt. Daarna stapt het boek over op investeringsanalyses van voorstellen voor nieuwe informatiesystemen. Er wordt een typologie gegeven van mogelijke baten en in een kort overzicht worden elf methoden voor investeringsanalyse behandeld. Dit betreft de volgende methoden: 'strategic match analysis and evaluation', 'value chain assessment', 'relative competitive performance', 'proportion of management vision achieved', 'work study assessment', 'economic assessment - I/O analysis', 'financial cost benefit analysis', 'user attitudes', 'user utility assessment', 'value added analysis', 'return on management' en 'multi-objective, multi-criteria methods'. Een uitgebreide baten/lasten-analyse ('cost benefit analysis') wordt in detail uitgewerkt en met veel voorbeelden en praktische tips geïllustreerd.

Ook op het gebied van de evaluatie van de gehele informatievoorziening komt de lezer ruimschoots aan zijn/haar trekken. Het boek bevat bijvoorbeeld een uitgebreide uitwerking van een enquête naar de tevredenheid van de gebruikers en inleidingen tot de 'value for money'- en 'health check review'-studies van de informatievoorziening. Daarnaast wordt nog veel informatie gegeven over het opstellen, houden en verwerken van enquêtes, en bevat het boek appendices met onder andere een uitgebreide behandeling van een voorbeeld en een inleiding in financiële ratio's en in factoranalyse.

Tot slot

Het boek is plezierig geschreven en bevat veel voorbeelden. Men kan duidelijk zien dat de auteurs behoorlijk wat ervaring met het onderwerp hebben opgedaan, maar er zijn duidelijk ook onderdelen voor verbetering vatbaar.

Het boek pretendeert ten onrechte de economische aspecten van de gehele levenscyclus van informatiesystemen af te dekken. Men gaat uitvoerig in op een manier om vooraf informatiesystemen te beoordelen en presenteert ook een drietal manieren om achteraf de gehele informatievoorziening te evalueren, maar er zijn vele auteurs die meer fasen identificeren en voor zover deze al worden behandeld, is de uitleg summier en van enige samenhang tussen de diverse fasen is al helemaal geen sprake. (Zie over dit onderwerp bijvoorbeeld het artikel *Investeren in informatietechnologie: take IT or leave IT*, Swinkels en Van Irsel, Compact 1992/2.) De auteurs onderkennen dit zelf ook als zij vermelden dat het boek weliswaar vernieuwend is, maar zeker niet het laatste boek over het onderwerp zal zijn. Daarnaast bevat het boek diverse slordigheden en is duidelijk merkbaar dat het door verschillende auteurs is geschreven. Echter, met de goede stukken van het boek kan iedere EDP-auditor direct aan de slag.

D.S.J. Remenyi, A. Money en A. Twite,
A guide to measuring and managing IT benefits, NCC Blackwell, Manchester/Oxford 1993,
ISBN 1-85554-378-8, *f* 116,64.

CUMULATIEF

Overzicht van eerder verschenen artikelen in Compact
Een compilatie van artikelen over informatica en recht die in eerdere Compacts zijn verschenen, is, aangevuld met actuele bijdragen over dit onderwerp, opgenomen in *Twintig over Informatietechnologie en recht*. Twintig auteurs behandelen een breed spectrum van aspecten van de raakvlakken van informatietechnologie en recht op voor EDP-auditor, manager, adviseur, jurist en accountant toegankelijke wijze.
Het boek is verkrijgbaar via de boekhandel onder nummer: ISBN 90 14 04634 0.

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

1 20e jaargang 93/1 lente 1993

Netwerkmanagement, de organisatorische opzet en financiële beheersing
ir. E.J. Evelo

Akzo en telecommunicatie, de organisatorische ontwikkeling
H. Reijn

SURFnet, beveiliging in een open netwerk
E. Zegwaart

Beveiliging van digitale kieslijnen
drs. ing. D. Brouwer

Secure Cash Management; an audit perspective
M. Kennett BA

Nieuwe ontwikkelingen in de cryptografie:
Kerberos en Digital Signature Standard
drs. T.P. de Vries

Beveiligingsperikelen rondom Novell NetWare
J.L. Ramos Najera

2 20e jaargang 93/2 zomer 1993

Informatietechnologie duur? I/T Assessment: een beproefde methode voor het beoordelen van effectiviteit en efficiëntie van de informatieverzorging
drs. B.T. Janssen, ing. W.J.D. Koot en ir. E.J. Mutsaers

Prioriteitenstelling met Decision
dr. P.J. van Meel RI

De audit van een IT-investeringsaanvraag
drs.ing. S.R.M. van den Biggelaar en drs. P.P.M.G.G. Brouwers

Verzekerbaarheid van automatiseringsrisico's
mw.mr.drs. A.W. Duthler

Beveiligingsstandaard voor informatiesystemen
prof.dr.ir. R. Paans RE

Global electronic mail: integratie van elektronische post met X.400
ir. A. van Kooij

3 20e jaargang 93/3 herfst 1993

De toegevoegde waarde van EDP-auditing bij systeemontwikkeling
ir. J.A. Verstelle

Normenstelsels voor systeemontwikkeling: hoe bruikbaar zijn deze?
mw.drs. C.D.M. van der Veen

Projectbeheersing en -audit: contingency-benadering vereist
ir. B.A.W.M. Bruns

De toegevoegde waarde van inspectietechnieken tijdens het ontwikkeltraject
B. Rooth

Invoering van informatiesystemen
drs. Th.H. van Hesteren

Twintig vuistregels voor 'foutloos' onderhoud
E. Bergler

4 20e jaargang 93/4 winter 1993

Ontwikkelingen in de accountantscontrole in een geautomatiseerde omgeving
drs. R.G.A. Fijneman RE RA

Aandacht voor interne controle tijdens systeemontwikkeling
drs. J.J. van Beek RE RA

Audit automation
drs. L.H. Dam RA en drs. P. Veltman RE RA

Operational auditing en EDP-auditing; is hier sprake van een begripsverwarring?
J.C. Boer RE RA

Accountant, EDP-auditor en jurist: een multidisciplinaire samenwerking
mw. mr. drs. A.W. Duthler

Automatiseringsrisico's, verzekeringen en de rol van de accountant
drs. G.J.W.C. Vankan

Geautomatiseerde betalingen
drs. R. Oudega en drs. P. Veltman RE RA

1 21e jaargang 94/1 lente 1994

De invloed van informatietechnologie op de beheersing van organisaties
prof. A.W. Neisingh RE RA

Rekencentra: normen voor menskracht
prof.dr.ir. R. Paans RE

Accountant en de kosten- en batenbeheersing van informatietechnologie
prof. H.B. Moonen RE RA

Informatiebeveiliging: de tijd is rijp
drs. H.G.Th. van Gils RE RA

Het beoordelen van het testen van systemen
P. van Berge