KWARTAALBLAD EDP-AUDITING

1994/3

DIGITALE SNELWEG

COMPACT HERFST

Compact ®
Jaargang 21, nummer 3
Een uitgave van KPMG Klynveld EDP Auditors en Samsom BedrijfsInformatie, werkmaatschappij van Wolters Kluwer NV.
Het blad verschijnt 4 x per jaar.

Redactie
Prof. A.W. Neisingh RE RA (hoofdredacteur)
J.C. Boer RE RA
Ir. J.A.M. Donkers
Drs. R.G.A. Fijneman RE RA
Drs. P. Veltman RE RA

Redactiesecretariaat
Mw. I. de Koning,
Samsom BedrijfsInformatie,
Postbus 4,
2400 MA Alphen aan den Rijn
Tel.: 01720 - 66 746
Fax : 01720 - 66 569

Vormgeving
Bureau Karakter, Delft

Aan dit nummer werkten mee
Mw.mr. G.P. van Duijvenvoorde
Mw. J.A.M. Holla
H. van Hulst
Ir. P. Kornelisse
Ir. J.H. Lie-Tjauw
Ing. G.H.M. Meijer RE

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

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.

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.

In allerlei publikaties wordt de laatste tijd veel aandacht besteed aan de ontwikkelingen rond de digitale snelweg, ook wel elektronische snelweg en information (super)highway genoemd. Uit deze publikaties wordt niet geheel duidelijk wat er precies onder moet worden verstaan, maar het gaat om een breedbandige telecommunicatie-infrastructuur die geschikt is voor interactieve multimediatoepassingen.

Of hier slechts sprake is van een mediahype is nog maar de vraag. Veelvuldig wordt het voorbeeld aangehaald van de overname van de filmmaatschappij Paramount door de kabelexploitant Viacom voor een bedrag van tien miljard dollar (drie maal de beurswaarde). Kennelijk neemt het (Amerikaanse) bedrijfsleven de ontwikkelingen serieus.

Ook de politiek toont zich geïnteresseerd, niet alleen in de Verenigde Staten maar ook in Europa en Japan. Zo heeft de Amerikaanse vice-president Al Gore een actieplan gelanceerd voor de vorming van een 'National Information Infrastructure', en hier ook - zij het beperkte - financiële ondersteuning voor toegezegd. Het 'witboek' van Delors is een vergelijkbaar Europees initiatief.
Intussen worden in Nederland de contouren zichtbaar van de nieuwe Wet op de telecommunicatievoorzieningen. Het is te hopen dat deze wet voldoende 'toekomstvast' is om de nieuwe ontwikkelingen niet in de weg te staan.

Wat er ook van de digitale snelweg moge komen, de voorloper ervan, Internet, bestaat al zo'n twintig jaar. Door sommigen wordt dit grootste netwerk ter wereld als synoniem beschouwd met de digitale snelweg, anderen zien nog veel (technische en financiële) obstakels voor het realiseren van de 'echte' snelweg.

Hoe dan ook, EDP-auditors zullen in hun dagelijkse praktijk steeds meer te maken krijgen met Internet. Met de stijgende populariteit van het besturingssysteem Unix wordt ook het netwerkprotocol TCP/IP, waarop Internet is gebaseerd en dat in 1982 aan Unix werd toegevoegd, steeds vaker toegepast. Daarnaast gaan steeds meer organisaties ertoe over hun netwerken aan te sluiten op Internet. Te verwachten is daarom dat op TCP/IP gebaseerde privé-netwerken en aansluitingen van privé-netwerken op het openbare Internet in toenemende mate object van EDP-audit zullen zijn.
Behalve object van onderzoek kan een Internetaansluiting ook een nuttig hulpmiddel zijn bij de beroepsuitoefening; Internet vormt een wereldwijd systeem voor elektronische post en elektronische bibliotheken, waar ook allerlei nuttige 'freeware' kan worden verkregen.

Drs. P. Veltman RE RA

Inleiding tot op TCP/IP gebaseerde netwerken

Ir. P. Kornelisse

Het op de TCP/IP-protocolfamilie gebaseerde Internet is door het bedrijfsleven lange tijd beschouwd als een netwerk behorend tot de wereld van de universitaire en militaire research-instellingen. Met de penetratie van Unix heeft echter ook TCP/IP op grote schaal zijn intrede gedaan in commerciële IT-omgevingen.
De vele publikaties over inbraken, virussen, wormen en wat dies meer zij in op Internet aangesloten (meestal Unix-) systemen roepen het beeld op van een inherent onveilige netwerk-omgeving. Kennis over de werking van TCP/IP kan dit beeld echter bijstellen. Kornelisse, die geldt als een specialist in Unix en TCP/IP, behandelt de verschillende onderdelen van TCP/IP en gaat in op de beheer- en beveiligingsmogelijkheden.

INLEIDING

In de jaren tachtig is veel energie besteed aan de standaardisatie van netwerkprotocollen volgens OSI (Open Systems Interconnection). Daarnaast heeft ook TCP/IP zich snel in de markt weten te ontwikkelen. Als gevolg hiervan is TCP/IP nu de de facto-standaard geworden. Er mag dus worden verwacht dat EDP-auditors steeds vaker TCP/IP zullen tegenkomen in een netwerkomgeving.
Sinds 1982, toen de TCP/IP-protocolfamilie werd toegevoegd aan Unix, heeft TCP/IP sterk aan populariteit gewonnen.

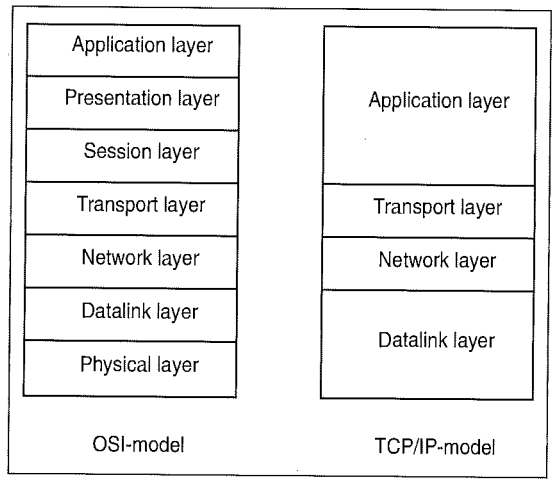
TCP/IP is een familie van netwerkprotocollen. Deze protocollen vinden de herkomst bij ARPA (Advanced Research Projects Agency) van het Department of Defence in de Verenigde Staten. Op basis van TCP/IP is eerst ARPANET in het leven geroepen. ARPANET is een netwerk tussen militaire installaties, universiteiten en research-instellingen. Intussen is dit netwerk uitgegroeid tot het bekende Internet, ofwel de digitale snelweg. Internet is het wereldomspannende netwerk met circa 20 miljoen gebruikers.

Bij TCP/IP is er sprake van host-to-host-netwerkverkeer. In een operationele situatie is geen centraal beheer noodzakelijk. Voordelen van TCP/IP zijn ook de onafhankelijkheid van leveranciers van besturingssystemen en netwerkcomponenten, de toepasbaarheid op PC's tot en met supercomputers en de toepasbaarheid voor zowel LAN's als WAN's.

TCP/IP-FAMILIE

De TCP/IP-protocolfamilie is gedefinieerd via RFC's[1] (Requests for Comments), onder beheer van de Internet Activities Board (RFC 1160). Om binnen de TCP/IP-protocolfamilie een protocol toe te voegen of te wijzigen dient een RFC te worden ingediend. Een RFC doorloopt diverse stadia, waarna het op een gegeven moment kan worden opgenomen als onderdeel van de TCP/IP-protocolfamilie.

In netwerkomgevingen onderkennen we tegenwoordig diverse protocolfamilies, zoals OSI, TCP/IP, SNA, IPX en DECnet. In figuur 1 wordt het TCP/IP-model afgebeeld in relatie tot OSI.



Figuur 1. OSI- en TCP/IP-model.

Het TCP/IP-model is verdeeld in een aantal lagen:

– *Applicatielaag*
Interface tussen de gebruikers(-programmatuur) en de netwerkprogrammatuur.

– *Transportlaag*
Interface ten behoeve van de verzorging van het transport van gegevens van gebruikers(-programmatuur).

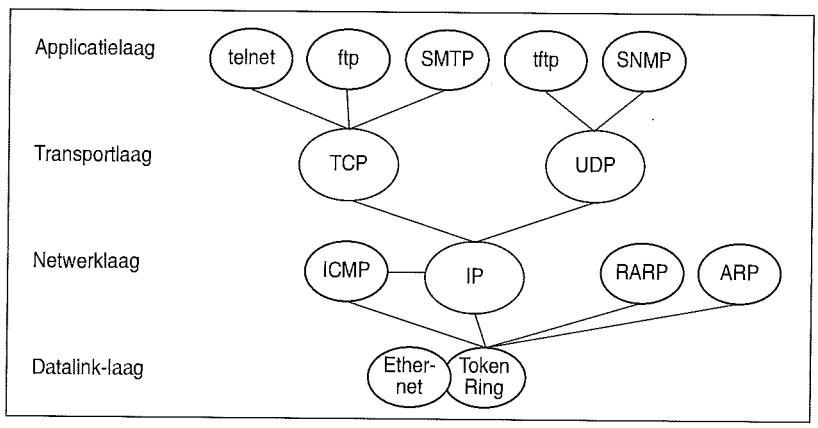
– *Netwerklaag*
Interface voor de verzending van datagrammen (gegevenspakketten) en routering van netwerkverkeer.

– *Datalink-laag*
Interface voor de overdracht van datagrammen aan fysieke netwerken.

In figuur 2 wordt een overzicht gegeven van de belangrijkste protocollen van de TCP/IP-familie. In de volgende paragraaf wordt elke laag van het TCP/IP-model nader toegelicht. In tabel 1 wordt de betekenis van de vermelde protocollen aangegeven.

1. *RFC's zijn opvraagbaar via Internet, gebruikmakend van de node ftp.uu.net.*

Figuur 2. TCP/IP-protocollen.



WERKING VAN TCP/IP

Nu enige TCP/IP-terminologie is toegelicht, wordt nader ingegaan op de werking van elk van de TCP/IP-lagen.

Datalink-laag

TCP/IP wordt gehanteerd onafhankelijk van de wijze waarop fysieke transmissie plaatsvindt. Er is een aantal protocollen beschikbaar, die hiertoe de interface tussen het IP-protocol en het feitelijke fysieke communicatieprotocol specificeren:
- Ethernet, verzending van IP-datagrammen over ethernet-netwerken (RFC 894);
- Token Ring, verzending van IP-datagrammen over token-ring-netwerken (RFC 1231).

Netwerklaag

Het internetprotocol (IP) verzorgt de verzending en ontvangst van datagrammen tussen hosts in het netwerk.
Er vinden geen controles plaats op de volgorde van de berichten en de inhoud van een datagram, en evenmin wordt een ontvangstbevestiging verstuurd. Bijgevolg is de betrouwbaarheid van IP slechts in beperkte mate gewaarborgd.

In elke host en in elke bridge en router van een TCP/IP-netwerk is functionaliteit aanwezig die zorgt voor de afhandeling van IP-datagrammen, zoals routering en foutcontrole op header-informatie.
Elk datagram wordt onafhankelijk van alle andere datagrammen verwerkt.

Hosts in het TCP/IP-netwerk kunnen elkaar foutberichten toesturen via het Internet Control Message Protocol (ICMP). Als bijvoorbeeld berichten afkomstig van host A bestemd voor host B te snel bij B aankomen, kan B aan A een ICMP-bericht sturen dat berichten te snel binnenkomen. A kan hierop de snelheid van de berichten van A naar B aanpassen.

telnet	**Remote Login (RFC 854)** Met telnet wordt een sessie opgebouwd met een host. De host wordt hierbij aangegeven als parameter.
ftp	**File Transfer Protocol (RFC 959)** De overdracht van bestanden tussen hosts in een netwerk kan worden bewerkstelligd met ftp.
SMTP	**Simple Mail Transfer Protocol (RFC 821)** Via SMTP vindt de afhandeling van E-mail plaats, zowel tussen gebruikers van een host als tussen gebruikers van meerdere hosts.
tftp	**Trivial File Transfer Protocol (RFC 783)** Met tftp kunnen gegevens zonder gebruikmaking van een password worden opgevraagd. Dit wordt bijvoorbeeld toegepast bij het opstarten van hosts zonder eigen harddisk. Deze hosts halen dan de initiële programmatuur op via tftp.
SNMP	**Simple Network Management Protocol (RFC 1157)** Via SNMP kan de controle en aansturing plaatsvinden van intelligente netwerkcomponenten (zie paragraaf Beheer).
TCP	**Transmission Control Protocol (RFC 793)** Met TCP vindt de verzorging plaats van betrouwbaar transport; berichten komen inhoudelijk juist en volledig en in de juiste volgorde aan bij de geadresseerde. Het TCP-protocol is verbindingsgeoriënteerd.
UDP	**User Datagram Protocol (RFC 768)** UDP levert in tegenstelling tot TCP geen betrouwbaar transport, net als de onderliggende protocollaag IP. UDP levert als servicelaag boven IP wel als toevoeging port-nummers en optionele checksums over de inhoud van een bericht. Er vindt echter niet automatisch foutcorrectie plaats.
ICMP	**Internet Control Message Protocol (RFC 792)** Met ICMP wordt de afhandeling van fouten en de verzending van controle-informatie tussen hosts verzorgd.
IP	**Internet Protocol (RFC 791)** IP verzorgt een datagram-transportservice. IP-datagrammen worden volgens de specificatie in de IP-header verstuurd aan de geadresseerde. Er vindt echter geen controle plaats op de juistheid en de volledigheid van een bericht, bijgevolg vindt ook geen foutcorrectie plaats.
RARP	**Reverse Address Resolution Protocol (RFC 903)** Bij de toepassing van configuraties met diskless hosts verzorgt RARP de opvraging van een Internet-adres op basis van een bekend ethernet-adres.
ARP	**Address Resolution Protocol (RFC 826)** ARP heeft de omgekeerde functie van RARP: de opvraging van een ethernet-adres op basis van een bekend TCP/IP-adres.
Ethernet	**A Standard for the Transmission of IP Datagrams over Ethernet Networks (RFC 894)** Op basis van dit protocol kan TCP/IP worden toegepast op de ethernet-netwerken, gebaseerd op de IEEE 802.2-standaard. Het protocol verzorgt de vertaling van TCP/IP-datagrammen naar ethernet-pakketten.
Token Ring	**IEEE 802.5 Token Ring MIB (RFC 1231)** Met dit protocol wordt zorg gedragen voor de vertaling van TCP/IP-datagrammen naar het token ring-protocol.

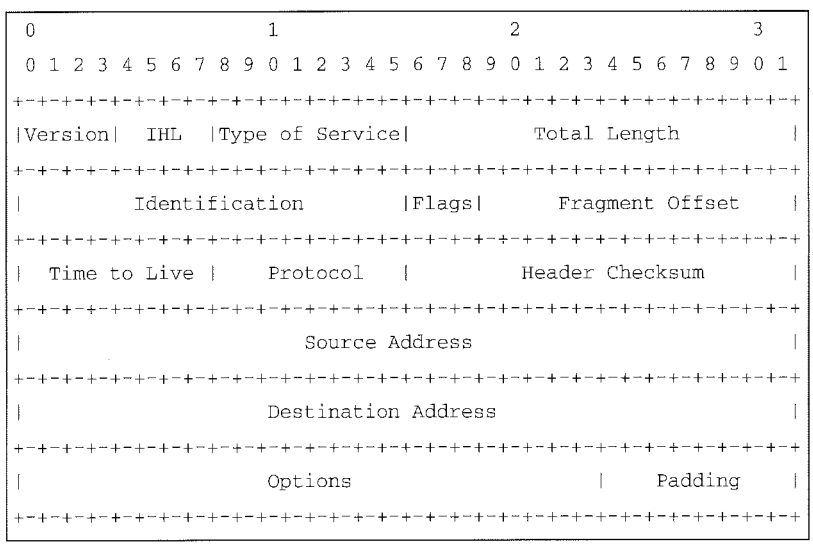
Tabel 1. Beschrijving van TCP/IP-protocollen.

Een risico van ICMP vormt de gebrekkige controle op de herkomst van deze ICMP-berichten. Een willekeurige host kan een vals ICMP-bericht aan een andere host versturen aangaande de bereikbaarheid van een derde host. Hiertegen zijn slechts beperkte maatregelen te treffen, bijvoorbeeld het niet accepteren van ICMP-berichten van bepaalde hosts. Hiervoor zou gebruik kunnen worden gemaakt van een firewall.
Een voorbeeld van een IP-header is weergegeven in figuur 3.

De belangrijkste componenten voor de juiste werking van het internetprotocol zijn:
- Type of Service;
- Time to Live;
- Header Checksum;
- Options.

Type of Service
Met de Type of Service-parameter wordt de kwaliteitsbehoefte van een bericht tijdens transport aangegeven, met kenmerken als delay, throughput en

Figuur 3. Voorbeeld IP-header (uit [RFC791]).



reliability. Met deze parameter kan voor zover mogelijk een route door het fysieke netwerk worden geselecteerd.

Een risico van het Internet Control Message Protocol vormt de gebrekkige controle op de herkomst van de ICMP-berichten.

Time to Live
Met de Time to Live-parameter wordt in seconden uitgedrukt hoe lang een datagram nog in het netwerk mag verkeren, ter voorkoming van opstoppingen als gevolg van berichten die te lang in het netwerk aanwezig zijn.
Bij de initiëring van een IP-datagram krijgt het datagram een zekere waarde voor de Time to Live. Bij elk netwerkknooppunt wordt deze waarde met ten minste één gereduceerd. Als de waarde van Time to Live gelijk is aan nul, wordt de verdere transmissie van het datagram beëindigd en wordt het datagram vernietigd.
De waarde van de Time to Live-parameter is dus een maximale waarde; doorgaans zal een datagram een korter leven hebben.

Header Checksum
In de header is een checksum opgenomen ter verificatie van de juistheid van de header. Deze checksum wordt met het 16 bit one's complement berekend van de one's complement som van alle 16 bit words in de header. Omdat de Time to Live op elk knooppunt verandert, wordt ook de header checksum op elk knooppunt opnieuw berekend. Bij deze berekening wordt in het header-veld voor de checksum de waarde nul toegepast.
Als de checksum onjuist blijkt, wordt het datagram vernietigd.

Options
Onder andere kunnen één of meer van de onderstaande opties worden aangegeven:
- *Security,* gebruikt voor de vastlegging van restricties zoals user groups, restrictie-codes en dergelijke.
- *Strict Source Routing,* het transport vindt plaats via een vooraf gespecificeerde route door het netwerk, in plaats dat gebruik wordt gemaakt van flexibele routingmogelijkheden in routers en dergelijke.
- *Record Route,* tijdens het transport vindt de vastlegging van de gevolgde route van het IP-datagram plaats, op de weg van de verzender naar de ontvanger.
- *Internet Timestamp,* laat van alle door het IP-datagram gepasseerde gateways het tijdstip van passeren vastleggen in het datagram.
- *End of Option list,* einde van de options-lijst.

Adressering
Een Internet-adres representeert precies één host. Een host daarentegen kan wel meerdere Internet-adressen hebben.

Een Internet-adres wordt gerepresenteerd door 32 bits en is opgebouwd uit een netwerk-id en een host-id. Voor de netwerk-id en de host-id is een aantal bits van de adresruimte gereserveerd. Hiertoe zijn vier verdelingen van de beschikbare adresruimte vastgesteld (zie tabel 2). Zo wordt bewerkstelligd dat op flexibele wijze toekenning van nummers aan netwerken en hosts kan geschieden.

High Order Bits	Verdeling van de adresruimte	Klasse
0	7 bits voor het netwerk 24 bits voor de host	A
10	14 bits voor het netwerk 16 bits voor de host	B
110	21 bits voor het netwerk 8 bits voor de host	C
111	gereserveerd voor extended addressing mode	

Tabel 2. Adresklassen.

De adresruimte voor de host-id kan ook worden benut om subnetwerken te definiëren. De adresruimte van de host-id wordt dan verdeeld in twee delen, een voor de subnetwerk-id en een voor de daadwerkelijke host-id (binnen het subnetwerk).
Als een netwerk op basis van TCP/IP wordt opgezet, is het gewenst dit netwerk direct formeel aan te melden bij het Network Information Center (NIC) van SRI International. Er wordt dan een uniek netwerknummer beschikbaar gesteld. Bij latere verbinding van het eigen netwerk met het wereldwijde Internet is dan reeds voor unieke netwerknummering gezorgd.
Bij koppeling van netwerken zonder gebruik van uniek toegekende netwerknummers zal of eenmalig hernummering van netwerknummers of structureel vertaling van netwerknummers moeten plaatsvinden.

Transportlaag

De transportlaag beschikt over twee protocollen: UDP en TCP. Deze twee protocollen bieden richting applicaties een verschillend serviceniveau. UDP verzorgt een datagram-georiënteerde verbinding, zonder foutcorrectie en dergelijke. Dit in tegenstelling tot TCP, dat waarborgen biedt voor een connection-georiënteerde verbinding, waarbij

wordt zorg gedragen voor het juiste transport van berichten (juiste en volledige inhoud, aankomst in de juiste volgorde) van zender naar ontvanger.

UDP
Het protocol UDP biedt als transportservice boven IP een optionele checksum over de inhoud van een bericht en het gebruik van port-nummers.
Met behulp van port-nummers kan bij de adressering niet alleen een host in het netwerk worden gespecificeerd, maar ook een specifiek proces op de andere host (aangegeven met een port-nummer).
Op deze wijze wordt bewerkstelligd dat interprocescommunicatie (IPC) tussen processen van verschillende hosts kan plaatsvinden.

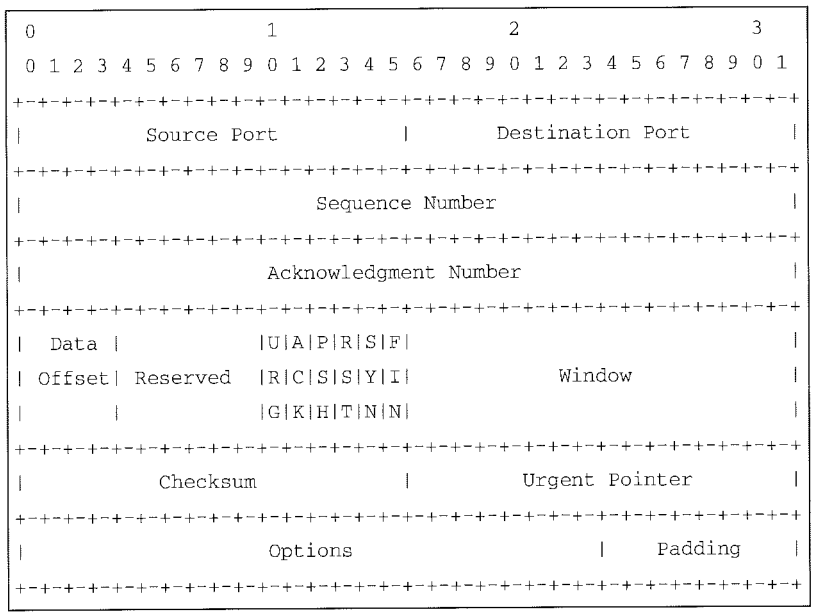
Een port-nummer is samengesteld uit 16 bits. De port-nummers 1-255 zijn gereserveerd voor specifieke doelen (bij diverse Unix-implementaties zijn de port-nummers 1-1023 gereserveerd).
De combinatie van een host-adres en een port-nummer wordt ook wel een socket genoemd.

TCP
Met TCP wordt zorg gedragen voor betrouwbaar host-to-host-gegevenstransport. Er wordt gewaarborgd dat herstel plaatsvindt van de volgende fouten:
- gewijzigde gegevens, via checksums over de met behulp van TCP getransporteerde gegevens;
- verloren gegevens, via de bevestiging van ontvangen berichten door de ontvanger aan de verzender. Indien een bericht verloren is gegaan, wordt zorg gedragen voor hertransmissie van het vermiste bericht;
- gedupliceerde gegevens, via controle op volgnummers;
- gegevens ontvangen in onjuiste volgorde, door het tijdelijk opslaan van berichten totdat berichten in juiste volgorde aan de applicatie kunnen worden doorgegeven.

De beschreven vormen van foutherstel gaan uit van het optreden van fouten zonder boze opzet. In de praktijk is het echter mogelijk het voor de foutcorrectie toegepaste foutdetectiemechanisme te omzeilen. Een bericht kan worden afgetapt en worden vervangen door een gewijzigd bericht. Als hierbij gebruik wordt gemaakt van de informatie die is vastgelegd in de TCP-header, kan voor het gewijzigde TCP-bericht een dusdanige TCP-header worden samengesteld, dat een ongeautoriseerde wijziging niet wordt gedetecteerd.

Applicatielaag

Er is een aantal standaard TCP/IP-applicaties ontwikkeld, zoals:
- ftp (RFC 959), File Transfer Protocol, waarmee bestanden kunnen worden uitgewisseld;
- telnet (RFC 854), voor het inloggen op een computer;
- SMTP (RFC 821), Simple Mail Transfer Protocol, voor de overdracht van E-mail-berichten tussen verschillende computers.



Figuur 4. TCP-header (uit [RFC793]).

Bij gebruik van applicaties als ftp en telnet dient een gebruiker eerst in te loggen met behulp van een password op de andere computer. Hierbij worden de passwords onversleuteld over het netwerk getransporteerd.

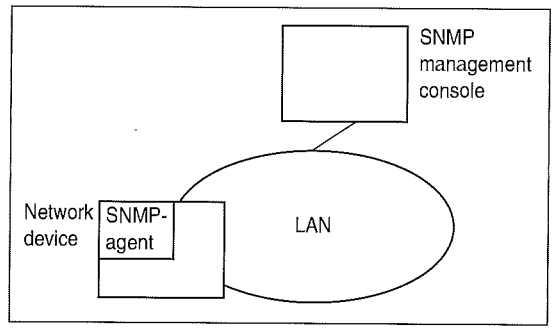
BEHEER

Het was de gedachte van het IAB (Internet Activities Board) dat voor de korte termijn het netwerkbeheer zou worden ingericht met het Simple Network Management Protocol (SNMP). Op de lange termijn, zo was de bedoeling, zou het OSI Netwerk Management Framework worden gevolgd. In de praktijk bleek SNMP echter snel ingeburgerd. Daarnaast zijn op OSI gebaseerde hulpmiddelen nog steeds beperkt beschikbaar. Dit heeft tot gevolg dat SNMP nu als de facto-standaard wordt toegepast in veel netwerkomgevingen.

SNMP

Bij SNMP is sprake van twee componenten, namelijk de network devices en het beherende SNMP management console (figuur 5).
De network devices betreffen onder andere routers en bridges, maar bijvoorbeeld ook PC's. De network devices beschikken elk over een SNMP-agent. Deze agent heeft als taak van het eigen network device informatie te verzamelen en op te slaan in een Management Information Base (MIB).

Door het management console (server) wordt via polling aan de network devices (clients) informatie gevraagd. Ook kan via het management console de instelling van het device worden gewijzigd (bijvoorbeeld het filteren van specifieke IP-adressen).



Figuur 5. De twee componenten van SNMP.

Daarnaast kunnen agents ook zelf informatie (alarms) uitsturen naar het management console. Netwerkbeheerhulpmiddelen als IBM NetView, HP OpenView en SunNet Manager zijn implementaties van SNMP management consoles.

Onder meer de volgende drie RFC's zijn vastgelegd aangaande netwerkbeheer met behulp van SNMP:
- RFC 1155: Structure of Management Information (SMI);
- RFC 1156: Management Information Base (MIB);
- RFC 1157: Simple Network Management Protocol (SNMP).

Een management console logt in op het network device gebruik makend van een password, waarna communicatie met de SNMP-agent van het device kan plaatsvinden. Bij het inloggen wordt het password echter in klare taal over het netwerk verzonden. Daardoor kan het password door derden worden afgetapt.

Bij grotere netwerken is het mogelijk dat een te grote hoeveelheid SNMP-informatie wordt getransporteerd.

Het mechanisme van informatie-overdracht tussen de SNMP-agents en het SNMP management console verloopt (te) goed. Dit kan tot gevolg hebben dat bij grotere netwerken door de polling van devices een te grote hoeveelheid aan SNMP-informatie over het netwerk wordt getransporteerd.
Ter oplossing van overload aan SNMP-informatie kan een netwerk worden verdeeld in subnetwerken met elk een eigen management console. Op deze wijze wordt de overdracht van informatie bij polling beperkt: alleen lokaal in een subnetwerk vindt dan polling plaats tussen devices en het lokale management console. Daarnaast vindt alleen overdracht van wijzigingen en alarms plaats tussen de lokale management consoles en indien aanwezig het centrale management console.

BEVEILIGING EN AUDIT

Een TCP/IP-netwerk wordt geconfronteerd met een aantal bedreigingen. Navolgend wordt eerst een toelichting gegeven op de voor TCP/IP onderkende bedreigingen, gevolgd door mogelijke maatregelen waarmee bedreigingen kunnen worden tegengegaan. Tot slot wordt aangegeven volgens welke fasering een audit hierop kan worden ingericht.

Bedreigingen

Bij TCP/IP-netwerkverkeer worden de volgende bedreigingen onderkend:

- *Afluisteren van berichten*
Door TCP/IP wordt geen encryptie toegepast. Bijgevolg kan het afluisteren slechts worden beperkt door de fysieke verspreiding van een bericht te beperken.

- *Analyse berichtenverkeer*
TCP/IP geeft in de header van berichten aan wie de verzender en de ontvanger van het bericht zijn. Het is dus mogelijk te analyseren welke hosts in het netwerk met elkaar communiceren.
Door het toevoegen van berichten aan het netwerkverkeer is het mogelijk onjuist berichtenverkeer te simuleren en in geval van aanvallen een dergelijke analyse te bemoeilijken.

- *Aanbrengen van wijzigingen in berichten*
Het IP-protocol beschikt slechts over een checksum voor de header. UDP beschikt over een optionele checksum voor controle van de juistheid van de inhoud van een bericht. Alle TCP-verkeer is standaard uitgerust met een checksum over de inhoud van het bericht en bijbehorende controle. Echter, gezien de eenvoud van de checksum-berekening kan bij wijziging van een bericht tevens aanpassing van de checksum plaatsvinden.

- *Initiëren van berichten*
Bij IP- en UDP-verkeer vindt geen controle plaats op het volgnummer van het datagram. Hierdoor is het mogelijk berichten toe te voegen aan het bestaande verkeer.
TCP beschikt wel over volgnummercontrole van berichten. Bij boze opzet is het echter mogelijk hierin wijzigingen aan te brengen.

- *Foutieve, dubbele of geen aflevering van een bericht*
Alleen TCP is in staat fouten in de inhoud van een bericht te detecteren. Voor dubbele of geen aflevering van berichten gelden dezelfde regels als genoemd bij Initiëren van berichten.

- *Ontkenning van verzending of ontvangst van een bericht*
Door TCP wordt na ontvangst een acknowledge-

ment gegeven van de volgnummers van ontvangen berichten, in tegenstelling tot bij IP en UDP. Het is echter bij TCP mogelijk hierin ongemerkt wijzigingen aan te brengen. Het is dus mogelijk de verzending of de ontvangst van een bericht te ontkennen, terwijl geen bewijs van ontvangst of verzending kan worden verkregen.

Maatregelen

Er zijn vele maatregelen te treffen ter realisatie van een beheersbaar, voldoende beveiligd en continu beschikbaar netwerk. Onderstaand wordt een overzicht gegeven van thans bestaande middelen om dit te bereiken.

Beheer
Het beheer van een netwerk vergt vaak aanzienlijke veel tijd. Dit kan onder andere worden beperkt door:

- *Unieke toekenning van IP-nummers aan de netwerkcomponenten*
Door centrale uitgifte van IP-nummer(series) kan worden bereikt dat elke netwerkcomponent een uniek IP-nummer draagt. Hiermee wordt op korte en langere termijn de kans op netwerkstoringen als gevolg van het gebruik van dezelfde IP-nummers door verschillende hosts beperkt.
Door tevens het bedrijfsnetwerk aan te melden bij het Network Information Center van SRI International - dat de netwerk-id-component van het adres verstrekt met klasse A, B of C, afhankelijk van de verwachte omvang van het netwerk - wordt een verzameling van wereldwijd unieke IP-nummers verkregen. Hierdoor wordt vermeden dat bij koppeling van het bedrijfsnetwerk met Internet elders dezelfde netwerknummers worden toegepast.

- *Gebruik beheerhulpmiddelen*
Door alleen gebruik te maken van network devices die beschikken over SNMP-agents, is het mogelijk via SNMP management consoles alle network devices op afstand te beheren.

Beveiliging
Beveiliging van TCP/IP-netwerkverkeer is van groot belang, mede omdat TCP/IP doorgaans wordt toegepast in combinatie met een broadcastprotocol als Ethernet. Dit geeft derden de mogelijkheid bedrijfsgegevens, passwords en dergelijke af te luisteren.

Als beveiligingsmiddelen kunnen worden toegepast:

- Encryptie van gegevens, bijvoorbeeld via Kerberos [Korn91].

- Toepassing van Secure-TCP/IP, zoals beschikbaar is bij IBM.

- Beperking van de beschikbaar gestelde services over TCP/IP voor het interne netwerk, indien gebruik wordt gemaakt van onveilige communicatieverbindingen, of als remote gebruikers en remote computers geen onderdeel zijn van een zogenaamde Trusted Computing Base.

- Toepassing van firewalls tussen het interne en het externe netwerk [Huls94], waarmee wordt gewaarborgd dat alleen vooraf gedefinieerd berichtenverkeer wordt getransporteerd tussen een extern netwerk en het interne bedrijfsnetwerk.

- Zonering van het netwerk, zowel logisch als fysiek. Logische afscherming van netwerkzones kan geschieden door gebruik van routers en bridges; fysieke afscherming kan plaatsvinden door gebruik van een dusdanige bekabelingsstructuur (topologie) dat niet zonder meer via bijvoorbeeld sniffers datacommunicatieverbindingen kunnen worden afgetapt.
Indien gebruik wordt gemaakt van een netwerkbackbone, waarover alle datacommunicatie tussen subnetwerken plaatsvindt, dan mogen daaraan alleen subnetwerken en geen gebruikers worden gekoppeld. Over het netwerk-backbone loopt namelijk al het berichtenverkeer dat plaatsvindt tussen de verschillende subnetwerken. Als gebruikers rechtstreeks op de backbone worden aangesloten, bestaat het risico dat dit berichtenverkeer wordt afgeluisterd.

Continuïteit
Continuïteit kan worden verkregen door het treffen van de volgende maatregelen:

- Gebruik van een Network Management Console voor de tijdige detectie van knelpunten in het netwerk.

- Dubbele uitvoering van netwerk-backbones en vastlegging van alternatieve routeringsmogelijkheden in de TCP/IP-routeringstabellen in routers. In de routeringstabellen wordt aangegeven welke routes beschikbaar zijn vanaf de router naar andere delen van het netwerk.

Audit

Bij een audit van een netwerk worden de navolgende stappen doorlopen:
- inventariseren netwerkconfiguratie;
- vaststellen betrouwbaarheids-, vertrouwelijkheids- en continuïteitseisen, gebaseerd op een afhankelijkheidsanalyse van de processen die van het netwerk gebruik maken;
- analyseren bedreigingen;
- vaststellen gewenste beveiligingsniveau;
- inventariseren en evalueren toegepaste maatregelen;
- analyseren restrisico's.

Ir. P. Kornelisse
Is afgestudeerd aan de Technische Universiteit Delft als ingenieur in de Informatica. Sinds 1990 is hij werkzaam bij KPMG Klynveld EDP Auditors. Hij is gespecialiseerd in technische infrastructuren, zoals Unix en datacommunicatienetwerken.

CONCLUSIES

Gezien de mogelijke inbreuken op de vertrouwelijkheid, betrouwbaarheid en continuïteit van berichtenverkeer in het algemeen en via TCP/IP in het bijzonder is het van belang een aantal maatregelen te treffen ter beperking van de aanwezige risico's.

Het beheer van een TCP/IP-netwerk vergt meer inspanning dan het eenmalig koppelen van de verschillende TCP/IP-netwerkcomponenten. Er is voortdurend beheer van een TCP/IP-netwerk noodzakelijk. Dit kan wel voor een groot deel geautomatiseerd en decentraal plaatsvinden.
Een bedrijfsnetwerk kan zelfstandig ten opzichte van gekoppelde netwerken (bijvoorbeeld het Internet) worden beheerd, mits gebruik wordt gemaakt van de centraal voor het Internet uitgegeven unieke IP-adresreeksen voor de hosts in het bedrijfsnetwerk.

LITERATUUR

[Stev90] R.W. Stevens, *UNIX Network Programming*, Prentice Hall, Englewood Cliffs 1990.

[Hunt92] C. Hunt, *TCP/IP Network Administration*, O'Reilly & Associates Inc, Sebastopol 1992.

[Huls94] H. van Hulst, *Firewalls*, Compact 1994/3.

[Korn91] P. Kornelisse, *Kerberos*, Compact 1991/4.

[RFC791] J. Postel, *Internet Protocol*, Internet Activities Board, 1981.

[RFC792] J. Postel, *Internet Control Message Protocol*, Internet Activities Board, 1981.

[RFC793] J. Postel, *Transmission Control Protocol*, Internet Activities Board, 1981.

Internet? Maar dan wel met een firewall!

H. van Hulst

De digitale snelweg komt, hieraan hoeft niet te worden getwijfeld. Organisaties die de mogelijkheden van de digitale snelweg niet willen missen, kunnen hun twijfels over een afdoende beveiliging van een netwerk als Internet (de reeds bestaande digitale snelweg) opzij zetten. De risico's die aansluiting met zich meebrengt, kunnen afdoende worden weggenomen door de inzet van de firewall-techniek. De auteur, als security consultant werkzaam bij Digital Equipment, beschrijft de technieken die deze organisatie hiertoe heeft ontwikkeld en reeds enige tijd toepast voor de koppeling van het interne Digital netwerk met het Internet.

INTRODUCTIE

Wereldwijd elektronisch communiceren is een feit. In een snel tempo wordt een globaal elektronisch netwerk gevormd tussen miljoenen computersystemen en het wereldomvattende telecommunicatienetwerk. De naam van dit verschijnsel is Internet en heeft sinds kort als synoniem de naam digitale snelweg. In het afgelopen jaar alleen al is het aantal aansluitingen met ongeveer zeventig procent toegenomen. Op het ogenblik maken reeds 20 miljoen mensen gebruik van een aansluiting op Internet. Ook veel bedrijven zijn aangesloten op Internet en andere bedrijven zullen zeker volgen, mede onder druk van gebruikers en de toename van het aantal beschikbare zakelijke netwerktoepassingen.

Via een Internet-aansluiting kan gebruik worden gemaakt van een groot aantal verschillende netwerkservices. De aansluiting kan worden benut voor elektronische post of file-transfer, maar ook voor het inloggen via het netwerk op een andere computer, voor systeembeheer op afstand en in toenemende mate tevens voor client/server-informatiediensten. Echter, aan elektronisch communiceren zijn - zeker op deze schaal - risico's verbonden.
Om veilig op Internet te kunnen aansluiten, is in de afgelopen jaren een aantal technieken ontwikkeld, de zogenaamde firewalls. Een firewall is een beveiligingsconstructie bestaande uit computerapparatuur en applicatiesoftware. Met een firewall wordt ervoor gezorgd dat al het computerverkeer met Internet wordt gefilterd. Alleen die berichten worden doorgelaten die voldoen aan de 'regels' die in de firewall zijn vastgelegd en worden gedicteerd door de beveiligingsprocedures van het bedrijf. Digital Equipment past voor haar interne netwerk al tien jaar het firewall-principe met succes toe. Het interne Digital computernetwerk is wereldwijd op twee locaties (Verenigde Staten en Europa) direct aan Internet gekoppeld.

Digital Equipment biedt bedrijven die hun bestaande en/of toekomstige verbindingen met Internet goed willen beveiligen, de service genaamd SEAL (Screening External Access Link). Met behulp hiervan kan een bedrijf een firewall samenstellen en het interne netwerk koppelen met Internet.

NETWERKRISICO'S

Het koppelen van externe netwerken is natuurlijk niet nieuw. Vele bedrijven hebben inmiddels ervaring opgedaan op dit gebied, onder andere door het gebruik van Datanet-1, al dan niet met Memocom (X.400), of het gebruik van Electronic Data Interchange (EDI). De hierbij toegepaste afscherming van deze koppeling tussen het interne netwerk en de buitenwereld is vaak beperkt tot een specifieke applicatie. Bovendien wordt er vaak een verbinding gemaakt met een bekende partij en is er sprake van een zeker vertrouwen.

Gedurende de laatste jaren is menig privé-netwerk geconfronteerd met de gevolgen van een 'hacker' op het interne netwerk.

Een aansluiting op een netwerk zoals Internet vergt echter een andere aanpak. Er wordt veelal verbinding gezocht met onbekenden, waardoor de basis van vertrouwen ontbreekt. Regelmatig komen incidenten op het gebied van beveiliging van dit soort aansluitingen in de publiciteit. Gedurende de laatste jaren is menig privé-netwerk geconfronteerd met de gevolgen van een 'hacker' op het interne netwerk, waarbij toegang tot het systeem werd verkregen en allerlei bedrijfsinformatie (al dan niet vertrouwelijk) werd ingezien en mogelijk zelfs buiten het interne netwerk werd gebracht.

Zeker in de beginfase van Internet was het 'kraken' een relatief eenvoudige klus. Door in te bellen via een onbeschermde en door iedereen te gebruiken kieslijn en eenvoudige wachtwoorden uit te proberen, hebben inbrekers menigmaal toegang verkregen tot privé-netwerken. Dit heeft geleid tot het op grote schaal toepassen van de terugbeltechniek, waarbij de authenticiteit van de opbeller wordt vastgesteld op basis van diens telefoonnummer.
Als externen ongewenst toegang kunnen krijgen tot een netwerk als Internet, is de integriteit van de bedrijfsinformatie ook in het geding. Daarnaast kunnen externen het bedrijf op kosten jagen, door ongemerkt en 'gratis' gebruik te maken van de netwerk- en dure communicatievoorzieningen. Ook kan door een externe een virus worden geplaatst in het interne netwerk. Deze risico's betekenen niet dat aansluiting op Internet per definitie een riskante onderneming is. Integendeel, door het nemen van de juiste maatregelen kan een verbinding met Internet op een verantwoorde en veilige wijze worden gerealiseerd.

HET PRINCIPE VAN EEN FIREWALL

In principe zou een aansluiting van Internet zonder aanvullende beveiliging mogelijk moeten zijn. Dit is echter alleen haalbaar als elk systeem afzonderlijk binnen het interne netwerk afdoende beveiligd is. Alleen dan heeft een aanval van buiten af geen succes. De realiteit is helaas anders. Veel systemen in het interne netwerk zijn onvoldoende beveiligd. Dit wordt onder meer veroorzaakt door gebrek aan kennis bij de eigenaar van de systemen of doordat de systemen technisch gezien moeilijk te beveiligen zijn (bijvoorbeeld PC's). Bovendien heeft men vaak te maken met software die geen honderd procent garantie kan bieden. Er zijn gevallen bekend waarbij hackers door een softwareprobleem toegang kregen tot systemen. Zonder passende veiligheidsmaatregelen is de kans groot dat een systeem in handen komt van een aanvaller en dat zo'n systeem vervolgens als springplank kan worden gebruikt om andere systemen aan te vallen. Zo'n aanval kan plaatsvinden zonder medeweten van de legale gebruiker. Enerzijds door gebrek aan kennis, anderzijds door tijdgebrek om allerlei audit-trails afzonderlijk te bekijken.

Om een optimale beveiliging van het interne netwerk te bereiken, wordt een firewall geïnstalleerd. Deze beperkt alle datacommunicatie tussen het interne en het externe netwerk tot alleen die services waartoe expliciet autorisatie is verleend. Verder laat de firewall geen directe communicatieverbinding toe tussen een interne computer en een computer in het externe netwerk. Deze communicatie verloopt altijd met inzet van minimaal één filter. Deze filter wordt voorzien van 'regels' en zorgt ervoor dat geen enkel bericht dat niet voldoet aan deze regels wordt doorgelaten. Het is afhankelijk van de opzet van de firewall, of een hacker zich toegang kan verschaffen tot het interne netwerk als hij erin zou slagen in te breken op de firewall.

OVERZICHT VAN FIREWALL-COMPONENTEN

Een firewall bestaat uit een aantal componenten met een specifieke functie:

Router
De hoofdtaak van een router bestaat uit het aansturen van de te volgen route van berichten tussen het externe en interne netwerk. De router ziet dus alleen toe op de gebruikte adressen van de datapakketten die aan de router worden aangeboden, niet op de inhoud ervan.

Gateway
De belangrijkste taak van de gateway ('portier') is om alle berichten te controleren en te bepalen of deze voldoen aan de vooraf gestelde regels. Als dit niet het geval is, wordt het bericht niet doorgelaten en wordt hiervan melding gemaakt. De gateway kijkt niet naar de feitelijke inhoud van een elektronisch bericht.

Relay
Een relay is het bruggehoofd tussen het interne en externe netwerk. Hier komen zowel interne als externe gebruikers terecht. De relay biedt gelegenheid aan gebruikers om onder controle van een applicatie bepaalde netwerkservices uit te voeren.

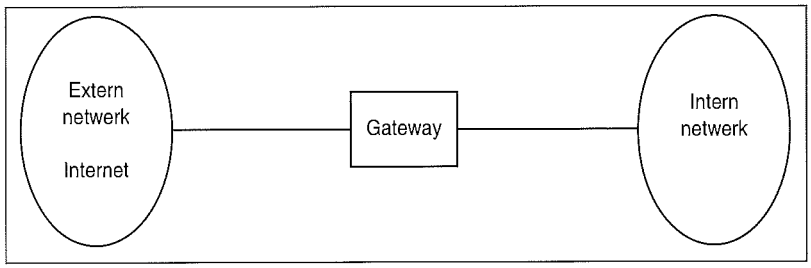
Voorbeeld
Een externe klant wenst informatie over een bepaald produkt van een leverancier. Deze klant zoekt verbinding en komt terecht op het 'relay-informatiesysteem' van de leverancier. Dit systeem vraagt door middel van een applicatie aan de klant welke informatie gewenst wordt en geeft dit verzoek door via de gateway aan een interne database met produktinformatie. Deze informatie wordt verstrekt aan het relay-systeem (bijvoorbeeld via een file-transfer), dat vervolgens de informatie aanbiedt aan de klant. Afhankelijk van de wensen van de klant kan dit in de vorm van een file-transfer of een elektronisch bericht. Indien een dergelijk relay-systeem wordt overmeesterd, blijft de schade beperkt tot dit relay-systeem. Bij een mini-firewall kunnen de bovengenoemde functies in één systeem worden gecombineerd. Bij een maxi-firewall-constructie zullen afzonderlijke systemen worden opgesteld.

FIREWALL-CONSTRUCTIES

Firewall-constructies bestaan minimaal uit een gateway en maximaal uit een aantal componenten die samen een apart subnetwerk vormen. De firewall wordt geplaatst tussen het interne en het externe netwerk.

Mini-firewall

Een mini-firewall bestaat uit een systeem dat tussen het interne en externe netwerk wordt geplaatst. Er zijn verder geen andere koppelingen tussen beide netwerken aanwezig, waardoor alle communicatie met Internet via het mini-firewall-systeem wordt afgehandeld (zie figuur 1). In deze firewall wordt een aantal functies, zoals de router-functie en de gateway-functie ter controle van de toegepaste netwerkservices, gecombineerd.
Zo'n miniconstructie kan een eerste aanzet zijn voor het koppelen van het bedrijfsnetwerk met Internet, zeker als het gebruik met Internet nog niet grootschalig is. Belangrijk hierbij is dat de communicatie met Internet structureel op één locatie binnen de organisatie wordt geregeld. Het beheer van en de controle op deze firewall kunnen doeltreffend en doelmatig worden uitgevoerd. Daarbij moet wel gerealiseerd worden dat de beveiliging van een miniconstructie niet optimaal is. De gateway blijft een enkelvoudige schakel, die kwetsbaar is. Bovendien wordt dit systeem samengesteld uit een aantal softwarecomponenten, die mogelijk bugs bevatten. Zeker het toestaan van inloggen op de firewall door externe gebruikers is een kritisch punt. De kwetsbaarheid van een mini-firewall wordt hierdoor aanzienlijk vergroot. Als



Figuur 1. Mini-firewall.

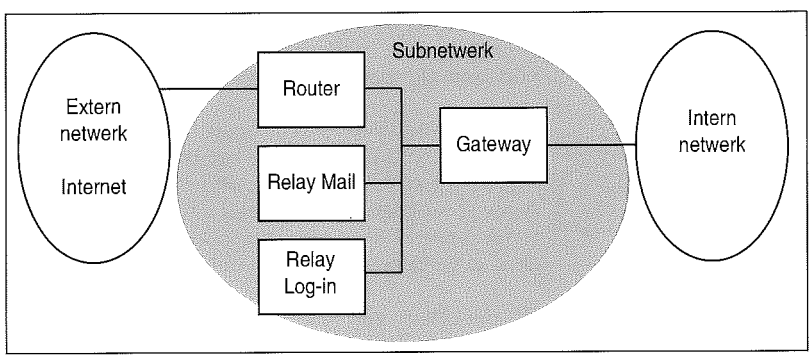
de firewall door een hacker wordt overmeesterd, is de hacker namelijk direct met het interne netwerk verbonden.

Maxi-firewall

Als het genoemde risico dat een mini-firewall met zich meebrengt niet acceptabel is (afweging tussen kosten en het accepteren van een risico), dan zullen extra beveiligingsvoorzieningen nodig zijn. Daarnaast kan een uitbreiding van een firewall ook noodzakelijk zijn vanwege een toename in het gebruik ervan. Een ander aspect is het optimaliseren van het systeembeheer, door bijvoorbeeld alle elektronische mail op een relay-systeem te concentreren. Door het gebruik van relay-systemen wordt een maxi-firewall geconstrueerd. Kenmerkend voor een maxi-firewall is het afzonderlijke subnetwerk dat als een soort 'niemandsland' tussen het externe en interne netwerk wordt aangebracht en waarin de relay-systemen worden geplaatst (zie figuur 2). De router is hierbij zodanig geprogrammeerd dat het externe verkeer alleen wordt toegelaten tot de relay-systemen. Deze relay-systemen bieden elk een bepaalde service aan. Zo kan de één zijn ingericht als mail-server en de andere als host-server, waar externe gebruikers op kunnen inloggen. Ook kan een relay-systeem een combinatie van services aanbieden.

De gateway is geplaatst tussen het subnetwerk en het interne netwerk en functioneert nu als een elektronische 'portier', die alleen berichten doorlaat die

Figuur 2. Maxi-firewall.



door de relay-systemen worden vrijgegeven of geaccepteerd. Deze berichten worden door de gateway gecontroleerd, waarbij wordt getoetst of de berichten voldoen aan de opgestelde regels. Tot deze gateway heeft alleen de systeembeheerder toegang. Verder worden er geen gebruikers of functies op het systeem toegelaten.

Door de juiste instelling van de auditvoorzieningen en de controle hierop is de kans groot dat een aanval op de gateway tijdig wordt ontdekt.

De toepassing van deze maxi-firewall-constructie verkleint de risico's aanzienlijk. Indien toch één van deze relay-systemen wordt gekraakt, zorgt de gateway ervoor dat directe toegang tot het interne netwerk nog steeds niet mogelijk is. Om toch toegang te krijgen, moet eerst nog de gateway worden overmeesterd. Door de juiste instelling van de auditvoorzieningen en de controle hierop is de kans groot dat een dergelijke aanval tijdig wordt ontdekt en er tegenmaatregelen kunnen worden genomen.

BEPERKING VAN SERVICES

De beveiliging die de firewall biedt, bestaat uit het beperken van het mogelijke berichtenverkeer. Hierbij kan onderscheid worden gemaakt tussen de richting en de aard van het berichtenverkeer.

In- en outbound-verkeer

De firewall heeft tot doel als verkeersagent toe te zien op het netwerkverkeer tussen het externe en het interne netwerk. Verkeer afkomstig van het interne netwerk naar het externe netwerk wordt ook wel outbound-verkeer genoemd. Verkeer in de omgekeerde richting heet ook wel inbound-verkeer.
Een bedrijf dat zich met een firewall wenst te beveiligen tegen de risico's die ontstaan bij koppeling van het interne netwerk met Internet, dient vast te stellen welke netwerkservices zijn geoorloofd, voor zowel inbound- als outbound-verkeer.

Bij het outbound-verkeer staat voorop dat wordt toegezien welke informatie het bedrijf niet zonder meer mag verlaten. Bij inbound-verkeer dient met name te worden gewaarborgd dat hosts van het interne netwerk niet ongeautoriseerd worden benaderd door gebruikers vanaf het externe netwerk.

Bij de opzet van een firewall zullen richtlijnen moeten worden vastgesteld met betrekking tot het beschikbaar stellen van informatie (outbound-verkeer). De inhoud van deze richtlijnen zal afhankelijk zijn van de waarde en de vertrouwelijkheid van dit soort informatie. De belangrijkste regel hierbij is dat het onmogelijk moet zijn voor een externe partij om ongeautoriseerd informatie uit het interne netwerk op te halen. Door de tussenkomst van de firewall kan dit gevaar volledig worden bezworen.
Men zou een firewall dus zodanig kunnen inrichten dat er geen bestanden naar buiten gebracht kunnen worden. Echter, een interne medewerker kan altijd nog een bestand met elektronische post of via een diskette naar buiten brengen.

Beperkingen kunnen eveneens worden gesteld aan het invoeren van informatie van buiten af (inbound-verkeer). Eén van de redenen om dit te beperken is het risico dat deze bestanden door een computervirus worden besmet, waardoor schade kan worden toegebracht aan de eigen systemen. Gezien de enorme hoeveelheid informatie bestaat eveneens het gevaar dat het eigen netwerk wordt overbelast met informatie. Hoewel de gateway de informatie-aanvoer zou kunnen beperken of zelfs geheel verhinderen, blijft het de verantwoordelijkheid van de gebruikers om zinvol met informatie om te gaan.

In de praktijk wordt een algemene bescherming voor inbound- of outbound-verkeer niet strikt toegepast. Steeds wordt per netwerkservice bepaald of beschermingsmaatregelen noodzakelijk zijn. De firewall kan per protocol worden ingesteld op het filteren van inbound- en/of outbound-verkeer.

Netwerkservices

De firewall wordt aangestuurd door een aantal regels (script) die aangeven welk soort netwerkverkeer (protocollen) toegelaten mag worden. Het Internet kent een grote verscheidenheid aan services. Het gebruik van een aantal van deze services dient uiterst zorgvuldig te worden geregeld. In dit artikel worden de belangrijkste van deze protocollen behandeld. Voor meer technische documentatie wordt verwezen naar de literatuurlijst.

Electronic Mail (SMTP-protocol)
Dit is verreweg de belangrijkste toepassing en in het algemeen zal de firewall het Simple Mail Transfer Protocol (SMTP) ongehinderd doorlaten. De firewall kan eventueel een aantal interne systemen de toegang ontzeggen tot berichtenuitwisseling met de buitenwereld.

Bulletin Boards (news-protocol)
Dit betreft het Network News Transfer Protocol (NNTP). Afhankelijk van de behoeften vanuit het bedrijf kan worden besloten het news-protocol niet toe te staan.

Host-toegang (telnet-protocol)
In het algemeen wordt niet toegestaan dat vanuit het externe netwerk direct wordt ingelogd op een

intern systeem. Een externe gebruiker kan alleen inloggen op een relay-systeem. Dit systeem verzorgt dan een tweede inlog-sessie naar een host in het interne netwerk. De gateway zal hierbij bewaken dat de externe gebruiker alleen toegang verkrijgt tot een host die daadwerkelijk vanaf het externe netwerk mag worden benaderd.

File transfer (ftp- en tftp-protocol)
In toenemende mate wordt ook 'anonymous ftp' populair om publieke informatie te verspreiden. Er moet dan wel extra aandacht worden besteed aan het feit dat deze service alleen publieke informatie uit het interne netwerk mag verstrekken. Ook kunnen bestanden worden overgebracht via electronic mail ('ftp by mail').

Internet-controleberichten (Internet Control Message Protocol (ICMP))
Dit protocol verstrekt informatie over de netwerkverbinding die tot stand wordt gebracht, zoals 'destination unreachable'. Verstrekking van dit soort informatie aan buitenstaanders dient vermeden te worden en moet door de firewall worden afgeschermd.

Gebruikersinformatie (finger-protocol)
Dit protocol wordt gebruikt om informatie over gebruikers op te vragen. Het toestaan van gebruik van deze service over de firewall dient zorgvuldig te worden afgewogen. In het verleden heeft dit protocol, door een probleem in de software, gezorgd voor de 'Morris worm', waardoor een groot deel van Internet werd ontwricht.

Naming- en time-services
Deze diensten zijn van belang om te synchroniseren met de Internet-tijd en om informatie uit te wisselen over benaming van logische componenten.

ORGANISATIE RONDOM EEN FIREWALL

Het inrichten van een firewall zal in overeenstemming moeten zijn met bestaande procedures en het beleid voor informatiebeveiliging. Indien deze procedures ontbreken of niet voldoende zijn uitgewerkt, zal dit de doeltreffendheid van de firewall niet ten goede komen. Het beheer van een firewall vereist eveneens goede administratieve procedures. Een goed werkende beheerorganisatie is noodzakelijk om de firewall-regels te implementeren en up-to-date te houden. Het gevaar bestaat anders dat gebruikers gefrustreerd raken over de beperkte services en andere communicatiepaden zullen opzetten. Een firewall is echter alleen zinvol als er geen alternatieve paden naar de buitenwereld beschikbaar zijn.

Door het gebruik van inkiesverbindingen en een PC-modem kunnen tegenwoordig op eenvoudige wijze netwerkachterdeurtjes door gebruikers worden opgezet. Dit gebeurt vaak door onkunde en het niet voldoende op de hoogte zijn van de risico's en van de procedures die binnen het bedrijf gelden. Als een organisatie op meerdere locaties een firewall heeft geïnstalleerd, is het van belang om de instelling van deze firewalls met elkaar in overeenstemming te brengen. Gezien de strategische positie van een firewall wordt regelmatige aandacht en controle door een security officer of een EDP-auditor aanbevolen.

Een firewall is alleen zinvol als er geen alternatieve paden naar de buitenwereld beschikbaar zijn.

BEVEILIGING VAN EEN FIREWALL

Het is van belang de beveiliging van de firewall zo goed mogelijk in te richten. Deze beveiliging zal regelmatig gecontroleerd moeten worden. Hiertoe is het gebruik van een compliance manager zeker aan te bevelen. Een compliance manager zorgt ervoor dat het niveau van de systeembeveiliging volledig in een aantal regels wordt beschreven en vastgelegd. Deze regels worden automatisch en regelmatig gecontroleerd. Bij een firewall kan een compliance manager worden toegepast om zo een afwijking in de beveiliging direct te signaleren. Wordt inderdaad een afwijking gemeld, dan zal door systeembeheer direct actie moeten worden ondernomen om de firewall weer op het juiste beveiligingsniveau te brengen.

Voor het detecteren van een mogelijke aanval en om misbruik van de firewall door een externe partij tegen te gaan, is het noodzakelijk een audit-trail op te zetten. Op de diverse systemen (gateway, relay) dient een audit-trail te worden geactiveerd, zowel op systeemniveau (firewall-besturingssysteem) als op applicatieniveau (netwerkservices). De resulterende auditgegevens dienen regelmatig door de systeembeheerder te worden geanalyseerd op afwijkingen.

Er kan gebruik worden gemaakt van automatische hulpmiddelen die de audit-trail op vreemde gebeurtenissen controleren. Deze controle verloopt volgens een aantal opgestelde regels. Indien iets vreemds wordt waargenomen, wordt dit direct gemeld aan de systeembeheerder. Op deze wijze blijft de schade beperkt doordat er geen tijd verloren gaat tussen gebeurtenis en moment waarop de audit-trail handmatig wordt gecontroleerd.

H. van Hulst
Is als consultant werkzaam bij Digital Equipment bv, waar hij in het verleden betrokken was bij het inrichten van grootschalige netwerken. De laatste jaren heeft hij zich gespecialiseerd in de logische beveiliging van informatiesystemen en adviseert hij gebruikers van Digitalapparatuur over beveiliging, het opzetten van security baselines en de daarbij behorende organisatorische infrastructuur.

PRESTATIES VAN EEN FIREWALL

Het is van groot belang de prestaties van de firewall te blijven volgen. Door de hoeveelheid verkeer en het aantal regels waaraan het berichtenverkeer moet worden getoetst, kan de firewall overbelast raken. Dit kan weer ongenoegen opwekken bij de gebruikers doordat lange wachttijden ontstaan. Met een splitsing van de firewall in een aantal relay-systemen of systemen met meer verwerkingscapaciteit kan dit eenvoudig worden opgelost. Daarnaast moet men rekening houden met de volgorde van de regels waaraan de firewall het berichtenverkeer toetst. Deze volgorde is direct van invloed op de prestatie van de firewall. Als elektronische post een groot gedeelte van het verkeer omvat, is het zinvol om met één van de eerste regels te bepalen of het een elektronisch bericht is. Dit voorkomt dat een groot deel van het verkeer aan niet van toepassing zijnde regels wordt getoetst.

Het bijhouden van audit-trails van berichten zal ook van invloed zijn op de prestatie van de firewall. Belangrijk is de registratie van berichten die niet voldoen aan de gestelde regels en dus geweigerd worden. Het gevaar blijft echter dat deze registratie haar doel voorbij schiet en een aanslag pleegt op de prestaties van de firewall.
Voorts is van belang dat de prestatie van de firewall wordt gemeten en geregistreerd, en eventueel wordt doorbelast aan de gebruikers (accounting).

CONCLUSIE

Aansluiting op externe netwerken is de realiteit en niet meer weg te denken uit de samenleving. Op dit moment zijn de belangrijkste applicaties: het verzenden van bestanden, het uitwisselen van elektronische post en het inloggen op een systeem. Er worden echter steeds nieuwe toepassingen gelanceerd, zoals het uitwisselen van informatie via bulletinboards, het uitwisselen van offerte-informatie en het plaatsen van bestellingen.
Beveiliging gaat in deze materie een steeds belangrijker rol spelen. Firewalls maken hierbij integraal onderdeel uit van geslaagde inspanningen om wereldwijd elektronisch communiceren veiliger en betrouwbaarder te maken. Zij zorgen ervoor dat ondanks de oprukkende techniek de grenzen tussen publieke en privé-gegevens gehandhaafd blijven.

LITERATUUR

[Mogu91] J. Mogul, *Using screend to Implement IP/TCP Security Policies*, Digital Network Systems Laboratory, Palo Alto, juli 1991.

[Wall94] P. Wallich, *Wire Pirates*, Scientific American, maart 1994.

Netwerkverbindingen in een OpenVMS-omgeving

Ir. J.H. Lie-Tjauw

Bij het koppelen van OpenVMS-nodes in een DECnet-netwerk ontstaan beveiligingsrisico's, waarvan de omvang mede afhankelijk is van het communicatieprotocol dat wordt toegepast. De auteur behandelt de risico's van DECnet en de beveiligingsmogelijkheden bij specifieke communicatieprotocollen.

INLEIDING

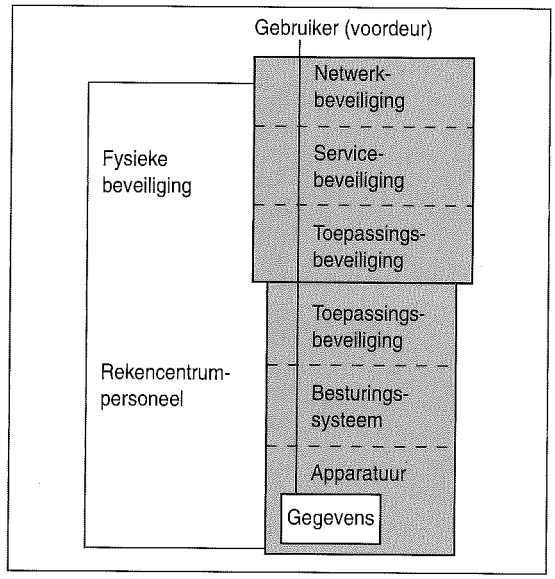
De afgelopen jaren is een toenemende integratie van computernetwerken waar te nemen. Steeds meer organisaties koppelen hun computersystemen met de computersystemen van andere organisaties. Was het zo dat eerst alleen zogenaamde 'domme' terminals bij andere organisaties (bijvoorbeeld een klant) werden opgesteld, nu zien we dat ook de computer(s) van andere organisaties op het eigen netwerk worden aangesloten. Ofschoon er meestal goede argumenten zijn om een externe netwerkverbinding te rechtvaardigen, moet de desbetreffende organisatie zich realiseren welke risico's hiermee gepaard gaan en aan welke voorwaarden moet zijn voldaan opdat een beheerste externe verbinding kan worden gerealiseerd. Naast een adequaat gebruik van de beveiligingsmogelijkheden van OpenVMS, is kennis vereist van de produkten waarmee externe koppelingen tot stand worden gebracht en de beveiligingsmogelijkheden die deze bieden.

In dit artikel wordt eerst ingegaan op de relatie tussen netwerkbeveiliging en overige maatregelen ter beveiliging van systemen en gegevens. Vervolgens wordt aangegeven welke netwerkconfiguraties mogelijk zijn met DECnet en op welke wijze een verbinding tussen twee OpenVMS-nodes tot stand kan worden gebracht. Op basis hiervan volgt een nadere behandeling van de netwerkconfiguratie Ethernet LAN en de aansluiting van DECnet op een X.25-netwerk. Hierbij wordt aangegeven welke risico's er bestaan en welke maatregelen kunnen worden getroffen om deze te beheersen.

DIGITAL NETWERKEN

Organisaties die hun computernetwerken koppelen aan netwerken van andere organisaties of aan openbare netwerken zullen maatregelen moeten nemen om misbruik en ongeautoriseerde toegang tot systemen en gegevens te voorkomen. Hierbij moet niet alleen worden gedacht aan het beveiligen van de eigen systemen en gegevens, maar ook aan de beveiliging van de systemen en gegevens van andere organisaties (bescherm uw zakenpartners tegen misbruik door uw gebruikers van hun systemen).

Om inzicht te krijgen in de problematiek om in een netwerkomgeving systemen en gegevens te beveiligen, kan het zes-lagenmodel worden gebruikt (zie figuur 1, ontleend aan [Paan94]).



Figuur 1. Het zes-lagenmodel van beveiliging in een netwerkomgeving.

In het zes-lagenmodel moet een gebruiker zes lagen passeren voordat hij toegang verkrijgt tot de gegevens. Het samenstel van maatregelen in de zes lagen is bepalend voor het uiteindelijk gerealiseerde niveau van gegevensbeveiliging.

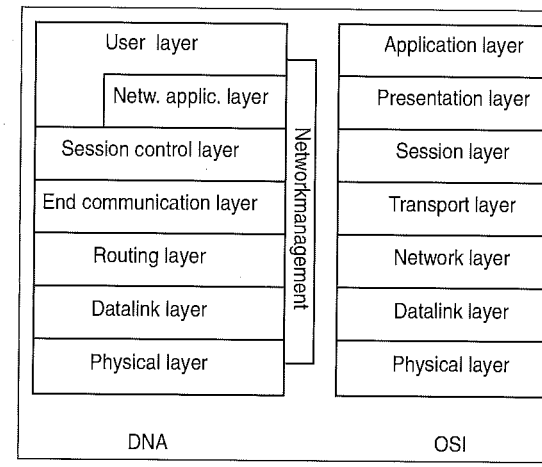
Netwerkbeveiliging is noodzakelijk als gebruikers toegang willen en moeten krijgen tot gegevens op een andere node. In dit artikel wordt onder een node verstaan een computersysteem dat DECnet-software gebruikt voor de communicatie met een ander computersysteem dat in het netwerk is opgenomen. VAX- en Alpha-computers zijn nodes in een DECnet-omgeving.
Met netwerkbeveiligingsmaatregelen kan een organisatie nodes en gebruikers autoriseren voor toegang tot haar nodes. De beveiliging van de objecten van een node zelf vindt plaats met behulp van maatregelen in de overige lagen van het model. Met netwerkbeveiliging wordt in feite een eerste en belangrijke laag van beveiliging gerealiseerd.

In het vervolg van deze paragraaf wordt nader ingegaan op DECnet en de mogelijkheden die DECnet biedt aan gebruikers om toegang te krijgen tot objecten op andere in het netwerk aangesloten nodes (netwerktoegang).

DECnet

Digital computers communiceren met elkaar via speciaal daarvoor ontwikkelde programmatuur. Deze programmatuur, DECnet genaamd, is ontwikkeld op basis van de Digital Network Architecture (DNA). DNA beschrijft de wijze waarop Digital computers aan elkaar kunnen worden gekoppeld opdat communicatie kan plaatsvinden. In DNA worden overeenkomstige netwerkfuncties gegroepeerd in een laag. Vergelijkbaar met het Basic Reference Model for Open Systems Interconnection (OSI-model) worden in DNA de volgende lagen onderscheiden:
- User Layer;
- Network Management Layer;
- Network Application Layer;
- Session Control Layer;
- End Communication Layer;
- Routing Layer;
- Data Link Layer;
- Physical Layer.

De relatie tussen de lagen volgens DNA en volgens het OSI-model is opgenomen in figuur 2.



Figuur 2. Relatie tussen DNA en het OSI-model.

De DNA-architectuur beschrijft twee soorten relaties tussen modules, waarbij een module een implementatie is van een netwerklaag (zie figuur 3):

- *Interfaces*

Een interface is de verticale relatie tussen twee naastgelegen modules op verschillend niveau. Een module in een laag heeft een interface met een module in de eerst onderliggende laag om een 'service' te ontvangen. Aan de eerst bovenliggende laag wordt een 'service' aangeboden.

– *Protocollen*
Protocollen geven de horizontale relatie aan tussen modules op een gelijk niveau. Deze protocollen bestaan uit een verzameling berichten met specifieke formaten en regels voor het uitwisselen van berichten.

Binnen DECnet worden de nodes als gelijkwaardige computers gezien. Speciale datacommunicatiecomputers zijn niet per se noodzakelijk. Elke node is in principe in staat de netwerkfunctie naast de overige functies uit te voeren.

Het koppelen van OpenVMS-nodes

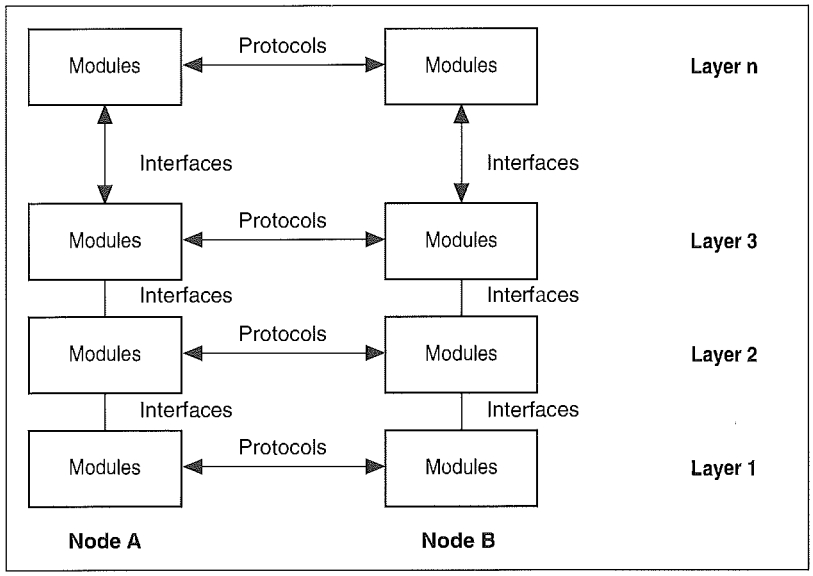
DECnet biedt diverse mogelijkheden om nodes te configureren tot een netwerk. Zowel Local Area Netwerken (LAN's), Wide Area Netwerken (WAN's) als combinaties hiervan kunnen worden ingericht.

Nodes worden via communicatielijnen aan elkaar gekoppeld. Een lijn verzorgt de fysieke communicatie en maakt deel uit van de Physical Layer. Op het niveau van de Data Link Layer ondersteunt DECnet de volgende vier protocollen:
- Digital Data Communications Message Protocol (DDCMP);
- Computer Interconnect (CI);
- Ethernet;
- X.25.

Digital Data Communications Message Protocol
DDCMP is een formele verzameling afspraken voor het verzorgen van foutloos datatransport over fysieke lijnen. DDCMP-lijnen kunnen point-to-point- of multipoint-verbindingen zijn. Een point-to-point-configuratie bestaat uit twee nodes die via een enkelvoudig communicatiekanaal zijn verbonden. Een voorbeeld is een kieslijnverbinding tussen twee nodes.
Een multipoint-configuratie bestaat uit twee of meer nodes die via een communicatiekanaal met elkaar zijn verbonden waarbij één node het kanaal beheerst.

Computer Interconnect
CI is een communicatiekanaal dat het mogelijk maakt nodes in een cluster op te nemen. Een cluster is een concept waarbij verschillende nodes gezamenlijk gebruik maken van schijven, systeemcomponenten en een gemeenschappelijk besturingssysteem.

Ethernet
Bij Ethernet zijn de nodes aangesloten op één gemeenschappelijk communicatiekanaal waarbij de nodes gelijke rechten hebben met betrekking tot het gebruik van het kanaal. Voor transmissie van gegevens wordt gebruik gemaakt van Carrier Sense, Multiple Access with Collision Detect (CSMA/CD). Ethernet is een 'broadcast'-protocol, wat inhoudt dat een bericht naar elke node wordt verzonden.



Figuur 3. Protocollen, interfaces en lagen.

X.25
X.25 is een protocol dat systemen in staat stelt te communiceren via een Packet Switched Data Network (PSDN).

Op Ethernet en X.25 wordt in dit artikel meer uitgebreid ingegaan.

Netwerktoegang

In een DECnet-omgeving bepaalt elke node zelf wie toegang krijgt tot zijn objecten (programmatuur, bestanden); elke node heeft een eigen implementatie van de *'reference monitor'* (zie [Heik90]).

DECnet biedt de volgende mogelijkheden voor netwerktoegang:
- gebruikersnaam en password;
- proxy account;
- via het default DECnet-account;
- DECnet-object-account.

Gebruikersnaam en password
Een mogelijkheid om gebruikers specifieke bevoegdheden te geven op een andere node (target node) is het definiëren van een gebruikersnaam en password op de desbetreffende node. Een gebruiker krijgt toegang tot de target node door expliciet gebruikersnaam en password op te geven.

Het gebruik van deze methode gaat gepaard met de volgende risico's:

- Bij het opgeven van het password wordt het password zichtbaar op het beeldscherm. Het is niet mogelijk dit te voorkomen. Gezien de lengte van de string 'node-naam, gebruikersnaam en password' komt het vaak voor dat gebruikers deze

string in een functietoets vastleggen. Andere gebruikers hoeven alleen maar deze toets in te drukken om (ongeautoriseerd) toegang te krijgen.

– Doordat node-naam, gebruikersnaam en password in 'plain text' via het netwerk worden verstuurd, bestaat de mogelijkheid dat deze worden afgeluisterd.

– Een gebruiker heeft op ten minste twee nodes een gebruikersnaam en password. Indien geen extra aandacht wordt besteed aan het passwordbeheer is het gevaar reëel dat gebruikers eenvoudige passwords kiezen, die door inbrekers kunnen worden geraden.

Indien ervoor wordt gekozen gebruikers toegang tot andere nodes te geven via het expliciet opgeven van een combinatie van gebruikersnaam en password, moet met bovenstaande risico's rekening worden gehouden.

Proxy accounts
Indien gebruik wordt gemaakt van proxy accounts heeft de gebruiker op de target node een eigen gebruikersnaam. In de reference monitor van de target node is een bestand opgenomen waarin de relatie wordt gelegd tussen de combinatie gebruikersnaam/source node-naam enerzijds en de bijbehorende gebruikersnaam waaronder wordt ingelogd op de target node anderzijds. Bij deze vorm van netwerktoegang vindt de authenticatie van de gebruiker op zijn eigen node (source node) plaats. Door middel van deze constructie hoeft de gebruiker geen passwords via het netwerk te versturen. De risico's die gepaard gaan met het via het netwerk verzenden van passwords zijn hier niet van toepassing.

Het gebruik van geprivilegieerde proxy accounts is zeker niet gewenst als de organisatie geen voldoende waarborgen heeft omtrent een adequate beveiliging van de source nodes.

Omdat de authenticatie van een gebruiker plaatsvindt op de source node is de beveiliging van de target afhankelijk van de beveiliging van de source node. Indien een organisatie proxy-toegang overweegt is het noodzakelijk om de mate van beveiliging op de source nodes in beschouwing te nemen. Het gebruik van geprivilegieerde proxy accounts is zeker niet gewenst als de organisatie geen voldoende waarborgen heeft omtrent een adequate beveiliging van de source nodes.

Default DECnet-account
Het default DECnet-account is een account dat in het algemeen op elke node aanwezig is. Netwerkobjecten maken van dit account gebruik. Een netwerkobject is een systeem- of gebruikersprogramma dat communicatie verzorgt tussen nodes in een DECnet-netwerk. Het default DECnet-account heet meestal DECnet. Elke gebruiker binnen het netwerk kan via het DECnet-account toegang krijgen tot een node waarop dit account is gedefinieerd (uiteraard moet deze gebruiker eerst zijn ingelogd op zijn eigen node). Een gebruiker hoeft niet zelf in te loggen onder het DECnet-account. Het inloggen vindt automatisch plaats als de gebruiker de node specificeert waarop het DECnet-account aanwezig is. Vanaf dit moment beschikt de gebruiker over alle mogelijkheden van het DECnet-account.

Uit oogpunt van beveiliging is het belangrijk dat men zich realiseert dat elke gebruiker die toegang heeft tot een systeem in het netwerk, ook toegang heeft tot het DECnet-account op andere in het netwerk opgenomen nodes, met de bevoegdheden die voor dit account zijn gedefinieerd.
Het definiëren van de mogelijkheden van het DECnet-account moet derhalve zeer zorgvuldig gebeuren.

DECnet-object-account
Standaard maken netwerkobjecten gebruik van het default DECnet-account. Een alternatief voor het default DECnet-account zijn DECnet-object-accounts. Voor elk netwerkobject kan een DECnet-object-account worden gedefinieerd. Op deze wijze kan het gebruik van de objecten beter worden bewaakt. Door middel van een commandoprocedure voor het DECnet-object-account kan toegang tot het object worden verleend of geweigerd op basis van de source node-naam en/of gebruikersnaam.

Het gebruik van netwerkobjecten en de daarmee gepaard gaande risico's wordt in de paragraaf Standaard-DECnet-objecten behandeld.

Samenvatting
Indien een gebruiker toegang wenst tot een object op een target node, worden de volgende controles uitgevoerd:
- Is expliciet een combinatie van gebruikersnaam en password opgegeven?
- Is voor de gebruiker een proxy account gedefinieerd op de target node?
- Is er een DECnet-object-account gedefinieerd voor het object op de target node?
- Is er een default DECnet-account gedefinieerd op de target node?

Standaard-DECnet-objecten

Wanneer twee nodes via het netwerk met elkaar communiceren ontstaat een logische verbinding tussen deze twee nodes. Het proces of programma waarmee de logische verbinding wordt gelegd, wordt een DECnet-object genoemd. Door Digital

geleverde objecten zijn standaard DECnet-objecten. Sommige hiervan kunnen worden misbruikt, waardoor de beveiliging in gevaar komt.

Navolgend wordt ingegaan op de beveiligingsrisico's van enkele standaard-DECnet-objecten.

File Access Listener (FAL)-object
Met het FAL-object is het mogelijk files via het netwerk op een andere node te plaatsen. Dit betekent dat bijvoorbeeld ook virussen naar een andere node kunnen worden overgebracht. Het is derhalve van groot belang dat op nodes die aan een netwerk zijn gekoppeld de beveiliging van de directories en files goed geregeld is. Vooral de directories waarvan de protectie W:W is vormen een risico. W:W houdt in dat gebruikers van de 'world'-categorie files en derhalve ook virussen kunnen installeren in de directory. Hierbij moet worden bedacht dat in een netwerkomgeving de world-categorie inderdaad vrijwel de hele wereld omvat.

Task-object
Met het Task-object is het mogelijk commando's of commandoprocedures op een andere node uit te voeren. Met de objectcombinatie FAL/Task is het mogelijk met FAL een virus te installeren op een node en vervolgens met Task de viruscode uit te voeren. Elke node met zowel het FAL- als het Task-object is hiervoor kwetsbaar.

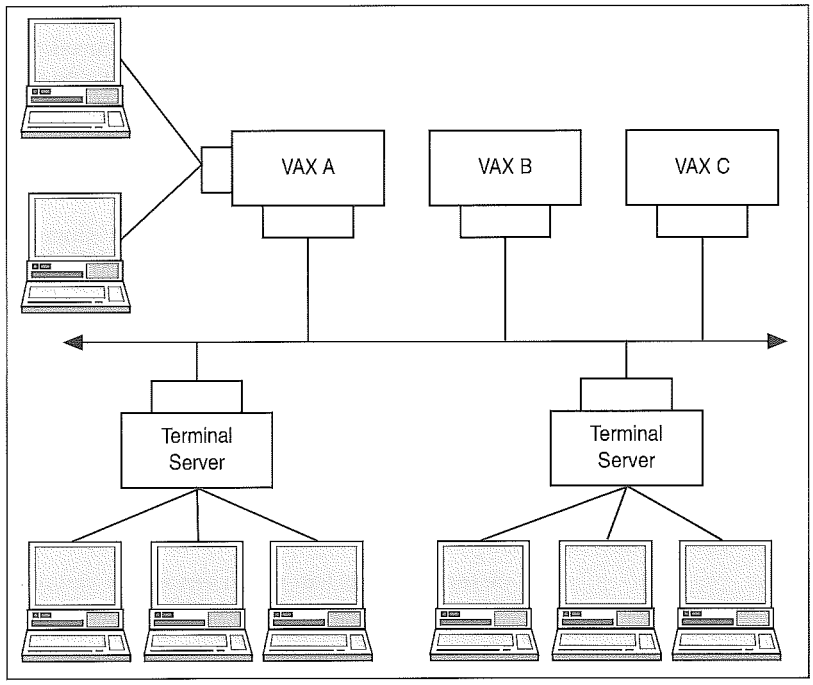
Mail-object
Aan het gebruik van het Mail-object zijn diverse risico's verbonden. Mail kan worden gebruikt om valide gebruikersnamen op een ander systeem te achterhalen. Door eenvoudig een bericht te sturen naar een potentiële gebruikersnaam op een ander systeem kan worden achterhaald of de opgegeven gebruikersnaam valide is. Als de gebruikersnaam niet valide is komt een foutmelding.
Een ander probleem van het Mail-object is dat zogenaamde 'captive' users (dit zijn gebruikers die alleen via menu's activiteiten op het systeem mogen uitvoeren) via Mail toch commandoprocedures kunnen laten uitvoeren.

ETHERNET LOCAL AREA NETWERKEN

Ethernet kan worden gebruikt om nodes te configureren tot een Local Area Netwerk (LAN). In deze paragraaf wordt ingegaan op het aansluiten van terminals op een Ethernet LAN en het onderling koppelen van LAN's.

Terminal Servers

In een Ethernet LAN zijn de terminals meestal via Terminal Servers aangesloten op Ethernet. Een Terminal Server moet gezien worden als een aparte netwerkcomputer met eigen operating-systeem. Voordat een gebruiker een verbinding kan maken met een OpenVMS-node moet eerst op de Terminal Server worden ingelogd.



Figuur 4. Netwerkconfiguratie met Terminal Servers.

Voor het beheer van een Terminal Server zijn diverse commando's beschikbaar. Met behulp van deze commando's kunnen waarden worden gegeven voor specifieke Terminal Server-karakteristieken en kan worden bepaald hoe de server moet werken. Het is van belang onderscheid te maken tussen de operationele database en de permanente database. De operationele database bevindt zich op de Terminal Server. In deze database staan de parameters die de karakteristieken van de Terminal Server bepalen. Wijzigingen die worden aangebracht in de operationele database, hebben direct invloed op de werking van de Terminal Server. De permanente database bevindt zich op de node (load host) van waaruit de Terminal Server wordt geladen. Bij het opnieuw initialiseren van de Terminal Server wordt de operationele database overschreven met de inhoud van de permanente database.

Met server-commando's kunnen de waarden van de Terminal Server-karakteristieken in de operationele database worden getoond of gewijzigd; Terminal Server Configurator (TSC)-commando's dienen voor het onderhoud van de Terminal Server-karakteristieken in de permanente database. Server-commando's worden op de local prompt van de Terminal Server gegeven. TSC-commando's worden op de load host gegeven.

Belangrijke beveiligingsmogelijkheden van een Terminal Server zijn:
- user security levels;
- passwords;
- limited view;
- dedicated services.

User security levels
Met behulp van security levels kan het gebruik van server-commando's worden beheerst. Er zijn drie security levels, met aflopende beveiliging:
- privileged;
- non-privileged;
- secure.

Een poort (een terminal is via een poort aangesloten op een Terminal Server) heeft default de non-privileged-status. In deze status weigert de poort de meeste commando's waarmee de karakteristieken van een poort kunnen worden aangepast. Een gebruiker die aangesloten is op een non-privileged poort kan:
- de karakteristieken van een poort vaststellen;
- een overzicht krijgen van alle beschikbare services;
- een sessie starten met de beschikbare services;
- switchen tussen verschillende services.

In de secure status kan alleen een subset van deze commando's worden gebruikt. Indien een poort in de privileged-status is kunnen alle server-commando's worden gebruikt.

Passwords
Het server-systeem kent verschillende typen passwords:

- *Privileged-password*

Met behulp van dit password kan de poort in de privileged-status worden gebracht. Hiertoe moet het commando SET PRIVILEGED worden gegeven. De server zal dan om het password vragen. Alle servers hebben standaard hetzelfde privileged-password; derhalve moet dit na installatie worden gewijzigd.

- *Log-in password*

Indien een log-in password is gedefinieerd, moet de gebruiker eerst het password invoeren voordat hij kan inloggen op de server. Een log-in password wordt per server gedefinieerd en kan per poort worden geactiveerd.

- *Lock password*

Een gebruiker kan tijdens een sessie, bijvoorbeeld het gebruik van een applicatie, een lock password voor zijn poort instellen. Door middel van het indrukken van een functietoets kan de gebruiker op de local prompt van de Terminal Server komen en vervolgens het lock-commando geven. De server zal vervolgens vragen om een password in te stellen; na het opgeven van het password is het gebruik van de terminal niet meer mogelijk. Indien het gebruik van de terminal moet worden hervat, moet de return-toets worden ingedrukt; de server zal dan om het password vragen. Na invoer van het ingestelde password kunnen de sessies worden hervat (een lock password verbreekt de lopende sessies niet).

Limited View
Met behulp van de Limited View-faciliteit is het mogelijk voor de poorten van een Terminal Server aan te geven dat geen gebruik kan worden gemaakt van het SHOW-commando. Dit betekent dat de commando's SHOW NODES en SHOW SERVICES niet kunnen worden gegeven vanaf de terminal die is aangesloten op de desbetreffende poort. Door deze beperking kan de gebruiker geen overzicht opvragen van de nodes of services die via de Terminal Server zijn te bereiken respectievelijk worden aangeboden.

Dedicated services
Een gebruiker die aangesloten is op een Terminal Server heeft in principe de mogelijkheid om een verbinding te leggen met elke in het netwerk opgenomen node. Door middel van het definiëren van een 'dedicated service poort' kan worden aangegeven met welke node(s) een verbinding kan worden gelegd.

Beveiliging
Door middel van het gebruik van security levels voor de Terminal Server-poorten, het definiëren van passwords, het beperken van de SHOW-commando's en het gebruik van dedicated services kan de beveiliging van het LAN worden verhoogd. Indien geen gebruik wordt gemaakt van deze mogelijkheden bestaat de mogelijkheid dat gebruikers het gehele LAN kunnen zien en kunnen proberen in te loggen op de aangesloten nodes. Een adequate instelling en een dito beheer van de Terminal Servers zijn derhalve essentieel voor de algehele beveiliging van de configuratie.

Koppeling van Local Area Netwerken

LAN's kunnen met behulp van de volgende middelen aan elkaar worden gekoppeld:
- repeater;
- bridge;
- router;
- gateway.

Repeater
Een repeater wordt gebruikt om op de fysieke laag twee LAN's aan elkaar te koppelen. In feite komt het neer op bit voor bit alles doorsluizen. Een repeater is protocol-onafhankelijk. Het gebruik van repeaters neemt af ten gunste van bridges en routers. Repeaters hebben geen intelligentie op beveiligingsgebied.

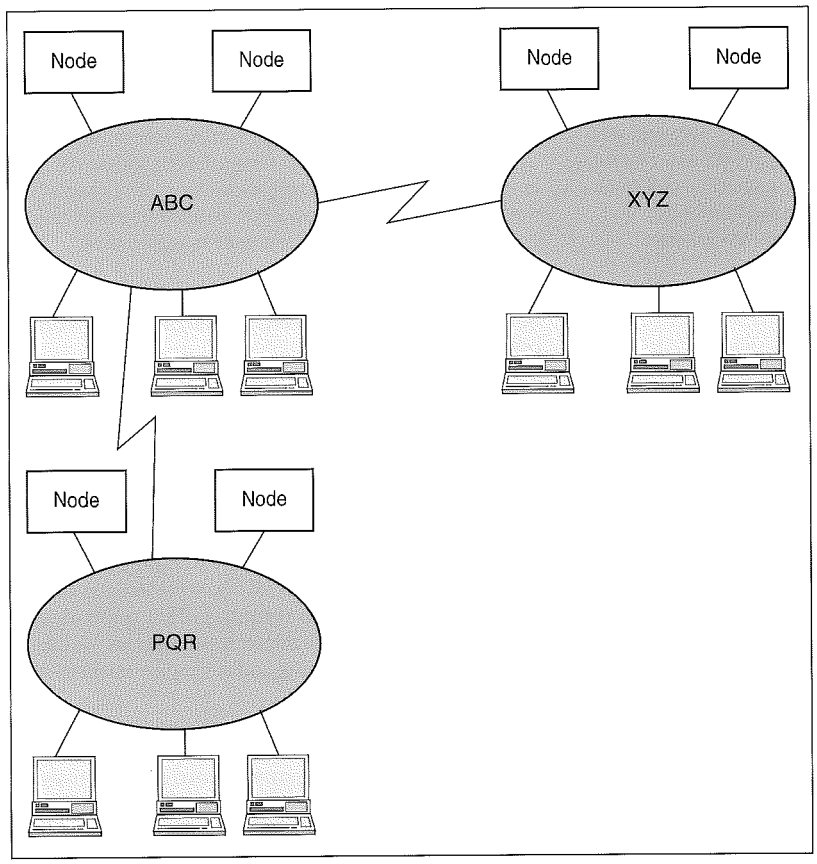
Bridge
Een bridge is een koppeling op het niveau van de datalink-laag. In tegenstelling tot een repeater schakelt een bridge niet per bit, maar per pakket. Een bridge kan netwerken van hetzelfde type of van verschillende typen aan elkaar koppelen (bijvoorbeeld een Ethernet aan een FDDI-ring).

Een bridge kan ook voor beveiliging worden gebruikt. Bridges kunnen zodanig worden ingesteld dat slechts pakketten van bepaalde gebruikers worden doorgegeven.

Router
Het koppelen van netwerken kan ook op het netwerkniveau worden geregeld, namelijk door het inzetten van routers.
Routers bieden uitgebreide beveiligingsmogelijkheden.

Gateway
Indien op netwerkniveau of hoger gebruik wordt gemaakt van verschillende protocollen, zullen gateways moeten worden toegepast. Een gateway kan verschillende functies uitvoeren. Een SNA-DECnet-gateway bijvoorbeeld maakt het mogelijk bestanden uit te wisselen of een terminal in het ene netwerk gebruik te laten maken van een applicatie op een computer in het andere netwerk.

Beveiliging
Op de markt zijn diverse modellen repeaters, bridges, routers en gateways beschikbaar. Uit oogpunt van beveiliging zijn met name de laatste drie netwerkcomponenten van belang. Indien organisatie ABC haar LAN via een bridge heeft aangesloten op een LAN van organisatie XYZ, kunnen gebruikers van bedrijf ABC proberen in te loggen op elke node van organisatie XYZ. Indien organisatie ABC haar LAN ook heeft aangesloten op een LAN van organisatie PQR, hebben gebruikers van organisatie PQR eveneens de mogelijkheid te proberen bij organisatie XYZ in te loggen. Indien dit niet gewenst is en er zijn geen maatregelen getroffen om dit te voorkomen, brengt dit risico's met zich mee (zie figuur 5).



Figuur 5. Een koppeling tussen LAN's. Organisatie PQR kan via het netwerk van organisatie ABC proberen toegang te krijgen tot de nodes van organisatie XYZ.

Indien een organisatie ervoor kiest haar computersysteem te koppelen met computersystemen van andere organisaties, dient zij adequaat gebruik te maken van de beveiligingsmogelijkheden van de hiervoor genoemde netwerkcomponenten. Deze beveiligingsmogelijkheden zijn veelal softwarematig in te stellen.

X.25-VERBINDINGEN

Organisaties kunnen hun OpenVMS-nodes aan elkaar koppelen door hun Ethernet LAN's met elkaar te verbinden. Een andere mogelijkheid is het koppelen van hun nodes aan een (openbaar) X.25-netwerk. In Nederland is dit Datanet-1 (DN-1). DN-1 is een Packet Switched Data Netwerk (PSDN). Voor eindgebruikers is het gebruik van een PSDN transparant; zij kunnen de PSDN als een black box beschouwen.

Het CCITT X.25-protocol beschrijft de koppeling tussen het lokale systeem en de netwerk-interface. Het lokale systeem wordt een Data Terminal Equipment (DTE) genoemd en kan worden gezien als het X.25-equivalent van een node. De netwerk-interface wordt een Data Circuit Terminating Equipment (DCE) genoemd.

VAX Packetnet System Interface

VAX Packetnet System Interface (PSI) maakt het mogelijk OpenVMS-nodes aan te sluiten op een X.25-netwerk. VAX PSI is een implementatie van CCITT X.25 en X.29.

VAX PSI kan op twee manieren worden geïnstalleerd:
- in *Native mode*. In deze mode biedt VAX PSI voor één OpenVMS-node directe toegang tot één of meer PSDN's;
- in *Multihost mode*. De OpenVMS-node waarop VAX PSI is geïnstalleerd, heeft directe toegang tot één of meer PSDN's. De andere OpenVMS-nodes hebben indirecte toegang. Op deze nodes moeten wel VAX PSI Access en DECnet zijn geïnstalleerd. VAX PSI Access stelt OpenVMS-nodes in staat via een VAX PSI Multihost-node toegang te krijgen tot een PSDN.

Ir. J.H. Lie-Tjauw
Is sedert 1990 werkzaam als EDP-auditor bij KPMG Klynveld EDP Auditors. Zijn aandachtsgebied betreft minicomputers en decentrale netwerken, met als specialisatie Digital DECnet- en OpenVMS-systemen.

Beveiliging

Indien een organisatie haar OpenVMS-nodes aansluit op een X.25-netwerk kan elke op het X.25-netwerk aangesloten gebruiker proberen in te loggen op de OpenVMS-nodes. Omgekeerd geldt dit ook: een gebruiker die is aangesloten op de OpenVMS-nodes, kan proberen op elke andere node in te loggen. Dit kan gepaard gaan met hoge kosten.

VAX PSI Security maakt het mogelijk het gebruik van VAX PSI te beheersen. De toegang kan worden beheerst:

- *naar* de OpenVMS-node van de desbetreffende organisatie: remote DTE's die 'incoming calls' maken naar local DTE's;
- *van* de OpenVMS-node van de desbetreffende organisatie: local DTE's die 'outgoing calls' maken naar remote DTE's.

Met PSI Security kan worden aangegeven welke remote DTE's incoming calls mogen maken en van welke applicaties deze remote DTE's gebruik mogen maken. Ook kan worden aangegeven welke lokale gebruikers outgoing calls mogen maken naar remote DTE's.

Bij de installatie van VAX PSI kan worden aangegeven of PSI Security moet worden geactiveerd. Default is de beveiliging niet actief. Wanneer een OpenVMS-node is aangesloten op een openbaar netwerk als DN-1, is het gebruik maken van PSI Security aan te bevelen als geen andere netwerkbeveiligingsfaciliteiten worden toegepast. In DN-1 zou anders elk aangesloten systeem kunnen proberen toegang te krijgen tot de desbetreffende OpenVMS-node.

CONCLUSIE

Digital en andere fabrikanten leveren produkten voor het onderling koppelen van LAN's en het aansluiten van OpenVMS-nodes op een (openbaar) X.25-netwerk zoals DN-1. Voordat een organisatie haar OpenVMS-nodes koppelt met nodes van andere organisaties of aansluit op een X.25-netwerk dient zij eerst de beveiliging van de OpenVMS-nodes op niveau te brengen. Doet zij dit niet, dan loopt zij het risico dat externe gebruikers toegang krijgen tot de resources van de nodes. Immers, in bijvoorbeeld een X.25-netwerk kan - tenzij er maatregelen zijn getroffen - in principe elke gebruiker proberen toegang te krijgen elke andere node die is aangesloten op het netwerk.

Naast het op niveau brengen van de beveiliging van de afzonderlijke OpenVMS-nodes is het essentieel dat adequaat gebruik wordt gemaakt van de beveiligingsmogelijkheden van de produkten voor het koppelen van OpenVMS-nodes. Hierdoor kan worden voorkomen dat wordt geprobeerd toegang te verkrijgen tot de OpenVMS-node zelf. Met deze produkten kan een eerste laag van toegangsbeveiliging worden aangebracht.

LITERATUUR

[DEC93] Digital Equipment Corporation, *OpenVMS VAX Guide to System Security*, 1993.

[DEC91] Digital Equipment Corporation, *DECnet concepts and usage Student Guide*, 1991.

[Heik90] G.J.C. Heikamp, *Beveiligingsaspecten van VAX/VMS-systemen*, Compact 1990/1.

[Matt93] R.L. Matthijssen e.a., *Computers, Datacommunicatie & Netwerken*, Academic Service, 1993.

[Paan94] R. Paans, Presentatie *Evolutie in Beveiligingsdenken*, 1994.

Enige juridische wegwijzers voor de elektronische snelweg

Mw.mr. G.P. van Duijvenvoorde

Is het bestaande nationale en internationale kader van telecommunicatiewetgeving toereikend om de voorziene groei van de elektronische snelweg mogelijk te maken? Welke eisen worden er vanuit deze ontwikkeling gesteld aan het juridische kader, en welke wetswijzigingen zijn eventueel gewenst?
Vanuit haar onderzoekswerk naar de toepassing van de Europese regels op de markt voor informatietechnologie, gaat de auteur in op deze vragen, en belicht daarbij aspecten als de aanleg-, exploitatie- en toegangsrechten, alsmede de beginselen van universele dienstverlening en interconnectie van netwerken.

INLEIDING

In de discussies rond de ontwikkeling van elektronische snelwegen rijst de vraag in hoeverre het juridisch kader toereikend is om deze ontwikkeling mogelijk te maken. Voor een belangrijk deel is dit juridisch kader te vinden in de telecommunicatieregelgeving zoals deze in Nederland en in de Europese Unie is opgesteld. Deze regelgeving is aan veranderingen onderhevig. Zo wordt de Nederlandse telecommunicatiewetgeving aangepast aan, onder andere, de Europese regelgeving. Op Europees niveau is in 1993 een actieplan opgesteld om de Europese telecommunicatiemarkt in de komende jaren te liberaliseren en te reguleren.

In dit artikel komen enige juridische aspecten van de elektronische snelweg aan de orde. In het eerste deel wordt het bestaande wettelijke kader met betrekking tot het telecommunicatierecht geschetst. Daarbij wordt in het kort het Nederlandse respectievelijk Europese juridische kader beschreven. Overige internationale telecommunicatieregelgeving, zoals bijvoorbeeld wordt uitgevaardigd door de Internationale Telecommunicatie Unie, blijft in dit overzicht buiten beschouwing.
Het tweede deel van dit overzicht behandelt enige aspecten van de elektronische snelweg in het licht van eerder geschetste juridische kaders. Aan de orde komen de aanleg en het beheer van de snelweg, de toegang tot de snelweg alsmede de communicatie op de snelweg.
In het derde deel wordt aandacht besteed aan de discussie over de invulling van telecommunicatiewetgeving in de toekomst. Deze discussie beperkt zich niet tot het wegnemen van juridische obstakels voor het realiseren van de elektronische snelweg, maar betreft ook de maatschappelijke en sociale aspecten van liberalisering van de telecommunicatiemarkt.
Tot slot volgen enkele afsluitende opmerkingen.

HET JURIDISCHE KADER

In dit eerste deel worden achtereenvolgens het bestaande Nederlandse en Europese juridische kader behandeld.

De Nederlandse telecommunicatieregelgeving

De Nederlandse telecommunicatiewetgeving is met name te vinden in de Wet op de telecommunicatievoorzieningen (hierna: de WTV).[1] De WTV is sinds 1 januari 1989 van kracht. Het uitgangspunt van de huidige WTV is dat Nederland te klein is voor meer dan één openbare telecommunicatie-infrastructuur. Vandaar dat KPN een exclusieve concessie heeft voor de aanleg, het beheer en de instandhouding van de telecommunicatie-infrastructuur (art. 3 WTV). Hier staat tegenover dat KPN als houder van de concessie verplicht is ervoor te zorgen dat de capaciteit, kwaliteit en eigenschappen van de telecommunicatie-infrastructuur voldoen voor een doelmatige verzorging van telecommunicatie (art. 3, lid 3 WTV). Anderen dan de concessiehouder mogen slechts zogenaamde telecommunicatie-inrichtingen van bijzondere aard of beperkte omvang aanleggen of exploiteren wanneer zij hiervoor een machtiging van de minister hebben ontvangen. De positie van deze machtiginghouders, zoals bijvoorbeeld van de kabeltelevisie-exploitanten, wordt in een apart hoofdstuk van de WTV geregeld.
KPN is als concessiehouder eveneens verplicht om een aantal diensten te leveren die maatschappelijk van belang worden geacht. Onder deze zogenaamde 'opgedragen diensten' vallen de telefoondiensten (art. 4, lid 1 WTV). De concessietaken van de KPN strekken zich voorts uit tot de plicht om een ieder tegen vergoeding het gebruik van vaste verbindingen (of huurlijnen) ter beschikking te stellen (art. 4, lid 2 WTV).
Alle overige diensten die niet als 'opgedragen diensten' kunnen worden beschouwd, kunnen door een ieder worden aangeboden. Dit geldt eveneens voor de randapparatuur mits deze is goedgekeurd (art. 29 WTV).

Met de invoering van de WTV werd een scheiding doorgevoerd van regelgevende activiteiten en exploitatie. De exploitatie van de concessietaken geschiedt door de concessiehouder (KPN), die de uitvoering van deze taken onder bepaalde voorwaarden kan overlaten aan een dochtermaatschappij waarin zij een meerderheidsbelang heeft (PTT Telecom BV).[2] De Hoofddirectie Telecommunicatie en Post (HDTP) van het Ministerie van Verkeer en Waterstaat is onder andere belast met het voorbereiden en opstellen van wet- en regelgeving, de vorming van overheidsbeleid, het frequentiebeheer en het houden van toezicht op de uitoefening van de concessietaken door KPN.

De toezichthoudende taak komt onder andere tot uiting in de zogenaamde algemene richtlijnen waarin voorschriften worden gegeven aan de concessiehouder (art. 8 WTV). Deze betreffen bijvoorbeeld de capaciteit, kwaliteit en eigenschappen van de telecommunicatie-infrastructuur. Tevens bevatten de algemene richtlijnen de uitgangspunten voor het in stand houden van een goede dienstverlening. Hieronder vallen aspecten als de wijze en mate van dienstverlening, de tariefstructuur, de beveiliging van de telecommunicatie-infrastructuur en geheimhoudingsplichten. Het Besluit algemene richtlijnen is in 1993 gewijzigd.[3] Deze wijzigingen betreffen met name toevoeging van een tariefbeheersingssysteem voor vaste verbindingen waardoor de concessiehouder wordt verplicht om een toerekeningssysteem voor de kosten en opbrengsten van deze vaste verbindingen op te stellen.

De huidige WTV is verouderd. Een nieuwe WTV is in voorbereiding. Zo werd medio 1993 een Hoofdlijnennotitie herziening WTV door de minister aan de Tweede Kamer aangeboden.[4] Hierin nam het kabinet een voorlopig standpunt in over het toekomstig telecommunicatiebeleid. Het definitieve standpunt over de hoofdlijnen herziening WTV werd in november 1993 geformuleerd.[5] Hierin kiest het kabinet voor een introductie van concurrentie op infrastructuurgebied. Verwacht wordt dat de eerste stap naar een duopolie in 1995 zal worden gezet. Concurrentie op het terrein van telefonie zal in 1998 plaatsvinden. De minister hoopt het gehele wetgevingstraject uiterlijk in 1995 af te ronden. In de tussenperiode zal de huidige WTV *ad hoc* worden aangepast om tegemoet te komen aan de wensen op de markt en aan de Europese telecommunicatieregelgeving.

De Europese telecommunicatieregelgeving

Een Europese WTV is niet voorhanden. De regulering van de Europese telecommunicatiemarkt geschiedt via de toepassing van de algemene instrumenten die door het EG-Verdrag worden aangereikt. Wel heeft de Europese Commissie in 1987 uiteengezet hoe deze algemene middelen specifiek voor de telecommunicatiemarkt dienen te worden ingezet. In dit zogenaamde Groenboek Telecommunicatie werd bepaald dat nationale telecommunicatie-organisaties (de nationale 'PTT's') in principe hun exclusieve rechten ten aanzien van de levering en exploitatie van de telecommunicatie-infrastructuur mochten behouden om hun verplichtingen als openbare dienst te kunnen nakomen. De exclusieve rechten die de PTT's hadden op het terrein van het aanbieden van de telecommunicatiediensten en -apparatuur moesten worden afgeschaft. Uitdrukkelijk werd echter een uitzondering gemaakt voor de zogenaamde spraaktelefoniediensten waarop de PTT's vooralsnog het monopolie konden behouden. Van de overige toegevoegde-waarde-diensten werd bepaald dat een ieder de mogelijkheid moest hebben om deze aan te bieden.

Liberalisatie en harmonisatie
Om vorm te geven aan het telecommunicatiebeleid wordt gebruik gemaakt van een aantal instrumenten. Allereerst worden richtlijnen uitgevaardigd om de telecommunicatiemarkt te *harmoniseren.* Achtergrond hiervoor is het opheffen van de verschillen in regelgeving in de desbetreffende lidstaten, bijvoorbeeld op het terrein van technische ei-

1. *Wet van 26 oktober 1988, Stb. 520 inclusief latere wijzigingen.*
2. *Zoals geregeld in artikel 11 WTV en in de Machtigingswet. Beide regelingen werden aangepast in het kader van de Wet beursgang KPN, Staatsblad 1994, nr. 159.*
3. *Wijziging Besluit algemene richtlijnen telecommunicatie, Staatscourant 27 van 9 februari 1993, p. 16.*
4. *Zie brief van 23 juli 1993, Tweede Kamer, vergaderjaar 1992-1993, 21 693, nr. 13. Ondersteunend onderzoek hiervoor werd verricht door McKinsey & Company en vastgelegd in het rapport 'Telecommunicatie in Nederland: op weg naar wereldklasse. Beleidsrichting ter versterking van het aanbod van diensten in telecommunicatie', juni 1993.*
5. *Zie Tweede Kamer, vergaderjaar 1993-1994, 21 693, nr. 14.*

sen, procedures voor keuring van randapparatuur of voorwaarden voor toegang tot en gebruik van telecommunicatienetwerken.
In de tweede plaats wordt gebruik gemaakt van de mededingingswetgeving in het EG-Verdrag om daarmee de telecommunicatiemarkt te *liberaliseren* en monopolies op bepaalde delen van de telecommunicatiemarkt op te heffen. In 1988 werden de eerste stappen tot het liberaliseren van de markt voor telecommunicatie-eindapparatuur gezet.[6] Twee jaren later, in 1990, vaardigde de Commissie de zogenaamde 'diensten-richtlijn'[7] uit waarmee de exclusieve rechten van de PTT's ten aanzien van de telecommunicatiediensten gefaseerd zouden worden opgeheven. Zoals in het Groenboek Telecommunicatie reeds was aangegeven, werd een uitzondering gemaakt voor spraaktelefonie. Eveneens werden telexdiensten, mobiele radiotelefonie, semafoon en satellietdiensten tijdelijk uitgezonderd van deze 'dienstenrichtlijn'.
Naast harmonisatie en liberalisatie wordt het *onderzoek* op het terrein van de telecommunicatie gestimuleerd door middel van projecten zoals RACE en STAR.

Met het in november 1993 in werking getreden 'Verdrag betreffende de Europese Unie' of het 'Verdrag van Maastricht' is aan het EG-Verdrag een titel XII toegevoegd ten aanzien van de zogenaamde *transeuropese netwerken* (de zogenaamde TEN's). Transeuropese netwerken betreffen niet alleen telecommunicatienetwerken maar ook netwerken op het terrein van het vervoer (bijvoorbeeld spoorwegen) en energie. De artikelen 129b-d EG-Verdrag verschaffen een basis voor het tot stand brengen van een onderlinge koppeling van tot nu toe nationaal georiënteerde telecommunicatie-infrastructuren alsmede van de interoperabiliteit tussen de verschillende netwerken. Dit beleid is noodzakelijk om daadwerkelijk een Europese elektronische snelweg te ontwikkelen.

In 1992 begon de Europese Commissie met een evaluatie van het Europees telecommunicatiebeleid op de apparatuur- en dienstenmarkt sinds het Groenboek Telecommunicatie.[8] Deze 'Review' heeft geleid tot een Resolutie waarin de Raad van Ministers instemde met de voorgestelde liberalisatie van het telefoonverkeer in 1998.[9] In deze Resolutie wordt een tijdsplan weergegeven voor de verschillende acties die, onder andere op het terrein van de regelgeving, in de komende jaren dienen te worden genomen.
In de eerste fase (1993-1995) zullen bestaande richtlijnen nader worden uitgewerkt, bijvoorbeeld op het terrein van de satellietcommunicatie. Tevens worden twee Groenboeken aangekondigd, namelijk een Groenboek Mobiele Communicatie en een Groenboek alternatieve infrastructuren en kabeltelevisienetten. Eerstgenoemd Groenboek Mobiele Communicatie werd in april 1994 gepubliceerd.[10] Het is een lijvig document, waarin de Commissie aankondigt dat alle beperkingen op het aanbieden van mobiele diensten dienen te worden afgeschaft.
De tweede fase (1996-1998) zal in het licht staan van een volledige liberalisatie van het telefoonverkeer in 1998. Tevens zal een kader voor regulering van publieke netwerkinfrastructuren worden geschetst.

DE BETEKENIS VAN HET JURIDISCHE KADER VOOR DE ELEKTRONISCHE SNELWEG

In de volgende drie subparagrafen zullen enkele aspecten van de elektronische snelweg in het licht van de hierboven omschreven regelgeving worden behandeld.

Aanleg en exploitatie van de elektronische snelweg

Het eerste aspect dat wordt behandeld, betreft de vraag wie de elektronische snelweg mag aanleggen, exploiteren en beheren.

Concessie KPN
Op basis van de huidige WTV heeft KPN in Nederland een exclusieve concessie voor de aanleg, de exploitatie en het beheer van de 'normale' telecommunicatie-infrastructuur. Deze exclusieve concessie omvat tevens de vaste verbindingen. De concessiehouder is echter verplicht om een dergelijke 'eigen weg' aan een ieder tegen vergoeding ter beschikking te stellen (art. 4, lid 2 WTV). De concessiehouder dient de snelweg goed te onderhouden zodat een doelmatige verzorging van telecommunicatie mogelijk is (art. 3, lid 2 WTV). Recentelijk heeft de minister een versoepeling bekend gemaakt van de in artikel 11 WTV genoemde voorwaarden waaronder KPN de uitvoering van de concessietaken aan een andere rechtspersoon kan overlaten. Hierdoor zou zij uitvoering van deze concessietaken bijvoorbeeld ook aan CASEMA en Unisource kunnen opdragen.[11]

Gemachtigde infrastructuren
De WTV bepaalt dat anderen dan de concessiehouder slechts telecommunicatie-inrichtingen van bijzondere aard of beperkte omvang mogen aanleggen wanneer zij voldoen aan hoofdstuk 3 van de WTV. Zo kan men een machtiging voor het aanleggen van radio-elektrische zendinrichtingen verkrijgen (art. 17 WTV). Aan het verstrekken van de machtiging kunnen voorschriften worden verbonden, bijvoorbeeld om een doelmatig gebruik van de ether te waarborgen.

Een belangrijke categorie machtiginghouders zijn de exploitanten van de in de wet aangeduide 'draadomroepinrichting' ofwel de kabeltelevisie-exploitanten (art. 21 WTV). De WTV bepaalt dat de exploitatie van deze kabeltelevisienetten in principe slechts plaatsvindt ten behoeve van het verspreiden van televisieprogramma's (art. 22, lid 1). Exploitanten dienen er dan ook voor te zorgen dat zij (eveneens) aan de regels van de Mediawet voldoen. Wil een exploitant het kabeltelevisienet gebruiken voor transport van andere diensten met betrekking tot de telecommunicatie dan dient hij een aanvullende machtiging in de zin van artikel 22, lid 2 WTV aan te vragen. Deze machtiging wordt geweigerd wanneer een doelmatige verzorging van de telecommunicatie in het algemeen

6. *Richtlijn van de Commissie betreffende de mededinging op de markten van telecommunicatie-apparatuur, Publikatieblad EG 1988, L 131, 73.*
7. *Richtlijn van de Commissie betreffende de mededinging op de markten voor telecommunicatiediensten, Publikatieblad EG 1990, L 192, 10.*
8. *Zie bijvoorbeeld Overzicht van de situatie in de sector telecommunicatiediensten (1992), Commissie van de Europese Gemeenschappen, SEC(92) 1048 def., Brussel, 21 oktober 1992.*
9. *Resolutie van de Raad van 22 juli 1993 inzake het overzicht van de situatie in de telecommunicatiesector en de noodzaak voor verdere ontwikkeling op die markt, Publikatieblad EG 1993, C 213, 1.*
10. *COM(94) 145 def.*
11. *Zie Bekendmaking inzake uitvoering telecommunicatieconcessie, Staatscourant 103, 3 juni 1994, p. 8.*

maatschappelijk en economisch belang zich tegen verlening hiervan verzet. Naast de machtiginghouders kent de WTV ook een categorie 'vrijgestelde' infrastructuren van zeer geringe omvang, zoals bijvoorbeeld kleine antenne-inrichtingen voor enkele woningen.

De interconnectie van de infrastructuren zodat een elektronische snelweg kan ontstaan, wordt niet expliciet in de WTV geregeld.

De regels voor aanleg en exploitatie in de WTV verschillen naargelang wordt gekozen voor een bepaalde categorie infrastructuur. De interconnectie van de infrastructuren zodat een elektronische snelweg kan ontstaan, wordt niet expliciet in de WTV geregeld. Daarentegen stelt de huidige WTV voor de kabeltelevisienetwerken de eis dat zij de grenzen van een gemeente niet mogen overschrijden (zie art. 21, lid 3 WTV).

Vergunninghouders voor mobiele communicatie
Het wetsvoorstel mobiele communicatie,[12] dat in juni 1994 door de Eerste Kamer werd aanvaard, doorbreekt de in artikel 3 WTV omschreven concessie van KPN. Het exclusieve recht van KPN wordt beperkt tot de aanleg en instandhouding van kabels, kabelwerken en satellietverbindingen. Naast KPN komen er vergunninghouders op de markt die bevoegd zijn tot de aanleg en het in stand houden van een telecommunicatie-infrastructuur, die nodig is voor het voor derden verzorgen van openbare mobiele telecommunicatiediensten. Het voorstel heeft betrekking op drie soorten mobiele communicatie, namelijk GSM, ERMES en DCS 1800. Voor ieder technisch systeem wordt in principe een tweede exploitant op de markt toegelaten. De regelingen voor deze vergunninghouders worden opgenomen in de artikelen 13a-13w, die worden gevoegd tussen de regelingen ten aanzien van de concessiehouder en de regelingen met betrekking tot de gemachtigde infrastructuren. Niet alleen voor wat betreft de positie in de WTV maar ook voor wat betreft de positie van de vergunninghouder geldt dat deze tussen die van de concessiehouder en de machtiginghouder inligt. Zo heeft de houder van de vergunning (evenals de concessiehouder) de plicht om de bij de vergunning opgelegde diensten landelijk te verzorgen en aan een ieder tegen vergoeding het gebruik daarvan ter beschikking te stellen (art. 13c, lid 2). Aan de houder van de vergunning worden eveneens verplichtingen opgelegd ten aanzien van de capaciteit, kwaliteit en eigenschappen (waaronder de technische aftapbaarheid) van de infrastructuur. Eveneens kunnen de regels 'het in stand houden van een kwalitatief hoogwaardige en innovatieve dienstverlening, aangepast aan de stand der ontwikkelingen' betreffen (art. 13g, lid 1, sub a en c). Hieronder vallen bijvoorbeeld regels ten aanzien van de beveiliging van de telecommunicatie-infrastructuur.

Voor de houder van de vergunning gelden ook regels die vergelijkbaar zijn met die van een machtiginghouder. Zo kunnen aan de vergunning voorschriften en beperkingen worden verbonden (art. 13l) en kan een vergunning worden ingetrokken wanneer een doelmatige verzorging van de telecommunicatie in het algemeen maatschappelijk en economisch belang dit vordert (art. 13v). Eveneens is een paragraaf over het koppelen van de telecommunicatie-infrastructuur van de vergunninghouder en de geschakelde telecommunicatie-infrastructuur van de concessiehouder opgenomen. Deze koppeling mag uitsluitend via de door de concessiehouder ter beschikking gestelde vaste verbindingen (huurlijnen) geschieden (art. 13p-13r).

Duopolie voor vaste infrastructuren
Zoals in het kabinetsstandpunt ten aanzien van herziening van de WTV is aangegeven, zal in een nieuwe WTV eveneens de concessie voor niet-mobiele infrastructuren worden doorbroken.[13] Er komt een duopolie. De minister heeft aangegeven dat voor deze tweede aanbieder van infrastructuur een samenwerkingsverband van exploitanten van gemachtigde infrastructuren in aanmerking kan komen. Deze tweede aanbieder krijgt in principe dezelfde verplichtingen als de concessiehouder opgelegd. Dus bijvoorbeeld eveneens een plicht om vaste verbindingen te leveren. De minister is op dit punt geen voorstander van asymmetrische wetgeving, waarbij de tweede aanbieder minder plichten krijgt opgelegd dan KPN.[14] In de beginsituatie heeft de tweede aanbieder echter nog geen landelijke leveringsplicht, zodat er dan wel sprake is van enige asymmetrie.

Exclusieve rechten
Binnen de Europese telecommunicatieregelgeving zijn geen specifieke regels gesteld ten aanzien van de aanleg en het beheer van telecommunicatie-infrastructuren. Zo wordt in de overwegingen bij de 'dienstenrichtlijn' betoogd dat de aanleg en de exploitatie van het telecommunicatienetwerk in de lidstaten door middel van de toekenning van uitsluitende rechten aan één of meer telecommunicatie-organisaties worden toevertrouwd. Hierdoor ontstaan wel machtsposities. De Europese regelgeving richt zich met name op het voorkomen van uitbreiding van dergelijke machtsposities naar andere telecommunicatiemarkten. Daarnaast worden telecommunicatie-organisaties met exclusieve rechten via specifieke aanbestedingsrichtlijnen verplicht om hun opdrachten tot levering van apparatuur en diensten openbaar aan te besteden wanneer deze de drempel van 600.000 ECU overschrijden.[15]
Regulering van de aanleg en het beheer van de infrastructuur valt wel in de toekomst te verwachten. Zo is reeds aangekondigd dat er vóór 1 januari 1995 een Groenboek over de zogenaamde alternatieve infrastructuren (bijvoorbeeld de door de spoorwegen en kabeltelevisie-exploitanten beheerde infrastructuren) zal verschijnen. De reeds hier-

12. *Wetsvoorstel mobiele communicatie, Tweede Kamer, vergaderjaar 1993-1994, 23 444, nrs. 1-2.*
13. *Tweede Kamer, vergaderjaar 1993-1994, 21 693, nr. 14.*
14. *Ibid.*
15. *Zie richtlijn 93/38/EEG houdende coördinatie van de procedures voor het plaatsen van opdrachten in de sectoren water- en energievoorziening, vervoer en telecommunicatie, zoals geïmplementeerd in de Nederlandse wetgeving en per 1 juli 1994 in werking getreden, Besluit van 30 mei 1994, Staatsblad 1994, nr. 376 en Staatsblad 1994, nr. 377.*

boven genoemde artikelen 129b-d EG-Verdrag met betrekking tot de transeuropese netwerken verschaffen eveneens een instrument om met name het koppelen van de verschillende infrastructuren te bevorderen.

Toegang tot de elektronische snelweg

Een belangrijke zaak betreft de vraag wie toegang krijgt tot de elektronische snelweg en onder welke voorwaarden. Opnieuw zal zowel vanuit de WTV als vanuit de Europese regelgeving op deze vraag worden ingegaan.

De WTV regelt niet expliciet onder welke voorwaarden men toegang heeft tot de telecommunicatie-infrastructuur. De concessiehouder heeft de plicht de infrastructuur aan een ieder tegen vergoeding ter beschikking te stellen, hetgeen in de algemene richtlijnen nader wordt uitgewerkt. De WTV geeft daarbij aan waarvoor de infrastructuur niet mag worden gebruikt. Artikel 4 noemt het verbod om via de infrastructuur het directe transport van gegevens te verzorgen. Eveneens vermeldt de tekst van artikel 5 dat de capaciteit van vaste verbindingen niet ter beschikking mag worden gesteld aan derden. De minister heeft evenwel in een Bekendmaking laten weten dat dit verbod inmiddels is opgeheven (hetgeen zij ook krachtens onderstaande EG-regelgeving verplicht was).[16] Randapparatuur die wordt aangesloten op de infrastructuur dient te voldoen aan de technische eisen van artikel 29 WTV.

Open Network Provision

De Europese telecommunicatiewetgeving omvat een aantal richtlijnen die de voorwaarden regelen waaronder gebruikers op uniforme en doorzichtige wijze toegang tot openbare telecommunicatienetwerken kunnen verkrijgen. Deze regelgeving wordt aangeduid als Open Network Provision (ONP).[17] Door middel van deze richtlijnen worden de voorwaarden voor een efficiënte en open toegang tot en gebruik van openbare telecommunicatienetwerken en -diensten geharmoniseerd. De ONP-voorwaarden mogen slechts betrekking hebben op drie typen (toegangs)voorwaarden, namelijk technische vereisten, gebruiksvoorwaarden en tarieven. Deze voorwaarden dienen te voldoen aan de basisbeginselen van objectiviteit, doorzichtigheid en toegangsgelijkheid. ONP-voorwaarden mogen de toegang tot openbare netwerken en diensten niet beperken, tenzij de beperkingen gegrond zijn op 'essentiële' eisen zoals de operationele veiligheid, het behoud van de netwerkintegriteit, de interoperabiliteit van diensten en de bescherming van gegevens. ONP-voorwaarden zijn reeds uitgewerkt voor huurlijnen, ISDN alsmede packet- en circuitgeschakelde datanetwerkdiensten.[18] Zo harmoniseert de ONP-richtlijn huurlijnen[19] de voorwaarden waaronder de nationale telecommunicatie-organisaties huurlijnen mogen aanbieden. Krachtens het non-discrimmatiebeginsel dienen huurlijnen op verzoek van elke gebruiker, zonder discriminatie, te worden aangeboden en geleverd. Een eventueel verbod van doorverkoop van transmissiecapaciteit voor huurlijnen mag alleen gebaseerd zijn op 'essentiële eisen'. Technische beperkingen ten aanzien van de onderlinge koppeling van huurlijnen of de koppeling van huurlijnen aan openbare netwerken dienen te worden opgeheven.

Technische beperkingen ten aanzien van de onderlinge koppeling van huurlijnen of de koppeling van huurlijnen aan openbare netwerken dienen te worden opgeheven.

De ONP-richtlijn huurlijnen diende vóór 5 juni 1993 in de Nederlandse wetgeving te zijn geïmplementeerd. Hiertoe heeft de Nederlandse wetgever (pas) in maart 1994 een voorstel ingediend.[20] Opmerkelijk is dat in dit voorstel geen inhoudelijke omschrijving van de ONP-voorwaarden te vinden is. Voorgesteld wordt om de regeling met betrekking tot de algemene richtlijnen (art. 8 WTV) uit te breiden tot de plicht van de concessiehouder om (gedetailleerde) informatie te verschaffen over de aangeboden huurlijnen. Verder zal er een bemiddelingsprocedure worden opgenomen in geval van geschillen tussen de leverancier van huurlijnen en de afnemer van die lijnen (in een nieuw artikel 40a). Wanneer de minister tot de conclusie komt dat de door de concessiehouder genomen maatregel onredelijk is, kan de minister een zogenaamde aanwijzing geven die de concessiehouder verplicht is op te volgen. Een op grond van de richtlijn vereist strakker toezichtsysteem voor de tarieven van huurlijnen werd reeds verwezenlijkt in de hierboven beschreven aanpassing van het Besluit algemene richtlijnen dat per 1 januari van dit jaar in werking trad.

Een duidelijke verwijzing naar de ONP-voorwaarden is te vinden in de wet mobiele communicatie. De houder van een vergunning voor aanleg en instandhouding van de mobiele telecommunicatie-infrastructuur is verplicht een ieder na een daartoe strekkend verzoek toegang te verschaffen (art. 13s wetsvoorstel). Wel kunnen regels ten aanzien van de 'wezenlijke vereisten' worden opgesteld maar deze mogen, volgens de Memorie van Toelichting, zich niet verder uitstrekken dan de in de ONP-richtlijn opgenomen 'essentiële vereisten', zoals bijvoorbeeld privacy-voorschriften. Met deze verwijzing naar de ONP-voorwaarden loopt de Neder-landse wetgever vooruit op de invulling van de ONP-voorwaarden op het terrein van mobiele communicatie zoals door de Europese wetgever wordt voorbereid.

16. *Zie Bekendmaking van de minister van Verkeer en Waterstaat van 14 december 1992, Staatscourant 1992, nr. 248.*
17. *Zie de Richtlijn van de Raad betreffende de totstandbrenging van de interne markt voor telecommunicatiediensten door middel van de tenuitvoerlegging van Open Network Provision (ONP), Publikatieblad EG 1990, L 192, 1.*
18. *De uitwerking van ONP op spraaktelefonie blijkt minder eenvoudig. Een (gewijzigd) voorstel werd gepubliceerd in Publikatieblad EG 1993, C 147, 12.*
19. *Richtlijn van de Raad betreffende de toepassing van Open Network Provision (ONP) op huurlijnen, Publikatieblad EG 1992, L 165, 27.*
20. *Wijziging WTV in verband met de uitvoering van richtlijn 92/44/EEG, Tweede Kamer, vergaderjaar 1993-1994, 23 632, nrs. 1-2.*

De communicatie op de snelweg

Wanneer men toegang heeft verkregen tot de telecommunicatie-infrastructuur, rijst de vraag welke diensten en onder welke voorwaarden deze diensten mogen worden aangeboden.

Allereerst de vraag welke diensten mogen worden aangeboden. Op grond van de Nederlandse WTV zijn dit alle diensten tenzij zij zijn opgedragen aan de concessiehouder. In december 1993 verscheen een Besluit waarin het oorspronkelijk Besluit opgedragen diensten werd gewijzigd.[21] Slechts de telefoondienst en telexdienst alsmede de datatransportdienst met en tussen mobiele gebruikers vallen nog onder de 'opgedragen diensten'. Het aanbieden van datatransportdiensten (en daarmee het ter beschikking stellen van huurlijnen ten behoeve van het verzorgen van deze diensten) kan door een ieder geschieden.

Gesloten gebruikersgroepen
Het aanbieden van spraaktelefonie via de publieke telecommunicatie-infrastructuur is (nog) niet toegestaan. De vraag is in hoeverre het aanbieden van spraaktelefonie die niet is bestemd voor het publiek (bijvoorbeeld via vaste verbindingen) wel is toegestaan. In dit verband kan worden verwezen naar de discussie rond de zogenaamde 'closed user groups' of 'gesloten gebruikersgroepen'. De redenering is dat het verzorgen van spraakverkeer voor dergelijke gesloten gebruikersgroepen niet onder het verzorgen van spraaktelefonie voor het publiek valt, waardoor deze spraaktelefoniediensten niet slechts aan KPN zijn voorbehouden. Om duidelijkheid te scheppen in deze discussie heeft de minister van Verkeer en Waterstaat op 3 juni 1994 een Bekendmaking inzake het begrip 'derden' bij spraakverkeer vaste verbindingen gepubliceerd.[22] Hierin wordt het begrip gesloten gebruikersgroepen omlijnd. Er is sprake van een gesloten gebruikersgroep indien het betreft: 'ondernemingen die deel uitmaken van dezelfde economische eenheid; groepen waarvan het voor de invoering van de dienstverlening duidelijk is, dat de leden beroepshalve duurzame relaties onderhouden van economische of professionele aard en dat de onderlinge communicatiebehoeften voortvloeien uit het gemeenschappelijk belang dat deze duurzame relatie schraagt'. Onder de eerste categorie vallen de concernnetwerken, zoals bijvoorbeeld ten behoeve van de communicatie tussen een naamloze vennootschap en haar dochters of filialen. Onder de tweede categorie valt bijvoorbeeld een branche waarbij de relatie tussen de leden van de groep bestaat uit gemeenschappelijke zakelijke activiteiten. De communicatiebehoefte van de branche is eigen aan de betrokken dienstverlening. Als voorbeelden worden genoemd de stoelreservering wat betreft luchtvaartmaatschappijen en informatietransfers tussen universiteiten die betrokken zijn bij een gemeenschappelijk onderzoekstraject. Ook ondernemingen die deel uitmaken van een relatienetwerk binnen een specifieke bedrijfskolom, zoals luchtvaartmaatschappijen en touroperators, kunnen een gesloten gebruikersgroep vormen. Overigens kunnen niet alleen beroepsrelaties van commerciële aard maar eveneens relaties zonder winstoogmerk onder de gesloten gebruikersgroepen vallen. De wederverkoop van capaciteit van huurlijnen ten behoeve van het aanbieden van spraaktelefonie binnen de gesloten gebruikersgroep wordt niet beschouwd als een doorverkoop ten behoeve van derden in de zin van artikel 5 WTV. Alhoewel artikel 5 WTV niet formeel is gewijzigd, heeft deze Bekendmaking van de minister tot gevolg dat deze bepaling met andere ogen dient te worden gelezen. Met een omlijning van deze gesloten gebruikersgroepen komt de minister tegemoet aan de behoefte van de aanbieders van telecommunicatiediensten om meer rechtszekerheid ten aanzien van de reikwijdte van dit begrip.

Het verzorgen van spraakverkeer voor gesloten gebruikersgroepen valt niet onder het verzorgen van spraaktelefonie voor het publiek.

Universele dienstverlening
Uitgangspunt van de Europese telecommunicatieregelgeving is dat de markt voor telecommunicatiediensten dient te worden geliberaliseerd. Dit betekent dat de in de 'dienstenrichtlijn' tijdelijk van liberalisatie uitgezonderde markten verder dienen te worden geliberaliseerd. Zo heeft de Commissie in december 1993 een voorstel ingediend om de dienstenrichtlijn (en apparatuurrichtlijn) uit te breiden tot satellietcommunicatie.[23] Hierdoor zal het aardsegment, dat wil zeggen het deel van het satellietcommunicatienetwerk dat de satellietgrondstations betreft, volledig worden geliberaliseerd. Verder wordt op Europees niveau gewerkt aan de voorbereidingen voor de liberalisatie van het telefoonverkeer in 1998. Een belangrijk aspect hierbij is de invulling van de zogenaamde universele dienstverlening (ofwel 'universal service'). Alle gebruikers, met inbegrip van specifieke maatschappelijke groeperingen, dienen tegen redelijke en betaalbare toegangs- en gebruiksvergoedingen gebruik te kunnen maken van de telefoondiensten. Behoud van universele dienstverlening op een geliberaliseerde markt is noodzakelijk in verband met de sociale functie van telefonie.[24]

Vergunningenstelsels
In het bovenstaande werd ingegaan op de vraag welke diensten langs de elektronische snelweg aangeboden mogen worden. Hieronder komen de voorwaarden waaronder deze diensten mogen worden aangeboden, aan de orde. Hierbij kunnen twee typen van voorwaarden worden onderscheiden. In de eerste plaats kunnen zij betrekking hebben op de voorwaarden voor het aanbieden van de telecommunicatiedienst (ongeacht welke dienst dit betreft). In de tweede plaats kunnen zij zien op de

21. *Staatsblad 1994, 21.*
22. *Staatscourant 103 van vrijdag 3 juni 1994, p. 14.*
23. *SEC (93) 1891 final.*
24. *Zie ook Resolutie van de Raad van Ministers en de verklaring van de Commissie over de beginselen voor universele dienstverlening in de telecommunicatiesector, Publikatieblad EG 1994, C 48, 1 en 8.*

voorwaarden die de inhoud van de specifieke diensten betreffen. Beide typen van voorwaarden zullen naar Nederlands respectievelijk Europees telecommunicatierecht worden uitgewerkt.

In de eerste plaats de voorwaarden waaronder een dienstenaanbieder zijn telecommunicatiediensten mag aanbieden. De huidige Nederlandse WTV heeft geen vergunningensysteem. Voor het aanbieden van telecommunicatiediensten is dan ook geen vergunning vereist. Wel legt de WTV formeel nog steeds de plicht op aan de exploitant van het kabeltelevisienetwerk om een aanvullende machtiging aan te vragen wanneer hij telecommunicatiediensten via het kabeltelevisienetwerk wil aanbieden (art. 22 WTV). Deze verplichting wordt opgelegd aan de exploitant en niet aan de aanbieder van de telecommunicatiediensten. Wanneer het telefoonverkeer zal worden geliberaliseerd, zal er voor de aanbieders van deze diensten wel een vergunningenstelsel worden ingevoerd.

Op dit moment is evenmin binnen de Europese Unie een vergunningenstelsel voorhanden. Wel staat de 'dienstenrichtlijn' toe dat nationale lidstaten een vergunningenstelsel voor het aanbieden van diensten hanteren. De meeste lidstaten kennen een vergunningenstelsel. De Europese Commissie streeft er echter naar om de procedures die worden gevolgd bij het verlenen van de vergunningen voor het aanbieden van telecommunicatiediensten te harmoniseren. Om deze reden werd in 1993 een ontwerp-richtlijn wederzijdse erkenning van licenties gepubliceerd, welke in 1994 werd gewijzigd.[25] Via het mechanisme van 'wederzijdse erkenning' wordt bereikt dat wanneer eenmaal volgens een gebalanceerde en efficiënte procedure toestemming is verkregen tot het aanbieden van telecommunicatiediensten in een bepaalde lidstaat, het aanbieden van deze diensten in een andere lidstaat in principe niet kan worden tegengehouden. Uiteindelijk zal worden gestreefd naar het invoeren van een Europese licentie voor het aanbieden van telecommunicatiediensten.

Cryptografie

Voor de inhoud van de criteria die worden gehanteerd voor het verwerven van een nationale licentie, geeft de 'dienstenrichtlijn' aan dat deze slechts betrekking mogen hebben op de 'essentiële vereisten' en dat zij objectief en non-discriminatoir dienen te worden toegepast. Beperking van toegang tot het openbare netwerk is toegestaan om redenen van de bescherming van gegevens, bijvoorbeeld wanneer het vertrouwelijk karakter van informatie dient te worden gewaarborgd. Beperkingen kunnen in verband met de openbare orde of de openbare veiligheid worden opgelegd. Deze beperkingen dienen echter restrictief te worden geïnterpreteerd en zij dienen in verhouding te staan tot de doelstellingen die met deze legitieme eisen worden beoogd. In dit verband kan als voorbeeld het, inmiddels weer ingetrokken, voorontwerp cryptografie worden genoemd.[26] Hiermee wilde de Nederlandse wetgever het aanbieden en gebruik maken van diensten waarbij gebruik wordt gemaakt van cryptografie, aan banden leggen. Cryptografie zou onder andere slechts toegestaan zijn wanneer de personen een machtiging van de minister hebben verkregen dan wel wanneer de cryptografie door de minister is toegelaten. In de toelichting bij het voorontwerp werd betoogd dat deze beperkingen uit het oog van criminaliteitsbestrijding of van staatsveiligheid toegelaten zijn, aangezien zij noodzakelijk zijn om deze doeleinden te bereiken en zij niet verder reiken dan nodig is om deze doelstellingen redelijkerwijs te bereiken. Het voorontwerp zou volgens de toelichting derhalve niet in strijd zijn met de 'dienstenrichtlijn'.
In het licht van bovenomschreven richtlijn wederzijdse erkenning van vergunningen zou men zich kunnen afvragen in hoeverre telecommunicatieaanbieders die in een andere lidstaat een vergunning hebben verkregen om diensten met encryptie aan te bieden, in Nederland eveneens deze diensten mogen aanbieden. In ieder geval wordt de ruimte voor het opstellen van een verstrekkende nationale Nederlandse regeling met betrekking tot cryptografie zoals in het voorontwerp werd voorgesteld, aanzienlijk beperkt door de Europese regelgeving. Mede in het licht van de felle kritiek die op het oorspronkelijke voorontwerp is geuit, zullen bij een nieuw op te stellen ontwerp de beperkingen op het gebruik van cryptografie beter in verhouding dienen te staan tot de doelstellingen die hiermee worden beoogd.

Bescherming van auteursrechten en privacy

Andere voorwaarden omtrent de inhoud van de berichten betreffen de voorwaarden die bijvoorbeeld op grond van het auteursrecht of de privacybescherming worden opgelegd. Deze regelgeving behoort niet specifiek tot het telecommunicatierecht, maar dient wel in beschouwing te worden genomen wanneer er een Europese elektronische snelweg zal ontstaan. Piraterij op de snelweg zal erg verleidelijk zijn. Zo zal men gemakkelijk auteursrechtelijk beschermde publikaties via de snelweg kunnen kopiëren en in Europa kunnen verspreiden zonder toestemming van de rechthebbende en zonder afdracht van een vergoeding aan de rechthebbende. Eveneens zullen bestanden waarin persoonsgegevens zijn opgenomen gemakkelijk verspreid of verhandeld kunnen worden. Europese regels om de privacy van betrokken personen te waarborgen zijn dan ook onmisbaar. Zo legt de Nederlandse Wet persoonsregistraties aan de houder van een persoonsregistratie de plicht op te zorgen voor de nodige voorzieningen van technische en organisatorische aard ter beveiliging van een persoonsregistratie. Overigens heeft de Registratiekamer in verband met deze eis aangegeven dat het oorspronkelijke voorontwerp cryptografie te weinig ruimte laat voor het gebruik van cryptografie ter beveiliging van bestanden met persoonsgegevens.[27]

Kortom, de aanbieders op de elektronische snelweg dienen zich niet alleen van de relevante telecommunicatiewetgeving rekenschap te geven, maar er eveneens voor te zorgen dat de inhoud van hun berichten in overeenstemming is met regelingen op het terrein van het auteursrecht en de privacy-bescherming.

25. *Gewijzigd voorstel voor een richtlijn van de Raad betreffende de wederzijdse erkenning van vergunningen en andere nationale machtigingen voor het exploiteren van telecommunicatiediensten, waarin begrepen de invoering van een communautaire telecommunicatievergunning en de instelling van het Communautair Telecommunicatiecomité, Publikatieblad EG 1994, C 108, 11.*

26. *Voorontwerp van wet inzake cryptografie, Wijziging van de Wet op de telecommunicatievoorzieningen in verband met de regeling van cryptografie. Het voorontwerp is onder andere gepubliceerd in Mediaforum Bijlage [6] 1994-6, B 49-B 55.*

27. *Zie brief van de Registratiekamer aan de Minister van Justitie van 3 mei 1994 en Staatscourant 96 van 25 mei 1994.*

Mw. mr. G.P. van Duijvenvoorde
Is universitair docent bij de Sectie Recht en Informatietechnologie, Faculteit Rechtsgeleerdheid van de Universiteit Utrecht. Zij doceert op het terrein van het informaticarecht en verricht onderzoek naar de toepassing van de Europese mededingingsregels op de markt voor informatietechnologie.

DE TELECOMMUNICATIEWETGEVING IN DE TOEKOMST

De huidige WTV is verouderd. Wetsvoorstellen, zoals het wetsvoorstel mobiele communicatie, voorzien in een aanpassing van de huidige WTV. Daarnaast vinden via wijziging van uitvoeringsbesluiten en publikatie van bekendmakingen *ad hoc*-wijzigingen van de telecommunicatieregelgeving plaats. Op deze wijze is de telecommunicatiewetgeving verbrokkeld. Een nieuwe, samenhangende WTV is onmisbaar. Ter voorbereiding van deze nieuwe wet dient een brede discussie op gang te komen. Deze discussie dient niet alleen te worden gedomineerd door economische en technische overwegingen.
In dit verband heeft de Nederlandse Organisatie voor Technologisch Aspectenonderzoek (NOTA)[28] gewezen op de noodzaak om in het debat over het telecommunicatiebeleid ook aandacht te besteden aan andere elementen, zoals de vrijheid van meningsuiting, privacybescherming, recht van intellectuele eigendom en mededingingsvrijheid. Daartoe heeft NOTA in november 1993 een agenda voor publieke discussie over telecommunicatie beschikbaar gesteld aan het Nederlandse parlement.[29] Op de agenda staan punten als het bepalen van de inhoud van de nutsdienst (universal service) alsmede de toegang, waaronder aspecten van ONP, interconnectiviteit, toegangscriteria, verdeling van schaarste en markttoetredingsvoorwaarden. Daarnaast besteedt de agenda aandacht aan democratische en economische controle. Voorgesteld wordt een zelfstandig bestuursorgaan in te stellen dat de telecommunicatiemarkt dient te reguleren. Alhoewel een aantal punten eveneens op de agenda van de Europese Unie staat, wordt er in de agenda op gewezen dat de nationale overheid zelf een verantwoordelijkheid heeft.
Met andere woorden, voor het opstellen van een nieuwe WTV dient niet slechts klakkeloos te worden gewacht op de richtlijnen uit Brussel, maar wordt aangedrongen op een duidelijk initiatief van de Nederlandse wetgever. Uiteraard dient dit initiatief wel verenigbaar te zijn met de Europese regelgeving.

TOT SLOT

Aan het begin van dit artikel werd de vraag gesteld in hoeverre het juridisch telecommunicatiekader toereikend is om de ontwikkeling van de elektronische snelweg mogelijk te maken. In het artikel is vervolgens ingegaan op het juridisch kader met betrekking tot de aanleg en exploitatie van de elektronische snelweg. Hieruit blijkt dat de huidige Nederlandse WTV verschillende regels kent naargelang het type infrastructuur. Een interconnectieverplichting, zoals thans in het EG-Verdrag opgenomen, ontbreekt in de huidige WTV. Door middel van het wetsvoorstel mobiele communicatie en de introductie van een duopolie op de vaste infrastructuur in de nabije toekomst, wordt de concessie van KPN doorbroken. Goede interconnectieafspraken en voorwaarden zijn dan onontbeerlijk. Voor wat betreft de toegang tot de infrastructuur kent de WTV geen expliciete uitwerking van de ONP-beginselen. Wel heeft de concessiehouder een leveringsplicht en wordt via algemene richtlijnen toezicht gehouden op de voorwaarden die door de concessiehouder aan gebruikers worden opgelegd. In de toekomst zullen dergelijke verplichtingen ook aan vergunninghouders worden opgelegd. Onder de huidige WTV behoeft de aanbieder van diensten geen vergunning te hebben. Er is dus een vrije communicatie mogelijk. Dit neemt niet weg dat de inhoud van de diensten in overeenstemming met de Auteurswet en de Wet persoonsregistraties dient te zijn.
Kortom, de telecommunicatieregelgeving in Nederland biedt in principe de basis voor een juridisch kader voor de ontwikkeling van de elektronische snelweg. Ook de Europese regelgeving voorziet in een toereikend kader voor de ontwikkeling van de elektronische snelwegen. Belangrijk is dat de beginselen zoals de universele dienstverlening en de interconnectie van netwerken nader worden uitgewerkt. Een nieuwe WTV, aangepast aan de Europese regelgeving, is noodzakelijk. Deze nieuwe WTV dient ervoor te zorgen dat Nederland een goede aansluiting krijgt op de Europese elektronische snelweg, al zal het aantal rijstroken in Nederland (voorlopig) beperkt blijven.

Dit overzicht werd afgesloten op 30 juni 1994. Na de sluitingsdatum van de kopij werd op 25 augustus 1994 de tekst van de Wet mobiele telecommunicatie officieel gepubliceerd in het Staatsblad (Staatsblad 1994, 628).

LITERATUUR

[Domm94] E.J. Dommering en N.A.N.M. van Eijk, *Agenda voor de publieke discussie over Telecommunicatie*, Computerrecht 1994/1, p. 9-19.

[Eijk93] N.A.N.M. van Eijk en P.B. Hugenholtz, *Toegang tot de kabel*, Instituut voor Informatierecht Amsterdam, 1993.

[Feij94] J.M.E. Feije en A.T. Ottow, *Telecommunicatie: van monopolie naar vrije markt?*, Nederlands Juristenblad 3 juni 1994, afl. 22, p. 745-749.

[Heyd94] M.A.J.M. van der Heyden, N.A.N.M. van Eijk, M. Joosten en B. Botein, *De digitale supersnelweg: Europa, Nederland, Groot-Brittannië en United States*, Mediaforum (6) 1994-4, p. 38-41.

[Rava94] P. Ravaioli en P. Sandler, *The European Union and Telecommunications: Recent Development in the Field of Competition*, in: The International Computer Lawyer, volume 2, number 2 (part I) en number 5 (part II), 1994.

[Slaa94] P. Slaa (red.), *Electronische snelweg. Op weg naar huis?*, Themanummer Informatie en Informatiebeleid, twaalfde jaargang, 1994, no. 1 (voorjaar).

28. *NOTA heeft haar naam recentelijk gewijzigd in het Rathenau Instituut.*
29. *NOTA, Bericht aan het Parlement (gepubliceerd in [Domm94]).*

Betrouwbaarheid en beveiliging van een CICS-omgeving

Ing. G.H.M. Meijer RE en
mw. J.A.M. Holla

De beveiligingsfunctionaliteit van het Customer Information Control System (CICS) is in de laatst verschenen versies sterk aan verandering onderhevig geweest. Hierbij heeft een verschuiving plaatsgevonden van de interne CICS-beveiliging naar beveiliging met behulp van een aanvullend beveiligingsprodukt.
De auteurs beschrijven de beveiligingsmogelijkheden van CICS versie 3.3 en de rol van het beveiligingspakket Resource Access Control Facility (RACF) hierbij. Hoewel er niet direct wordt ingegaan op auditaspecten, biedt dit artikel een goed uitgangspunt voor een audit naar het beheer en de implementatie van een CICS-omgeving.

INLEIDING

Geautomatiseerde gegevensverwerking is van oorsprong batch-georiënteerd. Bij het vastleggen van mutaties werden formulieren ingevuld, aan de hand waarvan later door een data entry-functionaris de mutatiegegevens in de computer werden ingevoerd. Periodiek werden deze gegevens door het computersysteem verwerkt.
Reeds lang geleden is een verschuiving opgetreden naar online/real time-verwerking. De mutaties worden door de eindgebruiker zelf rechtstreeks in het computersysteem vastgelegd, en in de meeste gevallen meteen verwerkt. Dit maakt het noodzakelijk dat de processen (programma's in uitvoering) voor vastlegging en verwerking van gegevens continu actief zijn en bovendien gelijktijdig door meerdere gebruikers kunnen worden aangeroepen. Hiervoor dient in het computersysteem een aparte omgeving te worden gecreëerd.

Het Customer Information Control System (CICS) van leverancier IBM is één van de hulpmiddelen waarmee een omgeving kan worden gecreëerd ten behoeve van online/real time-gegevensverwerking. Het wordt veel toegepast in IBM mainframe-omgevingen, onder besturing van Virtual Storage Extended (VSE) of Multiple Virtual Storage (MVS). Het systeem is echter ook beschikbaar voor OS/2-, OS/400- en RS/6000-omgevingen.
Met behulp van CICS kunnen schermfuncties worden gekoppeld aan in het systeem gedefinieerde transacties. Deze transacties kunnen op hun beurt worden gekoppeld aan programma's. Het activeren van een functie op het beeldscherm resulteert dan indirect in het uitvoeren van één of meer programma's.

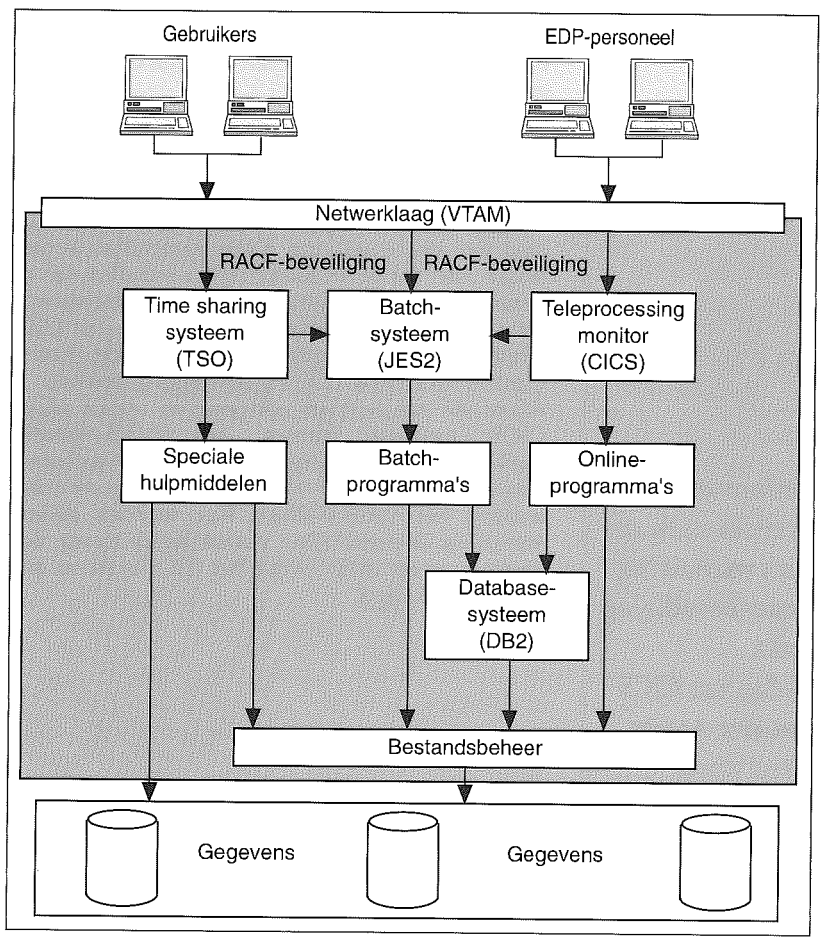
In dit artikel worden de beveiligingsaspecten van een CICS-omgeving beschreven. De versies die de laatste jaren van dit systeem zijn verschenen, vertonen onderling nogal wat verschillen op het gebied van de beveiliging. Deze verschillen komen onder meer tot uitdrukking bij het instellen van de parameters van het systeem. De beschrijvingen in dit artikel zijn gebaseerd op versie 3.3 van CICS binnen een MVS-omgeving met Resources Access Control Facility (RACF) als beveiligingspakket.
Allereerst zal worden aangegeven welke plaats CICS inneemt binnen het MVS-systeem. Vervolgens zal worden ingegaan op het technisch beheer van CICS, en wel met name op de wijze waarop het CICS-systeem kan worden gedefinieerd en onderhouden. Aansluitend wordt dan beschreven op welke wijze het CICS-systeem kan worden beveiligd.

POSITIE VAN CICS IN DE MVS-OMGEVING

In figuur 1 is een vereenvoudigd voorbeeld gegeven van de inrichting van een MVS-omgeving. In deze omgeving is CICS als online-omgeving één van de componenten met behulp waarvan programma's kunnen worden uitgevoerd of gegevens kunnen worden benaderd. In de praktijk wordt CICS veel toegepast in combinatie met databasemanagementsystemen zoals IMS of DB2. Het is echter ook mogelijk met behulp van CICS-programma's rechtstreeks bestanden te benaderen.

In de MVS-omgeving is CICS uiteindelijk maar een klein onderdeel van de te beveiligen omgeving. In een dergelijke omgeving is het uiteraard ook mogelijk op andere wijze programma's of gegevens te benaderen. Dit kan bijvoorbeeld met behulp van batch-programmatuur of krachtige online edit-programma's. Het aantal online-gebruikers is echter vaak veel groter dan het aantal gebruikers in bijvoorbeeld batch-omgevingen of omgevingen voor speciale hulpprogrammatuur.
In het voorbeeld is CICS als subsysteem gedefinieerd in een MVS-omgeving. Bij MVS kunnen subsystemen worden benaderd door middel van het logon-commando. Dit commando wordt opgegeven aan VTAM (netwerkbesturingsprogrammatuur): LOGON APPLID(CICS).
VTAM weet waar het subsysteem zich bevindt en zal als gevolg van dit commando een sessie tot stand brengen tussen CICS en de gebruiker. De gebruiker kan dan transacties initiëren, maar dient zich eerst kenbaar te maken aan het CICS-systeem. Dit gebeurt met behulp van een speciale transactie, als gevolg waarvan CICS een proces opstart dat de identiteit en authenticiteit van de gebruiker verifieert.

Figuur 1. CICS gepositioneerd in een MVS-omgeving.



De hiervoor beschreven werkwijze is geen gebruikersvriendelijke manier van toegang verlenen tot applicatiesystemen onder CICS. In de praktijk zal in veel gevallen sessie monitor-programmatuur zijn geïnstalleerd. Met behulp van deze programmatuur kan het VTAM logon-commando worden vervangen door een menugestuurd proces. Bovendien biedt dergelijke programmatuur ook voordelen op het gebied van beveiliging van de MVS-omgeving. In dit artikel is verder geen aandacht besteed aan de rol die deze programmatuur speelt in de beveiliging van een CICS-omgeving.

Binnen één MVS-omgeving kunnen meerdere CICS-omgevingen worden gerealiseerd. Deze CICS-omgevingen kunnen onderling informatie uitwisselen. Er kan echter ook communicatie plaatsvinden tussen CICS-omgevingen uit verschillende MVS-omgevingen. Hier wordt later in dit artikel op ingegaan.

Binnen CICS wordt aan transacties gerefereerd met behulp van een Transaction Code Identifier (TCI). Dit is een combinatie van vier posities (cijfers en letters). Het op deze wijze initiëren van transacties is echter niet gebruikersvriendelijk. Een alternatief hiervoor is het koppelen van transacties aan keuzemenu's op het beeldscherm. Een gebruiker geeft dan met behulp van bijvoorbeeld functietoetsen aan welke applicatiefunctie moet worden uitgevoerd. Binnen CICS worden deze functietoetsen dan weer gekoppeld aan transacties. Deze wijze wordt in de praktijk veelal toegepast.

DEFINITIE VAN EEN CICS-SYSTEEM

In dit artikel wordt veelvuldig het begrip resource gehanteerd. Het is een zeer ruim toepasbaar begrip en omvat eigenlijk alles wat nodig is om de CICS-omgeving te definiëren en met de gewenste functionaliteit te kunnen laten opereren. Het begrip is niet gerelateerd aan één 'niveau'. Zo is het van toepassing op zowel de CICS-bibliotheken - waarin de CICS-programmatuur is opgeslagen - als de in een tabel gedefinieerde terminals.

De definities ten behoeve van de configuratie en functionaliteit van de CICS-omgeving worden vastgelegd in tabellen alsmede in de CICS System Definition file (CSD). Voor het onderhouden van de tabellen en de CSD wordt gebruik gemaakt van twee verschillende hulpmiddelen:

- Resource Definition Macro (RDM) ten behoeve van de tabellen;
- Resource Definition Online (RDO) ten behoeve van de CSD.

Of een resource wordt gedefinieerd in een tabel of in de CSD is afhankelijk van het resource-type. Voor een beperkt aantal typen geldt dat de definities zowel in een tabel als in de CSD kunnen worden opgenomen.
Overigens kan per CICS-omgeving gebruik worden gemaakt van maximaal één CSD. Deze CSD kan echter wel gemeenschappelijk worden gebruikt door meerdere CICS-omgevingen. Voor elk type resource dat met behulp van een tabel wordt gedefinieerd, is een afzonderlijke tabel benodigd.

Resource Definition Macro

Met behulp van RDM worden tabellen opgebouwd waarin bepaalde resources van de CICS-omgeving worden gedefinieerd. Per type resource is een afzonderlijke tabel vereist, waarbij de naam van de tabel het type resource aangeeft. Zo zijn de terminaldefinities vastgelegd in DFHTCT, ook wel aangeduid met TCT. DFH is een prefix die voor de CICS-tabellen, maar ook voor bijvoorbeeld CICS-programma's, wordt gehanteerd. Overigens mag een aantal tabelnamen worden voorzien van een suffix, bijvoorbeeld DFHTCT01.
De tabellen worden opgebouwd en onderhouden met behulp van in assembler gecodeerde macro's. De source-code van deze tabellen wordt vertaald in een load-versie, welke wordt opgeslagen in een CICS-bibliotheek.

Tijdens het initialisatieproces leest CICS een tabel met systeeminitialisatieparameters: DFHSIT(xx), ook wel aangeduid als SIT. Vanuit deze tabel wordt, door middel van speciale parameters, verwezen naar de afzonderlijke tabellen. Deze parameters kunnen veelal drie waarden hebben:
- YES; dit betekent dat de tabel DFHTCT moet worden gelezen. Impliciet betekent het dus dat de naam van de tabel niet voorzien is van een suffix;
- xx als suffix; dit betekent dat de tabel DFHTCTxx moet worden gelezen;
- NO; dit betekent dat de tabel niet wordt gelezen.

Onderstaand zijn enkele voorbeelden van CICS-tabellen beschreven.

DFHSNT - Sign-on Table (SNT)
Deze tabel bevat algemene parameters met betrekking tot, alsmede afzonderlijke definities van CICS-gebruikers. De tabel is, in combinatie met RACF versie 1.9, niet meer noodzakelijk omdat alle relevante informatie in RACF kan worden vastgelegd. In tegenstelling tot andere tabellen mag de naam van deze tabel niet worden voorzien van een suffix. Verwijzing vanuit de SIT vindt niet plaats; de tabel wordt automatisch ingelezen indien deze aanwezig is.

DFHTCTxx - Terminal Control Table (TCT)
In de voorgaande versie van CICS bevatte deze tabel definities van terminals, printers en 'verbindingen' tussen CICS-omgevingen. Tegenwoordig moet een groot deel van deze definities worden vastgelegd in de CSD, zodat de TCT niet meer aanwezig hoeft te zijn in een CICS-installatie. De TCT wordt aangeroepen met behulp van de volgende parameter: TCT={YES | xx | NO}.

DFHPLTxx - Program List Table (PLT)
Deze tabel bevat programma's die worden uitgevoerd tijdens het initialiseren of het stoppen van een CICS-omgeving. Hiertoe dienen twee afzonderlijke PLT's te worden gedefinieerd. In de SIT zijn hiervoor twee verschillende parameters aanwezig:
- PLTPI={NO | xx | YES}; ten behoeve van de tabel met programma's die moeten worden uitgevoerd tijdens CICS-initialisatie;
- PLTSD={NO | xx | YES}; ten behoeve van de tabel met programma's die moeten worden uitgevoerd tijdens het stoppen van een CICS-omgeving.

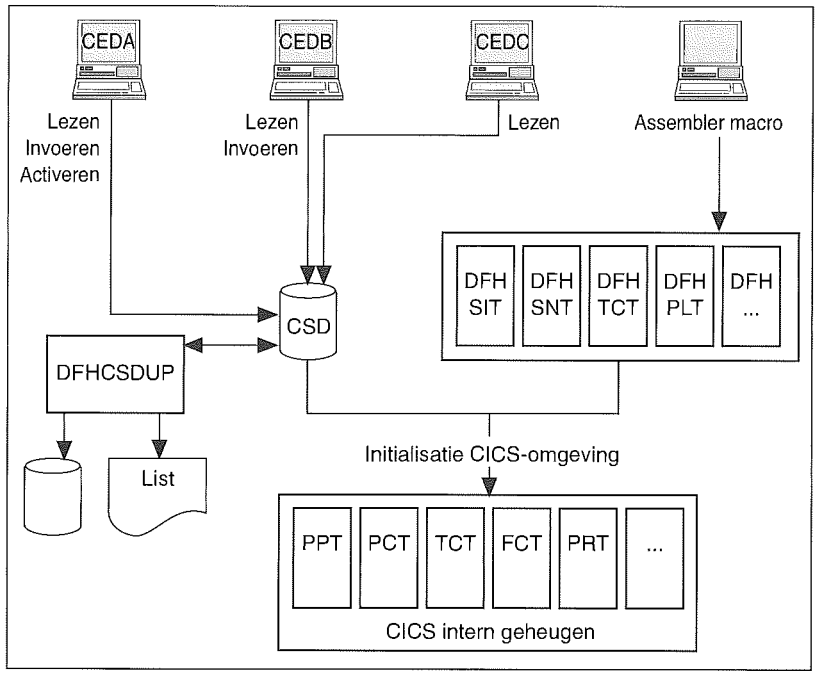
DFHSRTxx - System Recovery Table (SRT)
In deze tabel kunnen recovery-opties worden gedefinieerd. Hierbij gaat het om afwijkingen (zowel in positieve als in negatieve zin) van de herstelacties die CICS standaard uitvoert bij een storing.

Resource Definition Online

Bij RDO worden CICS-resources gedefinieerd met behulp van speciaal daarvoor meegeleverde transacties. De hiervoor gebruikte CICS-transacties zijn CEDA, CEDB en CEDC. Met behulp van CEDA kunnen wijzigingen worden ingevoerd en geactiveerd; met behulp van CEDB kunnen wijzigingen worden ingevoerd, maar niet worden geactiveerd; met behulp van CEDC kunnen slechts definities zichtbaar worden gemaakt.

In figuur 2 is schematisch weergegeven op welke wijze de resource-definities van RDM en RDO worden vastgelegd en hoe deze worden gebruikt voor het opbouwen van een CICS-omgeving. In één CSD kan meer worden beschreven dan voor één specifieke CICS-omgeving noodzakelijk is. Een CSD kan dan ook gemeenschappelijk worden gebruikt door meerdere omgevingen. In de SIT wordt aangegeven welk deel van de CSD voor de desbetreffende CICS-omgeving moet worden geladen.

De CSD kan ook worden onderhouden met behulp van het CICS System Definition Utility Program (DFHCSDUP). Dit programma biedt, naast het invoeren en activeren van de resource-definities, onder meer de volgende functies:
- INITIALIZE; het initialiseren van een CSD en het creëren van de standaard-CICS-resources. Hiermee wordt een CSD gecreëerd zoals deze door de leverancier wordt geleverd;
- MIGRATE; het converteren van CICS-tabellen naar de CSD;



Figuur 2. Systeemdefinities in een CICS-omgeving.

- LIST; het produceren van een listing van geselecteerde records uit de CSD;
- VERIFY; het opheffen van eventuele lock-situaties nadat een CICS-omgeving ongecontroleerd is gestopt.

De bescherming van RDO-functies tegen onbevoegd gebruik geschiedt door beveiliging van de desbetreffende CICS-transacties en het DFHCSDUP-programma. Het gebruik van het dit programma kan worden beveiligd door de beveiliging van de desbetreffende programmabibliotheek of door beveiliging van het programma zelf.
In de praktijk komt het voor dat het DFHCSDUP-programma wordt opgenomen in de linklist van het MVS-besturingssysteem. Dit betekent dat het programma door elke gebruiker kan worden opgestart. Voor de werking van het programma is het echter niet noodzakelijk dat het wordt opgenomen in de linklist; het kan ook worden opgestart vanuit een programmabibliotheek.

BEVEILIGING VAN EEN CICS-OMGEVING

In dit artikel is herhaaldelijk het begrip CICS-omgeving gehanteerd. Met CICS-omgeving wordt bedoeld het CICS-systeem in het interne geheugen van de computer, alsmede de produktiebestanden die door dit systeem zijn gealloceerd. Ook de libraries met daarin de CICS-programmatuur, de CSD en tabellen alsmede de JCL ten behoeve van de opstartprocedure worden in dit kader tot de CICS-omgeving gerekend.
Voor wat betreft het interne geheugen van de computer maakt één CICS-omgeving gebruik van één MVS-address space. Aan iedere address space in MVS is een afzonderlijke RACF user-id gekoppeld. In geval van CICS wordt dan gesproken over de RACF user-id van CICS.
Binnen de CICS-omgeving opereren gebruikers die ieder weer hun eigen RACF user-id hebben.

Een CICS-omgeving moet worden beveiligd tegen bedreigingen zoals het onbevoegd wijzigen van produktiegegevens en CICS resource-definities. CICS kan die beveiliging (in samenwerking met RACF) voor een deel zelf invullen, namelijk daar waar het gaat om acties die vanuit de CICS-address space worden geïnitieerd. Invloeden van buiten af vallen echter niet onder de controle van CICS en voor de beveiliging hiertegen is CICS volledig afhankelijk van RACF.

Teneinde inzicht te verkrijgen in de beveiligingsproblematiek rondom CICS is het zinvol onderscheid te maken in beveiliging tegen invloeden van buitenaf (zie subparagraaf Beveiliging van CICS als omgeving) en beveiliging tegen interne invloeden (zie subparagraaf Beveiliging binnen een CICS-omgeving).

Beveiliging van CICS als omgeving

Bedreigingen van buiten af worden gevormd doordat gebruikers onder meer in staat zijn buiten CICS om
- produktiegegevens van een CICS-omgeving te benaderen;
- definities van CICS-resources te wijzigen.

De CICS-produktiebestanden moeten zodanig worden beveiligd dat deze in principe alleen toegankelijk zijn voor de RACF user-id die gekoppeld is aan de CICS-omgeving en één of meer user-id's ten behoeve van batch-verwerking.

Het is niet noodzakelijk dat de RACF user-id's van de binnen de CICS-omgeving opererende gebruikers alle afzonderlijk toegang hebben tot de produktiebestanden van de CICS-omgeving. De gebruiker initieert weliswaar transacties binnen die omgeving maar het benaderen van bestanden als gevolg hiervan gebeurt door CICS zelf, waarbij RACF bij de autorisatie-evaluatie zal uitgaan van de RACF user-id van CICS.
Echter, de bestanden worden normaliter ook bewerkt door batch jobs. In de praktijk worden reguliere batch jobs vaak ingepland met behulp van een scheduling-pakket, waarbij de job de user-id overneemt van het scheduling-pakket. In dat geval dient ook deze user-id bevoegd te zijn tot het benaderen van CICS-bestanden.
Voor incidentele jobs ligt dit anders. In veel gevallen is het mogelijk ook de incidentele jobs met behulp van de scheduler te starten. Het komt echter nog vaak voor dat de werkvoorbereider de desbetreffende job vanuit bijvoorbeeld zijn eigen TSO-omgeving submit en de job de RACF user-id van de werkvoorbereider overneemt. In dit geval dient de RACF user-id van de werkvoorbereider ook toegang te hebben tot de CICS-bestanden. Hier ontstaat dan een probleem: de werkvoorbereider heeft ook TSO tot zijn beschikking en kan derhalve

rechtstreeks de produktiebestanden benaderen en manipuleren.

Eén van de oplossingen die hiervoor kan worden toegepast, is gebruik van het RACF surrogate user-mechanisme. Met behulp hiervan kan een speciale user-id worden toegekend aan batch jobs (deze wordt aangegeven in de JCL, hierbij wordt echter niet het password opgegeven). De user-id van de batch job wordt in RACF de 'original user' genoemd, de user-id van de werkvoorbereider wordt aangeduid met 'surrogate user'. Aan de werkvoorbereider kan de bevoegdheid worden toegekend om jobs te submitten met een specifieke original user-id.
Het spreekt voor zich dat de original user niet mag worden geautoriseerd tot het gebruik van TSO of CICS. Dit zou nog grotere beveiligingsrisico's opleveren. De original user mag uitsluitend worden gebruikt in de batch-verwerking.
Naast de hiervoor genoemde methoden moet het ook nog mogelijk zijn de CICS-produktiebestanden te benaderen met behulp van speciale programmatuur, bijvoorbeeld ten behoeve van back-up-doeleinden. Ook hiervoor kunnen batch-procedures worden gebruikt die met behulp van het surrogate user-mechanisme worden beveiligd.

Niet alleen de produktiebestanden van de CICS-omgeving dienen effectief te worden beveiligd. In het onbevoegd kunnen wijzigen van bepaalde CICS-resources zoals CICS-programmatuur, lokale modificaties en de CICS-opstartprocedure, schuilt het risico dat de functionaliteit van de CICS-omgeving niet meer voldoet aan de specificaties.
Als ondersteuning van procedures die erop zijn gericht de kwaliteit van het ontwikkelingsproces (op het gebied van zowel applicatie- als systeemprogrammering) te waarborgen, mogen de desbetreffende CICS-libraries slechts toegankelijk zijn voor de volgende user-id's:
- de user-id waaronder de opstartprocedure van CICS draait;
- de user-id die in het kader van het in produktie nemen van besturingsprogrammatuur de CICS-libraries vult met de CICS-programmatuur;
- een user-id voor eventuele calamiteiten.

Beveiliging binnen een CICS-omgeving

Bedreigingen van binnen uit worden gevormd door gebruikers die toegang hebben tot de CICS-omgeving. Door een niet-adequate definitie van autorisaties met betrekking tot het gebruik van transacties, programma's en gegevens, kunnen de in de organisatie gerealiseerde functiescheidingen worden doorbroken. Hierdoor kunnen gegevens ongeautoriseerd en onopgemerkt worden gemanipuleerd.
Het risico kan zich bovendien uitstrekken tot de integriteit van de CICS resource-definities. Dit is bijvoorbeeld het geval wanneer de autorisaties met betrekking tot de CICS-eigen transacties niet adequaat zijn gedefinieerd.

Deze functiescheidingen in de applicatiesfeer kunnen echter ook op een andere wijze worden doorbroken. In de praktijk wordt nagenoeg altijd autorisatie verleend voor het initiëren van transacties. Hierbij wordt niet rechtstreeks de relatie gelegd tussen gebruiker en gegevens. De autorisatie is gebaseerd op bepaalde functies van het programma dat aan de transactie is gekoppeld. Echter, het is mogelijk dat het programma meer of andere functies biedt dan wordt aangenomen.

In de praktijk is de kwaliteit van de beveiliging sterk afhankelijk van de functionaliteit van de programma's achter de transacties.

CICS biedt een aantal beveiligingsfunctionaliteiten met behulp waarvan de hiervoor genoemde bedreigingen worden tegengegaan. Zoals in de inleiding van dit artikel reeds is aangegeven, zijn in de laatst verschenen versies van CICS nogal wat verschillen te onderkennen met betrekking tot deze beveiligingsmogelijkheden. Zo was het in voorgaande versies van CICS (3.1 en eerder) mogelijk te kiezen tussen interne en externe beveiliging. Interne beveiliging hield in dat de beveiliging door CICS zelf werd geregeld. In geval van externe beveiliging werd een aanvullend produkt zoals RACF, ACF2 of Top Secret ingeschakeld voor het vastleggen van beveiligingsdefinities en het uitvoeren van de autorisatie-evaluatie. Bij deze versies van CICS was de standaardinstelling van de parameters zodanig dat de interne beveiliging niet werd geactiveerd en eveneens geen gebruik werd gemaakt van een aanvullend beveiligingshulpmiddel.
Bij interne CICS-beveiliging werd gebruik gemaakt van beveiligingscodes in de vorm van getallen. Aan een gebruiker konden, met behulp van de STCYKEY-parameter in de SNT, één of meer beveiligingscodes worden toegekend. Aan een transactie kon, met behulp van de TRANSEC-parameter in de transactiedefinitie, één beveiligingscode worden toegekend. In geval één van de toegangscodes van de gebruiker gelijk was aan die van een transactie, was de gebruiker bevoegd de transactie te initiëren.
Vergelijkbaar met transacties kon voor het gebruik van andere resources op soortgelijke wijze autorisatie worden verleend.

Vanaf CICS versie 3.2 is de interne beveiliging voor het grootste deel vervallen en kan, afgezien van de beveiliging van verbindingen tussen CICS-omgevingen onderling (zie later in dit artikel), slechts de keuze worden gemaakt tussen het wel of geen gebruik maken van een beveiligingspakket. De standaardinstelling van de parameters is zodanig dat een aanvullend beveiligingsprodukt wordt ingeschakeld.

In het vervolg van deze paragraaf zal de beveiligingsfunctionaliteit van CICS versie 3.3 worden behandeld. Hierbij zal waar nodig ook worden ingegaan op de relatie met RACF.

De SEC system initialization parameter
In de SIT kan worden aangegeven of de CICS-omgeving wel of niet moet worden beveiligd. De keuze heeft geen betrekking meer op interne of externe beveiliging, maar op het al dan niet activeren van de beveiligingsfuncties van het systeem. Activeren betekent automatisch dat er een aanvullend beveiligingshulpmiddel moet worden ingeschakeld.
Bij de SEC-parameter kan worden gekozen uit drie beveiligingsniveaus.
SEC=NO betekent dat voor deze CICS-omgeving de beveiligingsopties niet worden geactiveerd. Binnen de CICS-omgevingen kunnen dus alle resources door alle gebruikers worden benaderd.
SEC=MIGRATE betekent dat RACF wordt ingeschakeld voor de autorisatie-evaluatie, terwijl het gerealiseerde beveiligingsniveau, voor wat betreft het onderscheid tussen lees- en schrijfbevoegdheid, gelijkwaardig is aan dat van CICS versie 1.7 of CICS versie 2. READ-access op een transactie betekent dat de gebruiker de transactie mag initiëren, ongeacht wat de programma's achter deze transacties doen: lezen en/of schrijven van gegevens. De kwaliteit van de beveiliging en met name de technische ondersteuning van in de organisatie aangebrachte functiescheidingen, blijft in deze situatie dus sterk afhankelijk van de functionaliteit van de programma's achter de transacties.
SEC=YES betekent dat RACF wordt ingeschakeld voor autorisatie-evaluatie binnen de CICS-omgeving. Daarnaast kan in RACF niet meer worden volstaan met het definiëren van READ-access voor een transactie, maar moet expliciet worden aangegeven of, met behulp van de programma's achter die transactie, mag worden geschreven of gelezen.

De MIGRATE-optie van de SEC-parameter kan worden toegepast als overgangssituatie. De toegangsregels in RACF kunnen langzamerhand worden verfijnd. Als dit proces is afgerond, kan in één keer worden overgegaan naar de nieuwe situatie, waarbij UPDATE-access expliciet moet worden toegekend. Onderstaand is schematisch het verschil weergegeven tussen de MIGRATE- en de YES-optie van de SEC-parameter.

Tabel 1. Invloed van de SEC-parameter op de autorisatie-evaluatie.

Gebruikers-autorisatie in RACF	SEC=MIGRATE Toegangsaanvraag in de applicatie is READ of UPDATE	SEC=YES	
		Toegangsaanvraag in de applicatie is READ	Toegangsaanvraag in de applicatie is UPDATE
NONE	Geweigerd	Geweigerd	Geweigerd
READ	Toegestaan	Toegestaan	Geweigerd
UPDATE	Toegestaan	Toegestaan	Toegestaan

Naast de SEC-parameter dient, op een meer gedetailleerd niveau, te worden gedefinieerd welke beveiligingsfuncties van CICS/RACF dienen te worden geactiveerd. Zoals reeds gesteld wordt beveiliging op transactieniveau het meest toegepast. CICS biedt echter meer beveiligingsfuncties die afzonderlijk kunnen worden toegepast. Deze zijn onderstaand beschreven.

Terminal user security
Met terminal user security wordt bedoeld het identificeren en authenticeren van gebruikers. De gebruikers geven hun RACF user-id en password op tijdens de initiatie van de CICS login-transactie CESN. De verificatie van de identiteit en authenticiteit van de gebruiker wordt door CICS uitbesteed aan RACF. Bij een positief antwoord van RACF wordt dynamisch een element in de sign-on table (SNT) gecreëerd.

Preset terminal security
Voor specifieke doeleinden kan een 'preset' user-id worden gekoppeld aan een CICS-terminal. Dit betekent dat CICS de desbetreffende terminal automatisch inlogt zonder dat een gebruiker hier direct bij betrokken is. Deze faciliteit wordt veelal gebruikt in combinatie met apparatuur die niet voorzien is van een toetsenbord, zoals printers. Het is echter wel mogelijk dit toe te passen in combinatie met een traditionele terminal. Hierdoor kunnen alle gebruikers die fysiek toegang hebben tot deze terminal de transacties initiëren waartoe de preset user-id is geautoriseerd.
Met behulp van het onderstaande RACF- respectievelijk CICS-commando kan een terminal met preset security worden gedefinieerd:

```
ADDUSER
    user-id NAME
        (preset_terminal_user_name)
    OWNER
        (owner_user-id or group_user-id)
    DFLTGRP(group_name)

CEDA DEFINE
    TERMINAL(cics_terminal)
    NETNAME(vtam_term-id)
    USERID(user-id)
    TYPETERM(cics_typeterm)
```

Transaction security
Zoals met de SEC-parameter de RACF-beveiliging voor de gehele CICS-omgeving kan worden ingesteld, kan de XTRAN-parameter in de SIT worden gebruikt voor het activeren van de transactiebeveiliging. XTRAN=YES betekent dat CICS autorisatieverzoeken indient bij RACF op het moment dat een transactie wordt geïnitieerd.
Ten behoeve van de transactiebeveiliging worden door RACF twee general resource classes geboden: GCICSTRN en TCICSTRN. Met behulp van beveiligingsprofielen van het type TCICSTRN wordt steeds één individuele transactie beveiligd. De beveiligingsprofielen van het type GCICSTRN zijn bedoeld voor de beveiliging van groepen CICS-transacties. Het onderscheid tussen deze resource

classes is enigszins vergelijkbaar met het onderscheid tussen discrete en generieke profielen voor de beveiliging van datasets (zie hiervoor [Meij91]). Echter, generieke profielen voor datasets worden op een andere wijze gedefinieerd. Bij datasets wordt een groep geformeerd doordat één of meer high level qualifiers van een aantal datasets gelijk zijn. Voor CICS-transacties moeten de transacties in RACF expliciet worden gegroepeerd. Dit kan met behulp van het RACF RDEFINE-commando. In onderstaand voorbeeld wordt, met behulp van dit commando, een groep transacties gedefinieerd (en aldus een beveiligingsprofiel aangemaakt van het type GCICSTRN). Met behulp van het PERMIT-commando wordt de toegangslijst van het beveiligingsprofiel samengesteld.

```
RDEFINE
    GCICSTRN cics_transactie_groep
    NOTIFY(sec_administrator)
    UACC(NONE) ADDMEM
        (cicstran1, cicstran2, ...)

PERMIT
    cics_transactie_groep CLASS(GCICSTRN)
    ID(racf_group-id) ACCESS(READ)
```

In RACF is het mogelijk om, naast GCICSTRN en TCICSTRN, zelf general resource classes te definiëren ten behoeve van CICS-transacties. Deze dienen in RACF te worden toegevoegd aan de Class Descriptor Table. Tevens dient de naam van de general resource class te worden gespecificeerd met behulp van de XTRAN-parameter in de SIT.

Indien meerdere CICS-omgevingen zijn gedefinieerd binnen één RACF-omgeving, is het zonder aanvullende maatregelen niet mogelijk onderscheid te maken in de beveiliging van gelijknamige transacties in de diverse omgevingen. Om dit onderscheid te kunnen maken dient in de SIT de parameter SECPRFX=YES te worden gespecificeerd. Dit betekent dat de namen van de transacties bij autorisatieverzoeken aan RACF door CICS zullen worden 'geprefixed' met de user-id van de CICS-omgeving. Op deze wijze is het mogelijk een gebruiker te autoriseren tot het gebruik van de transactie CEDA in de omgeving CICSPRD1, zonder dat hij hierdoor tevens wordt geautoriseerd tot het gebruik van de gelijknamige transactie in de omgeving CICSPRD2.

```
RDEFINE
    TCICSTRN CICSPRD1.CEDA
    UACC(NONE) NOTIFY(sys_adm_user)

PERMIT
    CICSPRD1.CEDA CLASS(TCICSTRN)
    ID(group-id1) ACCESS(READ)

RDEFINE
    TCICSTRN CICSPRD2.CEDA
    UACC(NONE) NOTIFY(sys_adm_user)

PERMIT
    CICSPRD2.CEDA CLASS(TCICSTRN)
    ID(group-id2) ACCESS(READ)
```

Met behulp van de hiervoor weergegeven commando's wordt bewerkstelligd dat de CEDA-transacties van de omgevingen CICSPRD1 en CICSPRD2 beide een 'universal access code' hebben met de waarde NONE. Dit betekent dat niemand deze transactie mag initiëren tenzij specifiek autorisatie is verleend. Vervolgens wordt het initiëren van de transactie CEDA in de omgeving CICSPRD1 toegestaan voor de gebruikers binnen de groep group-id1, terwijl de gebruikers binnen de groep group-id2 bevoegd worden tot het initiëren van dezelfde transactie in omgeving CICSPRD2.

Zijn binnen één RACF-omgeving meerdere CICS-omgevingen gedefinieerd, dan zijn aanvullende maatregelen nodig voor de beveiliging van gelijknamige transacties in de diverse omgevingen.

CICS resource security
Behalve de transacties kunnen ook andere resources worden beveiligd. Deze resources worden nagenoeg altijd benaderd als gevolg van het initiëren van een transactie (en dus heeft er al een bepaalde autorisatie-evaluatie plaatsgevonden). Hierdoor kan het voorkomen dat een gebruiker geautoriseerd is een transactie te initiëren, terwijl hij geen autorisatie heeft tot het benaderen van bestanden of andere resources.

Teneinde de beveiliging van bepaalde typen resources te activeren moet aan de volgende voorwaarden worden voldaan:

- In de SIT dient SEC=YES te worden gespecificeerd.
- De typen resources die worden beveiligd, moeten in CICS worden aangegeven met behulp van de systeeminitialisatieparameters (vergelijkbaar met de XTRAN-parameter voor transacties). Tevens dienen in RACF - met behulp van het SETROPTS-commando - de corresponderende general resource classes te worden geactiveerd.
- Er dient RESSEC(YES) te worden gespecificeerd in de definitie van de desbetreffende (individuele) resource.
- Vervolgens dienen in RACF de beveiligingsprofielen van de te beveiligen resource profiles te worden gedefinieerd.

CICS-to-CICS security
Ten behoeve van interfaces tussen bepaalde applicatiesystemen in verschillende CICS-omgevingen is het vaak noodzakelijk dat deze CICS-omgevin-

gen met elkaar kunnen communiceren. Deze communicatie kan op twee manieren tot stand worden gebracht:

– *Multi Region Operation (MRO)*
MRO wordt toegepast voor de realisatie van communicatie tussen CICS-omgevingen binnen hetzelfde host-systeem. Omdat deze communicatie binnen dezelfde MVS-omgeving plaatsvindt, speelt SNA hierin geen rol, maar wordt de communicatie tot stand gebracht met behulp van MVS cross-memory services.

– *Inter System Communication (ISC)*
ISC heeft betrekking op communicatie tussen twee CICS-omgevingen in verschillende host-systemen. Bij deze communicatievorm wordt gebruik gemaakt van de SNA-verbinding tussen de twee host-systemen. De communicatie is gebaseerd op het LU 6.1- of LU 6.2-protocol.

De definitie van beide communicatievormen vindt op vergelijkbare wijze plaats. In dit artikel wordt alleen de communicatie met behulp van ISC beschreven.

Communicatie tussen twee CICS-omgevingen komt bijvoorbeeld tot stand wanneer vanuit een bepaalde CICS-omgeving een transactie in een andere CICS-omgeving wordt geïnitieerd.
In tabel 2 is een voorbeeld uitgewerkt waarin twee CICS-omgevingen zijn gedefinieerd in twee afzonderlijke host-systemen. In dit voorbeeld is het de bedoeling dat vanuit CICS01 de transactie TRN2 in CICS02 kan worden opgestart.
Hiertoe dienen allereerst een connectie en een sessie te zijn gedefinieerd. Tussen twee CICS-omgevingen is maximaal één connectie mogelijk. Over deze (logische) verbinding worden de sessies opgebouwd en vindt uitwisseling van informatie plaats. De beveiliging van de communicatie tussen de CICS-omgevingen vindt alleen plaats op het niveau van de connectie. Daarnaast zal een gebruiker uiteraard geautoriseerd moeten zijn tot het initiëren van de transactie TRN2 in de omgeving CICS02.

Tabel 2. Voorbeeld van ISC-definities.

NETWORK01 CICS01	NETWORK02 CICS02
CEDA DEFINE CONNECTION (CICS02) GROUP(groupname) ACCESSMETHOD(VTAM) PROTOCOL(APPC) NETNAME(vtam_applid) BINDPASSWORD(password) BINDSECURITY(NO) AUTOCONNECT(YES)	CEDA DEFINE CONNECTION (CICS01) GROUP(groupname) ACCESSMETHOD(VTAM) PROTOCOL(APPC) NETNAME(vtam_applid) BINDPASSWORD(password) BINDSECURITY(NO) AUTOCONNECT(YES)
CEDA DEFINE SESSION (CC0102) GROUP(groupname) PROTOCOL(APPC) CONNECTION(CICS02) AUTOCONNECT(YES)	CEDA DEFINE SESSION (CC0201) GROUP(groupname) PROTOCOL(APPC) CONNECTION(CICS01) AUTOCONNECT(YES)
CEDA DEFINE TRANSACTION(TRN1)	CEDA DEFINE TRANSACTION(TRN2)
CEDA DEFINE TRANSACTION(TRN2) REMOTE SYSTEM(CICS02)	

De beveiliging op het niveau van de connectie bestaat uit een soort 'handshaking'-procedure waarbij de omgevingen elkaars passwords uitwisselen. Deze passwords moeten gelijk zijn aan elkaar. De controle hierop kan zowel door CICS als door RACF worden uitgevoerd, en vindt plaats tijdens het afwerken van de VTAM-bindprocedure. Indien BINDSECURITY(NO) is gespecificeerd, draagt CICS zelf zorg voor uitvoering van dit proces.

Indien voor de beveiliging van de connectie gebruik wordt gemaakt van RACF, wordt de parameter BINDSECURITY(YES) gespecificeerd en doet een eventueel password in de BINDPASSWORD-parameter niet meer ter zake. In de SIT dient SEC=YES en XAPPC=YES te worden gespecificeerd. Vervolgens dient in RACF, met behulp van het SETROPTS-commando, de general resource class APPCLU te worden geactiveerd, en dient tevens een profiel te worden aangemaakt voor de desbetreffende connectie. Het is niet noodzakelijk dat beide deelnemers van de sessie gebruik maken van óf interne óf externe beveiliging. Het is mogelijk dat één kant wordt beveiligd met interne CICS-beveiliging, terwijl de andere kant wordt beveiligd door RACF.

Binnen één connectie kunnen meerdere sessies worden gedefinieerd. Een sessie kan op verschillende manieren worden opgestart. Een in de praktijk veel toegepaste wijze is het automatisch activeren van de sessie gedurende de initialisatie van de CICS-omgevingen. Hiertoe wordt, zowel in de connectie-parameters als in de sessie-parameters (van de omgeving die de actie initieert), AUTOCONNECT(YES) gespecificeerd. Indien dit in de connectie niet is gedefinieerd, komt de sessie niet automatisch tot stand.

Met behulp van 'link security' kan worden bereikt dat vanuit de ene CICS-omgeving slechts een beperkt aantal resources van de andere omgeving kan worden benaderd. Link security kan worden toegepast op een connectie of op een combinatie van een gebruiker of gebruikersgroep en een connectie. Om link security te activeren dienen specifieke parameters te worden opgegeven bij de definitie van de connectie.

SLOTOPMERKING

In dit artikel is de beveiliging van een CICS-omgeving behandeld. Hoewel CICS met de laatst verschenen versie (3.3) niet zelfstandig de beveiligingsevaluatie uitvoert maar hiervoor de hulp nodig heeft van een beveiligingspakket, moet een groot aantal parameters binnen de CICS-omgeving worden ingesteld op de juiste waarde om een ef-

fectieve interface met het beveiligingspakket te realiseren. Ook aan de kant van het beveiligingspakket moeten parameters worden ingesteld. Daarnaast moet aandacht worden besteed aan de interfaces met andere subsystemen, zoals DB2 en VTAM. Het voerde echter te ver om in het kader van dit artikel hierop in te gaan.
Bij gebruik van een ander beveiligingspakket dan RACF, zoals ACF2 of Top Secret, moet de interface aan de zijde van CICS in grote lijnen op dezelfde wijze worden geparametriseerd als bij RACF. De interface zoals die wordt gedefinieerd in het beveiligingspakket, wijkt voor de genoemde produkten uiteraard af.

Naast de beveiliging is ook de integriteit van CICS van groot belang voor een betrouwbare omgeving. Hiervoor is het noodzakelijk dat de CICS-omgeving in het interne geheugen van de computer voldoende wordt geïsoleerd van de andere processen. Door MVS worden hiertoe voldoende maatregelen geboden. Het is echter ook noodzakelijk dat de processen binnen één CICS-omgeving zodanig van elkaar worden geïsoleerd, dat zij elkaar niet ongeoorloofd kunnen beïnvloeden.
Van CICS is bekend dat onderlinge isolatie van deze processen te wensen overlaat en dat daardoor storingen kunnen optreden. In versie 4.1 van CICS zullen deze tekortkomingen volgens de leverancier worden weggenomen.

LITERATUUR

[Meij 91] G.H.M. Meijer, *RACF als access control software voor MVS-omgevingen*, Compact 1991/4.

[IBM92-1] CICS/ESA 3.3 - *Intercommunication Guide*, IBM publikatie SC33-0657-02, 1992.

[IBM92-2] CICS/ESA 3.3 - *CICS-RACF Security Guide*, IBM publikatie SC33-0749-0, 1992.

[IBM92-3] CICS/ESA 3.3 - *Installation Guide*, IBM publikatie SC33-0663-2, 1992.

[IBM92-4] CICS/ESA 3.3 - *System Definition Guide*, IBM publikatie SC33-0664-02, 1992.

[IBM92-5] CICS/ESA 3.3 - *Resource Definition Online*, IBM publikatie SC33-0667-2, 1992.

[IBM92-6] CICS/ESA 3.3 - *Resource Definition Macro*, IBM publikatie SC33-0666-2, 1992.

[IBM92-7] CICS/ESA 3.3 - *Operations Guide*, IBM publikatie SC33-0668-2, 1992.

Ing. G.H.M. Meijer RE
Is als EDP-audit-manager werkzaam bij KPMG Klynveld EDP Auditors. Zijn specialisatie betreft IBM mainframe-omgevingen, in het bijzonder, het gebied van MVS, beveiligingspakketten (zoals RACF, ACF2 en Top Secret), CICS, DB2 en VTAM/NCP. Hij geldt als een autoriteit op het gebied van beveiliging van dergelijke omgevingen. Van zijn hand zijn diverse publikaties op dit gebied verschenen.

Mw. J.A.M. Holla
Is als EDP-audit-assistant werkzaam bij KPMG Klynveld EDP Auditors. Zij heeft zich onder meer gespecialiseerd in de technische aspecten van rekencentra, en wel op het gebied van IBM mainframes.

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

2 21e jaargang 94/2 zomer 1994

Audit van een SNA-netwerk
M.M. Buijs RI en E.J.M. Ridderbeekx RE RI

Beveiliging van analoge kieslijnen
Drs.ing. D. Brouwer RE

Beveiliging van UNIX
Mw.drs. M.C. van Lith RE

Typologie van workflow-managementsystemen
Drs. D.J.P.Witte