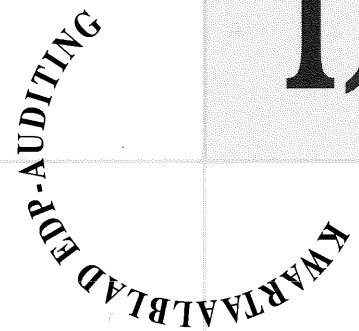
LENTE

COMPACT

FYSIEKE BEVEILIGING

1992/1



Compact ®
Jaargang 19, nummer 1
Een uitgave van KPMG Klynveld EDP Auditors en Samsom BedrijfsInformatie, werkmaatschappij van Wolters Kluwer NV.
Het blad verschijnt 4 x per jaar.

Redactie
D. Steeman RA (hoofdredacteur)
Drs. R.G.A. Fijneman RA
Prof. A.W. Neisingh RA
Drs. P. Veltman RA

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

Vormgeving
Bureau Karakter, Delft

Aan dit nummer werkten mee
J.F.C. van Epen, CISA
Drs. Th.H. van Hesteren
R.A. s'Jacob RA
Ing. J.F. Kuperus
Ing. G.H.M. Meijer
Ing. J.A.M. van Schaik
Drs. T.P. de Vries
Ir. B.J.M. van Wely
R. van de Wouw

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

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

Uitgever
J.R.M. Masselink
Lid van de Nederlandse organisatie van tijdschriftuitgevers NOTU

ISSN 0920 - 1645

INHOUDSOPGAVE

REDACTIONEEL

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

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

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

NOREA

Het verschijnen van het lentenummer van Compact geeft ons een goede gelegenheid met genoegen melding te maken van de oprichting van de Nederlandse Orde van Register EDP Auditors. Door verschillende beroepsbeoefenaren, onder wie schrijver van dit redactioneel, is gepleit voor het tot stand brengen van een beroepsorganisatie voor EDP-auditors. Het mag zo zijn dat, om vanuit de behoefte in de accountantscontrole om de automatisering "onder controle" te krijgen, registeraccountants in Nederland de aanzet tot de ontwikkeling van het vakgebied EDP-auditing hebben gegeven, steeds meer is gebleken dat met name uit de automatiseringsdiscipline EDP-auditors naar voren kwamen. Na de in circa 25 jaar in Nederland gegroeide beroepsuitoefening bestaat met het oprichten van deze Orde geen discussie meer over de volwassenheid van EDP-auditing. Het bij het destijds ter gelegenheid van het afscheid van voortrekker J.H. Urbanus georganiseerde seminar "EDP auditing volwassen?" geplaatste vraagteken kan derhalve vervallen.
Een blik op de concept-statuten leert dat alle elementen aanwezig zijn die het beroep tot een professie maken. De door de algemene vergadering in te stellen Raad van Tucht, die het sluitstuk op bewaking van de kwaliteit van de beroepsbeoefening zal zijn, is daarvoor het meest aansprekende kenmerk.
Of het ontbreken van een beroepsinstantie op de uitspraken van de Raad van Tucht aan het rechtsgevoel van veroordeelde beklaagden zal voldoen, moet worden afgewacht. Overigens fungeert de Raad van Tucht onder onafhankelijke "tot rechter in arrondissementsrechtbank" benoembare personen als voorzitter en plaatsvervangend voorzitter.
Een goede gedachte voor een volwassen doch jong beroep is het instellen van een Raad voor Beroepsethiek, welke anders dan bijvoorbeeld bij het NIVRA een permanente taak heeft in "de bewaking van de actualiteit" van het nog te ontwerpen gedrags- en beroepsreglement en het Reglement van Tucht.
Dat de Orde de mogelijkheid biedt voor studerenden om aspirant-lid te worden is eveneens een goede gedachte. Deze mogelijkheid leidt tot vroegtijdige binding aan beroep en Orde van jonge mensen die reeds werkzaam zijn in dan wel studerend zijn voor het EDP-audit-beroep, doch nog niet tot (stemgerechtigd) lid kunnen worden benoemd. Door het creëren van het geassocieerd lidmaatschap ten slotte biedt de Orde zichzelf en niet EDP-auditors zijnde anderen een mogelijkheid om in nog te creëren verbanden te discussiëren en gedachten uit te wisselen over grensoverschrijdende aangelegenheden.

Fysieke beveiliging

Het is een enigszins hachelijke zaak na alles wat over dit onderwerp reeds is geschreven toch nog een themanummer van Compact aan fysieke beveiliging te wijden. Er is echter een aantal redenen dit toch te doen:
- elk onderwerp dient ook om educatieve redenen van tijd tot tijd de aandacht te hebben;
- een verdieping op elementen is nuttig;
- leidinggevende functionarissen dienen van tijd tot tijd te worden geattendeerd op de blijvende noodzaak tot aandacht voor dit onderdeel van het beveiligingsbeleid.

Na een overzichtsartikel over het gehele gebied wordt uitgebreid ingegaan op brandpreventie en brandbestrijding en de mogelijkheden voor een EDP-auditor om bewakend en signalerend op te treden.
Een uiteraard essentieel onderdeel van fysieke beveiliging zijn de maatregelen ter voorkoming van storingen in de elektriciteitsvoorziening.
Naarmate huishoudingen meer steunen op de permanente beschikbaarheid van computers en netwerken voor hun operationele activiteiten dient uitval van verwerkingscapaciteit te worden geminimaliseerd. De bijdrage over netconditionering geeft inzicht in de technische complicaties van elektriciteitsvoorziening.
Wij allen worden ook in het dagelijks leven geconfronteerd met persoonlijk computergebruik. De pincode als mogelijkheid tot persoonlijke authenticatie en anderzijds beveiliging van geautomatiseerde systemen is een met name in Nederland terecht veel gehanteerde techniek. Het is de vraag of deze techniek blijft voldoen. Toepassing van chipcard-technologie geeft meer maar ook duurdere mogelijkheden. Bovendien geeft de chipcard meer gebruiksmogelijkheden dan alleen beveiliging, denk aan de elektronische beurs. De mogelijkheden van de chipcard-techniek worden uitgebreid aan de orde gesteld, mede op basis van praktijkervaring opgedaan bij de proef in Woerden.
In vervolg op het artikel in Compact 1991/3 over beveiligingsbeleid is het bijzonder nuttig nu een auteur over dit onderwerp te introduceren die de realisering van het beveiligingsbeleid in zijn (grote) onderneming beschrijft. Zoals in zovele andere gevallen is de automatiseringsafdeling hier de aanjager van dat beleid zowel naar haar "klanten" als naar het hoger liggende management. Wij hopen in een volgend nummer een artikel over het beveiligingsbeleid bij de centrale overheid te kunnen publiceren ten vervolge op deze reeks over dit onderwerp.
En dan ten slotte forensische EDP-auditing. Wie weet wat het is? Wie het niet weet, hij leze het desbetreffende artikel. Wellicht dat uit de kringen van advocatuur, rechtspraak en recherche zich de eerste geassocieerde leden voor de NOREA aandienen.
Een nieuwe lente, oude en nieuwe geluiden in Compact. Voor de volgende nummers staan thema's als "Bedrijfseconomische aspecten van IT", "EDI" en "Software als hulpmiddel bij audit en administratieve dienstverlening" op het programma.

D. Steeman RA

Fysieke beveiliging, een overzicht

J.F.C. van Epen, CISA

In Compact wordt veelvuldig aandacht besteed aan beveiligingsvraagstukken. Wat al lange tijd niet is behandeld, is het onderdeel fysieke beveiliging. De auteur geeft vanuit zijn ervaring in diverse werkgroepen en een aantal uitgevoerde opdrachten een overzicht van dit aandachtsgebied. Het moge dienen als kader voor onder andere enkele van de overige in dit nummer opgenomen artikelen.

INLEIDING

Over beveiliging in het algemeen en computerbeveiliging als onderdeel daarvan verschijnen regelmatig boeken en artikelen. Compact geeft eveneens structureel aandacht aan met name het onderdeel computerbeveiliging. Diverse organisaties houden zich ermee bezig en ook onder het Nederlands Genootschap voor Informatica (NGI) ressorteert een afdeling die specifiek is gericht op de beveiliging van de geautomatiseerde informatieverwerking.

Waarom zoveel aandacht voor dit onderwerp?

Hiervoor worden in de literatuur doorgaans de volgende argumenten aangevoerd:
- voortschrijdende penetratie van automatisering in organisaties;
- ten gevolge daarvan toegenomen afhankelijkheid van de automatisering voor de continuïteit van de organisatie als geheel of meer specifiek voor de operationele activiteiten, alsmede voor het management ten behoeve van diens besluitvorming;
- automatisering als belangrijk concurrentiemiddel.

Enkele daaraan toe te voegen argumenten zijn:
- de technologische ontwikkelingen op het terrein van de automatisering gaan doorgaans sneller dan het reageren daarop door middel van beveiligingsmaatregelen;
- bij de ontwikkeling van nieuwe (vormen van) automatisering en/of geautomatiseerde systemen wordt bij het beschikbaar stellen van investeringsbudgetten slechts in uitzonderingsgevallen voldoende rekening gehouden met het aspect "beveiliging".

Beveiliging kan derhalve worden gezien als het "kind van de (investerings)rekening". En hoewel ook op beveiligingsgebied steeds nieuwe ontwikkelingen het licht zien, kan worden geconstateerd dat de "gap" tussen de mate van automatisering en de mate van het beveiligen daarvan nauwelijks kleiner wordt. In sommige organisaties wordt deze zelfs groter.

Computerbeveiliging zal derhalve veel aandacht dienen te krijgen. In dit artikel zal - aan de hand van te onderkennen risico's - een overzicht worden gegeven van met name het terrein van de fysieke beveiliging en de in dat kader te treffen maatregelen. Fysieke beveiliging omvat [Belk79]:
- het onder alle omstandigheden optimaal en ongestoord doen werken van de computerfaciliteiten;
- de bescherming van alle programma's en gegevensverzamelingen.

De behandelde beveiligingsmaatregelen zijn niet specifiek gericht op het "grote" rekencentrum, maar zijn meestal ook van toepassing in de kleinschalige omgeving.

BEWUSTWORDING

Het realiseren van een adequate beveiliging is slechts mogelijk als aan twee voorwaarden is voldaan, namelijk dat de mensen behorende tot de organisatie zich bewust zijn van de noodzaak tot beveiligen en dat het beveiligingsgebeuren door het management wordt gedragen.

Beveiligen begint derhalve bij het management van een organisatie en als logisch vervolg op het bewustwordingsproces geeft dit de oekaze: "Gij zult beveiligen!" Dit leidt dan tot het formuleren van een beveiligingsbeleid, dat verder hiërarchisch wordt uitgewerkt. Dit wil zeggen dat naarmate het niveau in de organisatie lager is, de uitwerking van het beleid meer in detail zal plaatsvinden. Voor een beschrijving van een dergelijke methode wordt verwezen naar een eerder daarover in Compact gepubliceerd artikel [Heijt91].

Bij het vaststellen van het investeringsbudget voor automatisering is beveiliging nogal eens het kind van de rekening.

Computerbeveiliging betreft een omvangrijk gebied. Voor de duidelijkheid wordt dit daarom in een aantal deelgebieden onderverdeeld, die elk hun eigen benaderingswijze kennen. Het zal duidelijk zijn dat het aandacht geven aan slechts één of enkele deelgebieden nimmer kan leiden tot een adequaat beveiligingsniveau. Elk deelgebied is een schakel in het geheel; het spreekwoord over de sterkte van de ketting gaat derhalve ook hier op. Voor elk deelgebied zal een zodanige realisatiegraad moeten worden bereikt dat een evenwichtig stelsel van maatregelen ontstaat, waarbij bovendien een evenwicht wordt bereikt tussen kosten en nut.

Tot computerbeveiliging kan worden gerekend:
- het ontwikkelen van betrouwbare systemen;
- maatregelen gericht op een betrouwbare verwerking;
- maatregelen ter handhaving van de vertrouwelijkheid van gegevens;
- maatregelen gericht op het handhaven van de continue beschikbaarheid van de automatisering.

De maatregelen gericht op de betrouwbaarheid van de geautomatiseerde gegevensverwerking en het handhaven van de continuïteit daarvan kunnen weer worden onderscheiden naar organisatorische maatregelen (zoals interne controle), fysieke maatregelen en logische (geprogrammeerde) maatregelen. Tot de laatste categorie behoren onder meer de maatregelen gericht op het beveiligen van de toegang tot computers en netwerken via datacommunicatie. Dit aspect is in het voorgaande nummer van Compact aan de orde geweest [Velt91].

In het vervolg van dit artikel wordt uitsluitend ingegaan op de fysieke beveiligingsaspecten.

RISICO'S

Het treffen van beveiligingsmaatregelen kan plaatsvinden op grond van verschillende wijzen van benadering, zoals vanuit de risico's of vanuit de te beveiligen activa. Een behandeling van slechts een beperkt deel van het aandachtsgebied waartoe - zoals hiervoor geschetst - fysieke beveiliging moet worden gerekend, kan het best worden behandeld vanuit de bij dat gebied onderkende risico's.

Een hoofdindeling die in de literatuur nogal eens wordt aangetroffen, is het onderscheid tussen natuurrampen en menselijk falen, waarbij deze laatste categorie wordt onderverdeeld in ongelukken en kwade opzet. Technische storingen houden vaak dezelfde risico's in. Hieronder volgt een overzicht van de tot deze categorieën te rekenen risico's.

Overzicht risico's

Natuurrampen
- overstromingen;
- stormschade;
- blikseminslag;
- aardbevingen.

Ongelukken en technische storingen
- brand;
- explosie;
- waterschade;
- stroomuitval;
- kabelbreuk;
- fouten.

Kwade opzet
- diefstal;
- aftapping van communicatielijnen;
- geweldpleging;
- geweldloze acties.

De bespreking van de vermelde risico's kan kort worden gehouden. Het is niet moeilijk zich bij genoemde risico's een passende voorstelling te maken. De gegeven toelichtingen dienen dan ook als aanvulling daarop te worden gezien.
Het zal duidelijk zijn dat in een gegeven situatie niet alle genoemde risico's van even zwaar gewicht zijn. Slechts een (kwantificerende) risico-analyse of (kwalificerende) risico-afweging kan hierin enige duidelijkheid geven.

Natuurrampen

Deze komen in Nederland en België slechts in beperkte mate voor. De ligging van het gebouw

waarin de computerapparatuur is geplaatst, is met name van belang voor de gevoeligheid voor natuurrampen. De ligging binnendijks langs grote rivieren (bijvoorbeeld een deel langs de Maasoever in Rotterdam) of in ingepolderde gebieden kan risico's van *overstroming* inhouden. *Blikseminslag* is een bijna overal aanwezig risico. Slechts specialisten op dit gebied kunnen aangeven waar een dergelijk risico minder groot dan wel vrijwel afwezig is. Daar waar in de naaste omgeving het risico van blikseminslag bestaat, moet altijd met de terugslag rekening worden gehouden: het via de "aarde" in het elektriciteitsnet terugslaan van de zeer hoge spanning. Deze terugslag kan tot gevolg hebben dat de elektronische circuits in een computersysteem onmiddellijk of ook wel geleidelijk uitvallen.
Ook *stormschade* behoort in onze streken tot de normale risico's. Voor *aardbevingen* wordt dit niet als vanzelfsprekend beschouwd. Toch moet in bepaalde delen van Nederland en België (Noordoost Nederland - gaswinning - en Belgisch en Nederlands Limburg) rekening worden gehouden met eventuele aardbevingen. Vooral de laatste jaren doen deze zich met enige regelmaat voor.

Ongelukken en technische storingen

Ongelukken kunnen hun oorzaken hebben buiten het computercentrum en zelfs buiten de eigen organisatie, zoals branden en explosies in naburige opslagplaatsen van gevaarlijke stoffen of door het verkeer, een neerstortend vliegtuig en dergelijke.
Oorzaken binnen het computercentrum of het kantoorgebouw waar de apparatuur is geplaatst, kunnen zijn gelegen in menselijke fouten (hoofdoorzaak!), in niet "waterdichte" procedures, in technische onvolkomenheden van hardware en software of van de ondersteunende voorzieningen (energievoorziening, luchtbehandeling).
De als gevolg hiervan ontstane schade kan verschillende vormen aannemen: informatie kan verloren gaan of worden verminkt. Zij kan terecht komen bij personen of afdelingen waarvoor zij niet is bestemd. De gegevensverwerking kan voor kortere of langere tijd worden onderbroken. Dit alles kan al dan niet gepaard gaan met ernstige en kostbare materiële en immateriële schade.

Brand is een reëel en altijd aanwezig gevaar. Hij kan *explosies* veroorzaken, of daar juist het gevolg van zijn. Het is vooral het rekencentrum dat of de plaats waar de computer is opgesteld die daarvoor moet worden behoed. Vernietiging van de centrale computer of de netwerkserver is voor een organisatie een regelrechte ramp, die ten koste van alles moet worden voorkomen en - waar deze preventie faalt - effectief moet worden bestreden.
Het hier gestelde geldt ook voor de telefooncentrale (tegenwoordig ook vaak een computer), waarlangs meestal het externe lijnennet voor de datacommunicatie is geleid.
Brand en explosie kunnen het gevolg zijn van natuurverschijnselen (blikseminslag), menselijke fouten, technische storingen en van opzettelijk handelen. In het laatste geval kunnen de keuze van het tijdstip, van de plaatsen van aansteken en het aantal hiervan, het bestrijden van de brand extra moeilijk maken.

Zoals elke elektronische installatie is ook computerapparatuur min of meer gevoelig voor *water*. Bij de aanleg van waterleidingen en verwarmingsbuizen in of nabij het computercentrum dient hiermee rekening te worden gehouden, hetgeen eveneens geldt voor het plaatsen van watergekoelde installaties. Ook schade door bluswater bij een brand op een hoger gelegen verdieping dient zoveel mogelijk te worden voorkomen.
Vermelding verdient voorts de gevoeligheid van magnetische informatiedragers voor water.

Om de continue werking van de apparatuur te verzekeren zal men de *elektriciteitsvoorziening* in veel gevallen moeten beveiligen tegen onderbrekingen van (zeer) korte of langere duur. Dit kan door middel van een no-break-installatie, die afhankelijk van de energiebehoefte van de configuratie een onderbreking van enkele seconden tot soms wel een half uur kan opvangen. Beveiligen tegen langere onderbrekingen dient te geschieden met een noodstroomvoorziening (reserve-aggregaten). Men dient dan wel te bedenken dat men hier afhankelijk is van de, in beperkte mate, aanwezige hoeveelheid brandstof, of - bij het gebruik van aardgas voor de aandrijving van de generator - van de druk op het gasnet. Gebleken is dat bij een omvangrijke storing in de elektriciteitsvoorziening ook de druk op het gasnet kan wegvallen (Amsterdam-Zuid, najaar 1989).
Ook kleine computers kunnen op dit punt storingsgevoelig zijn. Nogal eens wordt voor een snellere verwerking door de programmatuur gebruik gemaakt van in het werkgeheugen gecreëerde grote databuffers en virtuele disks. Zelfs bij een zeer korte stroomonderbreking verliest dit deel van het werkgeheugen echter alle informatie, waardoor reeds verwerkte gegevens toch verloren gaan.

Ook *kabelbreuk* moet tot de fysieke risico's worden gerekend. Zowel intern als extern (in de grond) kunnen de datacommunicatielijnen worden beschadigd. Intern loopt men vooral gevaar bij de aansluitpunten aan het interne netwerk, indien deze laag bij de grond zijn aangebracht (bijvoorbeeld door stofzuigen); externe lijnen kunnen bij graafwerk worden vernield.

Verder kan worden gewezen op storingen van technische aard, bijvoorbeeld in de omgevingscondities voor de computer. Computerapparatuur dient immers in een "schone", geconditioneerde omgeving te worden opgesteld. Zoals alle elektronische apparatuur zijn ook de computer en de randapparatuur in meerdere of mindere mate gevoelig voor:
- stof en vuil;
- temperatuur en vocht;
- statische elektriciteit;
- magnetisme;
- radarstralen;
- röntgenstralen.

Fouten kunnen soms verstrekkende gevolgen hebben. Zij kunnen aanwezig zijn in de (systeem)programmatuur; gevolg kan zijn een verminking van de gegevensbestanden, zodat men moet terugvallen op kopieën. Ook bedieningsfouten kunnen sto-

ringen en verlies van programma's en/of gegevens ten gevolge hebben.

Kwade opzet

Hoe kleiner de apparatuur, hoe gevoeliger zij is voor *diefstal.* Met name wordt risico gelopen ten aanzien van kleinere centrale machines en netwerkservers. Met deze apparatuur gaan ook de programmatuur en de in de computers opgeslagen gegevens verloren.
Diefstal van informatiedragers behoort eveneens tot de reële mogelijkheden. Hiermee gaan ook data verloren of komen in onbevoegde handen.
Diefstal van documenten mag evenmin onvermeld blijven. Hiertoe doen zich verscheidene mogelijkheden voor, zoals:
- uit de veelal niet afgesloten kantoorruimten waaruit programma- en andere uitlijstingen vaak zonder meer kunnen worden meegenomen;
- uit voorraden papierafval (in gangen en kelders), waarin men grote hoeveelheden afgekeurde computeruitvoer kan aantreffen;
- uit (vaak open) rekken waar de uitvoer gereed ligt om door de gebruikers te worden afgehaald; of uitvoer die bij de klant wordt bezorgd, maar enige tijd onbeheerd blijft liggen.

Een bijzondere vorm van diefstal is de aftapping van communicatielijnen. Dit geschiedt vooral binnen de eigen gebouwen en kan soms een waardevolle oogst opleveren. Een andere vorm is het opvangen van de door de computerapparatuur opgewekte elektromagnetische straling, in de directe omgeving van deze apparatuur.

Bij het risico van *geweldpleging* kan onderscheid worden gemaakt tussen bedreigingen van binnen uit (het eigen personeel vormt hier de risicofactor) en van buiten af. Enkele jaren geleden was er, met name in Frankrijk, een golf van aanslagen op computercentra door terroristische groepen. Het is niet denkbeeldig dat vroeg of laat ook in andere landen een dergelijke vorm van actievoeren wordt toegepast. Deze acties onderscheiden zich van "normaal" vandalisme, doordat zij worden uitgevoerd door min of meer goed georganiseerde en uitgeruste groepen die door een of andere ideologie worden gedreven, zich bij hun acties alle middelen veroorloven en zelfs het gebruik van vuurwapens niet schuwen. Bij de bouw en de beveiliging van computercentra, vooral daar waar "actiegevoelige activiteiten" plaatsvinden, zal hiermee rekening moeten worden gehouden.

Een bepaalde maatregel kan soms meer dan één risico afdekken.

Ook geweldloze acties kunnen de verwerking aanzienlijk verstoren. Het lamleggen van de computerverwerking van binnen uit of door extern georganiseerde acties heeft dit reeds bewezen.
Stakingsacties, hoewel deze moeilijk onder "kwade opzet" kunnen worden gerangschikt, hebben een zelfde effect op de computerverwerking.

BEVEILIGINGSMAATREGELEN

De maatregelen te behandelen in dezelfde volgorde als de risico's is niet steeds mogelijk. Deze zijn daaraan namelijk niet eenduidig te relateren. Anders gezegd, met een bepaalde maatregel of categorie van maatregelen kan meer dan één risico worden afgedekt. De beveiligingsmaatregelen worden meestal gegroepeerd in:
- bouwkundige beveiligingsvoorzieningen;
- installaties;
- bewaking en toegangscontrole;
- gegevens- en informatiebeveiliging;
- uitwijk.

Bouwkundige beveiligingsvoorzieningen

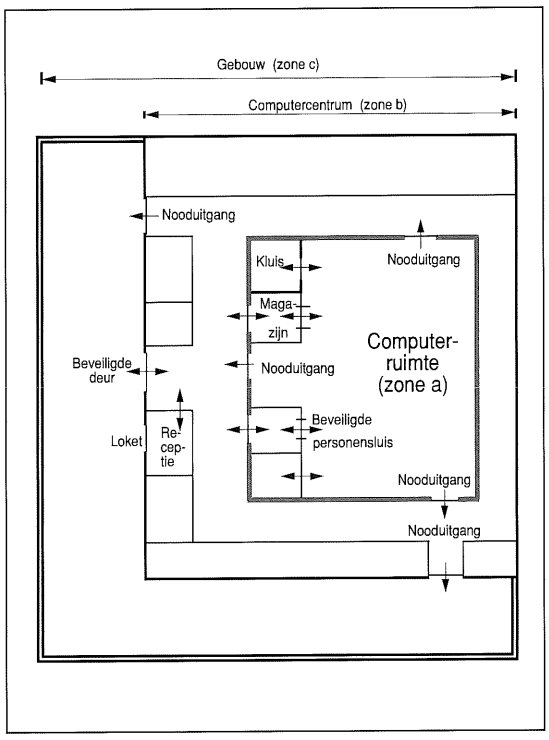
Het is van het grootste belang dat het gebouw en het daarin aanwezige computercentrum alsmede de directe omgeving daarvan in hoge mate bestendig zijn tegen het gevaar van brand en explosie. De keuze van de locatie voor het gebouw is daarom voor de beveiliging reeds van belang. Een bepaalde voorkeur kan niet worden uitgesproken; daarvoor zijn er te veel plaatselijke factoren in het geding. Wel kunnen enkele factoren worden genoemd, die bij de keuze van de locatie in overweging moeten worden genomen, zoals:
- zichtbaarheid vanaf de openbare weg;
- mogelijkheid tot beveiligen van de toegangsweg;
- bereikbaarheid voor de aan- en afvoer van goederen en personeel;
- het zo ver mogelijk verwijderd zijn van opslagplaatsen van brandbare stoffen, werkplaatsen waar met deze stoffen wordt gewerkt, keukens en kantines;
- voldoende afstand tot installaties die een elektromagnetisch veld opwekken en uitstralen.

Het gebouw dient te zijn opgetrokken uit materialen die in voldoende mate brandwerend zijn. Bouwkundige normen zijn hiervoor beschikbaar bij architecten, aannemers en verzekeraars. Soms kan het nodig zijn een onrechtmatige en soms gewelddadige toegang met behulp van bouwkundige voorzieningen zo goed mogelijk uit te sluiten. Dit dient op een zo onopvallend mogelijke wijze te geschieden.
Waar nodig kunnen vensters in buitenmuren van een rekencentrum van gelaagd ("slagvast") glas worden vervaardigd. Indien enigszins mogelijk moet worden voorkomen dat een op de begane grond gelegen computerruimte een van vensters voorziene buitenmuur bevat. Het inpandig situeren van deze ruimten moet worden nagestreefd.

In een computercentrum, dat als geheel een "beschermd" gebied is, bevinden zich enkele ruimten die door hun bestemming voor de gegevensverwerking van vitaal belang zijn. Tot deze *vitale ruimten* worden gerekend:

- computerruimten, waarbinnen de computer en de lokaal opgestelde randapparatuur zich bevinden;
- het banden- en schijvenarchief (bij kleinere centra de datakluis);
- de ruimte voor de datacommunicatie-apparatuur;
- technische ruimten, in het bijzonder die voor de energievoorziening en de luchtbehandeling.

Uit een oogpunt van beveiliging behoren deze ruimten:
- geïsoleerd te zijn van de voor het overige personeel en goederen bestemde routes binnen het gebouw;
- niet zichtbaar te zijn van buiten af;
- optimaal te zijn beveiligd tegen brand en andere calamiteiten;
- uitsluitend toegankelijk te zijn voor dat personeel dat daar werkzaam is; dit geldt ook voor kleinere rekencentra en serverruimten.



Figuur 1. Principeschets voor toegangscontrole tot en binnen het computercentrum.

Bovenstaande figuur geeft een algemene indruk van de indeling van een computercentrum, waarbij de volgende beveiligde zones kunnen worden onderscheiden:

a. De binnenste en best beveiligde zone, waarin de computer en lokale randapparatuur zich bevinden: de computerruimte; hierin kan, uit doelmatigheidsoverwegingen, de in- en uitvoerapparatuur gescheiden worden opgesteld.

b. Daaromheen de zone waarin de overige elementen van het computercentrum zijn ondergebracht, zoals voor de werkvoorbereiding, voor de afwerking van de uitvoer en voor de distributie van de uitvoer. Verder kunnen zich hier kantoren van de leiding en ten behoeve van de dienstverlening bevinden.

c. De zone rondom het rekencentrum.

Vitale ruimten, zoals het bandenarchief, de telecommunicatiecentrale (bij kleinere centra bevindt deze zich vaak in de computerruimte) en de ruimten waar de ondersteunende technische installaties zijn opgesteld, kunnen zich ook elders binnen het gebouw bevinden.

Installaties

De rondom een computersysteem aangebrachte installaties zijn technische hulpmiddelen van zeer uiteenlopende aard, die dienen om de continuïteit van de computerverwerking te garanderen. Zonder te streven naar volledigheid en zonder uitvoerig in te gaan op technische specificaties wordt hieronder een opsomming gegeven van een aantal met betrekking tot onder meer de geautomatiseerde gegevensverwerking belangrijke installaties. Elders in deze Compact wordt hierop meer specifiek ingegaan.
Welke installaties van belang zijn is sterk afhankelijk van de verwerkingsomgeving: welke eisen zijn door gebruikers met betrekking tot de continuïteit gesteld en welke apparatuur is opgesteld. Indien een specifieke situatie moet worden gecreëerd of beoordeeld, is het raadzaam gebruik te maken van een lijst met attentiepunten zoals de NGI Checklist Computerbeveiliging [NGI91].

Elektriciteitsvoorziening
Dient "schone" spanning te leveren van het juiste voltage.

No-break-installatie
Dient ter voorkoming van kortstondige verstoringen in de elektriciteitsvoorziening.

Noodstroomvoorziening
Dient ter voorkoming van langdurige verstoringen in de elektriciteitsvoorziening.

Airconditioning
Verzorgt de juiste luchtvochtigheid en -temperatuur.

Brandsignalering
Een automatisch werkend detectie- en alarmeringssysteem dient te zijn aangebracht, dat rook of het begin van brand zowel aan de brandweer, als aan het (doorlopend bezette) beveiligingscentrum van de organisatie meldt. Het signaal zal het luchtbehandelingssysteem en de energievoorziening dienen uit te schakelen (tenzij dit in het laatste geval schade aan de apparatuur zou veroorzaken). Melders zullen ook onder de verhoogde vloer en boven het verlaagde plafond moeten zijn geplaatst.

Inbraaksignalering
Afhankelijk van de grootte, de ligging en het belang van het computercentrum kan een keuze worden gemaakt uit diverse soorten signaleringsapparatuur. Het meest beperkt zijn trillingsdetectoren die op de ramen worden aangebracht. Alleen indien iemand zich langs deze weg toegang probeert te verschaffen zal een signaal worden afgegeven. Ook ruimtedetectoren zijn aan te bevelen. Deze werken meestal met warmte(infrarood)detectie of met lichtbundels, die niet doorbroken mogen worden. Aanvullend kan nog een gesloten tv-circuit worden aangebracht.
De signaleringsapparatuur zal meestal alleen in werking zijn indien het kantoorgebouw of het computercentrum niet bezet is. De signalen worden meestal automatisch doorgemeld aan een interne bewakingsfunctionaris of een externe bewakingsdienst, die voor eventuele doormelding aan de politie zorg dragen. Rechtstreekse doormelding naar de politie moet - tenzij daarover duidelijke afspraken zijn gemaakt - worden afgeraden, aangezien deze na enkele valse meldingen (waarvoor kosten in rekening worden gebracht) in het algemeen slechts met terughoudendheid zal reageren.

Brandblusapparatuur
In afwachting van de komst van de brandweer dient elke brand onmiddellijk na het ontstaan te worden bestreden, hetzij door een automatisch blussysteem, dan wel handmatig door het dichtstbijzijnde personeel.
In de computerruimte dienen brandblussers te zijn geplaatst, die geschikt zijn voor het blussen van branden in elektrische en elektronische apparaten. Men kent hierbij draagbare blustoestellen (meestal gevuld met CO_2 of met halongas) en stationaire automatische blusinstallaties. Laatstgenoemde installaties werken of met halongas of met water. In dit geval zijn zij uitgevoerd als zogenaamde "droge" sprinklerinstallatie, hetgeen wil zeggen dat er in de rustsituatie geen water aanwezig is in de leidingen. Eerst na een alarm vult het systeem zich met water, waarna het na enkele minuten met blussen begint, tenzij het alarm wordt ingetrokken. (De huidige computerapparatuur is redelijk tegen vocht bestand en kan na het droogföhnen ervan meestal weer normaal functioneren.)

Toegangsbeveiligingsapparatuur
Deze apparatuur ondersteunt de bouwkundige toegangsbeveiliging en zonering. Deze kan bestaan uit zeer eenvoudige apparatuur (slot met sleutels) tot zeer geavanceerde apparatuur, waarbij iedere persoon door het gebouw kan worden gevolgd door detectoren die op een centraal computersysteem zijn aangesloten. Deze personen kunnen zich alleen door het gebouw verplaatsen indien zij geautoriseerd zijn en uit dien hoofde beschikken over een speciale pas.

Bewaking en toegangscontrole

De toegang tot elk van de in de figuur getoonde zones dient zorgvuldig te worden bewaakt. De bewaking van het centrum behoort te zijn opgenomen in die van het gebouw of complex waarvan het deel uitmaakt en dient als bewaking van vitaal gebied bijzondere zorg en aandacht te krijgen. Dit laatste betreft dan vooral het voorkómen van alle vormen van fysieke schade, per ongeluk ontstaan of opzettelijk toegebracht (brand, vandalisme, enz.), alsmede de toegangscontrole.

Gegevens- en informatiebeveiliging

Eén der belangrijkste maatregelen voor het beveiligen van de continuïteit van gegevens is de backupprocedure. Backup-procedures trachten te bereiken dat bij het verloren gaan van (een deel van) de informatie, elders over actuele kopieën daarvan kan worden beschikt, zodat de gegevensverwerking binnen het eigen of een ander computersysteem zo snel en zo goed mogelijk kan worden voortgezet.
Dit betekent dus dat voor alle voor de gegevensverwerking benodigde informatie een volledige set buiten het computercentrum, of zelfs buiten het gebouw waarin dit centrum is gevestigd, moet zijn opgeslagen. Dit geldt voor het operating system en de overige systeem-software, de applicatie-software, bestanden, formulieren, documentatie, enz.

Bij de gegevensbestanden, en in mindere mate bij de programma's, doet zich een complicatie voor als gevolg van de doorlopende wijzigingen, waaraan vooral de eerste zijn onderworpen. Hiertoe zijn bepaalde technieken ontwikkeld, die neerkomen op een rouleringssysteem tussen enkele opeenvolgende generaties (het zogenaamde "grootvader-vader-zoon"-beginsel). De jongste generatie ("zoon") wordt voor de verwerking gebruikt; de vorige generatie ("vader") bevindt zich binnen het computercentrum om, indien nodig, de operationele versie onmiddellijk te kunnen vervangen. De derde en oudste generatie is opgeslagen in de eerder genoemde beveiligde locatie buiten het rekencentrum. Bij deze generatie zal tevens een bestand gevoegd moeten zijn met de tussen de "grootvader" en de "vader" verwerkte transacties teneinde, in geval van een zodanige calamiteit dat de "vader" ook verloren is, deze te kunnen reconstrueren. Zo zal ook een dergelijke vastlegging aanwezig moeten zijn van de transacties waarmee de "zoon" kan worden hersteld. Door een periodiek doorschuiven tracht men te bereiken, dat alle kopieën zoveel mogelijk up-to-date blijven. In de praktijk kan men diverse varianten op dit schema aantreffen, doch alle berustend op hetzelfde beginsel.

Bij de beveiliging van de buitenlocatie dient men erop te letten dat:
- deze op voldoende afstand van het computercentrum is gelegen, zodat niet beide door dezelfde calamiteit kunnen worden getroffen;
- het transport naar en van de locatie is beveiligd;
- de kopieën beveiligd zijn tegen brand, inbraak, enz.;
- de toegang tot de opslag goed wordt gecontroleerd.

Men dient goed te beseffen dat deze kopieën de laatste zijn waarover de organisatie beschikt!

Uitwijk

Eén van de hoofdtaken van de computerbeveiliging is het waarborgen van de continuïteit van de gegevensverwerking. Er zijn verschillende mogelijkheden om, bij een langdurige uitschakeling van het computercentrum, te kunnen terugvallen op een andere verwerkingscapaciteit. Wat ook wordt gekozen, er zal altijd aan een tweetal voorwaarden moeten worden voldaan:
- er moet een volledige backup van alle relevante bestanden en programmatuur, inclusief documentatie, aanwezig zijn op een locatie buiten het getroffen centrum;
- de over te hevelen "kritische" applicaties moeten nauwkeurig bekend zijn.

De leiding van de organisatie kan verder overwegen:

a. De reservecapaciteit binnen de organisatie te vinden:
- zonder dat bij de opzet van het computersysteem hiermee rekening werd gehouden;
- door deze bewust structureel op te nemen in het computersysteem.

b. De reservecapaciteit buiten de organisatie te zoeken door overeenkomsten met andere organisaties af te sluiten, op basis van een wederkerige steunverlening of door een verwerkingscapaciteit te huren, waarop in geval van nood onmiddellijk een beroep kan worden gedaan door gebruik te maken van:
- een uitwijkcentrum, waar al dan niet speciaal voor dit doel opgestelde apparatuur alsmede kantoorruimte aanwezig is;
- een mobiel vervangend centrum, dat kan worden gehuurd of in eigen beheer kan worden gehouden.

CONCLUSIE

Computerbeveiliging vormt een belangrijke investeringspost bij het automatiseren van de gegevensverwerking. Voor zover al niet wettelijk vereist (Wet Persoonsregistraties) is zij een bittere noodzaak teneinde de nodige drempels op te werpen tegen uitval van de computerverwerking.
Van het brede terrein van dit onderdeel van de automatisering is in dit artikel het onderdeel fysieke beveiliging behandeld, een facet van beveiliging waarbij in belangrijke mate kan worden gesteund op technische hulpmiddelen die bepaalde handelingen afdwingen. Toch blijft het een belangrijke zaak dat een organisatie die gebruik maakt van geautomatiseerde gegevensverwerking, zich bewust is van de gevaren die de computerverwerking bedreigen en derhalve een positieve houding ten opzichte van beveiliging inneemt.

Het is niet eenvoudig voor een gegeven situatie een evenwichtig beveiligingsplan op te stellen. Met name het optimaliseren van de verhouding tussen de aan de beveiliging te besteden kosten en het verkregen nut, is en blijft een arbitraire aangelegenheid. Soms wordt ter ondersteuning van de berekeningen gebruik gemaakt van risico-analysemethoden, waarmee de baten van beveiligingsmaatregelen zichtbaar kunnen worden gemaakt. Met nadruk zij erop gewezen dat dit slechts schijn is. Risico-analysemethoden werken met statistische gegevens (hoe vaak is een bepaalde calamiteit opgetreden) en voor computercentra als zodanig zijn deze gegevens niet beschikbaar. Men neemt dan zijn toevlucht tot Amerikaanse gegevens, die nu eenmaal niet op Nederland van toepassing zijn, of tot de bekende "natte vinger". Ook de schade na een calamiteit laat zich slechts op dezelfde wijze benaderen. Wanneer nu een slechte schadetaxatie wordt vermenigvuldigd met een "natte-vinger-risicobepaling" is het duidelijk dat de uitkomst van deze berekening discutabel is. Of anders gezegd: manipuleerbaar; het is maar wat men ermee wil bereiken.
Een beter alternatief is het maken van een risico-afweging, waartoe onder meer de NGI Checklist Computerbeveiliging een zeer bruikbaar hulpmiddel is. Met behulp van deze lijst is het mogelijk op maatregelniveau een soll-positie te bepalen. Na inventarisatie van de reeds getroffen maatregelen (ist-positie) resulteert daaruit een plan van nog te treffen maatregelen.

J.F.C. van Epen, CISA
Is sinds 1975 werkzaam in de EDP-auditing, sedert 1979 als EDP-auditor en thans als EDP-audit manager. Hij heeft een ruime praktijkervaring op vrijwel alle terreinen van de EDP-auditing. Zijn directe belangstellingsgebieden zijn computerbeveiliging, kleinschalige automatisering en micro-computers.
Van Epen participeerde in verscheidene werkgroepen, waaronder de NGI-werkgroep die de eerste versie van de Checklist Computerbeveiliging heeft vervaardigd.

Tot de hoofdtaken van de computerbeveiliging behoort het waarborgen van de continuïteit van de gegevensverwerking.

Nadat dit plan is gerealiseerd, kan worden gesteld dat een acceptabel beveiligingsniveau is verkregen. Echter na elke verandering in de automatiseringsomgeving dient een herhaling van deze werkzaamheden plaats te vinden. Dit dient dan een integraal onderdeel te zijn van de beveiligingsprocedures.

LITERATUUR

[Belk79] Prof. J.W. van Belkum e.a., *Automatisering van de Informatieverzorging*, 4e druk, Samsom, Alphen aan den Rijn.

[Heijt91] Mw. D. Jansen Heijtmajer, *Beveiligingsbeleid geautomatiseerde informatievoorziening*, Compact 1991/3.

[NGI91] Nederlands Genootschap voor Informatica (NGI), Sectie Beveiliging, *Checklist Computerbeveiliging*, Kluwer, Deventer.

[Velt91] Drs. P. Veltman RA, *Systemen voor logische toegangsbeveiliging*, Compact 1991/4.

Water en vuur. Effectiviteit van brandbeveiligingsmaatregelen in en om rekencentra

Ing. J.F. Kuperus en ing. G.H.M. Meijer

Brandpreventie en brandbestrijding, een "hot item" in veel organisaties! Maar gebeurt het wel goed?
En kan een EDP-auditor de getroffen maatregelen wel beoordelen?
In dit artikel vindt de lezer gedetailleerde informatie over dit onderwerp.

INLEIDING

Organisaties die vergaand afhankelijk zijn van geautomatiseerde gegevensverwerking zijn zich in toenemende mate bewust van de risico's die deze afhankelijkheid met zich meebrengt. Het continuïteitsaspect en dan met name het aspect brand wordt hierbij door het management doorgaans sterk belicht. Dit is ook niet zo vreemd als men bedenkt dat volgens Amerikaans cijfermateriaal meer dan de helft van de organisaties die getroffen zijn door een grote brand, dit op de langere termijn niet overleeft. In Nederland bedraagt, wat het bedrijfsleven betreft, alleen al de directe gevolgschade door brand ruim één miljard gulden per jaar.

Hoewel deze cijfers in feite niets zeggen over het risico van brand in een rekencentrum, zal het duidelijk zijn dat het management niet ten onrechte probeert de organisatie tegen de gevolgen van brand te beschermen.
De EDP-auditor wordt bij de uitvoering van zijn werkzaamheden mogelijkerwijs geconfronteerd met de vraagstelling of getroffen maatregelen in het kader van brandbeveiliging van een adequaat niveau zijn.
Dit artikel poogt de lezer meer inzicht te geven in het fenomeen brand en de te nemen maatregelen daartegen, in het bijzonder in relatie tot de geautomatiseerde gegevensverwerking. Na een algemene beschrijving van het begrip brand zal aan de hand van een aantal mogelijke maatregelen dieper op het beoordelingsaspect worden ingegaan.

BRAND

Voor het ontstaan en in stand houden van brand is een aantal elementen nodig. Dit zijn zuurstof, brandbaar materiaal en hitte. Bovendien is als vierde benodigd element een kataliserend proces te onderkennen. Door het wegnemen van één van deze elementen kan een brand worden gestopt.
Vuur of brand plant zich voort. De snelheid waarmee dit geschiedt wordt *brandvoortplanting* genoemd. Hoewel de mate van brandvoortplanting ook afhankelijk is van de hoeveelheid toegevoerde zuurstof (een sterke wind wakkert een brand aan), wordt deze voornamelijk bepaald door het soort materiaal dat wordt verbrand. Hierop wordt nog teruggekomen als gesproken wordt over de keuze van (bouw)materialen.

Een andere materiaal-afhankelijke factor is de *vuurbelasting*. De vuurbelasting geeft een indicatie van de hoeveelheid warmte die vrijkomt bij brand. Het is een in de praktijk ontwikkeld begrip dat wordt toegepast als eenheid van aanwezigheid van brandbare materialen en wordt uitgedrukt in kg vurehout per m^2. Het begrip wordt onder andere gebruikt bij de dimensionering van brandscheidingen (zie brandwerendheid).

Brandwerendheid wordt uitgedrukt in minuten en betekent dat een bepaalde constructie gedurende deze tijd weerstand biedt tegen branddoorslag (overslaan van de brand van de ene naar de andere ruimte) en in zekere mate thermisch isoleert. Deze thermische isolatie houdt grofweg in dat de temperatuur aan de niet-verhitte zijde van de wand niet meer dan 140 graden Celsius is toegenomen. De brandwerendheid in minuten betekent overigens ook dat het desbetreffende constructiedeel (wand, vloer, deur, etc.) gedurende deze tijd niet zal bezwijken.

Tenzij anders vermeld, wordt in dit artikel uitgegaan van een "normale" brand. Het temperatuurverloop van een "normale" brand is proefondervindelijk vastgesteld en wordt weergegeven in de "standaardbrandkromme". Overigens zal een gemiddelde brand (waar bijvoorbeeld een niet-overdadige vuurbelasting aanwezig is) binnen zestig minuten zijn gedoofd.

GEVOLGEN VAN BRAND

Brand vormt een bedreiging voor de continuïteit van de geautomatiseerde gegevensverwerking van een organisatie, doordat componenten die hierbij een rol spelen door brand worden beschadigd of vernietigd en daardoor niet meer beschikbaar zijn. Componenten in dit verband zijn onder andere huisvesting, bekabelingsinfrastructuur, apparatuur, gegevens en facilitaire voorzieningen.
Het niet meer beschikbaar zijn van één of meer van deze componenten bepaalt, in combinatie met de mate waarin een organisatie afhankelijk is van haar geautomatiseerde gegevensverwerking, het risico voor de organisatie.

Naast directe gevolgen van brand in een rekencentrum (het niet meer beschikbaar zijn van componenten) onderkennen we ook indirecte gevolgen. Het meest verstrekkende indirecte gevolg van brand is het niet meer of tijdelijk niet kunnen uitvoeren van de primaire bedrijfsprocessen.

Het meest verstrekkende indirecte gevolg van brand is het niet meer of tijdelijk niet kunnen uitvoeren van de primaire bedrijfsprocessen.

Behalve de bekende eigenschappen van brand, zoals het vrijkomen van hitte, oxidatie van materiaal en rook- en roetvorming, speelt het vrijkomen van gassen een belangrijke rol. Deze kunnen namelijk zeer agressief zijn.

Agressieve rookgassen, zoals bijvoorbeeld zoutzuur bij de verbranding van PVC, kunnen door het op gang brengen van een corrosieproces materialen ernstig aantasten, waardoor apparatuur direct of na enige tijd defect raakt.

De gevolgen van een brand voor de geautomatiseerde gegevensverwerking zijn daarnaast sterk afhankelijk van de locatie waar de brand heerst. Heerst een brand buiten het rekencentrum dan zullen rook, roet en agressieve rookgassen vaak alleen dan nadelige gevolgen hebben voor de geautomatiseerde gegevensverwerking als de brand ontstaat op dezelfde verdieping als het rekencentrum dan wel één of meer verdiepingen daaronder. Daarnaast is het denkbaar dat via airconditioningapparatuur rook en rookgassen naar het rekencentrum worden gevoerd.

Bij brand buiten het rekencentrum kan de datacommunicatiebekabeling of de stroomtoevoer worden aangetast, waardoor het rekencentrum niet meer kan functioneren. Evenzo dient bij brand buiten het rekencentrum rekening te worden gehouden met het feit dat leidingen voor blusmiddelen kunnen worden aangetast, waardoor automatische blusinstallaties niet meer functioneren.

Indien binnen het rekencentrum een grote brand ontstaat, kan worden gesteld dat de directe gevolgen (hittevorming, rook en roet, agressieve rookgassen en verbranding van materialen) bijna altijd desastreus zullen zijn.

MAATREGELEN TEGEN BRAND

In deze paragraaf is een aantal maatregelen beschreven die kunnen worden genomen ter voorkoming van brand dan wel ter beperking van de gevolgschade ervan.

Een organisatie kan op verschillende manieren maatregelen nemen tegen brand. Enerzijds zijn er maatregelen denkbaar ter voorkoming van brand (preventief), anderzijds teneinde een brand te bestrijden en de gevolgschade te beperken (repressief).

Maatregelen ter voorkoming van brand kunnen worden verdeeld in technische en organisatorische maatregelen. Bij organisatorische preventieve maatregelen moet worden gedacht aan procedures zoals een rookverbod in de computerruimte of een verbod van open vuur. Technische preventieve maatregelen zijn voornamelijk het toepassen van "onbrandbare" materialen en het aanbrengen van zones in een gebouw (compartimentering) door middel van brandwerende scheidingen.

Ook maatregelen ter bestrijding van brand dan wel het beperken van de gevolgschade zijn te verdelen in technische en organisatorische. Bij organisatorische repressieve maatregelen denken we aan richtlijnen en procedures zoals "wat te doen bij brand". Een technische repressieve maatregel kan onder meer zijn het aanbrengen van automatische signalerings- en blusapparatuur.

Teneinde op gefundeerde wijze te komen tot een stelsel van maatregelen, dient het management allereerst uitgangspunten te formuleren.

Teneinde op gefundeerde wijze te komen tot een stelsel van maatregelen, dient het management allereerst uitgangspunten te formuleren. Zo'n uitgangspunt kan bijvoorbeeld zijn het geven van een hoge prioriteit aan het behoud van bedrijfseigen middelen zoals gebouwen en programmatuur boven de niet-bedrijfseigen middelen zoals computers. Dit is gezien de huidige ontwikkelingen (korte levertijd) overigens een zeer legale keuze. Een ander belangrijk uitgangspunt in dezen is de maximaal te accepteren uitvaltijd van de geautomatiseerde gegevensverwerking.

Na het vaststellen van de uitgangspunten kan worden gekomen tot de keuze van te treffen maatregelen. Onderstaand zal een aantal technische maatregelen worden toegelicht. Organisatorische maatregelen zullen in dit artikel buiten beschouwing worden gelaten.

Compartimentering

Compartimentering in het kader van brand wil zeggen het dusdanig brandwerend afschermen van ruimten (door middel van constructiedelen met een hoge brandwerendheid) dat de brand wordt beperkt tot de ruimte waar deze is ontstaan. Het begrip ruimte kan in dit geval een aantal locaties betreffen die onderling gescheiden zijn door niet-brandwerende wanden. Een voorbeeld van compartimentering is het verdelen van een rekencentrum in de computerruimte (zaal), de datakluis en de overige ruimten (operator-ruimte, papiermagazijn, printerruimte, etc.).
Onderstaand wordt beschreven op welke wijze kan worden bepaald of en zo ja, hoe deze maatregel kan worden toegepast. Dit proces kan worden verdeeld in de volgende stappen:
- keuze van de af te schermen ruimten;
- bepalen van de vuurbelasting per ruimte;
- formuleren van eventuele verzwarende eisen;
- vaststellen van de vereiste brandwerendheid;
- keuze van materiaal en constructie.

Keuze van de af te schermen ruimten
Het management dient (op basis van bijvoorbeeld een risico-analyse) een uitspraak te doen over de gewenste beschikbaarheid van de componenten die van belang zijn voor de geautomatiseerde gegevensverwerking. Op basis van deze keuze kan de verdeling in brandwerende ruimten worden vastgesteld. Hierbij speelt, zoals later in dit artikel zal worden behandeld, de keuze tussen bescherming van objecten tegen de directe invloeden van brand versus de keuze voor een dusdanige bescherming dat de gegevensverwerking na de brand ongestoord doorgang kan vinden.

Bepalen van de vuurbelasting per ruimte
Het berekenen van de vuurbelasting is van belang omdat zal moeten worden bepaald of een eventuele brand in de desbetreffende ruimte een gemiddelde brand betreft, dan wel een brand is die groter en moeilijker te blussen zal zijn. Een moeilijk te blussen brand is langduriger en zal onder meer een hogere temperatuur in de omringende ruimten tot gevolg hebben, waardoor hogere eisen aan de brandwerendheid van de scheidingsconstructies moeten worden gesteld.

Het berekenen van de vuurbelasting is in het algemeen niet eenvoudig omdat de meeste locaties een veelheid aan materialen bevatten. Omdat kantoren normaliter een gemiddelde vuurbelasting hebben, hoeft voor een kantoorverdieping geen rekening te worden gehouden met het begrip vuurbelasting. Dit moet wél indien een ruimte een grote hoeveelheid brandbaar materiaal bevat. In en om rekencentra is in dit kader voornamelijk de vuurbelasting in ruimten waar papier ligt opgeslagen van belang. Als vuistregel kan deze vuurbelasting worden berekend door de maximaal aanwezige papiervoorraad, uitgedrukt in kg, te delen door de oppervlakte (in m^2) van de desbetreffende ruimte. Bevinden zich in de nabijheid van het rekencentrum andersoortige ruimten (bijvoorbeeld een machinekamer), dan kan het best overleg met de brandweer worden gepleegd. Deze kan op basis van ervaring de vuurbelasting van de aanwezige machines en mogelijke brandstoftanks snel bepalen.

Formuleren van verzwarende eisen
Verzwarende eisen met betrekking tot temperatuur en relatieve vochtigheid (RV) hebben voorna-

melijk betrekking op de bescherming van magnetische opslagmedia. Deze media worden overigens door een te hoge RV niet vernietigd, maar zullen ten gevolge van verkleving onbruikbaar worden. In het algemeen geldt voor deze media een maximaal toegestane temperatuur van 60 graden Celcius en een maximaal toegestane RV van 85 procent.

De huidige wijze waarop TNO de brandwerendheid van constructies vaststelt, biedt voor wat betreft deze verzwarende eisen geen uitkomst. Het begrip brandwerendheid zegt namelijk niets over de RV. Daarnaast mag volgens de desbetreffende norm de temperatuur aan de niet-verhitte zijde van de brandwerende scheiding oplopen tot gemiddeld 160 graden Celcius.
Wel kan TNO op verzoek van een leverancier een constructie op zulke afwijkende eisen beproeven. Dit zal in de praktijk alleen voorkomen bij in serie gemaakte produkten (verplaatsbare datakluizen en geprefabriceerde kluisdeuren). Deze zullen overigens meestal ook aan de VDMA-test (een Duitse test op het gebied van kluizen en kluisdeuren) zijn onderworpen, hetgeen eveneens voldoende waarborgen biedt. Wat betreft de in het werk gemaakte constructies (beton of metselwerk) kan bij het niet aanwezig zijn van een dusdanig testrapport, tabel 1 enige uitkomst bieden (een gemetselde wand heeft wat dit betreft met beton vergelijkbare eigenschappen).

De tabel is zeer globaal omdat de mogelijk te hoog oplopende RV veel invloed op de noodzakelijke wanddikte uitoefent. Bij verhitting van een wand of vloer kan namelijk vocht dat zich van nature in constructiedelen bevindt aan de niet-verhitte zijde naar buiten treden. Doordat de temperatuur van de ruimte in eerste instantie ook zal toenemen, is deze vochtafgifte voor wat betreft de RV geen probleem. Dit probleem kan echter ook na de brand ontstaan. Door het langzaam afnemen van de temperatuur zal de RV (omdat koudere lucht minder waterdamp kan bevatten) langzaam oplopen, zodat na het doven van de brand de opslagmedia alsnog gevaar lopen. Teneinde zeker te zijn dat de RV in verband met de opslag van magnetiseerbare media (bijvoorbeeld in een kluis) niet te hoog wordt, mag de temperatuur aan de niet-verhitte zijde van een wand dus slechts gering oplopen. Het eerder genoemde probleem bij afkoeling speelt in dat geval nagenoeg niet. Tevens zal de totale vochtafgifte uit de verhitte wand gering zijn.

Tabel 1. In het werk gemaakte constructies.

Dikte wand in mm	Verhitting gedurende	Max. temp. niet-verhitte zijde (graden Celsius)
100	60 min	50
100	90 min	100
100	120 min	140
200	60 min	-
200	90 min	27

Verzwarende eisen met betrekking tot temperatuur en relatieve vochtigheid hebben voornamelijk betrekking op de bescherming van magnetische opslagmedia.

Uit tabel 1 kan dan ook worden afgeleid dat een wand uitgevoerd in beton of metselwerk met een dikte van twintig centimeter voldoet aan de verzwarende eisen met betrekking tot temperatuur en RV. Een wand van tien centimeter is kritisch omdat na het doven van de brand nog geruime tijd verhitting van de ruimte zal plaatsvinden.

Vaststellen van de vereiste brandwerendheid
Op basis van ervaring van de brandweer kan worden gesteld dat een brand in het algemeen binnen zestig minuten is gedoofd. Derhalve kan, afgezien van ruimten waaraan verzwarende eisen zijn gesteld, globaal worden volstaan met een brandwerendheid van scheidingsconstructies van zestig minuten. Het Nederlands Normalisatie Instituut (NNI) hanteert in dit kader de vuistregel dat de brandwerendheid van een scheidingsconstructie gelijk dient te zijn aan zestig minuten plus de waarde van de vuurbelasting van de aangrenzende ruimte indien deze hoger is dan tien. Zoals reeds eerder gesteld, speelt het verhogen van de brandwerendheid voornamelijk een rol bij de opslag van papier.

Keuze materiaal en constructie
Op basis van de voorgaande stappen kan een keuze worden gemaakt met betrekking tot de toe te passen materialen en constructies teneinde de gewenste brandwerendheid te realiseren.
In het algemeen geldt de keuze tussen het in het werk fabriceren van constructies en het toepassen van geprefabriceerde constructies. Voor beide alternatieven geldt dat de aansluiting tussen de constructiedelen van essentieel belang is voor de uiteindelijk te realiseren brandwerendheid. Deze aansluiting is overigens voor geprefabriceerde constructies moeilijker te realiseren.

Toepassing van onbrandbare materialen

Een mogelijke maatregel in het kader van het tegengaan van brand is het toepassen van onbrandbare of nagenoeg onbrandbare materialen. Uit preventief oogpunt is het duidelijk dat toepassing van onbrandbare materialen de voorkeur geniet. Dit is uit technisch, financieel en/of ergonomisch oogpunt echter niet altijd mogelijk. Er zullen zowel op kantoorverdiepingen als in rekencentra altijd brandbare materialen worden toegepast. Het is dan wel van belang de hoeveelheid toegepaste brandbare materialen zoveel mogelijk te beperken. Daarnaast dienen de toegepaste niet-onbrandbare materialen zo min mogelijk bij te dragen aan de voortplanting van brand.

Wat dit betreft hanteert het NNI een indeling in klassen. Materialen in klasse 1 worden beschouwd als zwak bijdragend tot brandvoortplanting. Materialen in klasse 4 worden beschouwd sterk tot brandvoortplanting bij te dragen.

Het is duidelijk dat, indien toepassing van onbrandbare materialen niet mogelijk is, de voorkeur uitgaat naar toepassing van materialen die in klasse 1 zijn ingedeeld. Dit zijn bijvoorbeeld materialen als steenwol, glaswol en houtwolcement. Ook hiervoor geldt echter dat dit in de praktijk niet altijd haalbaar zal zijn. De EDP-auditor dient dan rekening te houden met de plaats en de hoeveelheid van toegepaste materialen die niet onbrandbaar zijn of niet tenminste in klasse 1 wat betreft de bijdrage tot brandvoortplanting zijn ingedeeld. Zo dient met name aandacht te worden besteed aan de vloer- en plafondafwerking.

Toepassing van materialen met een lage rookontwikkeling

Aansluitend op het bovenstaande is met betrekking tot de materiaalkeuze ook de rookontwikkeling van belang. Ook hiervoor geldt dat het best kan worden gekozen voor materialen die bij brand een zo laag mogelijke rookontwikkeling vertonen. De NNI-norm voor rookontwikkeling is uitgedrukt in een rookgetal. Materialen met een rookgetal van vijf worden hierbij beschouwd als materialen met een zwakke rookontwikkeling. Materialen met een rookgetal van maximaal vijf zullen bij brand het zicht overigens al beperken tot dertig à vijftig meter.

Het ligt voor de hand om in analogie met de bijdrage tot brandvoortplanting te eisen dat alle in het rekencentrum toegepaste materialen (zijnde niet-computerapparatuur en bekabeling) een maximaal rookgetal van vijf mogen hebben. Dit is helaas niet reëel. Er zijn wat dit betreft nog onvoldoende materialen beschikbaar die aan deze eis voldoen. Bovendien zegt het thans nog gehanteerde rookgetal alleen iets over de maximaal gemeten rookafgifte op zeker tijdstip gedurende de beproeving en niets met betrekking tot de gemiddelde rookafgifte over een tijdsinterval.

De organisatie heeft mogelijk verdergaande belangen dan de brandweer. Voor de brandweer is de rookafgifte in de eerste minuten na het ontstaan van een brand van belang. Deze moet zo laag mogelijk zijn zodat personen voldoende zicht hebben om te kunnen vluchten. Voor de organisatie is ook de totale rookafgifte van belang, omdat dit mede de aantasting van de voor de geautomatiseerde gegevensverwerking van belang zijnde componenten bepaalt.
Beide belangen (brandweer versus organisatie) komen niet tot uitdrukking in de huidige wijze van normering. Daarnaast geldt dat de mate van agressiviteit evenmin in dit getal tot uitdrukking komt.

Geconcludeerd kan worden dat het geen zin heeft te stellen dat alleen materialen met een zwakke rookontwikkeling mogen worden toegepast. Dit niet in het laatst omdat het in en rond rekencentra veelvuldig toegepaste PVC een rookgetal van tweehonderd heeft. Ter oriëntatie is in tabel 2 een opsomming gegeven van een aantal bekende materialen en het daarbij behorende rookgetal.

Materiaal	Rookgetal
Polyurethaanschuim	> 200
PVC	200
Polystyreen	100 - 200
Hardboard	120
Nylon	65
Teakhout	55
Spaanplaat	45
Zachtboard	22
Vurehout	14
Dennehout	6
Fenolformaldehydeschuim	1

Tabel 2. Rookgetal van veel gebruikte materialen.

Signaleren van brand

In principe kan brand worden gesignaleerd door het meten van een temperatuurstijging of een rookconcentratie. Een beginnende brand is echter moeilijk signaleerbaar. De hoeveelheid ontwikkelde rook zal evenals de optredende temperatuur in de directe omgeving namelijk beperkt zijn, en is derhalve ook voor de automatische signaleringsapparatuur moeilijk te detecteren.
Met betrekking tot de effectiviteit van de brandsignaleringspunten in een ruimte werkt de altijd aanwezige luchtstroming bovendien nog extra verstorend. Er vormt zich aan het plafond een klimatologisch luchtkussen dat de aanwezige rookgassen verhindert om de dichtstbijzijnde signaleringsapparatuur (aan het plafond) te bereiken. De luchtstroming is daarnaast ten gevolge van airconditioning en obstakels moeilijk voorspelbaar, waardoor het niet eenvoudig is de juiste plaats van de signaleringspunten te bepalen.

Bij uitputtende proeven in een volledig ingericht en operationeel rekencentrum is met betrekking tot de werking van signaleringsapparatuur gebleken dat een tijdige signalering van brand mogelijk is als één rookmelder een oppervlakte bestrijkt van:
- 15 tot 25 m^2 voor de computerruimte;
- 20 tot 30 m^2 voor het verlaagd plafond en de verhoogde vloer;
- 10 tot 30 m^2 voor kluizen voor magnetiseerbare gegevensdragers.

Tijdig kan in dit geval echter nog betekenen, dat er ongeveer tien minuten verstrijken tussen het uitbreken en het signaleren van de brand.

Blussen van brand

Sprinklerinstallaties
Sprinklerinstallaties zorgen bij brand voor een automatische blussing van de brandhaard, waarbij de

optredende temperaturen zodanig laag blijven dat constructies in beton na het doven van de brand nog intact zijn.
Het toepassen van sprinklers, met name in en om het rekencentrum, heeft in het verleden in een negatief daglicht gestaan. Steeds vaker blijkt echter dat het niet de computer maar het gebouw is dat als bedrijfseigen en dus onvervangbaar moet worden gezien. In de praktijk blijkt dan ook dat sprinklerinstallaties in rekencentra steeds vaker worden toegepast.

Hier is echter een kanttekening op zijn plaats. De snelheid van het in werking treden van een sprinklerinstallatie laat in de praktijk namelijk nogal te wensen over. Een sprinklerinstallatie zal pas in werking treden bij een temperatuur van ongeveer 70 graden Celcius (breken van de glazen ampul). Het tijdsverschil tussen het ontstaan van de brand en het aan het plafond bereiken van deze temperatuur kan oplopen tot twintig minuten. De temperatuur in de directe omgeving van de brandhaard kan intussen zijn opgelopen tot enkele honderden graden Celcius. Deze temperatuur is zoals gezegd niet gevaarlijk voor de constructie, echter wel voor de te beschermen computerapparatuur. Bovendien kan de vorming van agressieve rookgassen na twintig minuten reeds aanzienlijk zijn.

Halon- en CO_2-installaties
In tegenstelling tot een traditionele sprinklerinstallatie, die een mechanische branddetectie in zich heeft, wordt een automatische gasblusinstallatie toegepast in combinatie met een automatisch branddetectiesysteem.

Als vulling voor een automatische gasblusinstallatie worden CO_2 en halon toegepast. De werking van een gasblusmiddel is erop gebaseerd de ruimte voor een aantal procenten te vullen met het desbetreffende gas. Dit percentage wordt volume-procent (vol-%) genoemd. Dit vol-% dient gedurende enige tijd op niveau te blijven, anders wordt de werking van het blusmiddel teniet gedaan. Dit betekent dat alle ventilatie-openingen van de met gasblusmiddel gevulde ruimten tijdens en na de uitstoot van het gas gesloten dienen te zijn. Vanzelfsprekend mag ook de airconditioning niet meer werken en dienen de kleppen in de luchtbehandelingskanalen van deze installatie te worden gesloten.
Halon blijkt een effectief blusmiddel te zijn dat is gebaseerd op een anti-kataliserende werking. Een haloninstallatie wordt berekend op zes tot zeven vol-%. Een voordeel van halon is dat het de zuurstof niet aan de lucht onttrekt, waardoor het plotseling in werking treden van zo'n installatie geen direct gevaar oplevert voor eventueel nog aanwezig personeel.

De laatste jaren wordt er meer en meer aandacht besteed aan de milieuproblematiek. Halon is nogal in diskrediet geraakt doordat het de ozonlaag aantast. Het ligt in de lijn der verwachting dat, ten gevolge van recente metingen van de ozonlaag, halon (als blusmiddel) binnen afzienbare tijd verboden zal zijn.

De werking van CO_2 is dat het de zuurstof aan de lucht onttrekt, waardoor het vuur zal worden gedoofd. Dit levert direct gevaar op voor het aanwezige personeel (en bezoekers). Om dit risico te beperken wordt in de praktijk nogal eens een vertraging ingebouwd tussen de brandsignalering en het automatisch in werking treden van de blusinstallatie. Hierdoor heeft het personeel enige seconden de tijd de desbetreffende ruimte te verlaten.
Het benodigde vol-% voor CO_2 ligt beduidend hoger dan voor halon: dertig procent. Bij zowel een CO_2- als een haloninstallatie zal rekening moeten worden gehouden met de enorme kracht waarmee het gas wordt uitgestoten.

Sprinklerinstallaties worden in rekencentra steeds vaker toegepast.

AANDACHTSPUNTEN BIJ AUDIT

Onderstaand is een aantal aandachtspunten opgenomen die van belang kunnen zijn voor de EDP-auditor die is belast met het geven van een oordeel over de kwaliteit van de genomen fysieke maatregelen in het kader van de brandbeveiliging.

Compartimentering

De EDP-auditor zal op basis van de uitgangspunten van het management allereerst de vereiste brandwerendheid van constructiedelen moeten vaststellen. Is het uitgangspunt de bescherming van componenten tegen de directe gevolgen van brand, dan mag globaal worden uitgegaan van een minimale vereiste brandwerendheid van zestig minuten. Dit is gebaseerd op het bekende temperatuurverloop van een brand en het feit dat een brand veelal binnen zestig minuten is geblust. Indien de computerruimte gescheiden dient te worden van bijvoorbeeld een papiermagazijn (hoge vuurbelasting), dan gelden zoals eerder beschreven verzwarende eisen. Daarnaast speelt mogelijk de eis dat de temperatuur in een af te schermen ruimte niet boven de 60 graden Celcius mag stijgen (kritische temperatuur voor met name magnetiseerbare gegevensdragers).

Bij het beoordelen van de brandwerendheid van constructies dient onderscheid te worden gemaakt tussen wanden en vloeren.

Vloeren
Grofweg kan worden gesteld dat alleen vloeren uitgevoerd in beton of andere steenachtige materialen mogelijk een brandwerendheid van zestig

minuten bezitten. Voor vloerconstructies van andere materialen zullen zonder meer aanvullende voorzieningen dienen te worden getroffen. Het berekenen van de brandwerendheid van vloeren is zeer gecompliceerd. De EDP-auditor kan in het desbetreffende bouwbestek en bijbehorende programma van eisen nazoeken welke brandwerendheid de vloer in kwestie bezit. Zijn deze gegevens niet aanwezig, dan mag bij een in massief beton uitgevoerde vloer worden uitgegaan van een brandwerendheid van zestig minuten. Van andersoortige vloeren dient een testrapport te worden overhandigd.

Is de eis van het management dat de geautomatiseerde gegevensverwerking ook na een brand in een te onderzoeken ruimte moet kunnen worden voortgezet, dan gelden verzwarende eisen. Een ontwikkelde brand op de verdieping onder het rekencentrum zal, zonder het treffen van zeer zware thermisch isolerende voorzieningen, de constructie dusdanig aantasten dat geautomatiseerde gegevensverwerking op de bovengelegen verdieping niet meer mogelijk is.

Bij het ontwerpen van een gebouw kan namelijk wel met brand rekening zijn gehouden, maar een vloerconstructie in beton bijvoorbeeld wordt volgens de norm pas niet meer als brandwerend gezien als deze een doorbuiging vertoont van 1/30 van de overspanning. Bij een overspanning van zeven meter betekent dit reeds een doorbuiging van circa twintig centimeter. Al ver voor dit punt is de doorbuiging zodanig dat ten tijde van een brand de verwerking reeds gestaakt dient te worden.

Een oplossing in dit kader is het bekleden van de onderzijde van de vloer en de draagconstructie met thermisch isolerende materialen. Hoewel voor dit onderwerp nog geen normen zijn opgesteld, kan de thermische isolatie van een constructie proefondervindelijk (door het TNO) worden vastgesteld. In dit geval kan de EDP-auditor steunen op een testrapport. Simpelweg vertrouwen op alleen de aanwezigheid van bijvoorbeeld (de veel in parkeergarages toegepaste) houtwolcementplaten is niet voldoende. Dikte en aard van het materiaal en de wijze waarop het is aangebracht, spelen hierbij een belangrijke rol.

De brandwerendheid van ramen, deuren en luiken dient gelijk te zijn aan die van de omringende scheidingsconstructie.

Ook is het mogelijk de ruimte onder het rekencentrum van een sprinklerinstallatie te voorzien. In dit geval zal de aantasting van de vloer ten gevolge van brand gering zijn en kan worden vertrouwd op een goede brandwerendheid tijdens de brand en het blijvend vervullen van de dragende functie na de brand. Hierbij speelt ook nog dat er een vertrouwenswaardig keuringsinstituut voor sprinklerinstallaties bestaat, waarbij onder andere is voorzien in een halfjaarlijkse herkeuring van de installatie. De EDP-auditor dient in dit geval vast te stellen of een goedkeurend en recent certificaat aanwezig is.

Wanden

De wijze van bepalen van de vereiste en daadwerkelijke brandwerendheid van wanden en gevels is gelijk aan vloeren. Als vuistregel kan bij in beton of steen uitgevoerde wanden worden uitgegaan van een brandwerendheid van zestig minuten. Ten aanzien van de veelal toegepaste systeemwanden en geprefabriceerde geveldelen kan worden vertrouwd op TNO-testrapporten.

Hierbij dient nog aandacht te worden besteed aan deuren, ramen en luiken. Deze delen kunnen uiteraard ook weerstand bieden aan branddoorslag. De tijd dat de desbetreffende bouwdelen deze eigenschap bezitten moet weer worden ontleend aan door TNO uitgevoerde tests. Het spreekt voor zich dat de brandwerendheid van ramen, deuren en luiken gelijk dient te zijn aan die van de omringende scheidingsconstructie.

De brandwerendheid van raam-, deur- en luikconstructies houdt geen rekening met het weerstand kunnen bieden tegen het doorlaten van rookgassen. Indien deze eis aan een brandscheiding wordt gesteld, zullen aanvullende maatregelen nodig zijn. Te denken valt aan het in stand houden van een overdruk, die tijdens en na de brand dient te worden gehandhaafd!

In dit kader is een waarschuwing op zijn plaats. Een scheidingsconstructie (zijnde geen deur, raam of luik) die is getest op brandwerendheid kan ook, zij het in lichte mate, rookgassen doorlaten. Dit geldt overigens niet voor constructies uitgevoerd in beton of steen. Bij toepassing van andere materialen dient de EDP-auditor zich hiervan bewust te zijn.

Sparingen

Zowel in vloeren als in wanden zullen sparingen worden aangebracht ten behoeve van de doorvoer van water, lucht, elektra en data. Nadat leidingen en kabels zijn aangebracht, moeten deze sparingen dusdanig worden afgedicht dat de brandwerendheid gelijk is aan die van de omringende constructie. Het effect van een brandwerende scheiding gaat anders geheel verloren.

Voor de EDP-auditor is het echter een probleem de afdichting van een sparing op het aspect brandwerendheid te beoordelen. Er is een groot aantal TNO-geteste afdichtingssystemen op de markt die qua uiterlijk zeer verschillend zijn. Er zijn onder andere brandstopkussens, afdichtingspluggen, multi-doorvoerringen, bouwdoossystemen en brandmanchetten.

Wat betreft de goede werking van een afdichtingssysteem kan de EDP-auditor aan de leverancier het testrapport van TNO opvragen. Hierbij dient onder andere te worden beoordeeld of de afdichting

niet meer of dikkere doorgevoerde kabels en/of leidingen bevat dan aangegeven in het TNO-testrapport. Meer of dikkere kabels hebben namelijk een negatieve invloed op de brandwerendheid.

Certificaten

In dit artikel is meermalen opgemerkt dat een EDP-auditor in de praktijk kan worden geconfronteerd met certificaten of testrapporten die hem door de opdrachtgever worden voorgelegd. Mogelijk wil de EDP-auditor de desbetreffende documenten gebruiken ten behoeve van zijn werkzaamheden. Het kan zelfs zo zijn dat het certificaat het enige houvast is dat de EDP-auditor tot zijn beschikking heeft. In zo'n geval dient de EDP-auditor na te gaan door wie een certificaat c.q. verklaring is afgegeven, met betrekking tot welk object en met betrekking tot welke toepassing van het object.

Een sprinklerinstallatie dient, zoals reeds eerder opgemerkt, halfjaarlijks te worden gekeurd. In Nederland is een (beperkt) aantal bureaus bevoegd tot het uitvoeren van deze keuringen. Op basis van de door deze bureaus afgegeven certificaten kan de EDP-auditor een oordeel vormen over de kwaliteit van de sprinklerinstallatie.

Daarnaast zijn de testrapporten van TNO veelvuldig genoemd. Er wordt vaak gedacht dat TNO certificaten uitgeeft (bijvoorbeeld met betrekking tot de brandwerendheid). TNO geeft echter onderzoeksrapporten uit waarop de tijdens een beproeving gevonden gegevens staan vermeld. Deze onderzoeksrapporten ofwel testrapporten worden door TNO overhandigd aan de leverancier van het produkt, die dit desgewenst kan overleggen aan zijn cliënt, respectievelijk de EDP-auditor. De feitelijke bruikbaarheid van dit rapport voor de EDP-auditor hangt af van de situatie.

Indien een onderzoeksrapport betrekking heeft op de brandwerendheid van een scheidingsconstructie die als geheel (dus niet alleen de wand maar ook de stijlen die zorgen voor de stabiliteit van de wand) is getest, kan worden afgegaan op de in dit rapport vermelde gegevens. Is echter alleen het wandmateriaal getest en niet de combinatie met de constructie die in de stabiliteit van de wand voorziet, dan mogen de op het onderzoeksrapport vermelde gegevens niet als representatief worden aangemerkt. Hier is dus waakzaamheid geboden. TNO kan niet controleren voor welk doel de leverancier het onderzoeksrapport gebruikt.

Ook is reeds beschreven dat de EDP-auditor bij het beoordelen van sparingen op problemen stuit. Als het bedrijf dat de sparingen heeft gedicht, respectievelijk de opdrachtgever geen TNO-testrapport kan overhandigen, moet de afdichting als onvoldoende brandwerend worden aangemerkt. Indien wel een testrapport wordt overhandigd, rest voor de EDP-auditor de vraag of de constructie is aangebracht volgens de op het testrapport vermelde specificaties. Een testrapport betreft immers een bepaalde afdichtingsconstructie, die door de leverancier in de vorm van een proefstuk wordt afgeleverd bij TNO. De in het werk aangebrachte constructies worden niet afzonderlijk door TNO beoordeeld.

Een aantal zichtbare aspecten van een constructie waarvoor een testrapport is overhandigd, is echter wel te beoordelen. Dit geldt bijvoorbeeld in geval van een brandwerende systeemwand voor het aantal en de afmetingen van de stijlen per strekkende meter wand en, in geval van sparingen, voor het aantal kabels, de onderlinge afstand en de diameter daarvan.

Andere aspecten, zoals het al dan niet met zand gevuld zijn van aluminium stijlen (ter verhoging van de tijd gedurende welke een constructie bij brand haar stabiliteit bewaart) van de scheidingsconstructie of het materiaal waarmee de sparing wordt gevuld, zijn moeilijk of nagenoeg niet te beoordelen.

Bij het beoordelen van constructies aan de hand van certificaten dan wel onderzoeksrapporten dient daarnaast onderscheid te worden gemaakt tussen het beoordelen tijdens de bouwfase (dan is een en ander nog wel zichtbaar) en het beoordelen van een bestaande constructie (veel is dan weggewerkt, evenzo de mogelijke gebreken).
Overigens is het in de Nederlandse bouwsituatie zo dat, met name bij grotere bouwprojecten, continu een opzichter op het werk aanwezig is. Deze opzichter is in dienst van de architect (die opereert namens de opdrachtgever) en heeft dus belang bij een goede kwaliteit van het werk. Hij controleert met dit doel de aannemer die verantwoordelijk is voor de uitvoering van het werk. De opzichter mag worden beschouwd als algemeen, zij het niet onfeilbaar, deskundige. De EDP-auditor dient zich dan wel te realiseren dat het afdichten van een sparing ook ná het feitelijke bouwproces kan zijn gebeurd en hierdoor niet meer aan de beoordeling van een opzichter onderworpen is geweest.

Indien de EDP-auditor tijdens zijn werk wil of moet steunen op informatie van certificaten, onderhoudsverklaringen en onderzoeksrapporten, zal hij eerst moeten nagaan in hoeverre dit gerechtvaardigd is.

Voorts dient de EDP-auditor erop verdacht te zijn dat de kreet "erkende bedrijven" niet alles en soms nagenoeg niets zegt. Instituten als TNO en dergelijke houden zich niet bezig met het "erkennen" van bedrijven. In het gunstigste geval houdt "erkend" in dat de desbetreffende installateur/leverancier is aangesloten bij een vakorganisatie. Hoewel zo'n vakorganisatie erbij gebaat is alleen leden in te schrijven die werk leveren van goede kwaliteit, mag dit niet als waarborg voor de kwaliteit van de te beoordelen constructie worden aangemerkt.

Samengevat kan worden gesteld dat, indien de EDP-auditor tijdens zijn werk wil of moet steunen op informatie van certificaten, onderhoudsverklaringen en onderzoeksrapporten, hij eerst zal moeten nagaan in hoeverre dit gerechtvaardigd is. Hij zal dit voor een belangrijk deel doen op basis van "professional judgement".

Agressieve rookgassen

In de literatuur wordt menigmaal het gevaar van agressieve rookgassen als gevolg van brand beschreven. Deze agressieve rookgassen ontstaan, zoals reeds vermeld, als gevolg van verbranding van PVC en vele andere kunststoffen. Deze rookgassen (bijvoorbeeld chloriden) reageren met water uit de lucht tot zoutzuur en slaan vervolgens neer op de computerapparatuur alwaar een corrosieproces op gang komt.

De hoeveelheden zoutzuur die als gevolg van de verbranding van PVC kunnen ontstaan, zijn aanzienlijk. In dit kader is het van belang, welke condities er direct na de brand in de desbetreffende ruimte(n) heersen. Ventilatie van de ruimte kan het overgrote deel van vervuiling door rook en beschadiging door agressieve rookgassen voorkomen omdat de agressieve stoffen nog nagenoeg niet zijn neergeslagen. Een organisatie die in dit kader afhankelijk is van de gemeentebrandweer zal wat dit betreft niet op ondersteuning hoeven te rekenen. Hoewel de tendens enigszins verandert, is de gemeentebrandweer er immers voor het redden van personen en het blussen van de brand. Wanneer een organisatie over een eigen bedrijfsbrandweer beschikt kan deze brandweer een belangrijke rol vervullen in de te verrichten handelingen direct na de brand. De EDP-auditor kan dit bij zijn beoordeling betrekken.

Gezien het eigenbelang moet het meetresultaat van salvage-bedrijven kritisch worden beschouwd.

Afgezien van het ventileren van de ruimte kan het gevaar voor agressieve rookgassen eveneens sterk worden verminderd door het omlaag brengen van de hoeveelheid vocht in de lucht. Het verwarmen van de ruimte en het daardoor omlaag brengen van de RV heeft geen zin: er blijft absoluut gezien een zelfde hoeveelheid water in de lucht, waarmee bijvoorbeeld de chloriden zullen reageren.

Verzekeringsmaatschappijen schakelen salvagebedrijven in voor het schoonmaken van door brand vervuilde apparatuur en inrichting (meubilair, enz.). Hiertoe verrichten deze bedrijven namens de verzekeraars zelf eerst metingen teneinde de omvang van de vervuiling (en dus de schade) vast te stellen. Deze metingen worden dus niet onafhankelijk verricht: de salvage-bedrijven hebben namelijk belang bij een zo groot mogelijke vervuiling. Uit metingen (met gelijkwaardige en geijkte apparatuur) die zijn verricht door een door brand gedupeerd bedrijf, bleek dat de vervuiling van apparatuur door rook en agressieve rookgassen nogal meeviel vergeleken met de door het salvagebedrijf opgegeven vervuilingsgraad. Hoewel dit uiteraard geen uitgebreide test is geweest, moet het meetresultaat van de salvage-bedrijven, zeker gezien hun eigen belang, kritisch worden beschouwd. In ieder geval is het zeer goed mogelijk dat deze vorm van vervuiling c.q. beschadiging van apparatuur in de praktijk aanzienlijk minder is dan tot nu toe wordt aangenomen.

Overdruk in de computerruimte

Teneinde het gevaar van vervuiling door rook in geval van brand buiten het computercentrum te vermijden is het wenselijk in de computerruimte een overdruk te realiseren (grofweg 30 Pa). Deze overdruk moet dan continu gewaarborgd zijn. Op deze wijze zal rook van buitenaf nooit binnendringen in het computercentrum en derhalve ook geen schade aanrichten aan apparatuur en dergelijke. Bij het optreden van brand in het rekencentrum heeft overdruk geen zin omdat de rook dan toch al in de ruimte zelf is. In dit kader is het snel afzuigen van rook in de ruimte direct na de brand al genoemd.

De beoordeling van de overdrukmaatregel komt neer op de beoordeling van het totaal aan maatregelen, hetgeen niet eenvoudig is. De ongestoorde werking van de apparatuur die de overdruk moet realiseren, dient te worden beoordeeld. Daarnaast dient zekerheid te bestaan over de juiste plaatsing en werking van bijvoorbeeld terugslagkleppen en zelfsluitende kleppen in kanalen. Met name dit laatste is nagenoeg niet te beoordelen. Zoals reeds beschreven zal dan vertrouwd moeten worden op de installateur en de controle door de opzichter tijdens de bouwfase.

Gasblussing

Voor de effectieve werking van de gasblusinstallatie dienen onder de verhoogde vloer en boven het verlaagde plafond eveneens gaslozingspunten te worden aangebracht. Bij lozing alleen in de computerruimte zal er onvoldoende gas op deze plaatsen komen, zodat een brand die op deze plaats ontstaat niet tijdig zal worden gedoofd.

Ook dient rekening te worden gehouden met de enorme kracht waarmee het gas vrijkomt. Dit kan tot gevolg hebben dat objecten zoals vloer- en plafondplaten met grote kracht door de ruimte worden geslingerd. Het veelal op plafondplaten aanwezige stof kan een enorme vervuiling veroorzaken.

Wat de dimensionering van de installatie betreft zal de berekening van de installateur moeten worden beoordeeld. Een specifiek aandachtspunt hierbij is dat na een verbouwing van het rekencentrum de gasblusinstallatie mogelijkerwijs dient te worden aangepast teneinde te kunnen blijven voldoen aan het noodzakelijke vol-%.

Reconditionering van tapes na brand

Globaal kan worden gesteld dat magnetiseerbare media niet mogen worden verhit boven de 60 graden Celcius of worden bewaard in een ruimte met een RV van meer dan 85 procent. Er is een voldoende aanbod van datakluizen en in te bouwen kluisdeuren die aan deze eisen voldoen.

Het is echter niet zo dat een tape die onder deze grenzen is bewaard direct bruikbaar is. Eerst dient dit medium te worden gereconditioneerd. Hiervoor kan tot 24 uur benodigd zijn. Afhankelijk van de management-uitgangspunten (maximale uitvaltijd) kunnen derhalve verzwarende eisen met betrekking tot de brandwerendheid gewenst zijn. Algemeen kan worden gesteld dat kluizen die de VDMA-test hebben doorstaan, aan deze verzwarende criteria voldoen en dat in die gevallen reconditionering niet of nauwelijks nodig is.

SAMENVATTING EN CONCLUSIE

In dit artikel is beschreven wat brand is, wat de mogelijke gevolgen zijn en welke maatregelen kunnen worden genomen om de kans op en de gevolgen van brand te verkleinen respectievelijk te beperken. Wij hebben ons hierbij gericht op brand in en rond het rekencentrum.

Het spreekt voor zich dat te nemen maatregelen moeten worden afgezet tegen het mogelijke nut hiervan. Voorafgaand aan de keuze van preventieve en repressieve maatregelen dient op basis van bijvoorbeeld een risico-analyse een aantal uitgangspunten te worden geformuleerd.

De belangrijkste uitgangspunten voor de EDP-auditor zijn hierbij de maximaal te accepteren uitvaltijd, de keuze voor de te beschermen objecten en ten slotte of de geautomatiseerde gegevensverwerking in het desbetreffende computercentrum na een brand moet kunnen worden voortgezet.
We hebben gezien dat op basis van deze uitgangspunten maatregelen kunnen worden gekozen. Op het gebied van de technische maatregelen zijn de belangrijkste hiervan het brandwerend afschermen van ruimten (compartimentering), het toepassen van onbrandbare materialen en materialen met een lage rookontwikkeling en het installeren van signalerings- en blussystemen.

De keuze voor brandwerend af te schermen ruimten hangt hierbij af van de plaats van objecten die gezien worden als onvervangbaar of niet tijdig vervangbaar. In het algemeen zullen het rekencentrum (zaal) en de datakluis van elkaar en van de buitenwereld brandwerend worden afgeschermd. Het beoordelen of deze keuze terecht is kan door een EDP-auditor geschieden op basis van management-keuzen, kennis van leveringscondities, etc. De beoordeling of de getroffen maatregelen in dit kader adequaat zijn is gecompliceerder. Veelal moet worden gesteund op testrapporten van het TNO. Hierbij is een juiste interpretatie van de testresultaten en condities zeer belangrijk.

Is het bovenstaande met enige inspanning nog uitvoerbaar, het beoordelen of constructies volgens gelijke omstandigheden zijn aangebracht als waaronder ze door TNO zijn getest, is nagenoeg niet mogelijk. Vertrouwd moet worden op de goede naam en faam van de desbetreffende installateur, hetgeen geen objectieve basis is voor oordeelsvorming op dit gebied.

Ook is gebleken dat de EDP-auditor bij de beoordeling van blussystemen op problemen kan stuiten. Kan met betrekking tot een sprinklerinstallatie nog worden gesteund op een vertrouwenswaardig certificerend instituut en erkende installateurs, bij gasblussystemen is geen dergelijke constructie van instanties voorhanden. Daarnaast is de werking van gasblussystemen gebaseerd op het aanwezig zijn en gedurende enige tijd blijven van een aantal vol-% gas. Het beoordelen of in een ruimte geen gaslekken aanwezig zijn is echter schier onmogelijk.

De laatstgenoemde maatregel in dit kader is de materiaalkeuze. De voorkeur gaat hierbij uit naar onbrandbare materialen met een lage rookontwikkeling (in verband met de afscheiding van agressieve gassen). Dit blijkt echter, nog afgezien van de computers en datacommunicatieverbindingen waarin veel PVC is verwerkt, niet mogelijk. Er zijn onvoldoende materialen aanwezig die aan deze eisen voldoen. De EDP-auditor kan globaal beoordelen of concentraties brandbare materialen niet te hoog zijn.

Concluderend kan worden gesteld dat het beoordelen van preventieve en repressieve technische maatregelen in het kader van brand in en rond computercentra veelal specialistische kennis vereist welke doorgaans niet van een EDP-auditor kan worden verwacht. Toch kan, mede op basis van dit artikel, tot op zekere hoogte een uitspraak worden gedaan. Ten eerste kan de EDP-auditor het management wijzen op mogelijke zwakke schakels in de brandbeveiliging. Hoe groot de inspanningen op het gebied van brandpreventie namelijk ook zijn, bij een grote afhankelijkheid van de geautomatiseerde gegevensverwerking zal een uitwijkregeling noodzakelijk zijn.

Daarnaast kan de EDP-auditor in algemene zin een uitspraak doen over de getroffen maatregelen en adviserend optreden. Dit laatste bijvoorbeeld door het management te attenderen op mogelijke risico's en hieraangaande te verwijzen naar specialisten als TNO, adviesbureaus en niet in de laatste plaats de brandweer. Deze blijkt de laatste jaren namelijk, naast de bescherming van personen, in toenemende mate de bescherming van waarden als aandachtsgebied te hebben. Zeker in grotere steden hebben gemeentelijke brandweerkorpsen hiertoe voorlichtingsafdelingen in het leven geroepen.

Ing. J.F. Kuperus
Is werkzaam als EDP-auditor bij de Accountantsdienst, afdeling EDP Audit van de Rabobank Nederland. Hij heeft na de AMBI-opleiding de post-doctorale studie EDP-auditing voltooid aan de Erasmus Universiteit te Rotterdam. Zijn audit-ervaring ligt op het terrein van besturingssystemen, automatiseringsorganisaties en informatiesystemen.
Aansluitend op zijn bouwkundige opleiding heeft hij zich toegelegd op bouwkundige aspecten met betrekking tot de continuïteit van de geautomatiseerde gegevensverwerking en informatieverstrekking.

Ing. G.H.M. Meijer
Is sinds 1985 werkzaam bij KPMG Klynveld EDP Auditors. Na de AMBI-opleiding heeft hij de post-doctorale studie EDP-auditing aan de Erasmus Universiteit Rotterdam voltooid.
In de afgelopen jaren heeft hij zich beziggehouden met opdrachten uit de algemene EDP-audit-praktijk, alsmede opdrachten met de specifieke aandachtsgebieden besturingssystemen en beveiligingspakketten.
Door een vroeger genoten opleiding HTS-Bouwkunde te combineren met zijn auditervaring heeft hij zich tevens toegelegd op bouwtechnische maatregelen in het kader van de continuïteit van de geautomatiseerde gegevensverwerking.

LITERATUUR

Normen

NEN 3850 Technische grondslagen voor de berekening van bouwconstructies TGB 1972 (maart 1974).

NEN 3881 Bepaling van de onbrandbaarheid van bouwmaterialen (december 1975).

NEN 3883 Bepaling van de bijdrage tot de brandvoortplanting van bouwmaterialen en hun rookontwikkeling bij brand (december 1975).

NEN 3884 Bepaling van de brandwerendheid van bouwdelen (februari 1978).

Aanv. NEN 3884 Aanvulling op NEN 3884 Bepaling van de brandwerendheid van bouwdelen (oktober 1983).

NEN 3885 Bepaling van de brandwerendheid van deur-, luik- en raamconstructies van gebouwen (januari 1982).

NEN 3891 Richtlijnen brandbeveiliging van gebouwen Deel 1, Algemeen gedeelte (december 1971).

NPR 3900 Brandbeveiliging van gebouwen - computerafdelingen (november 1976).

Ontwerp-normen

Ontwerp NEN 1775 Bepaling van de bijdrage tot brandvoortplanting van vloeren (juli 1990).

Ontwerp NEN 6062 Bepaling van de brandveiligheid van rookafvoervoorzieningen (juli 1990).

Ontwerp NEN 6066 Bepaling van de rookproduktie bij brand van een bouwmateriaal (combinatie) (juli 1990).

Ontwerp NEN 6068 Bepaling van de weerstand tegen branddoorslag en brandoverslag tussen ruimten (juli 1990).

Ontwerp NEN 6069 Experimentele bepaling van de brandwerendheid van bouwdelen (juli 1990).

Ontwerp NEN 6071 Rekenkundige bepaling van de brandwerendheid van bouwdelen - Betonconstructies (juli 1990).

Ontwerp NEN 6075 Bepaling van de weerstand tegen rookdoorgang tussen ruimten (juli 1990).

Ontwerp NEN 6076 Experimentele bepaling van de brandwerendheid van ventilatiekanalen zonder brandkleppen (juli 1990).

Ontwerp NEN 6077 Experimentele bepaling van de brandwerendheid van ventilatiekanalen voorzien van brandkleppen (juli 1990).

Ontwerp NEN 6084 Brandveiligheid van gebouwen - kantoorgebouwen - Prestatie-eisen (juli 1990).

Ontwerp NEN 6090 Bepaling van de vuurbelasting (juli 1990).

Netconditionering

R. van de Wouw

Een computer of andere apparatuur werkend met elektronische intelligentie is uiterst gevoelig voor storingen in de elektriciteitsvoorziening.
In dit artikel worden oorzaken, gevolgen en te nemen (preventieve) maatregelen, het "hoe en waarom", op een heldere wijze gepresenteerd.

INLEIDING

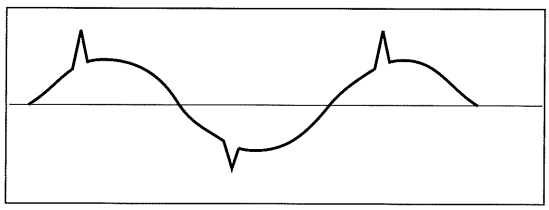
Bijna iedere computergebruiker kent wel het verschijnsel dat de computer ineens "hangt" of een onverklaarbare foutmelding geeft.
In verreweg de meeste gevallen worden netstoringen niet (h)erkend als de oorzaak van de computerstoring, maar wordt de schuld van de storing gegeven aan slechte hardware, een "bug" in het programma of een bedieningsfout. Als een dergelijke storing slechts incidenteel voorkomt en er na het herstarten van de computer niet al te veel problemen optreden, dan wordt er meestal tamelijk achteloos aan voorbijgegaan, maar als zij wel regelmatig voorkomt en bovendien beschadigde bestanden oplevert, dan wordt het wel wat anders.
Met het steeds groter en complexer worden van de besturingssystemen wordt er steeds meer werkgeheugen geëist terwijl ook de benodigde schijfcapaciteit snel toeneemt. Als gevolg daarvan wordt er steeds meer gewerkt met diskcaching en virtueel geheugen, waardoor de gevolgen van (net)storingen steeds desastreuzer worden, omdat na het herstarten niet meer precies bekend is wat de inhoud was van het cache en/of virtueel geheugen onmiddellijk voor de calamiteit.
Ook het hebben van een backup om bij incidentele storingen op terug te vallen is in lang niet alle gevallen een afdoende oplossing om de schade te beperken. Op Schiphol bijvoorbeeld, waar statistisch is gebleken dat ieder jaar het net gemiddeld drie keer uitvalt, zit een middelgrote luchtvaartmaatschappij die heeft ontdekt dat als haar computersysteem uitvalt dit weliswaar opnieuw kan worden opgestart, maar dat het bijna 24 uur duurt voordat weer precies de situatie van voor de storing is hersteld. (Als gevolg van enkele Gigabytes aan virtueel geheugen die worden gebruikt, is reconstructie erg moeilijk.) Al die tijd kunnen geen boekingen of andere gegevens worden ingevoerd!
Ook een normale administratieve computer die "plat gaat" levert in de meeste bedrijven heel wat problemen en tijdverlies op. En over de gevaren en kosten bij een industriële computer die een kritisch of gevaarlijk produktieproces bestuurt, zullen we het hier verder maar niet hebben.

ONDERSCHEID TUSSEN DE DIVERSE SOORTEN NETSTORINGEN

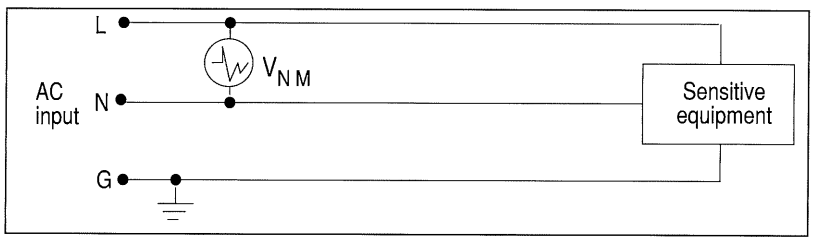
Dat storingen in het net in het algemeen, en bij computers in het bijzonder, problemen veroorzaken is wel bekend. Dat totale netuitval, waar de meeste mensen dan in eerste instantie aan denken, de minst voorkomende bron van computerstoringen als gevolg van netproblemen vormt, is echter slechts bij weinigen bekend. Een onderzoek dat enige jaren geleden door IBM in de Verenigde Staten is uitgevoerd, toonde aan dat de oorzaken van alle *door het lichtnet* veroorzaakte computerstoringen grofweg in drie groepen konden worden ingedeeld:
- spikes en/of ruis;
- spanningsfluctuaties;
- netuitval.

Spikes en/of ruis

Circa 85 procent van alle storingen wordt veroorzaakt door zeer kortdurende pieken (spikes) of ruis (noise) op het net terwijl de spanning zelf vrijwel constant blijft. Zie figuur 1.
Hoewel de situatie in Nederland in verhouding vrijwel zeker minder spikes en noise te zien geeft, omdat hier minder afgelegen gebieden zijn en hier ook nauwelijks nog met bovengrondse laagspanningsleidingen wordt gewerkt, komt deze oorzaak hier wel degelijk regelmatig voor.

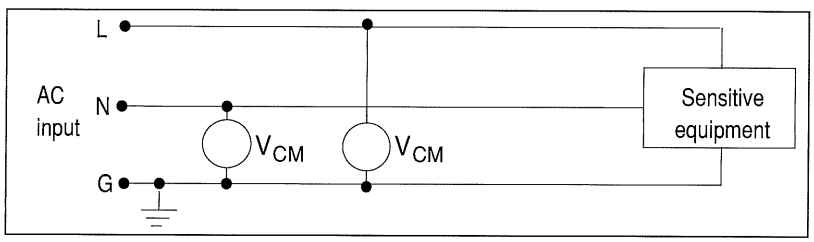


Figuur 1. Spikes.



Figuur 2. Normal-Mode-noise.

L = Line; spanningsvoerende leiding of "fase"
N = Neutral; niet-spanningsvoerende leiding
G = Aardleiding.



Figuur 3. Common-Mode-noise.

Deze storingen zijn nog onder te verdelen in twee belangrijke categorieën, namelijk:

- *Normal-Mode-storingen* (ook wel Transverse-Mode-storingen genoemd): dit zijn storingen die optreden tussen *een fase en de nul van het net.* Zolang de amplitude van de storing niet te groot is en de tijdsduur niet te lang, hebben de meeste computers hier niet zoveel last van omdat een goede voeding dit voor een groot deel zelf opvangt. Zie figuur 2.

- *Common-Mode-storingen:* dit zijn storingen die optreden tussen *zowel de fase als de nul en de (rand)aarde van het net.* Hiervoor zijn vooral computervoedingen erg gevoelig omdat ze zelf weinig doen aan de onderdrukking ervan. Zie figuur 3.

Spanningsfluctuaties (sags en/of surges)

Circa twaalf procent van alle storingen wordt veroorzaakt door langer durende spanningsfluctuaties; meestal zijn dit sags (te lage spanning) maar soms ook surges (te hoge spanning).

Netuitval

De overige drie procent van alle storingen wordt veroorzaakt door een volledige netuitval.
Uit recente (1988) onderzoeken van de Vereniging van Exploitanten van Elektriciteitsbedrijven in Nederland (VEEN) komt naar voren dat jaarlijks 17,5 procent van alle elektriciteitsgebruikers met een totale spanningsuitval wordt geconfronteerd die bovendien voornamelijk tijdens de normale werkuren optreedt! Dit levert uiteraard altijd een computerstoring op.
Hoewel over de verhouding van de diverse storingen in Nederland geen kwantitatieve cijfers beschikbaar zijn, blijkt uit het IBM-onderzoek duidelijk dat er een groter aantal computerstoringen wordt veroorzaakt door spikes, noise, sags of surges dan door netuitval, waarmee volgens het VEEN-onderzoek al één op de zes Nederlanders jaarlijks wordt geconfronteerd. Duidelijk is in ieder geval dat netconditionering in een groot aantal gevallen noodzakelijk is.

OORZAKEN VAN DE DIVERSE STORINGEN

Er zijn verschillende oorzaken van de diverse storingen:

Spikes en/of ruis

Deze worden voornamelijk veroorzaakt door het in- of uitschakelen van inductieve belastingen, zo-

als motoren, TL-buizen, lastransformatoren, kopieermachines, koelcompressors en dergelijke. Vooral als deze belastingen ook nog met zogenaamde fase-aansnijding ("Triac's") worden geregeld, vormen ze een bron van vooral Common-Mode-problemen.

Spanningsfluctuaties

Deze ontstaan bij het in- of uitschakelen van zware belastingen op een zwak net. Op afgelegen of oude industrieterreinen waar veel is uitgebreid, komt dit nogal eens voor, maar ook in oude stadskernen met een verouderd leidingnet (in sommige steden zijn nog straten met oude 127 Volt-netten; tussen twee fases heb je dan 220 Volt). In veel gevallen is er dan ook sprake van spikes.

Netuitval

Voornamelijk als gevolg van kortsluiting in het laagspanningsnet bij de gebruiker zelf en als gevolg van graafwerkzaamheden waarbij laagspannings- of 10 kV-kabels worden stukgetrokken.

Omdat het opsporen van de oorzaak meestal alleen maar mogelijk is door met tamelijk geavanceerde analysers aan het lichtnet te meten, is dit kostentechnisch alleen bij wat grotere vermogens (circa 3 kVA en groter) interessant. Voor kleinere vermogens geldt meestal dat een goede UPS die vrijwel ieder probleem oplost (hierop wordt nader ingegaan) niet zo duur is, zodat de kosten van een goede analyse niet opwegen tegen de besparing die - misschien - optreedt als zou blijken dat met een eenvoudige UPS als oplossing kan worden volstaan.

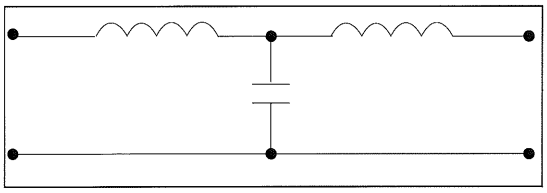
OPLOSSINGEN

Volgens de "Wet van Behoud van Ellende" geldt ook hier natuurlijk weer dat de beste oplossing (een UPS of No-Break, waarover later meer) ook altijd de duurste is. Om toch zoveel mogelijk storingen te voorkomen tegen een acceptabele prijs, is het nodig per geval te bekijken wat precies de oorzaak van de netstoringen is, zodat een op die storing toegesneden oplossing kan worden toegepast. In een aantal gevallen zal ook een andere, en meestal goedkopere, oplossing te gebruiken zijn.

Een eerste stap is het aansluiten van alle kritische apparaten op één of meer aparte groepen, waardoor een kortsluiting in een defect koffiezetapparaat of iets dergelijks in ieder geval de computer niet zonder spanning zet. Het is overigens een wijdverbreid misverstand dat hierdoor een "schone groep" zou ontstaan die tevens tegen spikes, noise en fluctuaties beschermt! Als gevoelige computerapparatuur dicht bij een storend apparaat op dezelfde groep (dus fase) is aangesloten, dan kan het aansluiten op een andere "schonere" fase natuurlijk wel verschil maken en ook geeft de grotere kabellengte tussen de "stoorbron" en de te beveiligen apparatuur wat demping tegen spikes en noise. Een afdoende onderdrukking van de storingen is dit echter maar zelden.
In de handel wordt een groot aantal oplossingen aangeboden die claimen de definitieve oplossing te bieden voor netstoringen. Aan de meeste van die aanbiedingen zitten toch wel wat haken en ogen. In vogelvlucht worden de diverse categorieën hieronder behandeld met de voornaamste eigenschappen, voor- en nadelen.

RFI-filters

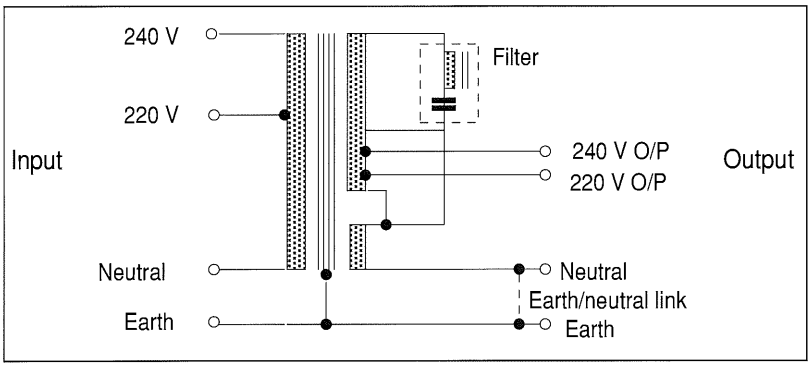
Dit zijn meestal vrij goedkope LC-filters die vaak voorkomen in de net-entree van een voeding of in een verdeeldoos. Helaas doen ze voor een computer niet zoveel behalve het tegenhouden van radiostoringen. Als netconditionering voor computers zijn zij eigenlijk waardeloos.



Figuur 4. Eenvoudig RFI-filter.

Ferro-resonant transformatoren

Een beproefd principe transformator dat al vele jaren wordt toegepast. Het betreft een transformator die bewust in verzadiging wordt gestuurd, met aan de secundaire kant een resonantiekring die ervoor zorgt dat de uitgangsspanning redelijk constant en sinusvormig blijft.
Hoewel hij veel wordt aangeboden, zitten er wel enkele vervelende nadelen aan.



Figuur 5. Ferro-resonant transformator.

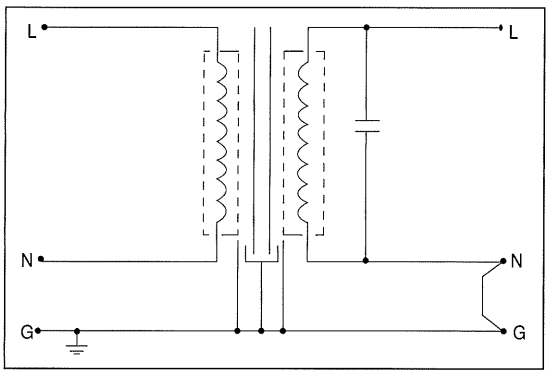
Nadelen:
- zwaar;
- slecht rendement (veel warmte-ontwikkeling);
- *moet* nominaal worden belast voor een goede werking;
- hoge uitgangsimpedantie en daardoor slechte dynamische stabiliteit, bij plotselinge belastingvariaties varieert de uitgangsspanning;

- slechte overbelastbaarheid, probleem bij opstarten;
- trage spanningsstabilisatie;
- sterk magnetisch veld, wat bij monitoren een duidelijk zichtbaar probleem oplevert;
- geeft nogal wat 50 Hz-brom;
- slechte Common-Mode-onderdrukking;
- enigszins vervormde uitgangsspanning (harmonische vervorming).

Voordelen:
- relatief goedkoop;
- betrouwbaar (weinig componenten);
- geeft redelijke spanningsstabilisatie;
- vangt ook diepe sags op als ze niet te lang duren;
- behoorlijke Normal-Mode-onderdrukking.

Ultra-Isolatoren

Een uitvinding die is gebaseerd op het principe dat Common-Mode-storingen kunnen worden onderdrukt in een transformator met een minimale capacitieve koppeling tussen de primaire en secundaire wikkelingen. In een Ultra-Isolator liggen de wikkelingen niet over elkaar, maar op aparte delen van het transformatorblik. Door het toepassen van "kooien van Faraday" om de twee wikkelingen en het plaatsen van een extra scherm ertussen, kan de capaciteit tussen de primaire en secundaire wikkelingen worden teruggebracht tot 0,005 pF! Als gevolg hiervan bedraagt de Common-Mode-onderdrukking liefst 146 dB of wel 20.000.000 : 1.



Figuur 6. Ultra-Isolator.

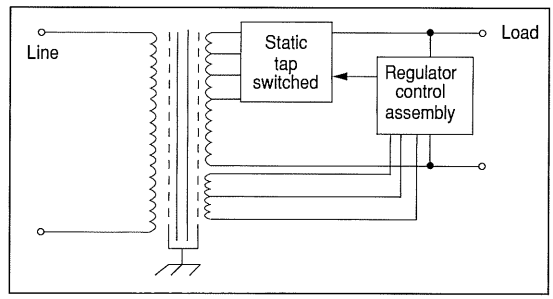
Nadelen:
- geen enkele spanningsstabilisatie;
- matige Normal-Mode-onderdrukking (die is gelukkig toch niet zo belangrijk omdat de computervoeding die grotendeels onderdrukt).

Voordelen:
- uitstekende, door niets geëvenaarde, Common-Mode-onderdrukking;
- zeer lage uitgangsimpedantie, waardoor belastingvariaties achter de trafo geen fluctuaties introduceren;
- zeer goede overbelastbaarheid;
- hoog rendement (>95%);
- betrouwbaar, kan écht niet stuk (mits afgezekerd);
- lage harmonische vervorming (<1%).

Power Conditioners

Power Conditioners zijn meestal gebaseerd op het principe van een Ultra-Isolator, maar beschikken daarnaast nog over een elektronisch geregelde voorziening om ook de spanning te kunnen regelen. Als gevolg van deze opzet beschermen ze zowel tegen spikes en noise als tegen spanningsfluctuaties en bieden dus eigenlijk een volledige bescherming tegen netvervuiling. De meeste Power Conditioners berusten op één van de twee volgende principes: Tapswitching of Transductor.

Tapswitching Power Conditioner
De Tapswitching Power Conditioner is in feite een normale Ultra-Isolator maar dan met meer secundaire aftakkingen. Met behulp van een microprocessor wordt aan de uitgang de spanning gemeten en naar behoefte wordt dan met behulp van Triac's op een stroomnuldoorgang naar de juiste aftakking van de trafo geschakeld ("tapswitching") om zo de gewenste uitgangsspanning te krijgen. Door de trafo-aftakkingen niet te ver uit elkaar te leggen kan de spanning zeer snel tussen acceptabele grenzen worden geregeld.



Figuur 7. Tapswitching Power Conditioner.

Nadelen:
- matige Normal-Mode-onderdrukking (gelukkig niet zo belangrijk);
- uitgangsspanning is niet echt constant, maar maakt kleine sprongetjes waardoor dit principe voor sommige toepassingen niet geschikt is (bijvoorbeeld bij gevoelige analoge meetopstellingen).

Voordelen:
- naast alle voordelen van de Ultra-Isolator komt hier nog bij dat de Tapswitching Power Conditioner een bijzonder snelle spanningsregeling heeft;
- groot ingangsbereik.

Transductor Power Conditioner
Ook bij de Transductor Power Conditioner wordt een Ultra-Isolator gebruikt voor de Common-Mode-onderdrukking, alleen wordt nu secundair de spanning geregeld met een Transductor-regeling in plaats van met een Triac-schakeling. Afhankelijk van de uitgangsspanning wordt met gelijkstroom een hulpwikkeling in verzadiging gestuurd waarmee de overbrengingsverhouding van de transformator traploos kan worden geregeld, wat in sommige applicaties noodzakelijk kan zijn.

Helaas gaat dit wel ten koste van de snelheid van de regeling. Het regelen van de verzadiging gaat niet zo snel, zodat de uitgangsspanning bij snelle belastingvariaties ook iets varieert. Bovendien is de harmonische vervorming wat hoger dan bij de Tapswitching Power Conditioners.

Nadelen:
- uitgangsspanning is niet echt constant bij een variërende belasting doordat de regeling relatief traag is;
- vrij groot en zwaar.

Voordelen:
- naast alle voordelen van de Ultra-Isolator komt hier nog bij dat de Transductor Power Conditioner een continu geregelde uitgangsspanning levert waardoor, mits de belasting redelijk constant is, een zeer stabiele spanning ontstaat;
- groot ingangsbereik.

Uninterruptible Power Systems

Uninterruptible Power Systems (UPS) of "ononderbroken noodstroomsystemen" zijn er in een groot aantal verschillende uitvoeringen. Het basisprincipe is echter voor allemaal hetzelfde en eigenlijk heel eenvoudig; het binnenkomende lichtnet gaat naar een "acculader" waaraan naast de accu's ook een inverter (omvormer) is gekoppeld die van de accuspanning weer 220 Volt maakt. Valt nu het lichtnet uit, dan gaat de inverter door op de accu's zodat de computer gewoon doorwerkt. Vaak zit er bij dit soort systemen nog een by-pass om de hele unit heen, zodat er ook rechtstreeks op het lichtnet kan worden gewerkt. Dit is van belang bij onderhoud (stofvrij maken, accu's of ventilator verwisselen of een defect repareren). Bij de duurdere systemen schakelt deze by-pass automatisch om naar het lichtnet als er storingen optreden in het systeem. Het is bij zo'n by-pass dan wel noodzakelijk dat de uitgang van de inverter gesynchroniseerd is met het lichtnet, omdat er anders direct een grote "dreun" volgt bij het schakelen.
Voor de inverter kan worden gekozen uit verschillende principes, bijvoorbeeld:

- De blokgolf inverter met blokvormige uitgangsspanning (eenvoudige en zeer goedkope transistorschakeling); in de kleine units tot 1 kVA die op de PC-markt worden aangeboden, komt dit principe vrij veel voor. De uitgangsspanning levert voor de PC meestal niet zoveel problemen op, maar de monitor en eventuele printer kunnen er vaak slecht tegen.

- De blokgolf inverter met een Ferro-resonant transformator om er een acceptabele sinus van te maken. Bij redelijk constante vermogens voldoet deze goed.

- De Puls Width Modulation (PWM) inverters; pulsbreedte modulatie-inverters worden tegenwoordig in veel moderne systemen gebruikt.

Elk principe inverter heeft zo zijn voor- en nadelen, maar de PWM-systemen worden algemeen wel als de beste beschouwd. Voor de meeste computertoepassingen voldoet een blokgolf inverter met Ferro-resonant transformator echter ook prima.

Een ander belangrijk punt is natuurlijk de "back-up-tijd"; deze moet lang genoeg zijn om de computer op een nette manier uit te schakelen of om de tijd te overbruggen die nodig is om een noodstroomgenerator op te starten. Deze "backup-tijd" hangt af van de capaciteit van de accu's en van de belasting van de UPS. Meestal ligt deze tijd tussen de vijf en twintig minuten bij honderd procent belasting *(bij nieuwe accu's, na een jaar of drie is dit misschien nog maar de helft. De accu's moeten dus wel op tijd worden vervangen!).*

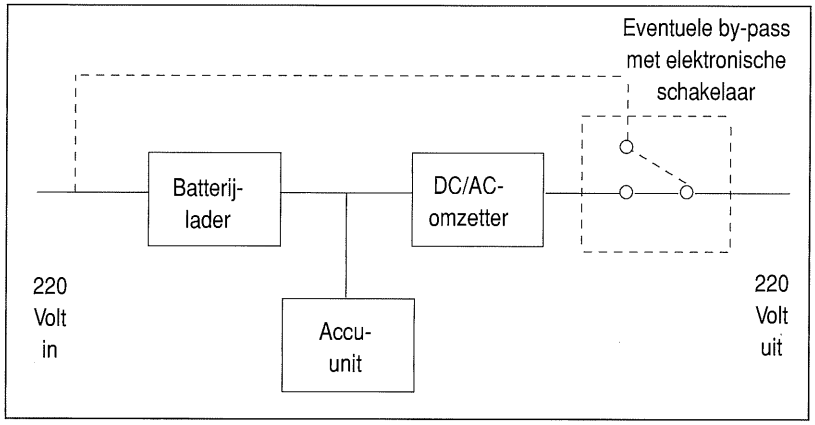
Verder is nog van belang of er een automatisch signaal van de UPS naar de computer gaat om te melden dat er op de accu's wordt overgeschakeld en dat er dus nog maar een paar minuten kan worden gewerkt. Bij de meeste mini- en mainframe-computers en bij lokale PC-netwerken zoals die van Novell, kan het uitschakelen dan automatisch op een nette manier gebeuren zonder tussenkomst van een operator. Als dit niet gebeurt moet er in ieder geval een duidelijk alarm worden gegeven zodat iemand handmatig de verwerking kan beëindigen voordat de accu's leegraken. Dit handmatig uitschakelen kan natuurlijk niet als er niemand aanwezig is, bijvoorbeeld 's avonds als het systeem aanblijft om een automatische tape-backup te maken of als de systeembeheerder die de computer moet uitschakelen niet in de buurt is.

Vooral bij kleinere computersystemen levert een UPS meestal de beste prijs/prestatie-verhouding.

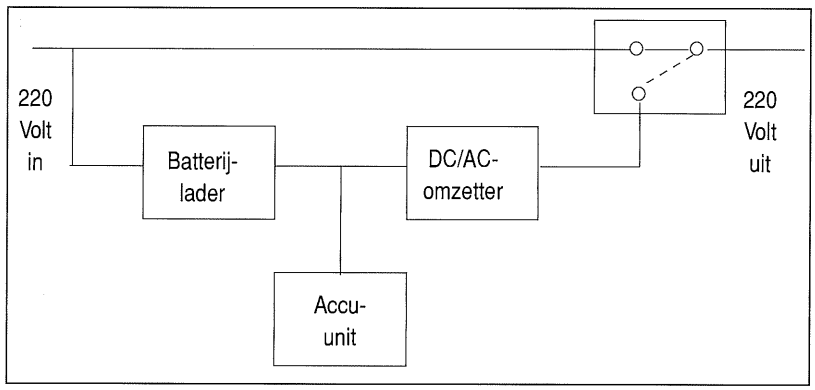
Een laatste punt om op te letten bij de keuze van een UPS is het rendement. Als er een UPS met een laag rendement wordt toegepast, geeft dit natuurlijk al een hogere energierekening. Indien de unit in een airconditioned (computer)ruimte wordt geplaatst, neemt het verbruik nog verder toe. Als bijvoorbeeld een 3 kVA UPS een rendement van tachtig procent heeft, moet er ongeveer 600 Watt extra worden gekoeld!

Naast de verschillende invertertypes die in UPS-systemen voorkomen is er nog een heel belangrijke onderverdeling te maken, namelijk tussen "on-line-" en "offline-"UPS-systemen.

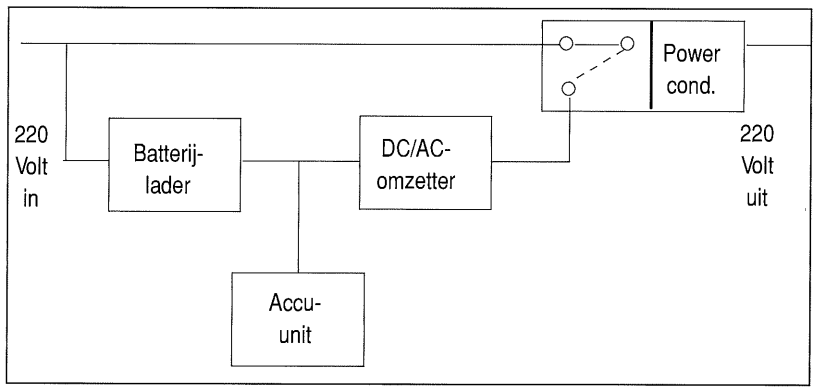
Online UPS of No-Break
Dit is de definitieve oplossing voor ieder lichtnet-probleem maar helaas ook de duurste. Bij deze systemen wordt de belasting altijd via de lader-accu-inverter-weg van spanning voorzien. Als er al een by-pass aanwezig is wordt hij alleen gebruikt bij defecten in de unit zelf of als daaraan onderhoud moet worden verricht. Zie figuur 8.



Figuur 8. Online UPS (met soms een by-pass).



Figuur 9. Offline UPS.



Figuur 10. Offline UPS met Power Conditioner in de by-pass.

Nadelen:
- duur, bevat niet alleen veel elektronica, maar omdat de Mean Time Between Failures (MTBF; de gemiddelde tijd tussen storingen in de unit) uiteraard zeer hoog moet zijn, worden er aan het ontwerp en de toegepaste componenten zeer hoge eisen gesteld;
- matig rendement (PWM-units hebben nog het beste rendement en halen circa tachtig à negentig procent);
- relatief hoge aansluitwaarde voor het lichtnet. Omdat de lader zowel het nominale vermogen van de belasting als de laadstroom voor de accu's moet kunnen leveren als die leeg zijn geraakt, is de aansluitwaarde vrijwel het dubbele van de nominale belasting!

Voordelen:
- lost ieder netstoringsprobleem op;
- geen enkele onderbreking van de netspanning (no-break).

Offline of Standby UPS-systemen

Offline UPS-systemen zijn ontwikkeld om de kosten te drukken. Het zijn eigenlijk online-systemen met een by-pass, alleen werken déze normaal via de by-pass en schakelt de unit pas om naar de inverter op het moment dat het net uitvalt of de ingangsspanning te laag of te hoog wordt; het principe is dus net andersom. De voordelen zijn simpel: bij een online-unit moet de "acculader" continu het complete uitgangsvermogen plus een laadstroom leveren, terwijl bij een offline-systeem alleen maar een laadstroom hoeft te worden geleverd met als gevolg een kleinere lader. Ook mag de MTBF van de inverter minder goed zijn omdat deze maar sporadisch behoeft te werken en dus is deze veel goedkoper te fabriceren. Wel moet de oscillator die de inverter stuurt altijd "lopen", want die moet gesynchroniseerd zijn met het lichtnet op het moment van overschakelen. Zie figuur 9.

Nadelen:
- beveiligt alleen tegen netuitval en grote sags of surges, maar niet tegen spikes (in de by-pass zit meestal alleen een RFI-filter);
- er is altijd sprake van een korte overnametijd op het moment van schakelen (bij goede units circa 4 ms en bij slechte units meer dan 15 ms);
- moet af en toe worden getest, want een defect wordt pas gesignaleerd als het net uitvalt.

Voordelen:
- betaalbaar;
- hoog rendement (weinig verliezen in stand-by mode) van 96 à 98 procent.

Offline of Standby UPS met ingebouwde Power Conditioner

Dit is een ontwikkeling van de laatste jaren waarbij de voordelen van een offline UPS (lage prijs en hoog rendement) worden gecombineerd met die van een Power Conditioner (volledige netontstoring). Soms worden deze systemen ook wel "semi online UPS" genoemd. Deze combinatie is in de meeste gevallen toch nog goedkoper dan een echte online UPS en biedt bijna dezelfde beveiliging. Het principe is dat in de by-pass-lijn van een offline UPS een Power Conditioner wordt geplaatst die voor de stooronderdrukking zorgt als het net aanwezig is, terwijl de UPS de energievoorziening overneemt als het net uitvalt. De meeste merken gebruiken als Power Conditioner een Ferro-resonant transformator die ze door wat slimme schakelingen ook gebruiken als uitgangstransformator voor de UPS. Dit heeft als voordeel dat de omschakeltijd praktisch nul is door het resonantieprincipe, maar heeft als nadeel dat de uitgangsimpedantie tamelijk hoog en de dynamische stabiliteit dus wat minder goed is. Zie figuur 10.

Nadelen:
- de uitvoeringen met een Ferro-resonant transformator in de by-pass hebben eigenlijk alle nadelen daarvan, zoals: een tamelijk hoge uitgangsimpedantie en als gevolg daarvan een matige dynamische stabiliteit, 50 Hz-brom, vrij sterk magnetisch veld en een tamelijk laag rendement;
- een echte online UPS biedt toch een betere Common- en Normal-Mode-onderdrukking.

Voordelen:
- meestal toch wel wat goedkoper dan een echte online UPS;
- biedt in 99 procent van de gevallen een oplossing voor alle netproblemen;
- het rendement is beter dan dat van een echte online UPS.

HET KIEZEN VAN DE JUISTE OPLOSSING

In het bovenstaande is geschetst wat de problemen en mogelijke oplossingen bij netstoringen zijn. Het kiezen van de beste oplossing in een bepaalde toepassing gebeurt op basis van een aantal criteria. Hoewel een UPS een volledige oplossing biedt is het zeker niet altijd nodig tot deze oplossing over te gaan omdat het probleem vaak ook met goedkopere systemen op te lossen is. Alleen bij kleinere vermogens is het selecteren uit de diverse mogelijke oplossingen niet rendabel, omdat de kleinere UPS-systemen tegenwoordig dermate concurrerend zijn geworden dat een dergelijk systeem meestal de beste keus is.

UPS
Een UPS is altijd nodig wanneer de computer moet blijven doorwerken als het lichtnet uitvalt of als het mogelijke tijd- en/of produktieverlies als gevolg van beschadigde bestanden onacceptabel wordt bevonden. Bij heel kritische toepassingen is ook een volledige beveiliging nodig tegen netvervuiling en zal dus meestal voor een online UPS worden gekozen. In situaties waar de kwaliteit van het net verder uitstekend is, kan bij minder kritische toepassingen met een offline UPS worden volstaan.
Als er voor het toepassen van een UPS wordt gekozen, is het wel zaak van tevoren nauwkeurig na te gaan welke apparatuur er allemaal op de UPS dient te worden aangesloten. *Bij netwerken waar bijvoorbeeld de routers, bridges, concentrators of repeaters essentieel zijn voor de werking van het netwerk zullen ook deze, naast de server(s) en één of meer werkstations, op een UPS moeten worden aangesloten!*

Een UPS is niet nodig wanneer het verlies aan tijd of produktie niet opweegt tegen de kosten van een UPS of als er geen noemenswaardig risico is voor beschadigde bestanden en de computer bovendien geen functie heeft na een netuitval, bijvoorbeeld omdat de machine die door de computer wordt bestuurd ook is uitgevallen. Bij kleine vermogens (globaal tot circa 3 kVA) wordt vanwege de geringe meerprijs ten opzichte van een Ferro-resonant transformator of Power Conditioner vaak toch voor een UPS gekozen.

Ferro-resonant transformator of Power Conditioner
Voor een Ferro-resonant transformator of Power Conditioner wordt gekozen als de computer niet hoeft te blijven werken na een netuitval, maar er wel duidelijk sprake is van lichtnetfluctuaties en spikes waardoor de computer wordt gestoord. Dit komt bijvoorbeeld veel voor bij computers die machines besturen in een produktiehal, waar door het in- en uitschakelen van zware motoren behoorlijke fluctuaties kunnen optreden. Van die fluctuaties hebben de meeste machines geen last, maar als het net uitvalt werkt de te besturen machine vanzelfsprekend ook niet meer en dus mag de computer ook uitvallen.

Ultra-Isolator
Voor een Ultra-Isolator wordt gekozen in soortgelijke gevallen als hiervoor, maar dan als er geen sprake is van fluctuaties maar alleen van spikes en/of noise. Aangezien die echter bijna altijd voorkomen in combinatie met spanningsfluctuaties worden Ultra-Isolatoren vrijwel niet meer toegepast.

Er zijn nog wel enkele andere systemen op de markt, maar de hierboven beschreven methoden vormen toch wel de meerderheid van de in Nederland gebruikte oplossingen. Andere principes, zoals servogestuurde spanningsregelaars en nog wat andere "exotische" oplossingen, komen hier zelden voor maar zijn vaak zeer geschikt voor derde-wereldlanden.
In principe geldt voor 3-fase toepassingen precies hetzelfde als voor 1-fase toepassingen. Vaak zijn er specifieke 3-fase oplossingen, met als alternatief drie stuks 1-fase oplossingen (mits het een sterschakeling is en geen driehoek).

R. van de Wouw
Heeft, na zijn opleiding elektronica, circa zeven jaar ervaring met netmetingen en netconditionering. Hij is thans product manager computers & peripherals (waaronder netconditioneringsapparatuur) bij Klaasing Electronics BV te Oosterhout.

Fysieke beveiliging en de chipcard-technologie

Drs. Th.H. van Hesteren, ing. J.A.M. van Schaik en drs. T.P. de Vries

Hoe kan de fysieke beveiliging worden geautomatiseerd? In dit artikel wordt een overzicht gegeven van de huidige mogelijkheden van het gebruik van chipcards en biometrische authenticatietechnieken, die gecombineerd kunnen leiden tot betrouwbare geautomatiseerde toegangscontrole in omgevingen waarin een hoge beveiligingsgraad noodzakelijk is.

INLEIDING

Gelijk met de ontwikkelingen in de automatisering in de laatste decennia hebben ook grote veranderingen plaatsgevonden op het gebied van (fysieke) beveiliging. Dit betreft niet alleen het feit dat een betere beveiliging noodzakelijk is geworden met betrekking tot geautomatiseerde omgevingen, maar tevens dat de nieuwste technologieën worden gebruikt bij het ontwikkelen van beveiligingstoepassingen, met andere woorden "de automatisering van de beveiliging".
Daarbij is onder andere een vermenging ontstaan van fysieke en logische toegangsbeveiliging; mechanische voorzieningen worden aangevuld met geprogrammeerde controles om een betere toegangscontrole te realiseren.
Het controleren van de identiteit van (on)bevoegde personen geschiedt steeds meer op geautomatiseerde wijze. Geautomatiseerde systemen voor toegangscontrole vervangen daarmee de controles door speciaal daarvoor aangesteld personeel.
In plaats van een visuele controle wordt de identiteit van een persoon aan de hand van een (fysiek) "token" op geautomatiseerde wijze vastgesteld. Met behulp van dit token kan vervolgens worden geverifieerd of de opgegeven identiteit toebehoort aan de bevoegde persoon (authenticatie).
Een goed voorbeeld van de opkomst van het gebruik van geautomatiseerde toegangscontroles is de betaalautomaat. De toegangscontrole tot een bankrekening is daarbij verschoven van verificatie, door de bankbediende, van de identiteit van de rekeninghouder aan de hand van het identiteitsbewijs en de handtekening, naar het gebruik van een token, gecombineerd met geautomatiseerde verificatie via het intoetsen van een PIN[1] door de kaarthouder.

In systemen van toegangsbeveiliging wordt in toenemende mate gebruik gemaakt van chipcardtechnologie. Bepaalde chipcards bieden de mogelijkheid door middel van een dialoog tussen het systeem en de kaart de authenticiteit van beide vast te stellen.
De chipcard wordt dan gebruikt als een (fysieke) sleutel, waarop aanvullende controlegegevens zijn vastgelegd om de authenticiteit van de kaarthouder door het geautomatiseerde systeem te kunnen vaststellen. In de meeste gevallen wordt hiervoor een wachtwoord of PIN gekoppeld aan de chipcard dat alleen bij de bevoegde kaarthouder bekend zou moeten zijn.
Door onzorgvuldig gebruik en de vaak beperkte set van mogelijke waarden zijn wachtwoorden en PIN's onvoldoende geschikt voor het realiseren van betrouwbare toegangscontrole in omgevingen die een hoge mate van beveiliging vereisen.
Het authenticatieprobleem kan worden ondervangen door gebruik te maken van unieke kenmerken die onlosmakelijk met een persoon verbonden zijn, zoals een vingerafdruk of een dynamische handtekening, ook wel biometrische authenticatietechnieken genoemd. Op deze manier kan worden voorkomen dat een onbevoegde gebruiker van een chipcard zich toch toegang kan verschaffen tot het te beveiligen systeem; de overdraagbaarheid van de PIN wordt hiermee ondervangen.

SOORTEN CHIPCARDS

De chipcard is een verzamelnaam voor verschillende soorten portable kaarten, waarop één of meer chips zijn aangebracht, die alleen kunnen functioneren binnen een bepaalde infrastructuur.
De chipcard-technologie heeft betrekking op de technologie waarbij een chip met ten minste geheugencapaciteit, maar vaak uitgebreid met capaciteit voor computer-processing ("intelligentie"), op een compacte wijze in een kaartvorm is ondergebracht.
De chipcard waarin enige vorm van "intelligentie" is aangebracht, wordt meestal aangeduid met de term smartcard; andere chipcards zijn hiervoor afhankelijk van de omgeving.

De chipcard-technologie vertoont een grote mate van overlap met de identificatietechnologie; deze overlap heeft betrekking op de identificatie van objecten (inclusief personen) met behulp van de chipcard.
Vooral in een omgeving waar hoge eisen aan de beveiliging worden gesteld, is de smartcard bij uitstek geschikt voor identificatiedoeleinden.
Chipcards zijn ook bruikbaar voor andere toepassingen, zoals beveiligde opslag van gegevens of geld, die niet direct betrekking hebben op het identificeren van personen (bijvoorbeeld elektronische portemonneefunctie).

Identificatie kan ook plaatsvinden zonder chipcard-technologie maar met gebruik van portable chips. Deze vorm van identificeren wordt aangeduid met de term elektronisch labelen en wordt hoofdzakelijk gebruikt in toepassingen die niet direct op personen betrekking hebben. Het label wordt bevestigd aan het voorwerp dat dient te worden geïdentificeerd en de aanwezige gegevens kunnen door middel van een radiografische verbinding op afstand worden uitgelezen.
Deze labels worden vaak aangeduid als (smart) tags of (smart) tokens. Uiterlijk zijn veel verschillende vormen mogelijk, en zoals bij chipcards kan de mate van "intelligentie" variëren.
Deze vorm van identificatie valt buiten het kader van dit artikel en zal verder niet worden behandeld.

Chipcards worden onderscheiden naar complexiteit (intelligentie), te weten de memorycard, de smartcard en de super smartcard.

Memorycard
De memorycard is de meest simpele uitvoering van de chipcard. Deze kaart dient slechts als opslagmedium voor bepaalde gegevens, en bevat daarvoor alleen een digitaal geheugen (en logica voor de communicatie). Deze geheugens kunnen nog worden onderscheiden naar eenmalig beschrijfbaar en herschrijfbaar.
De eenmalig beschrijfbare kaart wordt ook wel aangeduid als afwaardeerkaart, bevat één chip en de dimensies zijn die van de gebruikelijke bankkaart (conform ISO-standaarden).
Het grootste deel van de memorycards heeft echter een herschrijfbaar geheugen en wordt vooral gebruikt voor het opslaan van grote hoeveelheden data of programmatuur.
Aangezien de kaart geen eigen processor bevat, moet deze kaart voor gebruik altijd aan een intelligente unit worden gekoppeld.

De smartcard is bij uitstek geschikt voor identificatiedoeleinden in een omgeving waar hoge eisen aan de beveiliging worden gesteld.

Smartcard
De smartcard is veelal een "single chip" kaart zonder eigen invoer- en uitvoermogelijkheden, waarbij het geheugen en de processor in de chip zijn geïntegreerd. De processor maakt het mogelijk dat de kaart allerlei intelligente functies uitvoert.
De intelligentie van de smartcard kan worden gebruikt om de kaart te beveiligen met bijvoorbeeld een PIN, welke met externe randapparatuur dient te worden ingevoerd. De smartcard is daarbij zodanig opgezet dat elektronische sleutels op een veilige manier kunnen worden opgeslagen.

Super smartcard
De super smartcard heeft dezelfde functionaliteit als de smartcard, maar heeft een eigen display en toetsenbord. Hierdoor is het mogelijk de gegevens die in de chip zijn opgeslagen direct voor de kaarthouder zichtbaar te maken.
De op dit moment van dit type bestaande kaarten zijn te beveiligen met een PIN die door de gebruiker zelf kan worden vastgesteld. De kaart controleert zelf de geldigheid van de ingevoerde code.

De communicatie tussen een chipcard en zijn omgeving kan geschieden via elektrische contacten of via een draadloze (microgolf)verbinding. Deze kaarten worden aangeduid met respectievelijk contactkaart en contactloze kaart.
In het eerste geval zal de kaart fysiek contact moeten maken met een kaartlezer, die veel gelijkenis vertoont met de leesapparatuur voor magneetstripkaarten.
Voor de contactloze kaart geldt dat een eigen spanningsbron voor de kaart noodzakelijk is zodra de communicatie-afstand groter is dan enkele tientallen centimeters. Het signaal zou anders dermate sterk moeten zijn, dat toestemming voor het gebruik voor het desbetreffende frequentiegebied dient te worden aangevraagd.

De logische structuur van de chipcard verschilt per toepassing. In geval van de memorycard is sprake van één (groot) geheugengebied waarin de gegevens geordend kunnen worden opgeslagen, en waartoe met behulp van een intelligente unit toegang kan worden verkregen.
De (super) smartcard heeft naast de eigen processor verschillende geheugengebieden waarin gegevens in files en directories zijn geordend. De files en directories hebben hun eigen beveiligingsniveaus, waarmee de gegevens kunnen worden afge-

1 *Personal Identification Number; een vier- tot achtcijferig decimaal password ten behoeve van het verkrijgen van toegang tot een applicatie of een device (bijvoorbeeld een smartcard).*

schermd. Gevoelige gegevens zoals wachtwoorden, PIN's of cryptografische sleutels die de toegang tot een geheugengebied controleren, zijn opgeslagen in de "geheime zone" die alleen toegankelijk is voor de processor en die niet buiten de kaart kan worden gebracht.

Het gebruik van chipcard-technologie in commerciële toepassingen zal worden bepaald door de functionele meerwaarde die chipcards kunnen bieden ten opzichte van de bestaande en nog in ontwikkeling zijnde technologieën.
Rekening moet worden gehouden met alternatieve ontwikkelingen zoals de opticalcard of lasercard. Daarbij wordt gebruik gemaakt van de opslagtechnologie van de compact disc om grote hoeveelheden gegevens eenmalig op te slaan.

Momenteel zijn de kosten en de organisatorische invoeringsproblematiek de meest vertragende factoren voor grootschalig gebruik van chipcards.

Momenteel zijn de kosten en de organisatorische invoeringsproblematiek de meest vertragende factoren voor grootschalig gebruik van chipcards.
De huidige prijs van de chipcard varieert van enkele guldens voor een simpele chipcard tot ongeveer 150 gulden voor de super smartcard, terwijl de prijs van technologische alternatieven zoals de magneetkaart varieert van slechts enkele centen tot minder dan één gulden.

De toepassingsmogelijkheden voor de chipcard zullen worden vergroot door de verdergaande (technologische) ontwikkelingen. Geheugencapaciteit en verwerkingssnelheid zullen verder toenemen, en naar verwachting zullen de verschillende chipcards worden gestandaardiseerd.
Verder wordt verwacht dat de kosten van de chipcard omlaag gaan als gevolg van massaproduktie en ontwikkelingen in de chipcard-technologie.

BEVEILIGINGSTOEPASSINGEN SMARTCARD

De toepassingsmogelijkheden van de intelligente chipcards zijn gebaseerd op een aantal functionele eigenschappen van de kaart ten aanzien van beveiliging.

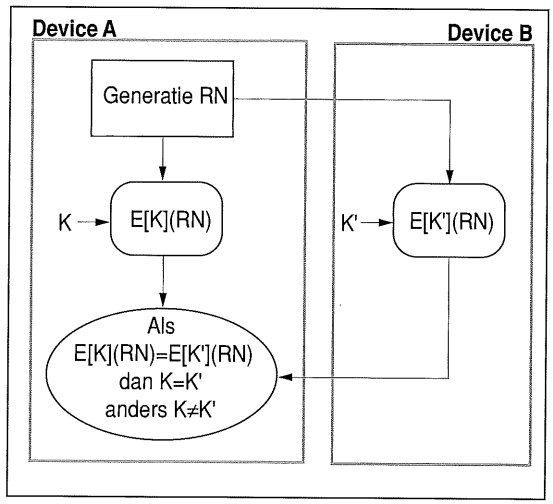
De op magneetstripkaarten en memorycards (kaarten zonder intelligentie) vastgelegde gegevens zijn in principe op relatief eenvoudige wijze te kopiëren. De smartcard daarentegen biedt betere beveiligingsmogelijkheden vanwege de cryptografische mogelijkheden van de kaart en het in de chip geladen kunnen blijven van de geheime sleutels voor encryptie.

Bij het gebruik van smartcards in een beveiligingssysteem zijn drie verschillende objecten betrokken, namelijk de kaart zelf, de kaarthouder en het verwerkende device van het systeem.
In de techniek van toegangscontrole met behulp van smartcards spelen de volgende activiteiten een belangrijke rol:
- *authenticatie van kaart en device:* wederzijds vaststellen van de echtheid van de door de kaarthouder aangeboden kaart en het verwerkende device.
- *authenticatie van kaarthouder:* vaststellen en verifiëren van de identiteit zoals opgegeven door de kaarthouder door het verwerkende device.

Authenticatie van kaart en device

In deze stap vindt controle plaats op de echtheid (authenticiteit) van de verschillende devices (inclusief smartcard) en/of applicaties van het systeem. Dit gebeurt op basis van een cryptografische sessie (challenge response).

Een device A is in staat de authenticiteit van een device B vast te stellen indien beide beschikken over eigen verwerkingscapaciteit en een zelfde encryptie-algoritme.
Het verifiërende device A genereert een willekeurige waarde RN en zendt de waarde naar het te verifiëren device B. Beide devices vercijferen met behulp van het encryptie-algoritme en hun gemeenschappelijke encryptiesleutel dit willekeurige getal. Device B zendt het resultaat naar device A dat het resultaat van de door hem zelf uitgevoerde vercijfering vergelijkt met het van device B binnengekomen vercijferde willekeurige getal RN. Indien beide waarden gelijk zijn constateert device A dat device B beschikt over de gemeenschappelijke sleutel en dus een authentiek device moet zijn.



Figuur 1. Een grafische weergave van het verloop van de authenticatiesessie.

Via kaartauthenticatie stellen één of meer devices van het systeem (device A) de echtheid van een aangeboden kaart (device B) vast.

Alvorens zijn verificatiegegevens in te voeren in een kaartlezer wil de kaarthouder kunnen vaststellen met een legale onveranderde lezer van doen te hebben (device-authenticatie). Zonder deze zekerheid is het mogelijk dat de kaarthouder zijn kaart en verificatiegegevens invoert in een illegale lezer, die de kaartinhoud en de verificatiegegevens vastlegt.
Device-authenticatie kan worden verkregen door het uitvoeren van het authenticatieproces waarbij de smartcard het verifiërende device A voorstelt en de kaartlezer (device B) op authenticiteit wordt geverifieerd.

Authenticatie van de kaarthouder

Authenticatie van de opgegeven identiteit vindt plaats nadat de kaarthouder zijn smartcard heeft aangeboden aan een verwerkend device en (wederzijdse) authenticatie tussen kaart en device is uitgevoerd.
Om authenticatie van de kaarthouder te kunnen uitvoeren, zal de kaarthouder een uniek en geheim gegeven dienen op te geven. Bij de conventionele systemen wordt op grote schaal gebruik gemaakt van de PIN: een discrete waarde die altijd of helemaal goed of helemaal fout is. PIN-verificatie wordt beschouwd als een negatieve vorm van verificatie: een foutieve PIN wijst ondubbelzinnig op onjuist gebruik, maar een correcte PIN bewijst niet automatisch een rechtmatig gebruik.
Voor omgevingen die een hoge mate van beveiliging vereisen, wordt echter niet meer volstaan met een dergelijke fraudegevoelige methode. De voorkeur gaat dan uit naar positieve verificatie: alleen de rechtmatige eigenaar beschikt over de juiste karakteristiek. Hiervan is bijvoorbeeld sprake bij gebruik van biometrische authenticatie.

Het gebied in het geheugen van de smartcard met het cryptografische sleutelmateriaal en de geheime gegevens, zoals bijvoorbeeld de PIN of de biometrische karakteristiek, is alleen toegankelijk voor de processor zelf. De opgeslagen authenticatiegegevens en de encryptiesleutel kunnen dit geheugengebied niet verlaten: verificatie van de ingevoerde authenticatiegegevens wordt intern uitgevoerd.

Alleen na een succesvolle authenticatie kan de processor van de smartcard beschikken over de binnen het beveiligde geheugengebied aanwezige encryptiesleutels.
De cryptografische sleutels worden onder meer gebruikt voor de beveiliging van de door (een) applicatie(s) uit te voeren functies.

Voor alle duidelijkheid dient te worden opgemerkt dat de verifiërende processen alleen kunnen worden uitgevoerd door devices die in het bezit zijn van een eigen verwerkingscapaciteit.

BIOMETRISCHE AUTHENTICATIE

Door de International Biometric Association (IBA) wordt biometrie gedefinieerd als "een meetbare fysieke eigenschap of persoonsgebonden gedrag dat gebruikt kan worden voor het op geautomatiseerde wijze vaststellen van de identiteit, of het verifiëren van de opgegeven identiteit, van een persoon".

Door gebruik van biometrie wordt de overdraagbaarheid van de PIN ondervangen.

In deze definitie worden twee verschillende toepassingen van biometrie onderkend, namelijk biometrische authenticatie en biometrische herkenning.

Biometrische authenticatie betreft de mogelijkheid om een opgegeven identiteit van een gebruiker te verifiëren, nadat deze gebruiker zich aan het systeem kenbaar heeft gemaakt via een user-id (gebruikerscode). Verificatie geschiedt vervolgens op basis van "iets" wat alleen de echte gebruiker kenmerkt (karakteristiek), in plaats van "iets" wat alleen de echte gebruiker kan weten (wachtwoord) of kan bezitten (token).
Volgens de definitie dient biometrische authenticatie op geautomatiseerde wijze te geschieden. Een bepaalde karakteristiek wordt "gemeten" en omgezet in een digitaal signaal. Dit ingevoerde signaal wordt vervolgens (met een bepaalde tolerantie) vergeleken met het opgeslagen signaal (controlesignaal) zoals dat initieel is vastgelegd in de toepassing bij de opgegeven identiteit.
Biometrische authenticatie wordt vooral gebruikt in toepassingen voor toegangsbeveiliging.

In geval van *biometrische herkenning* kan aan de hand van de karakteristiek direct de identiteit van een gebruiker worden vastgesteld; identificatie en verificatie worden in dat geval tegelijkertijd uitgevoerd. Toepassingen die hierop gebaseerd zijn, kunnen alleen in kleinschalige omgevingen worden gebruikt, aangezien elk signaal zal moeten worden vergeleken met alle opgeslagen signalen.
Ten opzichte van biometrische authenticatie zal extra capaciteit nodig zijn om deze verwerking binnen acceptabele tijd te kunnen uitvoeren. Daarnaast zal het beveiligingsniveau lager zijn doordat de onbevoegde gebruikers een grotere trefkans zullen hebben bij het proberen van mogelijke karakteristieken.
Concrete toepassingen van biometrische herkenning zijn meestal niet direct gericht op beveiliging, maar hebben bijvoorbeeld betrekking op het analyseren van vingerafdrukken door justitie.
In het kader van dit artikel zal nader worden ingegaan op biometrische authenticatie; de meeste opmerkingen zullen echter ook van toepassing zijn op biometrische herkenning.

Bij biometrie wordt gebruik gemaakt van bepaalde kenmerken die een persoon op unieke wijze kunnen identificeren. Deze kenmerken zijn te onderscheiden in twee verschillende klassen, namelijk fysieke en gedragsmatige karakteristieken.

Fysieke karakteristieken hebben betrekking op de (statische) kenmerken die bij elke persoon aanwe-

zig zijn en die, theoretisch gezien, niet aan veranderingen onderhevig zijn. Dit betreft onder andere de vingerafdruk, de vorm van de hand en de structuur van de retina.

Gedragsmatige karakteristieken betreffen de (dynamische) kenmerken van handelingen of gewoonten die bij elke persoon kunnen worden gemeten. Deze kenmerken zijn minder stabiel van aard aangezien de persoon zowel bewust als onbewust bij de uitvoering ervan, deze kan veranderen. Vooral psychologische factoren kunnen de dynamiek van bijvoorbeeld de handtekening, spraak of de aanslag op een toetsenbord op een zodanige manier beïnvloeden dat verificatie hierdoor niet mogelijk is.

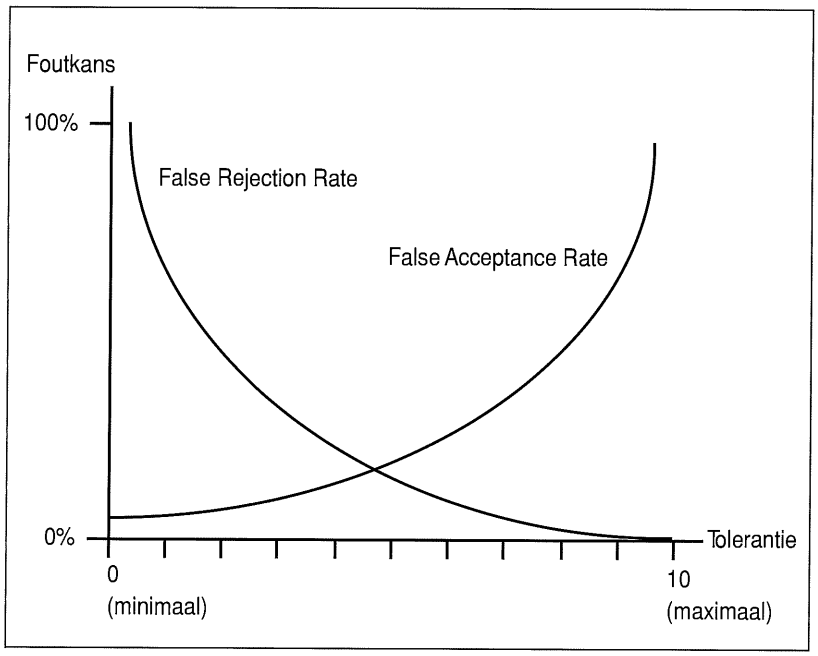
Biometrische toepassingen kunnen op verschillende aspecten worden beoordeeld, zoals performance (foutkansen), snelheid, kosten, sociale acceptatie (gebruikersgemak en ongewenste reacties van gebruikers), integratiemogelijkheden met andersoortige toepassingen en aansluiting bij bepaalde standaarden. Op de twee belangrijkste aspecten, performance en snelheid, zal nu nader worden ingegaan.

Performance

Het gebruik van biometrische toepassingen wordt bepaald door de mate waarin de verificatie van de opgegeven identiteit correct kan worden uitgevoerd. Binnen een beperkte hoeveelheid tijd (tot maximaal twee seconden) dient te worden vastgesteld of de te controleren karakteristiek toebehoort aan een bevoegde gebruiker.
Aangezien een karakteristiek aan veranderingen onderhevig kan zijn en de meting niet exact kan worden uitgevoerd, zal verificatie meestal binnen bepaalde marges moeten plaatsvinden. Ten gevolge van deze toegestane tolerantie zal verificatie tot onjuiste beslissingen kunnen leiden; de bijbehorende foutkansen zijn als volgt te definiëren:

- "type 1" = de kans dat verificatie ten onrechte een negatief resultaat oplevert (ook wel: False Rejection Rate (FRR) of Insult Rate);
- "type 2" = de kans dat verificatie ten onrechte een positief resultaat oplevert (ook wel: False Acceptance Rate (FAR) of Impostor Rate).

Figuur 2. De foutkansen bij verschillende toleranties.



Deze foutkansen zijn omgekeerd evenredig aan elkaar. Zodra de marges worden aangescherpt om het aantal ten onrechte geaccepteerde personen te verminderen (verhogen van de beveiliging), zal een groter aantal bevoegde personen worden geweigerd; verruiming van de marges om het aantal ten onrechte geweigerde personen te verkleinen (verbeteren van de gebruikersvriendelijkheid), zal ertoe leiden dat meer onbevoegde personen worden geaccepteerd.

De meeste toepassingen bieden de mogelijkheid meerdere pogingen (tot een maximum van drie) uit te voeren om een geslaagde verificatie te realiseren. Hierdoor vindt in feite een verschuiving plaats van de eerste foutkans naar de tweede foutkans; het aantal ten onrechte geweigerde personen zal door de geboden herkansingsmogelijkheden verminderen, terwijl terecht geweigerde personen nogmaals zullen proberen te worden geaccepteerd.

Momenteel wordt door de leveranciers van verschillende biometrische toepassingen veel aandacht besteed aan het reduceren van de foutkans van het type 1; het blijkt echter dat deze fout al aanzienlijk vermindert als de gebruikers enige ervaring met de desbetreffende toepassing hebben opgedaan.
Voor de meeste biometrische toepassingen geldt dat de foutkans van het type 1 bijna nul procent bedraagt, en dat de foutkans van het type 2 in de buurt van één à twee procent ligt.

In sommige toepassingen wordt het controlesignaal bij een geslaagde verificatie bijgewerkt met het ingevoerde signaal. Deze aanpassing is met name zinvol bij gebruik van gedragsmatige karakteristieken, omdat deze karakteristieken de neiging hebben in de loop der tijd te veranderen, waardoor de foutkans van het type 1 zou kunnen toenemen.

Snelheid

De acceptatie van biometrische toepassingen is sterk afhankelijk van de snelheid waarmee verificatie bij dagelijks gebruik kan plaatsvinden. Door gebruik van de nieuwste technologieën is de benodigde tijdsduur voor verificatie bij de meeste toepassingen teruggebracht tot minder dan twee seconden.
Alleen voor de initiële opslag van het controlesignaal zal bij de meeste toepassingen meer tijd van de (toekomstige) gebruiker worden gevraagd, omdat de karakteristiek enkele malen moet worden ingevoerd.

TOEPASSINGEN VAN BIOMETRISCHE AUTHENTICATIE

In deze paragraaf worden verschillende biometrische authenticatietechnieken kort besproken.

In bepaalde toepassingen van spraakherkenning wordt gebruik gemaakt van een set van woorden; bij authenticatie zal de gebruiker direct moeten reageren op een willekeurig gekozen woord.
Het grootste probleem bij spraakherkenning is de mogelijke variantie bij het inspreken. Achtergrondgeluiden, een verkoudheid of een slecht humeur kunnen ertoe leiden dat de spraak te veel afwijkt van het controlesignaal.

Bij de dynamiek van de handtekening worden met behulp van een gevoelige pen en/of tableau de uitgevoerde bewegingen met de bijbehorende snelheden (tijdsfactor) vastgelegd. In plaats van te controleren op het resultaat wordt de totstandkoming gecontroleerd, zodat de kans op een geslaagde falsificatie sterk wordt gereduceerd.

In tegenstelling tot de meeste karakteristieken, waarbij slechts de mogelijkheid bestaat een momentcontrole uit te voeren, kan de dynamiek van de toetsaanslag worden gebruikt om de gebruiker continu te controleren. Vooral omgevingen met terminals waarin dient te worden voorkomen dat substitutie van personen kan plaatsvinden, zijn geschikt voor deze vorm van beveiliging.

Bij handgeometrie wordt gecontroleerd op een combinatie van vingerlengte, transparantie van de huid en de vorm van de (palm van de) hand. Door de opkomst van toepassingen waarin andere, meer betrouwbare authenticatietechnieken worden gebruikt, wordt deze vorm van authenticatie steeds minder gehanteerd.

De vingerafdruk is de meest gebruikte karakteristiek voor identificatie van de mens. Uit onderzoeken is gebleken dat de kans dat twee verschillende personen (inclusief tweelingen) een gelijke vingerafdruk hebben, minder bedraagt dan één op het miljard. De beperkte sociale acceptatie van deze techniek kan onder andere worden verklaard door het gebruik van deze techniek door justitie.

De retina kan met infrarood licht van een lage intensiteit worden onderzocht. Aan de hand van het teruggekaatste licht wordt daarmee de unieke structuur van de bloedvaten op de achterzijde van het oog bepaald. Deze karakteristiek heeft als voordeel dat de structuur alleen bij ernstige hersenbeschadiging zal veranderen.
Deze relatief dure techniek wordt op beperkte schaal toegepast in omgevingen waarvoor een hoog beveiligingsniveau is vereist.

De laatste ontwikkelingen hebben betrekking op gezichtsherkenning met behulp van neurale netwerken.

Met name de dynamische handtekening en spraak lijken zeer geschikte alternatieven voor de conventionele authenticatietechnieken. Biometrie kan bijvoorbeeld worden gekoppeld aan een token om een zeer betrouwbare toegangscontrole te realiseren. Toegang tot het systeem zal alleen worden verleend indien de tokenhouder zowel dit token in bezit heeft als het bijbehorende veilig opgeslagen biometrisch signaal kan reproduceren. Het probleem van de overdraagbaarheid van een token zal hiermee volledig kunnen worden ondervangen.

	Performance	Snelheid	Kosten	Sociale acceptatie	Integratiemogelijkheden
Spraak	**	***	***	***	***
Handtekening dynamiek	**	**	**	***	**
Toetsaanslag dynamiek	**	**	**	***	***
Handgeometrie	*	***	**	**	**
Vingerafdruk	**	**	*	*	**
Retinastructuur	***	**	*	*	**
*** = sterk, ** = gemiddeld, * = zwak.					

Tabel 1. De plus- en minpunten van de belangrijkste biometrische authenticatietechnieken.

Een recent geïmplementeerde toepassing op dit gebied is de Schiphol Travel Pass (STP). De houder van deze STP behoeft bij aankomst op Schiphol niet meer zijn paspoort aan de marechaussee te tonen.
Deze controle is vervangen door een speciale sluis, waarbij de identiteit van de houder van de Schiphol Travel Pass op geautomatiseerde wijze wordt geverifieerd. Indien de vingerafdruk van de houder van de STP overeenstemt met het in de chipcard opgeslagen patroon, kan de houder van de Schiphol Travel Pass de sluis verlaten om zijn reis te vervolgen.

BEVEILIGING VAN DE SMARTCARD ZELF

De mate van beveiliging die met behulp van smartcards kan worden gerealiseerd, is sterk afhankelijk van de wijze waarop de smartcard zelf is beveiligd.

Fysieke beveiliging

Een kritische voorwaarde bij het gebruik van encryptie-algoritmen is het sleutelbeheer (key management). Het sleutelbeheer betreft het op betrouwbare wijze genereren, installeren, opslaan en onderhouden van cryptografische sleutels.

Grote systemen gebruiken veelal zogenaamde Security Modules voor de veilige opslag van klare waarden van sleutels. Deze Security Modules beschikken over fysieke beveiligingsvoorzieningen,

zoals temperatuur- en lichtgevoelige censoren, netwerk van afschermende contactdraden (wire meshes) en het gieten in epoxy. Al deze maatregelen zijn gericht op het voorkomen van het ongeoorloofd uitlezen van de opgeslagen sleutels.

Het niveau van beveiliging dat noodzakelijk is voor een Security Module behoeft echter niet door een smartcard te worden gehaald. Een goed sleutelbeheer is namelijk zodanig opgezet dat het compromitteren van één of meer sleutels uit een kaart geen gevolgen zal hebben voor andere kaarten in het systeem. Elke smartcard wordt voorzien van één of meer unieke sleutels, zodat een eventueel uitgelekte sleutel betrekking heeft op één kaart en niet op het volledige systeem.

De smartcard beschikt zelf over een aanvaardbaar niveau van fysieke beveiliging.

Toch beschikt een smartcard over een aanvaardbaar niveau van fysieke beveiliging. Wanneer men toegang tot de gegevens in de chip zou willen verkrijgen, dient men de kaart open te breken om toegang tot de chip zelf te krijgen. Zou de chip onbeschadigd uit de kaart worden verwijderd, dan is het nog niet mogelijk een geheugendump te maken, aangezien de testcontacten van de chip tijdens de produktie worden verwijderd.
Sleutelmateriaal zou eventueel kunnen worden uitgelezen onder laboratoriumomstandigheden, maar gezien de bijkomende kosten zal het rendement hiervan moeten worden betwijfeld.

Sinds enige tijd zijn zogenaamde security-chips op de markt. Het uitlezen van geheime gegevens uit deze chip wordt extra bemoeilijkt door de wijze van fysieke opbouw van de chip.

Logische structuur

De smartcard beschikt over eigen verwerkingscapaciteit en geheugen. Overeenkomstig een normale computer is dit geheugen opgebouwd uit files en directories. Elke file en directory wordt beveiligd tegen onbevoegd gebruik. Toegang tot een file of directory wordt verleend op basis van een PIN of een ander authenticatiegegeven.
Het geheugen van de smartcard wordt opgedeeld in een aantal zones met verschillende beveiligingsniveaus:

1. *De "geheime zone".*
Een individueel geheugengebied met het cryptografische sleutelmateriaal en de geheime gegevens die alleen door de processor van de smartcard worden aangesproken via de encryptiefuncties. De gegevens zijn niet buiten de kaart beschikbaar en mogen alleen bij initialisatie worden geladen.

2. *De "confidentiële zone".*
Een gemeenschappelijk geheugengebied met gegevens die alleen door de processor van de smartcard worden gelezen of geschreven na authenticatie- en autorisatie-operaties.

3. *De "publieke zone".*
De gegevens in dit gebied zijn van niet-vertrouwelijke aard en kunnen door iedereen zonder tussenkomst van beveiligingsmechanismen worden benaderd.

Alhoewel authenticatiegegevens niet uit de "geheime zone" kunnen worden gelezen, kan de kaart zodanig geconstrueerd zijn dat deze gegevens door de gebruiker kunnen worden gewijzigd.

Encryptie

Om te voorkomen dat derden kennis kunnen nemen van de berichtenuitwisseling tussen de smartcard en een applicatie, is het noodzakelijk de berichten te versleutelen. Via een encryptie-algoritme kan een bericht door de zender worden gecodeerd, dat door de ontvanger met behulp van de juiste sleutel kan worden gedecodeerd.

Het bekendste en meest verbreide encryptie-algoritme is de Data Encryption Standard (DES), een symmetrisch algoritme (de sleutel is bij de zender en de ontvanger gelijk) dat gebruik maakt van een 64-bits sleutel (effectief 56 bits).

Bij asymmetrische algoritmen of public key algoritmen wordt gebruik gemaakt van een sleutelpaar: bij decryptie van een bericht wordt een andere sleutel gebruikt dan bij encryptie van het bericht. Afhankelijk van het gestelde doel kan één van beide sleutels openbaar worden gemaakt; de andere sleutel dient daarbij geheim te blijven.
Een bekend voorbeeld is RSA (genoemd naar zijn ontwikkelaars Rivest, Shamir en Adleman), waarbij sleutels ter lengte van 512 bits en meer worden gebruikt. Dit algoritme maakt gebruik van het feit dat het factoriseren van zeer grote getallen (nog) niet op efficiënte wijze kan worden uitgevoerd.

Door het verschil in de achterliggende wiskundige concepten van de twee belangrijkste encryptie-algoritmen, DES en RSA, bestaat een duidelijk verschil in verwerkingssnelheid. DES berust op eenvoudige bewerkingen, zoals permutaties en translaties, die redelijk snel door de computer kunnen worden uitgevoerd, terwijl RSA op relatief langzame bewerkingen is gebaseerd, zoals exponentiatie en modulorekening.
Tot nu toe zijn geen commerciële RSA-smartcards op de markt beschikbaar; prototypen bevinden zich nog in de testfase. Een groot aantal leveranciers heeft een DES-smartcard reeds in de produktlijn opgenomen.
Het voordeel van DES ten opzichte van RSA is dat grote hoeveelheden gegevens zeer snel kunnen worden versleuteld; RSA kan daarbij eventueel worden gebruikt voor het veilig uitwisselen van de geheime DES-sleutels.

VOORDELEN EN STERKE PUNTEN

Tot nu toe is voornamelijk ingegaan op de gebruiksmogelijkheden van de smartcard bij fysieke beveiliging en de beveiligingsaspecten van de kaart zelf. De smartcard biedt als medium echter meer mogelijkheden door de beschikbare verwerkings- en opslagcapaciteit en de beperkte omvang.

De smartcard beschikt, net als een computer, over eigen verwerkings- en opslagcapaciteit. Smartcards kunnen hierdoor snel en op relatief eenvoudige wijze worden geherprogrammeerd (binnen stringente autorisatieprocedures). Door de intelligentie van de kaart kunnen bewerkingen in de kaart zelf plaatsvinden en kunnen er, al of niet tijdelijk, gegevens in worden opgeslagen. Daarmee ontstaat de mogelijkheid tot bijvoorbeeld monitoring, waarmee achteraf kan worden vastgesteld op welke locaties iemand aanwezig is geweest en of dat overeenkomstig zijn bevoegdheden was toegestaan. Dit is bijvoorbeeld relevant voor bewakers die hun ronde maken.
De smartcard biedt talloze mogelijkheden die - doordat de capaciteit van de chips toeneemt - qua prijs/prestatie-verhouding steeds aantrekkelijker worden. Hierdoor biedt de smartcard de gebruikers de mogelijkheid zelf relevante informatie met zich mee te dragen, waardoor toepassingsmogelijkheden minder locatiegebonden worden.
Daarmee vervalt de noodzaak bepaalde gegevens in computersystemen op te slaan en voorzieningen te treffen die het mogelijk maken die gegevens op alle relevante locaties ter beschikking te stellen.

De chipcard heeft over het algemeen de afmetingen van een (plastic) creditcard. De kaart kan daardoor in de portefeuille worden meegedragen en heeft daarmee een hoge portabiliteitsgraad.
De technische karakteristieken van de chipcard, samen met een steeds aantrekkelijker prijs/prestatieverhouding, maken dat er functionele mogelijkheden ontstaan die leiden tot een brede toepasbaarheid van chipcards.

Steeds meer kaarten worden in de markt uitgezet door een toenemend aantal verschillende kaartuitgevers voor verschillende toepassingsgebieden. De toegenomen verwerkings- en opslagcapaciteit van de chipcard maakt het mogelijk een en dezelfde kaart voor verschillende toepassingen te gebruiken. Hiermee kan het ongemak voor de gebruiker van de noodzaak tot het bezitten van verschillende kaarten voor verschillende gelegenheden worden verlaagd.
Daarnaast bestaat de mogelijkheid de kaart te individualiseren, hetgeen met name bij fysieke beveiliging een voordeel kan zijn. Afhankelijk van de taken en verantwoordelijkheden van de gebruiker wordt op de kaart bijvoorbeeld vastgelegd welke beveiligingsbeperkingen er voor deze gebruiker gelden. Indien ook andere toepassingsfuncties (betaalkaart voor het restaurant, registratie gebruik kopieermachines) op de kaart worden aangebracht, neemt de kans toe dat de gebruiker de kaart altijd bij zich heeft en minder snel aan anderen zal uitlenen.
In alle gevallen dient te worden vastgesteld of beveiligingseisen zich laten combineren met kaarten die voor andere doeleinden worden gebruikt en eventueel door andere partijen worden uitgegeven.

CONCLUSIE

De huidige manier van authenticatie bij gebruik van de smartcard gebeurt hoofdzakelijk via de PIN; toegangscontrole wordt uitgevoerd op basis van het bezit van de kaart in combinatie met kennis van de code. Deze controle garandeert geen volledig betrouwbare beveiliging, aangezien zowel de kaart als de code overdraagbaar respectievelijk kopieerbaar is.

Het persoonsgebonden maken van de smartcard kan worden geregeld door authenticatie op basis van de biometrische karakteristieken te laten uitvoeren in plaats van de relatief "gevoelige" PIN.

Bij grootschalig gebruik is het ondoenlijk biometrische controlegegevens overal ter beschikking te hebben. De smartcard, met zijn eigen verwerkingscapaciteit en uitgebreide en goed te beveiligen opslagcapaciteit, is het geëigende medium om deze gegevens op vast te leggen en de kaarthouder zelf voor het beschikbaar stellen van die gegevens te laten zorg dragen.

LITERATUUR

[Guin90] D. Guinier, *Identification by Biometrics: An Introduction and a Survey;* ACM SIG Security, Audit & Control Review, 1990, nr. 2 p.1-11.

[Hyde91a] J. Hyde, *Biometric Access: Control Systems: Market Overview;* DATAPRO report on Information Security, 1991, p.301-305.

[Hyde91b] J. Hyde, *Biometric Access: Control Systems: Technology Overview;* DATAPRO report on Information Security, 1991, p.321-325.

[Inte90] Intercai, *Chipcards en elektronische labels, een verkenning;* rapportage Intercai in opdracht van het Ministerie van Economische Zaken, september 1990.

[Mill87] B.L. Miller, *Biometrics - Getting Computers to Identify People;* Canadian Data Systems, 1987, p.56-65.

[Sher91] R. Sherman, *Biometric Research: The Way Forward;* DATAPRO report on Information Security, 1991, p.201-212.

[Warf89] G.H. Warfel, *Biometrics - Positive ID for Operating Personnel;* Information Security Guide, 1989/90, p.43-46.

Drs. Th.H. van Hesteren
Heeft zijn studie Informatica aan de Rijksuniversiteit Leiden begin 1989 afgerond en volgt momenteel de post-doctorale EDP-auditing-opleiding aan de Erasmus Universiteit te Rotterdam. Na zijn studie te Leiden heeft hij zich met name bezig-gehouden met de ontwikkeling van management informatie-systemen bij verschillende buitenlandse vestigingen van een Nederlandse bank. Begin 1991 is Van Hesteren in dienst getreden bij KPMG Klynveld EDP Auditors. Hij heeft diverse opdrachten uit-gevoerd op het gebied van systeemontwikkeling, zoals het begeleiden van conversies en het beoordelen van (functionele ontwerpen van) geautomatiseerde informatiesystemen.

Ing. J.A.M. van Schaik
Is als organisatie-adviseur werkzaam bij KPMG Klynveld Management Consultants. Hij is als technisch projectleider verantwoordelijk geweest voor de realisatie van de chipcard-proef Woerden. In 1991 vervulde hij de secretarisfunctie voor de subsidieregeling Telematica Gidsprojecten voor het Ministerie van Economische Zaken.

Drs. T.P. de Vries
Studeerde Wiskunde aan de Universiteit van Amsterdam. Hij is thans werkzaam bij KPMG Klynveld Management Consultants en heeft zich gespecialiseerd in de beveiligingsmethoden voor het elektronisch berichtenverkeer, smartcard- en magneetstripkaarttoepassingen en de onderliggende mathematische en cryptografische principes. Hij is betrokken bij opdrachten in het kader van de beveiliging van het elektronisch berichtenverkeer met behulp van cryptografische technieken bij financiële instellingen, creditcardmaatschappijen en de detailhandel.

Beveiligingsbeleid gegevens en gegevensverwerking, een praktisch voorbeeld

Ir. B.J.M. van Wely

Is beleidsvorming langs hiërarchische paden (top-down) een noodzaak voor een goed eindresultaat?
In bijgaand artikel wordt vanuit de praktijk (enigszins beperkt tot een "voorbeeldsituatie") aangetoond dat deelbeleid, geïnitieerd in de lagere regionen van een organisatie, ook tot succes kan leiden.

INLEIDING

Het eind 1986 door het toenmalige KKC in opdracht van een staatscommissie uitgevoerd inventariserend onderzoek bracht aan het licht, dat van de grootschalige bedrijven slechts 52 procent een vastgelegd beveiligingsbeleid had en dat slechts 36 procent maatregelen koos op grond van een uitgevoerde risico-analyse. De indruk bestaat dat veel bedrijven sindsdien actiever op dit gebied zijn geworden, maar dat van een geconsolideerde situatie nog geen sprake is. De mate van aandacht van het topmanagement voor dit specifieke beleidsonderdeel is groeiend, maar uiteraard zowel in aard als omvang afhankelijk van de branche en de traditie van de organisatie.

Dit artikel schetst een praktisch voorbeeld van een poging te komen tot een beveiligingsbeleid in een omvangrijke basisindustriële omgeving met een enkele jaren geleden van een functionele naar een produkt- en servicegroepgewijze indeling veranderde organisatie.

Het artikel *Beveiligingsbeleid geautomatiseerde informatievoorziening* van mevrouw D. Jansen Heijtmajer RI [Heijt91] in Compact 91/3 gaf een uitstekend beeld van de vorming van beveiligingsbeleid, geënt op het doel van de organisatie en beleid in het algemeen.

Dit artikel tracht aan te tonen dat een meer bottom-up aanpak ook mogelijk is, gezien vanuit een IS-servicegroep (Servicegroep Informatiesystemen).

In het genoemde artikel werd beargumenteerd gekozen voor de zogenaamde procesbenadering, ook wel genoemd systeembenadering, boven de eveneens kort beschreven activabenadering. Naast deze twee meest gebruikte wijzen van benaderen worden in de literatuur, zoals in het recente studierapport van de NGI-sectie EDP-Auditing [NGI91], nog enkele andere benaderingen onderscheiden, waaronder de doelstellingenbenadering en de gevarenbenadering. Over het algemeen wordt daarbij gesteld dat de voorkeur voor een bepaalde benadering wordt bepaald door zowel de achtergrond van de uitvoerder als de te bestuderen situatie.

Dit artikel schetst een praktisch voorbeeld van een poging de bovengenoemde benaderingen te combineren, gebruik makend van een beveiligingsmodel.

In de titel is bewust gekozen voor de neutrale termen "gegevens en gegevensverwerking" in plaats van "informatie" of "informatievoorziening". Onder informatie wordt immers meestal verstaan datgene wat mensen interpreteren en concluderen uit onder andere gegevens.
In deze strikte zin is informatie niet hetgene wat we pretenderen te beveiligen.

ONTSTAAN VAN DE BELEIDSVORMING

Het eerste thema van dit artikel betreft het vormen van beveiligingsbeleid in een relatief weinig gevoelige omgeving, waar bovendien sprake is van een "gekantelde" organisatie. De schets hiervan vindt plaats tegen een meer algemene beschouwing.

In een klassieke, functioneel gestructureerde grote organisatie wordt deelbeleid op allerlei gebieden als vanzelfsprekend opgepakt door de voor dat deelgebied aanwezige afdeling. De adviezen of beleidsvoorstellen vanuit de functies worden door het topmanagement weliswaar financieel getoetst, maar veelal niet echt inhoudelijk beschouwd, vooral als de indruk overheerst dat het gaat om een "technische" zaak. Temeer als het een weinig concreet voorstelbaar onderwerp betreft of de financiële consequenties niet expliciet blijken, wordt gaarne de verantwoordelijkheid aan de functie overgelaten.

In zo'n organisatie hebben de functies, mede door het genoemde verschijnsel, een zekere macht om buiten expliciete toestemming van het topmanagement andere afdelingen bepaalde zaken of handelwijzen op te dringen. Op de functiegebonden zaken wordt zodoende een stuk verantwoordelijkheid voor de totale organisatie genomen. Mede hierdoor wordt het beleid niet altijd duidelijk en expliciet geformuleerd. De functie doet naar beste vak-"eer en geweten" haar best, hetgeen - objectief beschouwd - vaak inderdaad tot een goede situatie leidt.

Bij een meer zelfstandig resultaatverantwoordelijke indeling van een organisatie worden de oude "technische" functies verdeeld over de resultaatgroepen, dan wel apart gehandhaafd als, overigens zelf ook resultaatverantwoordelijke, service-afdelingen. Tussen de service-afdeling en haar interne "klanten" heerst een meer met de buitenwereld vergelijkbaar relatiepatroon, ook wel aangeduid met "klant/leverancier-relatie".

Bij overgang van de functionele naar de resultaatgebiedsorganisatie valt een aantal vanzelfsprekendheden, zoals vele vormen van centraal bepaald deelbeleid, officieel weg, maar leeft daarentegen in de gewenningsperiode nog voort. De servicefuncties staan voor de situatie hun beleid meer expliciet te maken en bovendien te "verkopen" aan de klanten en, voor zover nog nodig, aan het topmanagement.

Een beveiligingsbeleid is, weliswaar enigszins vereenvoudigd beschouwd, een typisch voorbeeld van bovenstaande ontwikkeling. Zeker in een relatief weinig gevoelige basisindustriële omgeving was beveiliging van gegevens en gegevensverwerking grotendeels een functionele aangelegenheid. Een expliciet geformuleerd bedrijfsbeleid ontbrak dan ook in dit licht.

Een geheel andere invalshoek betreft het in de afgelopen jaren meer in de belangstelling staan van beveiliging van gegevens en gegevensverwerking in het algemeen. Diverse elders beschreven ontwikkelingen geven aanleiding nadrukkelijker dan voorheen geordende aandacht aan dit onderwerp te besteden.

Voor het in dit artikel onderhavige bedrijf golden beide bovenbeschreven omstandigheden vrijwel gelijktijdig, hetgeen leidde tot het initiatief vanuit de IS-functie, thans IS-servicegroep, een beveiligingsbeleid te vormen, dat in dit artikel verder zal worden beschreven.

METABELEID

Het tweede thema van dit artikel betreft de manier waarop beleidsformulering vanuit een deel van de organisatie kan plaatsvinden. In deze paragraaf komt de legitimering ervan aan de orde, gevolgd door de inhoudelijkheid in de paragraaf Beleid.

Zoals in het artikel *Beveiligingsbeleid geautomatiseerde informatievoorziening* uitgebreid is toegelicht, dient deelbeleid, zoals bijvoorbeeld beveiligingsbeleid, afgeleid te zijn van het beleid van de organisatie als geheel. Zoals in de paragraaf Ontstaan van de beleidsvorming is besproken, blijkt het in de praktijk een illusie, dit principe altijd te volgen. Indien een onderdeel van de organisatie een deelbeleid tracht te vormen ontbreekt, zeker in eerste instantie, deze rechtstreekse hiërarchische relatie. Het is echter een bekend feit dat goede dingen zowel top-down als bottom-up tot stand kunnen komen.

Een wellicht wat formalistisch aandoende uitweg uit dit dilemma is het naast het eigenlijke deelbeleid formuleren van metabeleidspunten. Een metabeleid zegt iets over de omgeving waarin het deelbeleid wordt gepositioneerd, welke voorwaarden en veronderstelde uitgangspunten gelden en de wijze waarop met het eigenlijke deelbeleid wordt omgegaan.

In de voorbeeldsituatie waarvan in dit artikel wordt uitgegaan, is een aantal metabeleidspunten geformuleerd. De eerste betreffen de positionering:

- De voorkeur van de IS-servicegroep gaat uit naar een informatiebeveiligingsbeleid op bedrijfsniveau. Het beveiligingsbeleid van de IS-servicegroep zou daaraan ondergeschikt moeten zijn.

- Zolang en voor zover het bedrijf geen expliciet en integraal beleid ten aanzien van dit onderwerp heeft geformuleerd, acht de IS-servicegroep het tot haar verantwoordelijkheid behoren op eigen initiatief een beleid te voeren.
Deze verantwoordelijkheid wordt enerzijds afgeleid van het onderdeel van de doelstelling van de IS-servicegroep een interne kwaliteitsleverancier te zijn. Beveiliging wordt daarbij geacht een onderdeel van kwaliteit uit te maken. Anderzijds geldt dat de IS-servicegroep, als deel van de totale organisatie, toch nog een zekere vakverantwoordelijkheid draagt.

– De IS-servicegroep tracht voor het bovenstaande aandacht te krijgen van het topmanagement.

Deze drie punten gelden meer als mededeling dan als aan het topmanagement voor te dragen beslispunten. Zij zijn namelijk rechtstreeks afleidbaar van reeds gegeven opdrachten.

Deelbeleid kan worden gevoerd zonder hiervoor expliciete goedkeuring van het topmanagement te hoeven vragen.

Vervolgens geldt een aantal metabeleidspunten ten aanzien van veronderstelde uitgangspunten:

– De IS-servicegroep gaat ervan uit dat het lijnmanagement verantwoordelijk is voor beveiliging in het algemeen en dus ook voor wat betreft gegevens en gegevensverwerking. Een deel van de uitvoering wordt uitbesteed aan de IS-servicegroep.

– De IS-servicegroep gaat ervan uit dat haar interne klanten zelf attent zijn op specifieke extra in- of externe eisen, die aan de beveiliging worden gesteld. De IS-servicegroep zal naar vermogen meedenken, maar kan onmogelijk gehouden worden deze eisen op alle mogelijke gebieden te kennen.

Voor deze twee punten, waarbij het tweede eigenlijk nog afleidbaar is van het eerste, geldt dat zij zo logisch zijn en bovendien impliciet voortvloeien uit de gekozen organisatiestructuur van het bedrijf, dat goedkeuring ervan niet nodig lijkt.

Ter verduidelijking van de uit het bovenstaande voortvloeiende praktische positie en ter explicitering van de grenzen van haar beleid zijn de volgende punten toegevoegd:

Het beleid van de IS-servicegroep strekt zich uit tot:
- de onder de servicegroep ressorterende c.q. door haar in regie uitgevoerde activiteiten;
- advies aan (interne) klanten voor daarbuiten liggende zaken;
- eventueel advies aan het topmanagement.

In lijn hiermee geldt ten aanzien van de door de IS-servicegroep te treffen beveiligingsmaatregelen bij het uitvoeren van diensten voor de (interne) klanten:
- er worden autonoom standaardmaatregelen genomen, die voor alle klanten gelden;
- er worden specifieke maatregelenopties geboden, die expliciet door de klant kunnen worden gekozen;
- er worden hulpmiddelen ter beschikking gesteld, waarmee de klant zelf de door hem gewenste beveiliging kan kiezen.

Tot slot is een aantal metabeleidspunten geformuleerd aangaande de wijze waarop het beleid zal worden uitgedragen en betreffende enkele specifieke afspraken met andere afdelingen binnen het bedrijf. Deze punten lenen zich niet voor openbaarmaking, behalve het volgende:

– Voor het uitdragen van het beveiligingsbeleid aan de klanten zal geen losstaande algemene voorlichtingsronde worden geïnitieerd. De applicatieontwikkelingsfunctionarissen van de IS-servicegroep zullen dit in hun normale contactpatroon met de klant meenemen.

De in deze paragraaf besproken metabeleidspunten vormen in de praktijk natuurlijk een geheel met de eigenlijke beleidspunten. Het is meer de wijze van ontstaan en de beoogde zuiverheid van redeneren, die aparte behandeling en betiteling vergen. Voorts is aangetoond dat een servicegroep deelbeleid kan voeren zonder hiervoor expliciete goedkeuring van het topmanagement te hoeven vragen.

BELEID

Na de positionering door middel van metabeleid komt thans de inhoudelijke kant aan de orde.

Er zijn twee visies mogelijk omtrent het begrip beleid. De ene visie gaat ervan uit dat het bepalen van de doelstelling de eerste stap van beleidsvorming is. De andere visie stelt de formulering van de doelstelling apart en acht beleid beperkt tot het aangeven van de wijzen waarop de doelstelling bereikt dient te worden.

Bij het onderwerp "beveiliging" is formulering van het doel hetzij vrijwel nietszeggend - het tot een aanvaardbaar niveau beperken van risico's - , hetzij in termen van te nemen acties en dus eigenlijk beleid. Men vergelijke dit bijvoorbeeld met een wel duidelijk bedrijfsdoel: het verkopen van x ton produkt y in het volgende jaar.

De conclusie is dat doel en beleid niet goed te scheiden zijn bij het onderwerp beveiliging. De formulering in het onderhavige voorbeeld is dan ook een variant op de bekende vorm.

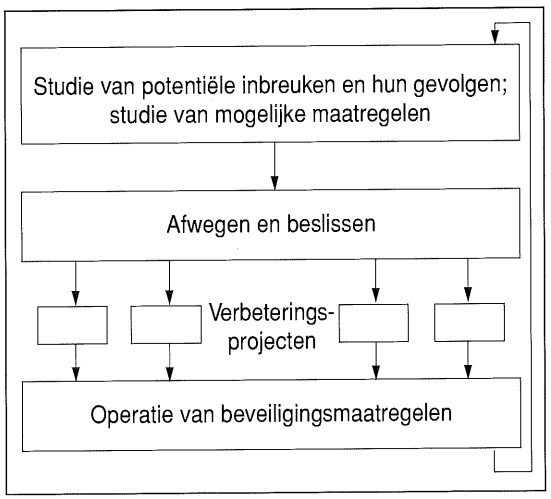
Doelstelling: het *beheersbaar* hebben van *risico's* ten aanzien van gegevens en gegevensverwerking.

Risicobeheersing is:
- het bewust, integraal en dynamisch *onderkennen* van potentiële inbreuken en hun gevolgen;
- het *introduceren* en
- het *handhaven* van een evenwichtig samenstel van maatregelen om de schade te beperken tot een voor het management aanvaardbaar niveau.

Men merke op dat het woord risico alleen in de eerste zin voorkomt in samenhang met beheersen en vervolgens direct als samenstel wordt gedefinieerd. Dit is een bewuste vermijding van het onduidelijke en voor meerdere uitleg vatbare begrip risico.

Het gebruik van woorden als inbreuk en schade zal in de paragraaf Beveiligingsmodel worden verduidelijkt.
Verdere uitleg van deze definitie is in dit blad overbodig. Bij interne voorlichtingen in het bedrijf wordt uiteraard wel stilgestaan bij enkele van de vele in de korte formulering toch aanwezige elementen.

De splitsing in drie subzinnen is een poging de dynamiek van het proces aan te geven. De dynamiek is echter beter in schemavorm weer te geven, zoals in figuur 1 wordt getoond.



Figuur 1. Dynamiek van het proces.

Naast het formuleren van de doelstelling behoren tot het in deze paragraaf besproken beleid slechts een constatering en een beperkt aantal beleidspunten.

Er wordt geconstateerd dat er al lange tijd aandacht is geschonken aan beveiliging en dat veel maatregelen zijn genomen, zij het niet vanuit expliciet geformuleerd beleid. Bovendien verricht de sectie EDP-auditing van de interne accountantsdienst van het concern regelmatig onderzoeken naar specifieke aspecten en systemen. Haar rapporten worden steeds in onderling overleg voorzien van een actieplan van de IS-servicegroep. Er vinden bovendien voortdurend verbeteringen plaats vanuit vakmanschap en het meegroeien met de stand van de techniek.

Toch wordt deze situatie in het licht van de doelstelling als onvoldoende ervaren. Het is namelijk onzeker of geen belangrijke risico's over het hoofd zijn gezien. Daarom is in de *eerste plaats* besloten de eerder gestarte top-down studie voort te zetten. In de paragraaf Praktische toepassingen is een mogelijke werkwijze hiervoor beschreven.

In de *tweede plaats* zijn een organisatie en een taakverdeling ten aanzien van beveiliging binnen de IS-servicegroep bepaald. De diverse lijn(sub-)afdelingen zijn daarbij verantwoordelijk voor de uitvoering, instandhouding en operationele sturing van bestaande maatregelen. Een commissie, waarin enkele afdelingsmanagers alsmede deskundigen zitting hebben, stuurt namens de afdelingsleiding het verbeteringstraject. De afdeling Kwaliteitszorg voert incidenteel audits uit op het bovenstaande.

In de *derde plaats* is een aantal methodologische afspraken gemaakt, waaronder de volgende:
- er wordt een beveiligingsmodel gekozen, zoals in de volgende paragrafen beschreven;
- er wordt *niet* gekozen voor de minimum standaardbenadering;
- er wordt *niet* geforceerd voor alles een financiële of anderszins cijfermatige waardering gezocht;
- er worden zelf geen inbreukpogingen opgezet met quasi-malafide middelen.

BEVEILIGINGSMODEL

Na de behandeling van de eerste twee thema's van dit artikel betreffende beleidsvorming volgt thans het derde thema, een wijze van benaderen van de beveiligingsmaterie, ofwel het hanteren van een bepaald beveiligingsmodel.

In veel artikelen omtrent beleid, risico-analyse en het kiezen van maatregelen wordt geworsteld met het begrippenkader. Eenduidigheid is nog niet bereikt, hetgeen wellicht eigen is aan aard en leeftijd van het vakgebied. Kuiper [Kuip89] is in dit blad in 1989 reeds uitgebreid ingegaan op deze problematiek.

Toch is het aanbevelenswaardig binnen een organisatie een keuze te maken voor een bepaald denkmodel. Zo'n denkmodel dient ten minste de volgende zaken goed te ondersteunen:
- het efficiënter kunnen voeren van discussies en het sneller leiden tot de essenties;
- het toetsen van ad hoc aangedragen vraagstukken en voorgestelde oplossingen;
- het ordelijk kunnen uitvoeren van integrale analyses.

In de voorbeeldsituatie van dit artikel is een bepaalde keuze gemaakt uit de beschikbare begrippen, zijn eigen accenten toegevoegd en is een nieuwe wijze van representeren ontworpen.

In het vervolg van deze paragraaf komen de elementen van het model aan de orde, in de eerste plaats een aantal hoofdbegrippen, vervolgens enkele intermediaire begrippen en tot slot een schema dat het verband tussen deze begrippen aantoont. In de paragraaf Praktische toepassing zal het gebruik van het model aan de orde komen en zal toetsing plaatsvinden van de bovengenoemde doelstellingen van het model.

Tot slot zal in de paragraaf Ruimtelijk beveiligingsmodel als toegift een meer mathematisch georiënteerde representatie aan de orde komen.

Ontstaanswijze van de hoofdbegrippen

De hoofdbegrippen van beveiliging kunnen ten to-

nele worden gevoerd door het werkwoord "beveiligen" in taalkundig verband te beschouwen en enkele in dat kader logische vragen te stellen. De antwoorden dienen te luiden in de meest neutrale en ultieme termen.

De eerste vraag is: "Wat moet beveiligd worden?"
Het meest neutrale antwoord hierop is ongetwijfeld *objecten van beveiliging*.

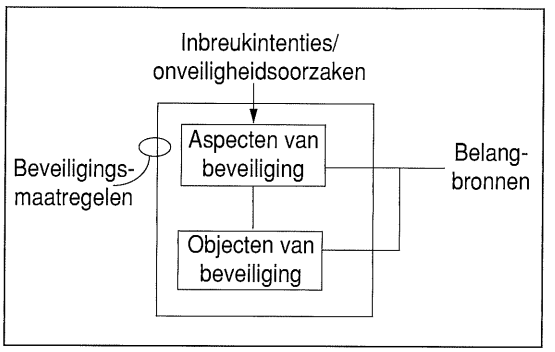
De tweede vraag is: "Ten aanzien van wat moeten de objecten beveiligd worden?"
Het meest neutrale antwoord hierop lijkt *aspecten van beveiliging*.

De derde vraag is: "Waarom moet beveiligd worden?"
Een neutraal en ultiem antwoord is, dat er bronnen moeten zijn, van waaruit belang kan worden gehecht aan beveiligen, kort gezegd: *belangbronnen*.

De vierde vraag is: "Tegen wat moet beveiligd worden?"
Een neutraal en ultiem antwoord is, dat er sprake is van *inbreukintenties of onveiligheidsoorzaken*.

De vijfde vraag is: "Waarmee moet beveiligd worden?"
Het antwoord hierop is natuurlijk *beveiligingsmaatregelen*.

Figuur 2 toont de meest simpele visualisatie van de antwoorden op de basisvragen.



Figuur 2. Hoofdbegrippen in schema.

De aspecten van objecten worden met beveiligingsmaatregelen beveiligd tegen inbreukintenties/onveiligheidsoorzaken teneinde de belangbronnen te dienen.

Toelichting en globale decompositie van de hoofdbegrippen

De aldus ontstane hoofdbegrippen vergen nadere toelichting en voor praktisch gebruik een zekere decompositie. Het gaat in deze paragraaf slechts om het overbrengen van de basisgedachte; volledige uitwerking vindt niet plaats.

Objecten van beveiliging
De lezer merke op dat de hoofdbegrippen geenszins beperkt zijn tot informatiebeveiliging. Pas door definiëring van de objecten krijgt het model een gebiedsgebonden karakter.

In dit geval beperken we ons tot het gebied "gegevens" en "gegevensverwerking". Fundamenteel geredeneerd vormen semantische inhoudelijkheden van gegevens en gegevensverwerking het primaire onderwerp. Meer praktisch is het, ook syntactisch geordende logische objecten als data en programma's te beschouwen. Deze zijn op hun beurt geïmplementeerd op fysieke objecten als papier, schijven, computersystemen, netwerken, ook wel genoemd "media". Zelfs de mens is te beschouwen als medium, waarop logische objecten als kennis en redeneren zijn geïmplementeerd. Al deze media zijn evenwel weer afhankelijk van fysieke objecten als airconditioning, gebouwen en kabelgoten, kortom "faciliteiten".

Al deze typen objecten vormen potentieel onderwerp van beveiliging, hetgeen leidt tot de volgende lijst:

Logische objecten:
- signalen;
- data;
- programma's, instructies;
- kennis.

Fysieke objecten:
- media (papier, disks, tapes);
- klassieke objecten (hangmap, kast, kluis);
- computersystemen;
- netwerken;
- faciliteiten;
- de mens.

Men realisere dat hierbij gekozen is voor een bottom-up aanpak. De begrippen (applicatie)systeem of proces komen niet voor, maar zijn hogere ordeningen van verzamelingen van logische detailobjecten.
Zorgvuldig is ook het gebruik van termen als "activa" of "assets" vermeden, aangezien deze in de eerste plaats niet waardevrij zijn en in de tweede plaats door niet-accountants vrijwel niet in deze zin worden verstaan.

Aspecten van beveiliging
Binnen het kader van het terrein van gegevens en gegevensverwerking is niet alles wat fout kan gaan voor elk object interessant. Overeenkomend met gangbare EDP-literatuur is de meest praktische decompositie:
- betrouwbaarheid;
- continuïteit;
- exclusiviteit.

Exclusiviteit is hierbij een bijzonder aspect aangezien het zowel op zichzelf staand als de andere aspecten dienend kan voorkomen.

Belangbronnen
De belangbron is de oorsprong van het belang dat gediend wordt met beveiliging. Een praktische decompositie is de volgende:

Externe belangbronnen (van buiten het bedrijf afkomende eisen, waaraan moet worden voldaan):
- wettelijke;
- civiel-rechtelijke (contracten);
- overige.

Interne belangbronnen (die het bedrijf vanuit zijn eigen doelstellingen heeft):
- met betrekking tot directe financiële schade: fraude, industrieel eigendom, directe herstelkosten;
- met betrekking tot directe gevolgschade: ongestoorde operatie, juistheid van bedrijfsvoering, efficiëntie van bedrijfsvoering;
- met betrekking tot indirecte gevolgschade: externe concurrentie, imago en marktpositie, onderhandelingspositie.

Inbreukintenties/onveiligheidsoorzaken
In veel artikelen worden begrippen als bedreiging of zelfs risico gebruikt om aan te geven waartegen moet worden beveiligd. Meer neutraal en ultiem kunnen woorden als "intentie" of "oorzaak" worden gebruikt. Intentie is daarbij beperkt tot bewuste menselijke strevingen, terwijl oorzaak zowel menselijk onbewust of onbedoeld als zakelijk kan zijn. Het is daarbij jammer dat de Nederlandse taal (evenmin als de Engelse overigens) geen verzamelwoord voor beide categorieën kent.
In sommige talen en culturen kunnen "dingen" ook intenties hebben.

Beveiligingsmaatregelen
Het lijkt praktisch beveiligingsmaatregelen enerzijds te decomponeren naar werkingsdomein en anderzijds naar werkingsprincipe. Beide decomposities vormen te zamen een tweedimensionale matrix.

Naar werkingsdomein:
- *technische maatregelen:*
  - fysieke maatregelen (bijvoorbeeld slot op PC);
  - logische maatregelen (bijvoorbeeld password);
- *niet-technische maatregelen:*
  - organisatorische;
  - juridische.

Naar werkingsprincipe:
- *preventieve maatregelen:*
  - afschrikking;
  - uitsluiting/verhindering;
- *niet-preventieve maatregelen:*
  - bijvoorbeeld detectieve en correctieve maatregelen.

Het probleem bij werkingsprincipe is dat het woord preventief over het algemeen eenduidig wordt verstaan, maar dat de tegenhanger meestal met begrippen wordt aangeduid, die hetzij elkaar niet uitsluiten, hetzij niet eenduidig zijn. Het woord "repressief" heeft bijvoorbeeld te veel bijbetekenis. Om deze reden is gekozen voor het neutrale "niet-preventief".

Beide hoofdcategorieën zijn zodanig anders van aard dat eigenlijk zelfs sprake is van twee afzonderlijke hoofdbegrippen, zoals hierna verder zal worden toegelicht.

Intermediaire begrippen

Door min of meer taalkundig "wat-vragen" te stellen met betrekking tot het werkwoord beveiligen kwam een aantal hoofdbegrippen naar voren. Vragen naar de relaties tussen deze begrippen binnen het totale *proces* beveiligen levert vervolgens een aantal intermediaire begrippen op.

Men kan zeggen dat een bepaald aspect van een bepaald object een *specifiek belang* heeft ten opzichte van een bepaalde belangbron.
Het specifieke belang is het eerste intermediaire begrip. De som van alle specifieke belangen van een object over alle aspecten en belangbronnen heen is dan het totale belang van dat object.

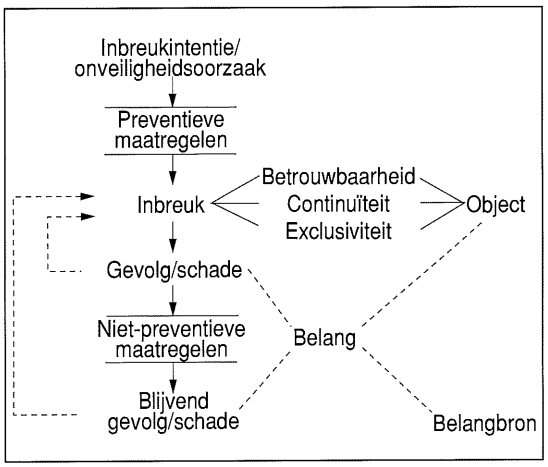
Evenzo kan men zeggen dat de relatie van een inbreukintentie/onveiligheidsoorzaak met een bepaald aspect van een bepaald object wordt gerepresenteerd door het begrip *inbreuk*, preciezer uitgedrukt *specifieke inbreuk*. De specifieke inbreuk is het tweede intermediaire begrip.

Tot slot kunnen deze beide begrippen onderling weer worden gerelateerd. Men kan dan zeggen, dat een specifieke inbreuk ten opzichte van een specifiek belang een *specifieke schade* oplevert. Hiermee ontstaat het derde intermediaire begrip. Soms is niet zozeer meteen sprake van schade, maar slechts van gevolgen. Een gevolg kan bijvoorbeeld het veroorzaken van een inbreuk op een ander object zijn.

Verbandschema

De oorspronkelijke zes hoofdbegrippen, met preventieve en niet-preventieve maatregelen daarbij afzonderlijk geteld, vormen samen met de intermediaire begrippen een negental met elkaar samenhangende elementen van het beveiligingsproces. De visualisatie van figuur 3 verschaft hiervan een overzicht in het platte vlak.

Figuur 3. Verbandschema.



Het verbandschema dient van boven naar beneden te worden gelezen. Inbreukintenties/onveiligheidsoorzaken worden zo mogelijk tegengehouden door preventieve maatregelen. Indien dit niet lukt, treedt een inbreuk op ten aanzien van één of meer aspecten van een object. De inbreuk veroorzaakt directe schade of gevolgen. De schade wordt bepaald door de specifieke belangen, die op hun beurt worden bepaald door de belangbronnen in relatie tot de objecten. Het directe gevolg kan een inbreuk op een ander object betekenen, aangegeven door de relatiepijl terug van gevolg naar inbreuk. Vervolgens treden niet-preventieve maatregelen in werking met als resultaat al of niet blijvende schade of gevolgen.

PRAKTISCHE TOEPASSING

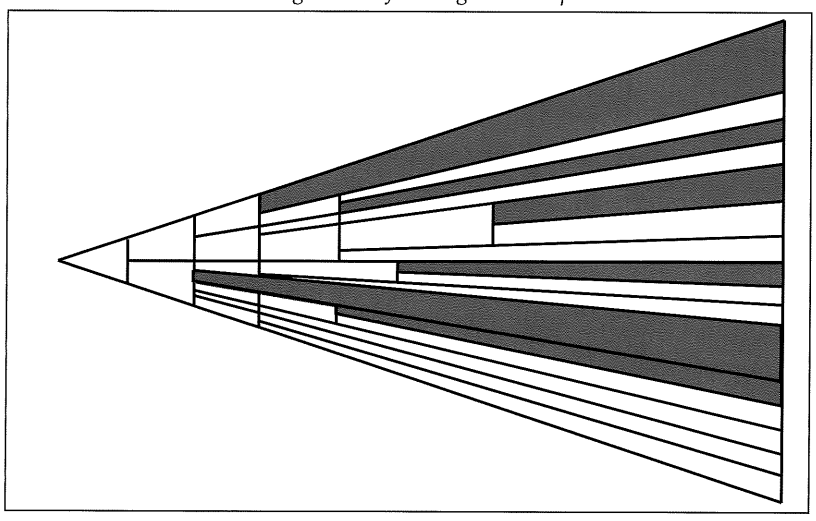
Zoals in de inleiding van de paragraaf Beveiligingsmodel is vermeld, dient een denkmodel ervoor discussies efficiënter te voeren, ad hoc-kwesties gemakkelijker te doorzien en integrale analyses te kunnen uitvoeren. Ter verduidelijking volgen enkele toepassingsvoorbeelden, te beginnen met het laatste, de integrale analyse.

Integrale analyse

Tijdens het ontwikkelen van het Beveiligingsbeleid is een top-down studie gestart. Zorgvuldig is hierbij de term "risico-analyse" vermeden om begripsverwarring te voorkomen. Thans kan mede aan de hand van het model kort worden toegelicht wat in dit geval voor ogen stond, gevolgd door enkele voorbeelden.

Als eerste stap worden de hoofdbegrippen afzonderlijk bestudeerd. Zij worden top-down gedecomponeerd, waarbij op zo hoog mogelijk niveau een oordeel wordt gevormd en een (beleids)uitspraak wordt gedaan. Het is hierbij van groot belang zodanige uitspraken te doen, dat het gehele veld onderliggende details wordt afgedekt. In eerste instantie wordt hierbij uitgegaan van de bestaande situatie met betrekking tot de maatregelen. In figuur 4 is getracht de werkwijze te visualiseren.

Figuur 4. Afdekking door uitspraken.



De gearceerde gedeelten zijn afgedekt door uitspraken.

Als tweede stap kan een drietal analyses worden uitgevoerd, waarbij de intermediaire begrippen en de maatregelen centraal staan:
- een analyse van het verband tussen belangbronnen en objecten met hun aspecten (belangenanalyse);
- een analyse van het verband tussen inbreuken, niet-preventieve maatregelen en de schade;
- een analyse van het verband tussen inbreukintentie/onveiligheidsoorzaak, preventieve maatregelen en inbreuken.

Ook deze analyses worden top-down uitgevoerd, waarbij elke gewenste ordening of decompositie kan worden toegepast die resultaat oplevert. De bijvoorbeeld bij de belangenanalyse toegepaste ordening behoeft geenszins de basis te vormen voor de analyse van inbreuken en niet-preventieve maatregelen.
Men merke op dat door het bestuderen van alle begrippen afzonderlijk, er geen sprake is van één bepaalde benadering, zoals activa- of procesbenadering. In feite worden alle benaderingen parallel opgepakt, echter tot op zekere mate van detail.
Een aantal op deze plaats niet openbaar te beschrijven belangrijke ombuigingen en het beter kunnen inkaderen van onderhanden werk vormen reeds het resultaat van het top-gedeelte van deze studie. Aan het down-gedeelte wordt - zij het met minder prioriteit en daardoor in langere doorlooptijd - gewerkt.

Voorbeelden analyses

Gezien de aard van het onderwerp kunnen in het openbaar slechts enkele, niet geheel representatieve voorbeelden worden gegeven.

Bij de bestudering van *objecten*, subcategorie faciliteiten, wordt bijvoorbeeld ten aanzien van elektriciteitsvoorziening de uitspraak gedaan dat gezien de aard, inrichting en werkwijze van het bedrijf extra aandacht voor computersystemen buiten het normaal gebruikelijke niet nodig is.
Ten aanzien van logische objecten, subcategorie historische gegevens die niet van andere zijn af te leiden, is besloten een speciale studie te starten.

Bij de bestudering van *aspecten*, categorie exclusiviteit, wordt uitgesproken dat aangezien het overgrote deel van de gegevens niet zeer gevoelig is en de maatregelen daarvoor adequaat zijn, besloten wordt de hoogst gevoelige gegevens niet in gemeenschappelijk gebruikte omgevingen op te nemen.

Bij de bestudering van *inbreukintenties* wordt de categorie "menselijk opzettelijk" verder gedecomponeerd volgens de "formule":

mensen × motieven = daden → inbreuken

Bestudering van categorieën mensen levert bij-

voorbeeld de uitspraak: "Opnemen op actielijst: situatie rond systeemprogrammeurs nog eens bekijken".

Bestudering van motieven levert bijvoorbeeld de uitspraak: "Ten aanzien van irrationele en ideële motieven wordt uitgesproken dat buiten de normale geen extra preventieve maatregelen worden genomen. Wel is besloten een studie naar signalerende maatregelen uit te voeren."

Bij de bestudering van *belangbronnen* wordt ten aanzien van de categorie ongestoorde fabrieksoperatie vastgesteld, dat de continuïteitseis voor de meeste betrokken geautomatiseerde systemen in verhouding moet worden gezien met de beschikbaarheden van de fabrieksinstallaties zelf. In zijn algemeenheid rechtvaardigt dit geen dubbele systemen.

Bij de bestudering van *maatregelen* wordt uitgesproken dat voor externe verbindingen naast authenticatie door middel van passwords tevens controle op afzenderadres zal plaatsvinden, bijvoorbeeld door middel van terugbelapparatuur.

Bij de verbandstudie van *inbreuken, niet-preventieve maatregelen en schade* wordt uitgesproken, dat het bedrijf 24 uur per dag met eigen mankracht in staat is omvangrijke reparaties/herstelacties te verrichten aan decentrale hardware. Tevens zijn adequate voorraden reservedelen aanwezig. Geconcludeerd wordt dat daarenboven geen extra niet-preventieve maatregelen nodig zijn.

Bij de verbandstudie van *inbreukintenties, preventieve maatregelen en inbreuken* wordt uitgesproken dat voor de decentrale systemen de logische beveiliging procedureel nog iets verder moet worden ontwikkeld.

In zijn *algemeenheid* is geconstateerd, dat in een matig gevoelige omgeving met redelijke niet-preventieve maatregelen, de preventieve maatregelen al snel adequaat kunnen zijn. Dit bespaart potentieel veel kosten en moeite.

Voorbeelden ad hoc-zaken en discussies

Ook in deze categorie kunnen slechts enkele, niet geheel representatieve voorbeelden worden gegeven.

Men is geneigd de voorbereiding van niet-preventieve maatregelen preventief te noemen. Vage redeneringen omtrent kans op inbreuk worden daarbij vaak mede betrokken. Toch is het maken van onderscheid erg belangrijk. Zo is het maken van backups geen preventieve maatregel, maar de voorbereiding van een niet-preventieve: het restoren. Dit dient te allen tijde te geschieden, los van de kansen op inbreuken.

Als reactie op een intern accountantsonderzoek is nog eens expliciet vastgesteld dat er niet vóóraf fijnzinnige prioriteitenlijsten worden gemaakt voor het reactiveren van de verschillende (applicatie)systemen na een grote calamiteit. Het hiervoor benodigde werk en de moeizame discussies met interne klanten worden niet in verhouding geacht tot het nut ervan.

In een matig gevoelige omgeving met redelijke niet-preventieve maatregelen kunnen de preventieve maatregelen al snel adequaat zijn.

Toetsing nut van het model

Hopelijk is aan de hand van de voorbeelden met betrekking tot analyses en ad hoc-zaken in deze paragraaf aan de lezer enigszins verduidelijkt, wat voor soort uitspraken mogelijk zijn. Tevens is de mogelijkheid van ordelijke ophanging aan elementen van het model getoond. Het eigenlijke nut van het model treedt echter op in het proces om te komen tot de uitspraken, met andere woorden bij de discussies. Er wordt daarvoor een beroep gedaan op het voorstellingsvermogen van de lezer, aangezien een meer precieze beschrijving van dat proces in dit korte bestek niet mogelijk is.

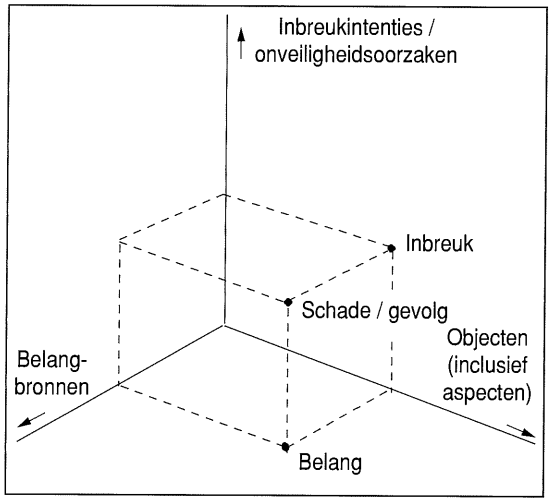
RUIMTELIJK BEVEILIGINGSMODEL

Deze paragraaf is bedoeld als toegift voor geïnteresseerden. Hij behoort niet onlosmakelijk bij de hoofdthema's van dit artikel.

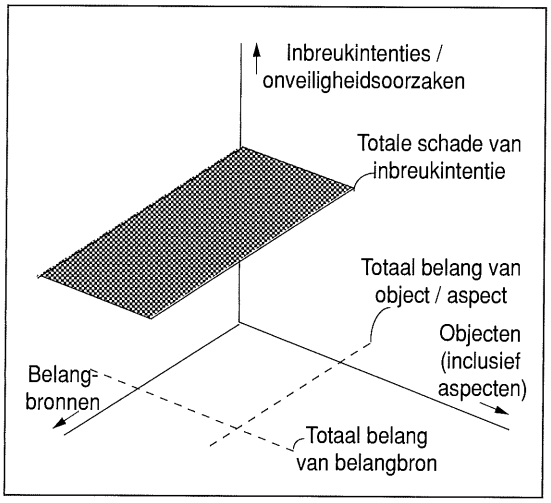
Uitgaande van dezelfde begrippen als genoemd in voorgaande paragrafen, is een andere representatiewijze mogelijk, die geënt is op een meer mathematische voorstelling van zaken. Dit artikel pretendeert echter niet een volledig sluitend en rigoureus mathematisch model te presenteren. Het gaat meer om een wijze van denken, die verhelderend kan zijn. In de praktijk is gebleken dat sommigen hiermee worden geholpen, maar dat anderen in verwarring raken. De lezer die moeite ondervindt, zij dus bij voorbaat geëxcuseerd.

Men stelle de totale beveiligingswereld voor als een eindige discrete multidimensionele ruimte, bespannen door de oorspronkelijke zes hoofdbegrippen, waarbij preventieve en niet-preventieve maatregelen apart tellen.
Discreet betekent dat op de assen geen continu variabele waarde wordt ingenomen, maar dat alle bestaanbare voorkomens van de dimensie naast elkaar staan. Sortering of ordening kan op elke gewenste manier plaatsvinden. Op de as "objecten" staan bijvoorbeeld alle denkbare logische en fysieke objecten op een rij, mogelijk geordend volgens de beschreven decompositie.

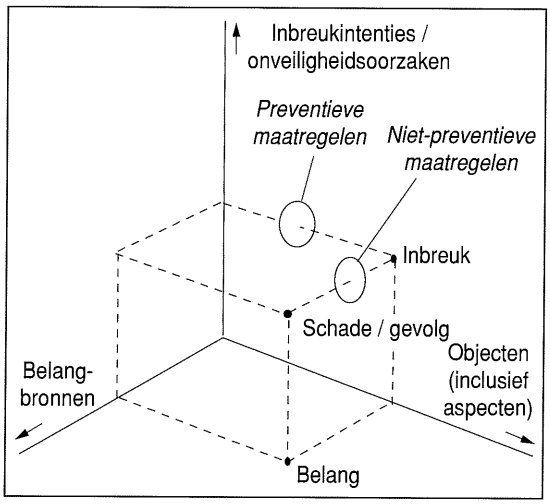
Een punt in deze ruimte verbindt specifieke voorkomens van de dimensies. De continuïteit (aspect) van een PC-programma (logisch object) kan bij-



Figuur 5. Ruimtemodel.



Figuur 6. Integraties in het ruimtemodel.



Figuur 7. Maatregelen symbolisch aangegeven.

voorbeeld tegen een virus worden beveiligd (onveiligheidsoorzaak) door geen spelletjes te spelen (preventieve maatregel) en goede backup- en restore-procedures te hebben (niet-preventieve maatregel) teneinde de effectiviteit van de bedrijfsvoering (belangbron) te dienen.

Het "resultaat" ofwel de waarde van het specifieke punt in de ruimte kan worden beschouwd als de zevende dimensie, anders gezegd als een functie in de mathematische zin van de zes hoofdbegrippen. Deze zevende dimensie representeert het begrip (blijvende) schade.

(blijvende) specifieke schade = f (dim1, dim2, dim3, dim4, dim5, dim6)

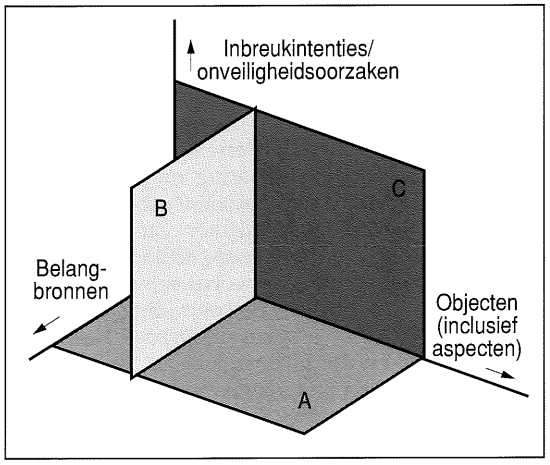
Deze beschreven ruimte is in zijn algemeenheid erg leeg. Slechts een relatief beperkt aantal punten heeft een zinnige betekenis. Bovendien is de praktische bepaalbaarheid van de specifieke schade alsmede het nut ervan niet duidelijk. Wel interessant zijn bepaalde integraties, of beter gezegd discrete sommaties, over lijnen, vlakken en meerdimensionele subruimten. Door integratie ontstaan zinvolle begrippen zoals de totale blijvende schade ten opzichte van een bepaalde belangbron over alle objecten, aspecten, maatregelen, etc. heen.

Tot zover lijkt het model wellicht vergezocht en erg theoretisch. We proberen daarom een meer inzichtelijke manier van voorstellen door het tekenen van de ruimte. Nu is een ruimte met meer dan drie dimensies op papier niet te tekenen, zodat bepaalde dimensies moeten worden weggelaten of samengetrokken met andere.
Zo trekken we objecten en hun aspecten samen op één as, laten in eerste instantie de maatregelen weg en stellen ons de zevende dimensie, de schade, voor als gerepresenteerd door het punt in de ruimte. Daarmee ontstaat de tekenbare driedimensionele ruimte van figuur 5.
Het aardige van deze ruimte is het feit dat de geïntroduceerde intermediaire begrippen hun plaats krijgen, zoals is aangegeven. De inbreuk bijvoorbeeld is immers de combinatie, ofwel het snijpunt, tussen inbreukintentie en object/aspect.

Integratie over één of meer dimensies is in figuur 6 aangegeven met vlakken en lijnen.

In de subruimte kunnen de beide typen maatregelen hun plaats krijgen volgens figuur 7. De preventieve maatregelen "staan" tussen de inbreukintentie en de inbreuk zelf. De niet-preventieve maatregelen staan tussen de inbreuk en de schade. Uiteraard is dit slechts symbolisch bedoeld.

De in de paragraaf Praktische toepassingen genoemde verbandstudies kunnen symbolisch door bestudering van een drietal subruimten worden gerepresenteerd. In figuur 8 zijn deze aangegeven met vlakken.
Het grondvlak A betreft het inventariseren van de met belangbronnen samenhangende objecten met hun aspecten, ofwel het bepalen van belangen. De objecten/aspecten-dimensie kan op iedere gewenste wijze worden geordend, bijvoorbeeld naar proces of naar (groep van) activa.



Figuur 8. Inventarisatievlakken.

Het opstaande vlak B betreft het inventariseren van inbreuken, niet-preventieve maatregelen en de overblijvende schade.

Het achtervlak C betreft het inventariseren van inbreukintenties/onveiligheidsoorzaken, preventieve maatregelen en de desondanks optredende inbreuken.

Het zal duidelijk zijn dat het gepresenteerde ruimtemodel lang niet alle logische relaties tussen de begrippen aankan. Zo is één van de simplificaties, dat het ruimtemodel geen recursie bevat tussen schade/gevolg en inbreuk.

Een andere simplificatie is het verabsoluteren van de begrippen en daarmee het weglaten van statistische effecten. Zo is "inbreuk" eigenlijk de (jaarlijkse) kans ofwel verwachte frequentie van het optreden van de specifieke inbreuk.

Zoals aan het begin van de paragraaf is aangestipt, is de bedoeling van het ruimtemodel meer gelegen in de symboliek dan in het zuiver mathematisch vastleggen. De auteur is zich ten volle bewust van dit beperkte karakter. Anderzijds moet het toch mogelijk zijn dit model nog wat te verbeteren en praktische toepassing te laten vinden.

CONCLUSIE

Het is mogelijk gebleken vanuit de IS-servicegroep een zinnig deelbeleid op te zetten. Bestudering van het top-gedeelte van het daarbij gekozen beveiligingsmodel heeft geleid tot ombuigingen en ideeën die eerder niet of onvoldoende naar boven waren gekomen.

LITERATUUR

[Park81] Donn B. Parker, *Computer Security Management*, ISBN 0-8359-0905-0.

[NGI91] Werkgroep Toepassen Risico-analyse NGI-sectie EDP-Auditing, *Studierapport inzake Toepassing van Risico-analyse bij geautomatiseerde Gegevensverwerking*, NGI 1991.

[Kuip89] Drs. J. Kuipers RA, *De keuze van beveiligingsmaatregelen in een geautomatiseerde omgeving*, Compact 1989/49.

[Kock89] Drs. H.C. Kocks RA en drs.ing. H.A.J.M. Spape RA, *Informatiebeveiliging in het kader van automatisering*, Compact 1989/49.

[Heijt91] Mw. D. Jansen Heijtmajer RI, *Beveiligingsbeleid geautomatiseerde informatievoorziening*, Compact 1991/3.

Ir. B.J.M. van Wely
Heeft ruime ervaring op het gebied van gegevens en gegevensverwerking. Thans fungeert hij onder andere als coördinator op het gebied van beveiliging bij de servicegroep InformatieSystemen en Automatisering van het Staalbedrijf Hoogovens IJmuiden, deel uitmakend van de Hoogovens Groep BV.

Forensische EDP-auditing

De rol van de registeraccountant/EDP-auditor bij de bestrijding van computermisbruik

R.A. s'Jacob RA

**Is een EDP-auditor in staat als deskundige op te treden in rechtszaken?
Over welke kennis moet hij of zij beschikken?
Hoe diepgaand moet een onderzoek zijn?
Vragen waarin s'Jacob zich intens heeft verdiept. Bijgaand artikel is een verkorte weergave van diens afstudeerscriptie voor het NIVRA-accountantsexamen, waarin de problematiek op een boeiende en bondige wijze is samengevat.**

INLEIDING

In een eerder in Compact gepubliceerd artikel [s'Jac90] is uitgebreid ingegaan op de (mogelijke) strafbaarstelling van computermisbruik. Strafbaarstelling impliceert dat opsporing mogelijk is. Enkele probleempunten ten aanzien van de opsporing van de verschillende vormen van computermisbruik zijn in het gerefereerde artikel reeds aangegeven. In het navolgende wordt een nieuwe discipline geïntroduceerd die de bestrijding van computermisbruik tot object van onderzoek heeft: forensische EDP-auditing. Ingegaan zal worden op het werkterrein van de forensische EDP-auditor en diens benodigde kwalificaties. Het optreden als gerechtelijk deskundige en de mogelijke fricties tussen dit optreden en de Gedrags- en Beroepsregels Registeraccountants zullen afzonderlijk worden belicht.

FORENSISCHE EDP-AUDITING

Het begrip forensisch is afkomstig van het Latijnse woord "forensis": van, bij of in (rechts)processen op het forum. Het forum was in de Romeinse tijd het middelpunt van het openbare leven. Hier kwamen de Romeinen dagelijks bijeen om hun geld- en rechtszaken af te doen, pleidooien en nieuwtjes te horen, stemmen te werven bij verkiezingen en dergelijke. Het huidige begrip "forensisch" kan worden omschreven als: *betrekking hebbend op het gerecht*, waarbij met nadruk wordt gesteld dat deze definitie niet wordt beperkt tot alleen het strafrecht, maar ook de andere vormen van recht omsluit.

Forensische EDP-auditing kan worden gedefinieerd als:

het vakgebied dat zich ten behoeve van het gerecht bezighoudt met het beoordelen van de kwaliteit van (onderdelen van) de informatievoorziening in een omgeving waarbij sprake is van misbruik van informatietechnologie (computermisbruik).

Forensische EDP-auditing vertoont overeenkomsten met andere forensische disciplines. De meest bekende daarvan zijn:
- forensische geneeskunde en psychiatrie;
- forensisch schrift- en documenttechnisch onderzoek;
- forensische toxicologie.

Zowel in Nederland als in het buitenland zijn diverse organisaties actief op het terrein van bovengenoemde forensische disciplines. Forensische EDP-auditing is, voor zover onderzoek dat heeft aangetoond, tot nu toe geen aandachtsgebied van deze organisaties. In Nederland bestaat geen overkoepelend forensisch instituut waarin de forensische disciplines samenwerken. Een dergelijke samenwerking is op het gebied van de bestrijding van computermisbruik wel gewenst, bijvoorbeeld in geval van een milieufraude, met registraties vastgelegd in geautomatiseerde systemen waarbij gebruik is gemaakt van vervalste documenten.

PARALLELLEN MET ANDERE FORENSISCHE DISCIPLINES

De meest bekende forensische discipline is de forensische geneeskunde. De eerste gestructureerde publikatie over dit onderwerp, gedateerd in 1598, is van de hand van de Italiaan Fortunatus Fidelis. Al meer dan duizend jaar daarvoor speelden medici een rol bij rechtszaken. De autopsie is één der belangrijkste middelen van de forensische medicus, bijvoorbeeld ter bepaling van de doodsoorzaak of ter bepaling van de identiteit van een slachtoffer bij misdrijven en ongevallen. De autopsie wordt meestal uitgevoerd door een patholoog-anatoom. Het verrichten van onderzoek op geneeskundig gebied, in het bijzonder op het gebied van pathologie en pathologische anatomie, ten behoeve van justitie en politie in strafzaken, behoort tot de taken van het Laboratorium voor Gerechtelijke Pathologie, een onderdeel van het Ministerie van Justitie. Voorts bestaat het Forensisch Medisch Genootschap, dat zich ten doel stelt de gerechtelijke geneeskunde in Nederland te bevorderen door onderlinge overdracht van kennis, ervaring en informatie, door nauwe onderlinge samenwerking en door nauwe samenwerking met de justitiële autoriteiten. Zo verleent het genootschap ondersteuning bij een cursus forensische geneeskunde voor afgestudeerde artsen, georganiseerd door de Stichting voor Sociale Gezondheidszorg. De forensische geneeskunde heeft in Nederland nauwe relaties met de openbare geneeskunde. Wetgeving op het gebied van de forensische geneeskunde bestaat (nog) niet. In 1987 is het zogeheten "Sevilla Manifest" aan het Europees Parlement aangeboden om tot harmonisatie, standaardisatie en uniformering van opleiding en beroepsuitoefening in de gerechtelijke geneeskunde te komen.

In de negentiende eeuw ontstonden ook de forensische psychiatrie en de forensische toxicologie. Na de Tweede Wereldoorlog is het inzicht in de betekenis van de forensische psychiatrie zowel bij de jurist als bij de psychiater sterk toegenomen. Er kwam in Utrecht een observatiekliniek tot stand, die uitgroeide tot het in 1978 geopende Pieter Baan Centrum. Later volgden er meer klinieken. De taken van de forensische psychiatrie omvatten: adviseren over de vraag naar de toerekeningsvatbaarheid, adviseren over de vraag welke (straf)maatregel het meest doeltreffend zal zijn en het verschaffen van inzicht in de persoonlijkheid van de dader door een analyse van de drijfveren. Over de forensische psychiatrie is eveneens veel gepubliceerd.

De forensische toxicologie vindt haar toepassing momenteel bij (chemische) analyses van verdovende middelen, vergiftigingen en milieuverontreiniging. Het Gerechtelijk Laboratorium, eveneens een onderdeel van het Ministerie van Justitie, heeft als taak het verrichten van forensisch natuur- en technisch-wetenschappelijk onderzoek. Hiertoe behoren niet alleen analyses van verdovende middelen, maar bijvoorbeeld ook analyses van bloedsporen, metaalonderzoek en DNA-onderzoek. Tot de taak van het Gerechtelijk Laboratorium behoort eveneens het verrichten van (elektronisch) sporenonderzoek aan in beslag genomen hardware en software. Een aantal private laboratoria levert in Nederland eveneens diensten op het gebied van forensisch natuur- en technisch-wetenschappelijk onderzoek.

Het Nederlands Instituut voor Forensisch Onderzoek (NIFO) heeft baanbrekend werk verricht op het gebied van forensische schriftonderzoeken. Met behulp van geautomatiseerde hulpmiddelen kunnen bijvoorbeeld handschriften worden vergeleken. Het NIFO ontplooit ook activiteiten op het gebied van andere forensische disciplines.

Tot slot de forensische accountancy. In Nederland is deze discipline geconcentreerd binnen de forensische accountantsgroep van de Centrale Recherche Informatiedienst. Daarnaast treden registeraccountants werkzaam bij publieke accountantskan-

toren incidenteel op als deskundige in civiele en strafrechtelijke procedures. In de opleiding voor registeraccountant krijgt het verschijnsel computermisbruik vooralsnog weinig aandacht. Het optreden als deskundige in gerechtelijke procedures krijgt geen aandacht in het opleidingspakket.

DE SITUATIE IN HET BUITENLAND

De ontwikkeling van forensische disciplines is in Nederland minder sterk geïnstitutionaliseerd dan in het buitenland. De discipline forensische EDP-auditing komt, voor zover onderzoek heeft uitgewezen, in het geheel niet voor.

Een vooraanstaand forensisch instituut is de Canadian Society of Forensic Science (La Société Canadienne des Sciences Judiciaires). De doelstelling van dit instituut staat vermeld in het intern reglement. In grote lijnen komt deze doelstelling neer op het, in de meest ruime zin des woords, bevorderen van de forensische wetenschappen. Binnen dit instituut zijn de volgende secties actief:
- biology;
- chemistry;
- counterfeit, identification and deterrence;
- documents;
- engineering;
- medical;
- odontology;
- toxicology.

Alhoewel het reglement dit wel toestaat, is er tot nu toe geen sectie forensische accountancy opgericht. Het reglement vermeldt ten aanzien van het lidmaatschap (waaraan geen examen is verbonden) onder andere:

"Membership in the Society shall be open to individuals who have demonstrated an active interest in forensic science and who have exhibited the qualities of related professional competence, integrity and good moral character."

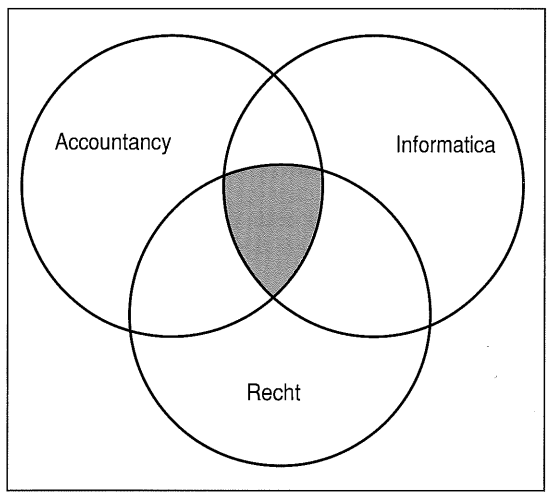
Een soortgelijk instituut in Engeland is "The Forensic Science Society". Ook dit instituut kent de forensische accountancy-discipline niet.

Forensische accountancy is in het buitenland voornamelijk geconcentreerd bij de diverse opsporings- en inlichtingendiensten, belast met verschillende vormen van fraude, van fiscale fraude tot aan corruptie. De accountants van bijvoorbeeld het Amerikaanse Internal Revenue Service (IRS) profileren zich op diverse wijzen als forensische accountants. De situatie in Duitsland is vergelijkbaar met de Nederlandse situatie (waar forensische accountants in dienst staan van justitie en politie). In landen als Denemarken en Canada worden per onderzoek accountants van openbare accountantskantoren aangetrokken. Overigens zijn bij de Royal Canadian Mounted Police ook forensische accountants werkzaam. In de Verenigde Staten en Engeland komen mengvormen voor. Met name het Serious Fraud Office in Groot-Brittannië kan worden genoemd, waar officieren van Justitie, rechercheurs, overheidsaccountants en van openbare accountantskantoren gedetacheerde accountants werken.

De situatie in Canada verdient overigens om nog een andere reden bijzondere aandacht: KPMG Peat Marwick Thorne, The Lindquist Forensic and Investigative Accounting Practice is een accountantskantoor dat gespecialiseerd is in forensische accountancy en over de gehele wereld actief is. Ook in Engeland is KPMG actief op dit gebied.

HET WERKTERREIN VAN DE FORENSISCHE EDP-AUDITOR

Bij het in kaart brengen van het werkterrein van de forensische EDP-auditor kan het volgende model worden gehanteerd:



Figuur 1. Het werkterrein van de forensische EDP-auditor (gearceerd).

Daar waar de forensische accountant werkzaam is op het grensvlak tussen het recht en de accountancy en de forensische informaticus werkzaam is op het grensvlak tussen het recht en de informatica, is het de forensische EDP-auditor die werkzaam is op het grensvlak tussen het recht, de accountancy en de informatica (het gearceerde gedeelte in figuur 1). Hij fungeert als het ware als "trait-d'union" tussen deze gebieden en is in staat juridische vraagstukken te vertalen naar vraagstukken die automatisering en controle betreffen en vice versa. De relatie tussen deze drie forensische disciplines kan het beste aan de hand van het volgende voorbeeld duidelijk worden gemaakt. Bij een geval van computerfraude is het:
- de forensische EDP-auditor die de wijze waarop, alsmede de omstandigheden waaronder de fraude is gepleegd, in kaart brengt (het systeem als het ware in kaart brengt);
- de forensische informaticus die de in het geautomatiseerde systeem opgeslagen gegevens zichtbaar maakt (de gegevens als het ware uit het systeem haalt);
- de forensische accountant die deze gegevens analyseert en controleert.

Het is niet geheel uitgesloten dat de forensische accountant en de forensische EDP-auditor een en dezelfde persoon zijn; in de meeste gevallen echter zal de forensische accountant te weinig kennis en ervaring hebben op het gebied van automatisering en de forensische EDP-auditor te weinig kennis van en ervaring met het analyseren en controleren van financiële gegevens, en is derhalve de inzet van twee deskundigen vereist.
Het werkterrein van de forensische EDP-auditor kan op een combinatie van elk van de aangegeven deelgebieden liggen. De volgende voorbeelden mogen dit verduidelijken:

- Het in opdracht van een rechter in een civiele procedure beoordelen van de hoogte van een schadeclaim ingediend naar aanleiding van schade veroorzaakt door met een computervirus besmette applicatie-software.

- Het in opdracht van een rechter-commissaris in strafzaken verlenen van assistentie bij het verrichten van een huiszoeking en het aangeven van de modus operandi van de vermoedelijke dader.

- Het in opdracht van een service center geven van een oordeel over de mate van beveiliging in het kader van een schadeclaim door een gebruiker van dit service center wegens het uitlekken van persoonsgegevens.

- Het verlenen van ondersteuning bij het voorbereiden van een aangifte van computerfraude in opdracht van het management van de gedupeerde onderneming.

- Het verlenen van ondersteuning aan een collega-accountant in een tuchtrechtprocedure in verband met een vermoeden van het niet naleven van de NIVRA-richtlijn inzake verantwoordelijkheid voor en handelwijze bij het ontdekken van onjuistheden in de verantwoording.

- Het geven van een deskundig advies ter terechtzitting in opdracht van de raadsman van een verdachte.

Het werkterrein is te divers om hiervan een limitatieve opsomming te geven. Bovenstaande voorbeelden dienen om de beeldvorming ten aanzien van het werkterrein van de forensische EDP-auditor te verhelderen.

KWALIFICATIES VAN DE FORENSISCHE EDP-AUDITOR

Om op zijn werkterrein actief te kunnen zijn, zal de forensische EDP-auditor zijn vaktechnische kennis moeten uitbreiden met juridische kennis. Onderscheid kan worden gemaakt tussen het materiële recht en het formele recht. Kennis van het materiële recht (en andere regelgeving) dient minimaal de volgende onderwerpen te omvatten:
- beveiligingsplicht in het kader van de Wet Persoonsregistraties;
- strafbaarstelling van computermisbruik;
- wanprestatie en onrechtmatige daad (toerekenbare tekortkomingen), overmacht (niet-toerekenbare tekortkoming), risico-aansprakelijkheid;
- beveiligingsverklaring en de rol van de registeraccountant in het kader van het jaarrekeningrecht;
- NIVRA-richtlijn inzake de verantwoordelijkheid voor en handelwijze bij het ontdekken van onjuistheden in de verantwoording.

Voor wat betreft strafrechtelijke procedures zal de forensische EDP-auditor in veel gevallen gevraagd worden naar een advies inzake de toepassing van opsporings- en dwangmiddelen in een geautomatiseerde omgeving. Van hem wordt verwacht een belangenafweging te kunnen maken en de rechter-commissaris te behoeden voor onevenredig handelen. Het kennisniveau van de forensische EDP-auditor zal hierop moeten zijn afgestemd.

Kennis van het formele recht dient minimaal de volgende gebieden te omvatten:
- burgerlijk procesrecht;
- strafprocesrecht (inclusief de toepassing van opsporings- en dwangmiddelen).

Kennis van de rol van de deskundige in het procesrecht en de te stellen eisen ten aanzien van de bewijsvoering zijn daarbij voorname aspecten. Het bewijs in strafzaken zal veel eenduidiger moeten worden geleverd dan het bewijs in civiele zaken. In het strafrecht geldt het principe "geen straf zonder expliciete strafbaarstelling". Dit houdt mede in dat bewezen moet worden dat het feit conform de strafbaarstelling en door de verdachte is gepleegd. Bovendien moet het bewijs voor de rechter in strafzaken overtuigend worden geleverd. In het burgerlijk recht gaat het vaak om begrippen als zorgvuldigheid en redelijkheid. De forensische EDP-auditor dient hiermee rekening te houden.

Van een forensische EDP-auditor mag niet worden verwacht dat zijn juridische kennis dezelfde mate van diepgang heeft op de hierboven aangegeven gebieden als die van een jurist. Kennis in hoofdlijnen is onontbeerlijk, diepgaande kennis kan beter aan juristen worden overgelaten. Per opdracht moet het juridisch kader door de opdrachtgever worden omschreven. In voorkomende gevallen zal de forensische EDP-auditor in multidisciplinair verband met een jurist moeten samenwerken.

Ten slotte kan nog worden vermeld dat de forensische EDP-auditor in staat moet zijn het eigen vakgebied duidelijk en eenvoudig aan op dit gebied ondeskundigen over te brengen (daaronder begrepen de rechterlijke macht). De praktijk heeft tot nu toe uitgewezen dat er een grote communicatiekloof bestaat tussen juristen en EDP-auditors. Het behoort tot de kwalificaties van de forensische EDP-auditor deze communicatiekloof te overbruggen.

HET OPTREDEN ALS GERECHTELIJK DESKUNDIGE

Op diverse plaatsen in de wet zijn regels aangaande de positie van de deskundige te vinden. Veel helderheid is aan deze wetsbepalingen evenwel niet te ontlenen, omdat deze zeer algemeen zijn geformuleerd. Over de rol van de deskundige in het Nederlands recht is relatief weinig gepubliceerd.

De positie van de deskundige mag niet worden verward met de positie van de getuige en de in de praktijk veel gehanteerde term "getuige-deskundige" (dit is een "deskundige" getuige). De getuige brengt de rechter nieuwe gegevens, de deskundige helpt hem in de waardering. Een ander verschil is dat de deskundige geacht wordt neutraal (onpartijdig) te zijn.
Hieronder wordt aan de hand van de desbetreffende wetsbepalingen in hoofdlijnen ingegaan op de juridische aspecten van het optreden als deskundige in civiele en strafrechtelijke procedures. Op de wettelijke bepalingen ten aanzien van de rol van de getuige en het verschoningsrecht van deze wordt niet ingegaan; dit valt buiten het kader van dit artikel.

De deskundige die zijn benoeming heeft aanvaard, is verplicht de opdracht onpartijdig en naar beste weten te volbrengen.

In de artikelen 221-236 Wetboek van Burgerlijke Rechtsvordering (Rv.) wordt ingegaan op de deskundige in civiele procedures. De rechter kan op verzoek van één der partijen of ambtshalve een verhoor van deskundigen bevelen. Het vonnis vermeldt de punten waaromtrent het oordeel van deskundigen wordt gevraagd. De rechter benoemt na overleg met partijen bij het vonnis of bij een latere rolbeschikking één of meer deskundigen, met de opdracht aan hem een schriftelijk bericht in te leveren of mondeling verslag uit te brengen (art. 221 Rv.). De deskundigen kunnen weigeren gehoor te geven aan het bevel. De deskundige die zijn benoeming heeft aanvaard, is verplicht de opdracht onpartijdig en naar beste weten te volbrengen (art. 222 Rv.). De rechter bepaalt waar en wanneer het onderzoek moet worden uitgevoerd. De deskundigen stellen hun onderzoek in, hetzij onder leiding van een rechter-commissaris, hetzij zelfstandig. De deskundigen moeten bij hun onderzoek partijen in de gelegenheid stellen opmerkingen te maken en verzoeken te doen. Uit het schriftelijk bericht moet blijken of aan dit voorschrift is voldaan. Van de inhoud van de opmerkingen en verzoeken zal in het schriftelijk bericht melding worden gemaakt. Het proces-verbaal van de slotsom van het mondeling verslag wordt, na voorlezing door de griffier, ondertekend door de rechter en de deskundigen. Verklaart een deskundige niet te kunnen ondertekenen, dan wordt die verklaring inhoudende de oorzaak van verhindering, in het proces-verbaal vermeld (art. 223 Rv.). Het schriftelijk bericht is met redenen omkleed zonder dat het persoonlijk gevoelen van ieder der deskundigen behoeft te blijken. Ieder der deskundigen kan van zijn afwijkende mening doen blijken (art. 224 Rv.).

Algemene bepalingen over de taak en positie van de deskundige in strafrechtelijke procedures zijn te vinden in de artikelen 151, 158 en 227 e.v. Wetboek van Strafvordering (Sv.). Tijdens het gerechtelijk vooronderzoek kan de rechter-commissaris hetzij ambtshalve, hetzij op vordering van de officier van Justitie of het verzoek van de verdachte één of meer deskundigen benoemen, teneinde hem voor te lichten of bij te staan en, zo nodig, met opdracht het door hem gevorderde onderzoek in te stellen en hem een met redenen omkleed verslag uit te brengen (art. 227 Sv.). Tijdens het opsporingsonderzoek komt deze bevoegdheid in bepaalde gevallen toe aan de officier van Justitie of diens hulpofficieren (artt. 151 en 158 Sv.). Ieder die tot deskundige is benoemd, is verplicht de door de rechter-commissaris gevorderde diensten te bewijzen (art. 227 Sv.). De deskundige wordt door de rechter-commissaris beëdigd dat hij zijn taak naar geweten zal vervullen. Van degene die, op vordering van het openbaar ministerie, door het Gerechtshof in welks ressort hij woont, als vast gerechtelijk deskundige is beëdigd, wordt ter zake van het uitbrengen van een schriftelijk verslag geen verdere eed gevorderd (art. 228 Sv.). Aan de benoeming tot vast gerechtelijk deskundige is een bepaalde maatschappelijke status verbonden, alhoewel de voorwaarden waaronder deze benoeming geschiedt, niet zijn geëxpliciteerd. Er bestaat derhalve geen directe relatie tussen het optreden als vast gerechtelijk deskundige en het daarbij behorende deskundigheidsniveau.

De rechter-commissaris bepaalt het tijdstip waarop het onderzoek van de deskundigen zal worden aangevangen en de termijn waarbinnen dit moet zijn afgerond (art. 229 Sv.). De rechter-commissaris, de officier van Justitie, de verdachte, diens raadsman en een door de verdachte aangewezen deskundige kunnen onder bepaalde voorwaarden het onderzoek van de deskundige geheel of gedeeltelijk bijwonen. Zij hebben ook de bevoegdheid met betrekking tot dat onderzoek aanwijzingen te doen en opmerkingen te maken (artt. 231 en 232 Sv.). De verdachte heeft tevens de bevoegdheid het verslag van de deskundige door een andere deskundige te laten onderzoeken (art. 233 Sv.). De rechter-commissaris kan de deskundige geheimhouding opleggen (art. 236 Sv.).

Bij het onderzoek ter terechtzitting zijn alle bepalingen ten aanzien van getuigen en hun verklaringen ook van toepassing op deskundigen en hun verklaringen, behoudens (art. 296 Sv.):
- dat de deskundige (met uitzondering van de vast gerechtelijk deskundige die een schriftelijk verslag uitbrengt) wordt beëdigd dat hij zijn taak (het uitbrengen en verdedigen van het verslag) naar geweten zal vervullen;

- dat de deskundige bij zijn verklaring niet verplicht is zijn redenen van wetenschap op te geven;
- dat gijzeling (als straf op het bij het verhoor zonder wettige grond weigeren de gestelde vragen te beantwoorden) niet is toegelaten.

De verklaringen en verslagen van deskundigen zijn met redenen omkleed. De deskundigen zijn verplicht de door de rechtbank gevorderde diensten te bewijzen.

Het bewijs dat de verdachte het ten laste gelegde feit heeft begaan, kan door de rechter slechts worden aangenomen, indien hij daarvan uit het onderzoek op de terechtzitting door de inhoud van wettige bewijsmiddelen de overtuiging heeft bekomen (art. 338 Sv.). Als wettige bewijsmiddelen worden onder andere erkend verklaringen van deskundigen en verslagen van deskundigen behelzende hun gevoelen betreffende hetgeen hun wetenschap hen leert omtrent datgene wat aan hun oordeel onderworpen is (artt. 339 en 344 Sv.).

RELATIE MET DE GEDRAGS- EN BEROEPSREGELS REGISTERACCOUNTANTS

Het accountantsberoep is wettelijk geregeld in de Wet Registeraccountants. Bij deze wet is ingesteld een openbaar register waarin kunnen worden ingeschreven degenen die aan de in de wet gestelde eisen van deskundigheid voldoen. Slechts degenen die in dit register zijn ingeschreven, mogen zich als registeraccountant aanduiden (deskundigheidsaanduiding). Zij zijn van rechtswege onderworpen aan de tuchtrechtspraak en zij zijn van rechtswege lid van het openbaar lichaam: Nederlands Instituut van Registeraccountants (NIVRA). Dit instituut heeft tot taak de bevordering van een goede beroepsuitoefening, de behartiging van het gemeenschappelijk belang, de zorg voor de eer van de stand en het verzorgen van een opleiding tot registeraccountant. Op twee van deze taken hebben de Gedrags- en Beroepsregels Registeraccountants (GBR), een verordening van het NIVRA die bindend is voor alle registeraccountants, betrekking: bevordering van een goede beroepsuitoefening en de zorg voor de eer van de stand.

De GBR zijn voornamelijk gericht op de als accountant optredende registeraccountant. Hiervan is onder andere sprake indien hij of zij zich als zodanig bekend maakt, beroepshalve de getrouwheid van een verantwoording controleert of optreedt onder gemeenschappelijke naam met een andere als accountant optredende registeraccountant. Daarnaast wordt mede aandacht besteed aan de als openbaar accountant optredende registeraccountant. Hiervan is onder meer sprake indien hij of zij of degene met wie hij of zij onder gemeenschappelijke naam optreedt, zich als zodanig bekend maakt of gedoogt dat een door hem gegeven verklaring openbaar wordt gemaakt. Voor niet als (openbaar) accountant optredende registeraccountants bevatten de GBR slechts één voor dit artikel relevante bepaling: de registeraccountant onthoudt zich van al hetgeen schadelijk is voor de eer van de stand der accountants. De GBR zijn uiteraard niet van toepassing op de forensische EDP-auditor die geen registeraccountant is.

In deze paragraaf zal nader worden stilgestaan bij de forensische EDP-auditor zijnde een registeraccountant die onder gemeenschappelijke naam optreedt met een als openbaar accountant optredende registeraccountant.

Kernbegrippen uit de GBR van toepassing op als openbaar accountant optredende registeraccountants:

- De eis van een deugdelijke grondslag voor mededelingen omtrent de uitkomst van accountantsarbeid, alsmede de eis van duidelijkheid van die mededelingen.

- De eis van onpartijdigheid en onafhankelijkheid ten opzichte van de opdrachtgever.

- Geheimhouding van al hetgeen in de uitoefening van het beroep hem als geheim is toevertrouwd of wat daarbij als een vertrouwelijke aangelegenheid is toevertrouwd.

- Collegiaal overleg bij aanvaarding van opdrachten.

De eis van een deugdelijke grondslag (art. 11 GBR) voor mededelingen houdt voor de forensische EDP-auditor mede in dat hij de juridische reikwijdte van zijn mededeling overziet en niet in de schoenen van de rechter gaat staan. Dit geldt met name voor strafrechtelijke procedures. De forensische EDP-auditor moet zich realiseren dat het niet gaat om een globale oordeelsvorming maar om een concreet antwoord op de gestelde vragen; bijvoorbeeld de vraag welke activiteiten een bepaalde verdachte wanneer onder welke omstandigheden heeft verricht. De beantwoording van de vraag of een verdachte schuldig is, is voorbehouden aan de rechter. Forensisch onderzoek vereist een grote mate van diepgang met een zeer geringe tolerantie. Kenmerk van het optreden als forensische EDP-auditor is het feit dat de deugdelijke grondslag in het openbaar ter discussie staat. Voor de als openbaar accountant optredende registeraccountant is dit niet het geval. Om geschillen omtrent de uitkomst van de gedane arbeid te voorkomen, is het noodzakelijk dat de forensische EDP-auditor een goede opdrachtbevestiging met de scope van het onderzoek (de vragen waarop een antwoord moet worden gegeven) opstelt. Van een rechter(-commissaris) mag niet worden verwacht dat hij of zij hiertoe zelfstandig in staat is. Zoals eerder gesteld behoort het tot de taak van de forensische EDP-auditor een goede vertaalslag te kunnen maken van de juridische vraagstukken naar vaktechnische vraagstukken en vice versa. Goed overleg tussen opdrachtgever en opdrachtnemer is essentieel!

De eis van onpartijdigheid in het oordeel van de als (openbaar) accountant optredende registeraccountant is vastgelegd in artikel 9 GBR. Deze be-

paling bevestigt het uitgangspunt dat accountantsoordelen hun betekenis voor een groot deel ontlenen aan de omstandigheid dat deze niet vooringenomen, niet geleid door persoonlijke belangen, voorkeur of genegenheid, zijn gevormd en gegeven. Bij de vorming van zijn of haar oordeel mag de forensische EDP-auditor zich dan ook niet eenzijdig laten beïnvloeden door het standpunt of het belang van één der partijen die betrokken zijn bij zijn activiteiten.

Kenmerk van het optreden als forensische EDP-auditor is het feit dat de deugdelijke grondslag in het openbaar ter discussie staat.

Voornaamste knelpunt bij het aanvaarden van opdrachten door de forensische EDP-auditor is de onafhankelijkheid (artt. 22 tot en met 25 GBR). De benoeming tot deskundige is slechts mogelijk onder de voorwaarde dat geen der betrokkenen (verdachte of procespartijen) een bestaande relatie (cliënt) is van de registeraccountant of diens maatschap. Uit de voorgaande paragraaf mag worden afgeleid dat in strafrechtelijke procedures het optreden als deskundige door de rechter-commissaris afgedwongen zou kunnen worden. Indien de betrokken registeraccountant (of diens maatschap) bepaalde relaties heeft (gehad) met de verdachte, kan de onafhankelijkheid in het geding zijn. In de praktijk zullen registeraccountants die een bepaalde mate van betrokkenheid met één of meer partijen hebben, echter niet als deskundige maar als getuige worden opgeroepen. Zoals eerder vermeld valt het optreden als getuige buiten het kader van dit artikel. In de praktijk maakt de rechter-commissaris wel gebruik van zijn bevoegdheid medewerking af te dwingen, indien hij of zij een beroep doet op een specialistische medewerker van een accountantskantoor, die van zijn of haar organisatie (om andere redenen dan de onafhankelijkheid) geen toestemming krijgt. Het is immers de medewerker die, op grond van zijn of haar specifieke deskundigheid, gevraagd wordt op persoonlijke titel een advies of oordeel te geven over een bepaalde aangelegenheid en daarmee dus niet, zoals te doen gebruikelijk is, namens de maatschap optreedt.

Voor wat betreft de geheimhoudingsplicht (art. 10 GBR) wordt opgemerkt dat de forensische EDP-auditor zeer zorgvuldig moet omgaan met de aan hem bekend gemaakte gegevens. Het rapport van de deskundige is een openbaar document waarin alleen die gegevens behoren te worden opgenomen die in het kader van de opdracht van belang zijn. Er ontstaat derhalve een spanningsveld tussen de geheimhoudingsplicht en het bekend maken van die gegevens die voor een deugdelijke grondslag moeten worden bekend gemaakt. Het op een goede wijze omgaan met dit spanningsveld behoort tot de vaardigheden van de forensische EDP-auditor en behoeft in de praktijk niet op problemen te stuiten.

De GBR bepalen onder andere dat het de registeraccountant verboden is in te gaan op een verzoek tot het aanvaarden van een opdracht, alvorens hij van de openbaar accountant die reeds voor dezelfde opdrachtgever bij dezelfde huishouding optreedt of laatstelijk is opgetreden, inlichtingen heeft gevraagd (art. 29 GBR). In gevallen waarin de rechter(-commissaris) een opdracht aan een forensische EDP-auditor verstrekt, is geen sprake van dezelfde opdrachtgever (de openbaar accountant ontvangt de opdracht immers van het management van de huishouding) en is collegiaal overleg niet verplicht. Het getuigt overigens wel van een goede beroepsuitoefening en het verkrijgen van een deugdelijke grondslag, indien dit overleg wordt gevoerd. Het is de registeraccountant verboden een oordeel te geven omtrent de arbeid van een andere als accountant optredende registeraccountant, alvorens hem in de gelegenheid te hebben gesteld inlichtingen te geven (art. 31 GBR). Dit is met name van belang indien de forensische EDP-auditor een opdracht van de tuchtrechter aanvaardt of een contra-expertise verricht. Bij dergelijke opdrachten wordt impliciet of expliciet een oordeel over het werk van een andere registeraccountant gevraagd.

Het is niet onwaarschijnlijk dat zich strafrechtelijke onderzoeken zullen voordoen waarbij een als openbaar accountant optredende registeraccountant door de rechter-commissaris wordt gevraagd een oordeel over de arbeid van een andere (verdachte) registeraccountant te geven. Indien het collegiaal overleg schadelijk is voor het onderzoek van de rechter-commissaris, ontstaat een probleem. De GBR stellen het collegiaal overleg verplicht, terwijl de rechter-commissaris de bevoegdheid heeft dit overleg te verbieden. Het is de taak van de deskundige registeraccountant de rechter-commissaris te wijzen op dit probleem. Indien de rechter-commissaris niet kan worden overtuigd en deze dreigt gebruik te maken van diens bevoegdheid medewerking af te dwingen, dan moet collegiaal overleg achterwege blijven; een wet heeft immers een hogere juridische status dan een verordening van een publiekrechtelijk lichaam. Het verdient overigens aanbeveling deze situatie door de rechter-commissaris te laten vastleggen en in de rapportage te vermelden.

Voor het doen van mededelingen in opdracht van de rechter(-commissaris) kan de forensische EDP-auditor persoonlijk verantwoordelijk worden gesteld. Deze verantwoordelijkheid wordt tot uitdrukking gebracht bij het ondertekenen van het rapport of het proces-verbaal van het mondeling verslag. Indien het onderzoek door meerdere deskundigen wordt uitgevoerd, zijn allen verantwoordelijk voor het geheel. Zoals vermeld in de vorige paragraaf, bestaat in civielrechtelijke procedures de mogelijkheid dat een afwijkende mening in het rapport (deskundigenbericht) kan worden vastgelegd. In gevallen waarbij de forensische EDP-auditor bij zijn onderzoek gebruik maakt van assistenten die zeer specifieke kennis hebben op deelgebieden, bijvoorbeeld cryptologie, kan de vraag wor-

den gesteld in hoeverre de forensische EDP-auditor de kwaliteit van het werk van die assistenten kan beoordelen. In feite is deze vraag niet nieuw: in de EDP-audit-praktijk is dit een veel voorkomend probleem. De verantwoordelijke accountant richt zich dan met name op integrale dossierbeoordeling, gesprekken inzake de oordeelsvorming, beoordeling door een tweede deskundige op het desbetreffende gebied en het sturen van de kwaliteit door middel van opleidingsprogramma's.
Opdrachtgevers nemen bovendien vaak genoegen met het laten verdedigen van gedeelten van rapporten door de desbetreffende assistenten.

Een nog groter probleem is het kunnen instaan voor mededelingen van deskundigen die door de rechter in het onderzoeksteam zijn benoemd, maar niet tot de eigen organisatie van de forensische EDP-auditor behoren. Andere middelen dan integrale dossierreview, gesprekken en het beoordelen van de kwaliteit van de persoonlijke prestaties van die deskundige in het verleden, zijn dan niet beschikbaar. Per opdracht zal de forensische EDP-auditor moeten beoordelen in hoeverre hij zijn verantwoordelijkheid kan dragen. Hij zal rekening moeten houden met het feit dat naar zijn persoonlijke mening zal worden gevraagd. Dit benadrukt nogmaals het belang van een deugdelijke grondslag.

Speciale aandacht verdient het optreden als deskundige ten behoeve van een verdachte in een strafrechtelijke procedure. Een argument om dit te weigeren is de vrees voor negatieve publiciteit; de naam van een registeraccountant of diens maatschap zou kunnen worden verbonden met (het goedkeuren van) crimineel gedrag. Per geval zal een standpunt ter zake moeten worden bepaald.

Resumerend betekent een en ander dat het aanvaarden van opdrachten door de forensische EDP-auditor die onder gemeenschappelijke naam optreedt met een als een openbaar accountant optredende registeraccountant mogelijk is onder de voorwaarde van het in acht nemen van de GBR, met name inzake:
- deugdelijke grondslag;
- onpartijdigheid;
- onafhankelijkheid;
- geheimhouding;
- collegiaal overleg.

Het is noodzakelijk deze aspecten in een opdrachtbevestiging vast te leggen, die mede ten doel heeft een zo helder mogelijk verwachtingspatroon bij de opdrachtgever te scheppen. In deze opdrachtbevestiging moeten ook worden opgenomen de vragen waarop het onderzoek antwoord moet geven, de termijn waarbinnen het onderzoek moet zijn afgerond, de kosten en de vereisten ten aanzien van de rapportage.

EEN NEDERLANDS FORENSISCH INSTITUUT?

Uitgaande van de gesignaleerde behoefte aan forensische EDP-auditing, zal aan een Nederlands forensisch instituut vorm moeten worden gegeven. De ontwikkeling van de forensische EDP-auditing kan het beste gestalte krijgen binnen de bestaande EDP-audit-afdelingen van de (grote) openbare accountantskantoren. Binnen deze afdelingen wordt zeer veel tijd en geld besteed aan gerichte vakontwikkeling en worden meerdere disciplines samengevoegd. Binnen KPMG Klynveld EDP Auditors zijn bijvoorbeeld deskundigen (op academisch niveau) werkzaam op het gebied van accountancy, bestuurlijke informatievoorziening, informatica, telecommunicatie, encryptie, hardware, besturingsprogrammatuur, rechtswetenschappen en organisatiekunde. Een dergelijke bundeling van expertises biedt een uitstekende basis voor de ontwikkeling van de forensische EDP-auditing.
Het geïsoleerd binnen de openbare accountantskantoren en (voor wat betreft strafrechtelijke procedures) de opsporingsinstanties ontwikkelen van de forensische EDP-auditing komt deze discipline niet ten goede. Het uitwisselen van ervaringen, het ontwikkelen van een visie op de toekomst van de discipline, het bevorderen en bewaken van (vaktechnische, juridische en persoonlijke) kwalificaties en het onderhouden van contacten met andere forensische disciplines zal dan onvoldoende aandacht krijgen. Bovendien is het voor de staande en zittende magistratuur en het maatschappelijk verkeer van grote importantie een aanspreekpunt voor kennis en kunde te hebben, zeker gezien het feit dat niet elk accountantskantoor elke opdracht mag aanvaarden. Deze argumenten vormen de basis voor de gedachte dat er een Nederlands forensisch instituut moet worden opgericht. Op deze wijze kan niet alleen de forensische EDP-auditing worden gestimuleerd, maar kan ook een breder draagvlak voor de ontwikkeling van de forensische wetenschappen in het algemeen worden gecreëerd.
Verwacht mag worden dat er nog een lange weg is te gaan. In dit artikel is een aanzet gegeven tot de ontwikkeling van de forensische EDP-auditing-discipline. Er zullen nog vele jaren verstrijken voordat gesproken kan worden van een volwaardige en maatschappelijk erkende discipline.
Bovendien bestaat het gevaar dat zich slechts enkele deskundigen zullen aanbieden. Als gevolg daarvan kan zich een door de rechterlijke macht niet te controleren groep experts vormen die bij alle zaken zullen worden betrokken. Contra-expertise, een zeer waardevol instrument voor de rechterlijke macht, verliest bij gebrek aan deskundigen haar waarde. Deze situatie moet zoveel mogelijk worden vermeden. Het op te richten Nederlands forensisch instituut kan hierbij een grote rol spelen.

LITERATUUR

[s'Jac90] R.A. s'Jacob, *Strafbaarstelling van computermisbruik*, Compact 1990/4.

R.A. s'Jacob RA
Is sinds 1987 werkzaam als EDP-auditor bij KPMG Klynveld EDP Auditors. In september 1991 heeft hij het NIVRA-accountantsexamen behaald. Gedurende zijn opleiding heeft hij onder andere stage gelopen bij de toenmalige Fraude Centrale van de Centrale Recherche Informatiedienst. Recentelijk heeft hij als projectleider een omvangrijk onderzoek geleid naar het technisch en organisatorisch instrumentarium benodigd voor de bestrijding van computermisbruik in Nederland.

EDP AUDITORIUM

RAPPORTBESPREKING

Systems Auditability and Control Report: Contingency planning

Drs. M.W. van Aalst en F.J. Pop

Inleiding

In 1991 is door de Research Foundation van het Institute of Internal Auditors (IAA) het rapport Systems Auditability and Control (SAC) opnieuw uitgegeven. Dit rapport richt zich op de risico's, beheersing en auditing van toepassing van informatietechnologie in organisaties en is bestemd voor ieder die zich bezighoudt met de beheersing en beoordeling van informatietechnologie.

Het rapport is een volledig geactualiseerde versie van het in 1977 verschenen SAC-rapport. Herziening was nodig door de ingrijpende veranderingen in de informatietechnologie sinds 1977, grotere rijpheid van organisaties in de toepassing van informatietechnologie en veranderingen in de interne audit-functie. Het SAC-rapport beoogt een leidraad te bieden op het gebied van beheersmaatregelen voor informatietechnologie en het beoordelen van deze maatregelen.

Het SAC-rapport bestaat uit tien modules die elk een specifiek onderwerp behandelen, een Executive summary (module 1) en een Index (module 12). De modules 2 tot en met 11 behandelen: Audit and control environment, Using information technology in auditing, Managing computer resources, Managing information and developing systems, Business systems, End-user and departmental computing, Telecommunications, Security, Contingency planning en Emerging technologies.

Gezien de relatie met het thema van deze Compact, fysieke beveiliging, zal in deze rubriek worden ingegaan op module 10 van het SAC-rapport, die is gewijd aan contingency planning.

Contingency planning

In het SAC-rapport wordt contingency planning gedefinieerd als het deel van het stelsel van interne controle bedoeld om, bij een verstoring van de geautomatiseerde gegevensverwerking, te voorzien in de beschikbaarheid van waardevolle gegevens en middelen. In het resultaat van het planningsproces, het contingency plan (in het Nederlands noodvoorzieningen- of rampenplan), zijn gedetailleerde herstelprocedures vastgelegd om snel en soepel de verwerkingscapaciteit van de organisatie te herstellen wanneer de computer of communicatiefaciliteiten niet meer functioneren of beschikbaar zijn.

Het contingency plan dat zich richt op informatiesystemen zou deel moeten uitmaken van een ruimer plan dat de gehele organisatie omvat (het Business recovery plan).
Onderdeel van het planningsproces is de definitie voor de organisatie van een ramp (ter onderscheiding van een operationele storing). Risico-analyse kan worden gebruikt voor de definitie van een operationele storing en de verschillende niveaus van rampen. Voor effectieve contingency planning is begrip van de behoefte van de organisatie aan gegevensverwerking van essentieel belang.

Het rapport geeft als voornaamste doelen van contingency planning:
- het waarborgen van de continuïteit van het primaire proces van de organisatie;
- het minimaliseren van de hersteltijd;
- het ondersteunen van het Business recovery plan;
- het voldoen aan wettelijke en contractuele verplichtingen.

Als voorwaarden voor effectieve contingency planning worden genoemd dat zij moet worden gedragen door het hoogste management, dat voldoende personele en financiële middelen worden toegewezen en dat actieve betrokkenheid op alle niveaus in de organisatie wordt verkregen.

Het rapport gaat uitgebreid in op het contingency planningsproces en de succesfactoren daarvan, zowel ten aanzien van het eenmalig projectmatig opstellen van het plan als de organisatie van het onderhoud van het plan. Hierbij wordt aandacht besteed aan risico-analyse, de keuze van een contingency planningsstrategie, de inhoud en wijze van documenteren en het testen van het plan.

In een afzonderlijk hoofdstuk wordt ingegaan op de risico's die een organisatie loopt indien onvoldoende aandacht wordt besteed aan contingency planning en aan beheersmaatregelen om de werking van het plan in een noodsituatie te waarborgen.

Ook is een hoofdstuk gewijd aan de audit van een contingency plan. Hierin wordt een vrij summier overzicht gegeven van aandachtspunten voor de audit. Daarbij wordt onderscheid gemaakt tussen enerzijds het beoordelen van de inhoud van het plan en anderzijds het toetsen van de naleving.

Ten slotte zijn in de module opgenomen: een case study van een succesvolle toepassing van contingency planning, een globale behandeling van de aanpak van een beoordeling van verzekeringen, aandachtspunten voor en een voorbeeld van een uitwijkcontract, en een voorbeeld van een inhoudsopgave voor een noodvoorzieningenplan.

Conclusie

Deze module van het SAC-rapport geeft een goed theoretisch, internationaal geldend inzicht in contingency planning, waarbij een degelijke normatieve uitwerking wordt gegeven van het planningsproces, het plan zelf en het testen en onderhouden daarvan.
De diepgang van het hoofdstuk over de audit van een noodvoorzieningenplan stelt, gezien de doelstelling van het rapport, enigszins teleur; een auditor zal echter in het rapport voldoende aanknopingspunten vinden om tot een goede aanpak te kunnen komen.

De module is bijzonder interessant voor organisaties die van plan zijn contingency planning structureel aan te pakken. Daarnaast is hij goed bruikbaar voor auditors die kennis van contingency planning willen opdoen.

Als de overige modules van dezelfde kwaliteit zijn, kan het rapport een waardevolle aanvulling van de automatiseringsbibliotheek vormen.

SCHADEN TEN GEVOLGE VAN FALENDE BEVEILIGING

J.F.C. van Epen, CISA

Onder de kop "Poor computer security costs £1.1 bn a year" werd in de Financial Times van 30 januari 1992 het daags daarvoor gepubliceerde rapport inzake een onderzoek naar de schade ten gevolge van inbreuken op de computerbeveiliging besproken. Het onderzoek werd uitgevoerd door het National Computing Centre met steun van ICL en negenhonderd bedrijven werden daarbij ondervraagd. Aan het licht kwam dat in het Verenigd Koninkrijk computermisbruik wijd verspreid is. De helft van de onderzochte bedrijven meldde een belangrijke inbreuk op de beveiliging gedurende de laatste vijf jaren.
De grootst gerapporteerde calamiteit betrof een grote brand bij een financiële instelling, waarbij alle computers werden vernield. De directe schade bedroeg £8m, ofwel circa *f* 27 miljoen. De indirecte gevolgschade echter bleek drie keer zo groot te zijn. Als bijzonderheid werd vermeld dat deze organisatie over een goed calamiteitenplan beschikte en binnen een week weer operationeel was.

Schaden ten gevolge van fysieke calamiteiten (brand, wateroverlast, blikseminslag, verstoringen van de elektriciteitsvoorziening, diefstal) bedroegen in totaal circa £580m (*f* 2 miljard); schaden die werden veroorzaakt door logische calamiteiten ("hacking", virussen, software-problemen) bijna evenveel, namelijk £530m (*f* 1,7 miljard).
Onder de fysieke calamiteiten kwamen de verstoringen van de elektriciteitsvoorziening het meest voor, gevolgd door diefstal. Aan de logische zijde bleek dat het in gebruik nemen van niet-geteste programmatuur de grootste boosdoener was, onmiddellijk gevolgd door virussen. Het gemiddelde schadebedrag ten gevolge van "hacking" was £23.000 (*f* 78.000). De bij de onderzochte bedrijven aangetroffen grootste schade door "hacking" bedroeg £50.000 (*f* 170.000).

Dit onderzoek vond plaats in het Verenigd Koninkrijk. "Daar heerst een andere automatiseringscultuur dan op het continent en zeker dan in Nederland." Dit is - blijkens enige waarneming onzerzijds - een gangbare opvatting hier ten lande. Een dergelijk intensief onderzoek is echter in Nederland nog nooit uitgevoerd. Zou dit wel plaatsvinden, dan zou wel eens kunnen blijken dat het beeld dat wij van ons zelf hebben gevormd, minder juist is.

CUMULATIEF

Overzicht van eerder verschenen artikelen in Compact

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

4 17e jaargang 90/4 winter 1990

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

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

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

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

Strafbaarstelling van computermisbruik
R.A. s'Jacob

1 18e jaargang 91/1 lente 1991

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

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

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

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

Computercriminaliteit in Nederland
mr. V.A. de Pous

2 18e jaargang 91/2 zomer 1991

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

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

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

Detectie en bestrijding van computervirussen
J. Brinkman

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

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

3 18e jaargang 91/3 herfst 1991

Beveiligingsbeleid geautomatiseerde informatievoorziening
mw. D. Jansen Heijtmajer

Geautomatiseerde produktiebesturing
E.J.M. Ridderbeekx

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

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

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

4 18e jaargang 91/4 winter 1991

Systemen voor logische toegangsbeveiliging
drs. P. Veltman RA

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

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

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

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

Implementatie van een beveiligingspakket
J.H. Diekema