COMPACT WINTER

ACCESS CONTROL SOFTWARE

1991/4

KWARTAALBLAD EDP-AUDITING

Compact ®
Jaargang 18, nummer 4
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,
Mw. D. Jansen Heijtmajer RI,
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
Drs. M.A. Bongers RA,
J.H. Diekema,
K.E.A. van Dijk,
M.M.J.A. van Dijk,
Ing. D.J. Huis,
J-M. van Leerdam,
Ing. G.H.M. Meijer,
Drs. P. Veltman RA.

Abonnementen
f 135,- per jaar incl. BTW. Losse nummers f 50,- 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.

Overname artikelen
Het overnemen en vermenigvuldigen van artikelen en berichten is slechts geoorloofd na schriftelijke toestemming van de uitgever.

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.

Access Control Software is programmatuur met een zeer specifieke functie: de beheersing van de toegang tot geautomatiseerde systemen. Bij veel computersystemen vormt deze programmatuur een geïntegreerd onderdeel van het operating system; waar dit niet het geval is moet deze functie worden vervuld door zelf te ontwikkelen programmatuur of (meestal) door op de markt verkrijgbare pakketten.

Computerbeveiliging is lange tijd een onderwerp geweest dat in de vakliteratuur en in de praktijk van alledag nogal stiefmoederlijk is behandeld; ook bij de verschillende opleidingen werd er weinig aandacht aan besteed. Tegenwoordig bestaat er echter geen discussie meer over het belang van computerbeveiliging.

In deze uitgave van Compact staan de nieuwste ontwikkelingen op het gebied van logische (geprogrammeerde) beveiliging van computersystemen centraal, voor zover deze beveiliging geschiedt met behulp van toegevoegde software. De beveiligingsmogelijkheden van de meest voorkomende besturingssystemen zelf zijn in een eerdere uitgave beschreven (1990/1). In een recent nummer (1991/2) is de specifieke beveiligingsproblematiek van personal computers aan de orde geweest.

Sinds jaar en dag vormen met name de IBM-mainframes een belangrijke markt voor toegevoegde beveiligings-software. Oorzaak hiervan is de kennelijke filosofie van IBM om elke functie van de besturingsprogrammatuur te laten uitvoeren door een apart programma. Hierdoor ontstaat een opeenstapeling van lagen van besturingsprogrammatuur, met ruimte voor andere leveranciers om alternatieve programmaprodukten aan te bieden. In het verleden waren deze produkten van derde-leveranciers vooral gericht op de beveiliging van de teleprocessing-omgeving (met name CICS), maar met de huidige pakketten wordt beoogd beveiliging te bieden voor het systeem als geheel (op het niveau van het operating system).

Zowel Tandem- als Unisys A Serie computers worden veelvuldig gebruikt in bancaire omgevingen. Naar de huidige inzichten bieden de besturingssystemen van deze computers, zeker voor fraudegevoelige, bancaire toepassingen, onvoldoende beveiligingsmogelijkheden; hiervoor zijn dan ook aparte beveiligingsprodukten beschikbaar gekomen.

In dit themanummer van Compact wordt ingegaan op de beveiligingsfaciliteiten van afzonderlijke pakketten voor bovengenoemde computersystemen. Hierbij worden niet alleen de verschillende produkten behandeld, maar worden deze ook in het perspectief geplaatst van het gehele stelsel van computerbeveiligingsmaatregelen, en wordt aandacht besteed aan het moeizame proces van implementatie in de praktijk.

Drs. P. Veltman RA

Systemen voor logische toegangsbeveiliging

Drs. P. Veltman RA

Welke plaats neemt logische beveiliging in ten opzichte van andere beveiligingsmaatregelen? Welke functies kan logische beveiliging vervullen? Wat is de kracht en de zwakheid van hedendaags beschikbare beveiligingssystemen en wat is in dit verband de betekenis van beveiligingsstandaarden als "TCSEC" (het Orange book)?
In dit inleidend artikel gaat de auteur uitgebreid op deze vragen in; hij belicht hierbij in het bijzonder de achtergrond van logische beveiliging in het algemeen, maar besteedt ook aandacht aan concrete beveiligingsprodukten (al dan niet geïntegreerd in het operating system).

INLEIDING

Systemen of pakketten voor logische toegangsbeveiliging hebben tot doel de beveiliging van een bepaald type computersysteem te verbeteren. Dergelijke pakketten kunnen afkomstig zijn van de leverancier van het computersysteem of van derden. Eenmaal geïnstalleerd maakt het pakket deel uit van de besturingsprogrammatuur van de computer en regelt het de toegang van subjecten (in het algemeen gebruikers) tot objecten (het computersysteem zelf, programma's, bestanden, etc.).

"Beveiliging" wordt in Van Dale omschreven als "het beveiligen", dit is "het onttrekken aan bedreiging, gevaar of schade", of als "hetgeen beveiligt". Toegangsbeveiliging houdt dan in dat de beveiliging geschiedt door bedreigingen geen toegang te laten krijgen tot hetgeen wordt beveiligd. De toevoeging "logisch" geeft aan dat de toegangsbeveiliging wordt gerealiseerd met behulp van geprogrammeerde controles. In het Engels wordt voor dergelijke pakketten de term "access control software" gehanteerd.

Access control software ontleent zijn bestaansrecht aan de gebrekkige beveiligingsmogelijkheden van sommige typen computersystemen (combinatie van hardware en besturingssysteem). De belangrijkste markt voor dergelijke software wordt momenteel gevormd door de IBM-mainframes met het besturingssysteem MVS. Een andere belangrijke markt is die van de personal computers.

In dit artikel zal, na een korte inleiding over beveiliging in het algemeen, achtereenvolgens worden ingegaan op de functies van logische toegangsbeveiliging, eisen die eraan kunnen worden gesteld, organisatorische en technische randvoorwaarden en standaardisatie. Het artikel wordt besloten met een korte beschrijving van de aandachtspunten bij een audit van logische beveiliging.

In het algemeen wordt in dit artikel geen onderscheid gemaakt tussen beveiligings-software die een onderdeel vormt van het besturingssysteem en beveiligings-software die als een afzonderlijk pakket wordt geïnstalleerd, tenzij anders is aangegeven.
Logische toegangsbeveiliging kan ook op een ander niveau plaatsvinden dan op het niveau van het besturingssysteem: in ondersteunende besturingsprogrammatuur ("monitoren"[1] en database managementsysteem) en in applicaties. In dit artikel blijven deze vormen van logische toegangsbeveiliging verder buiten beschouwing.

Hoewel encryptie een essentieel element is van logische beveiliging, zal aan dit specialistische onderwerp in dit artikel geen afzonderlijke aandacht worden besteed.

BEVEILIGING ALGEMEEN

Logische toegangsbeveiliging vormt een onderdeel van het geheel aan maatregelen ter voorkoming van het optreden van bedreigingen van de geautomatiseerde gegevensverwerking en ter beperking van de schade als een bedreiging toch manifest is geworden. In de (Angelsaksische) literatuur wordt gewoonlijk onderscheid gemaakt tussen bedreigingen (threats), afbreukrisico's (exposures) en kwetsbare plekken (vulnerabilities).
Bedreigingen zijn potentiële inbreuken op de betrouwbaarheid, vertrouwelijkheid en/of beschikbaarheid van gegevens c.q. faciliteiten voor gegevensverwerking. De exposure geeft aan welke schade een organisatie lijdt als een dergelijke inbreuk optreedt. Vulnerabilities zijn plekken in het systeem (bijvoorbeeld de hardware, software, datacommunicatieverbindingen, randapparatuur) waar bedreigingen manifest zouden kunnen worden.

Beveiligingsmaatregelen kunnen in verschillende categorieën worden ingedeeld. Een veel gehanteerd onderscheid is dat naar preventieve, detectieve, repressieve en correctieve maatregelen. Preventieve maatregelen zijn gericht op het voorkomen van het optreden van bedreigingen, detectieve op het (tijdig) signaleren van een dergelijk optreden, repressieve op het beperken van de schade en correctieve op het herstellen van de oorspronkelijke situatie.

Een andere indeling is die naar fysieke, organisatorische en logische maatregelen. Maatregelen van fysieke aard betreffen de bouwkundige en andere mechanische voorzieningen ter beveiliging van de gegevens(verwerking). Het is een veelomvattend terrein, uiteenlopend van bunkers met slotgrachten om onbevoegden te weren tot "tempest"[2]-technologie om elektromagnetische straling van terminals af te schermen.
Organisatorische beveiliging heeft betrekking op de toewijzing van taken, bevoegdheden en verantwoordelijkheden aan mensen. De belangrijkste beveiligingsmaatregel van organisatorische aard is functiescheiding, ondersteund door procedures.
Logische beveiligingsmaatregelen zijn de beveiligingsmaatregelen die worden uitgevoerd door computerprogramma's. In ruime zin omvatten zij alle geprogrammeerde controles om inbreuken op de betrouwbaarheid, vertrouwelijkheid en beschikbaarheid te voorkomen, te signaleren of de nadelige gevolgen ervan te beperken. Zij variëren van invoerscreening (bestaanbaarheidscontroles en dergelijke) tot automatische recovery-procedures. Logische toegangsbeveiliging vormt een onderdeel van deze categorie maatregelen en is gericht op het beheersen van de toegang tot het computersysteem en de objecten binnen het computersysteem. Beheerste toegang houdt onder andere in dat onbevoegden worden geweerd en dat de toegangspogingen (al dan niet geslaagd) worden geregistreerd.

De beveiligingsmaatregelen van verschillende aard vullen elkaar aan. De effectiviteit van logische toegangsbeveiliging is sterk afhankelijk van organisatorische maatregelen, zoals functiescheiding bij het beheer en het gebruik van de software, en van bepaalde hardware-voorzieningen, die vooral tot doel hebben te verhinderen dat processen in het interne geheugen elkaar ongewenst beïnvloeden.
Bij het vaststellen welke beveiligingsmaatregelen door een organisatie moeten worden getroffen, wordt gewoonlijk een vorm van risico-analyse toegepast. Risico-analyse heeft tot doel op basis van een afweging van kosten van schades en kosten van beveiligingsmaatregelen, te komen tot een evenwichtig stelsel van maatregelen.

FUNCTIES VAN LOGISCHE TOEGANGSBEVEILIGING

Om de toegang van subjecten tot objecten binnen een computersysteem beheerst te kunnen laten plaatsvinden, dient het systeem voor logische toegangsbeveiliging (hierna: beveiligingssysteem) de beschikking te hebben over een registratie van de subjecten en objecten en van de toegangsrechten die tussen deze zijn toegekend (autorisatie). Alvorens toegang te verlenen zal het beveiligingssysteem moeten vaststellen dat het toegang verzoekende subject authentiek is (authenticatie). De derde hoofdfunctie van het beveiligingssysteem is het registreren van de toegangsverzoeken, zowel toegestane als geweigerde auditing.

Authenticatie

Authenticatie behelst de controle of het subject inderdaad degene is voor wie hij zich uitgeeft, dat wil zeggen of de opgegeven identiteit juist is. Gewoonlijk identificeert een subject (gebruiker) zich door middel van zijn gebruikerscode of user-id, en authenticeert hij zich met zijn wachtwoord (password). Hiertoe houdt het beveiligingssysteem, naast een registratie van toegangsrechten tussen subjecten en objecten, tevens een tabel bij met user-id/password-combinaties. Hoewel veelvuldig toegepast en voor de meeste situaties voldoende veilig, kleven aan deze vorm van authenticatie verschillende bezwaren:

- Passwords, c.q. user-id/password-combinaties, kunnen vrij gemakkelijk bekend raken bij derden (bijvoorbeeld door slordigheid van de gebruiker).
- De authenticatie geschiedt slechts één kant op. De gebruiker moet zich bekend maken bij het beveiligingssysteem en daaraan geheime informatie verstrekken, zonder dat hij in staat is de authenticiteit van dat systeem vast te stellen. Handige programmeurs kunnen hiervan misbruik maken door via een namaak-aanlogscherm user-id/password-combinaties te weten te komen.

De meeste beveiligingssystemen bieden voorzieningen om het risico van het gecompromitteerd raken van passwords te verminderen, zoals het hanteren van syntaxregels voor passwords, het af-

1 *Met de term monitoren worden besturingsprogramma's aangeduid voor de ondersteuning van online/real-time-gegevensverwerking, en van persoonlijk computergebruik op een centrale computer.*

2 *"Tempest" is de aanduiding van een Amerikaans regeringsprogramma waaronder computerapparatuur kan worden gecertificeerd voor het niet uitzenden van detecteerbare straling.*

dwingen van regelmatig wijzigen en het toestaan van slechts een gelimiteerd aantal aanlogpogingen. Vaak belangrijker dan deze technische voorzieningen zijn organisatorische maatregelen, die tot doel hebben de eigen verantwoordelijkheid van de gebruiker voor zijn password te benadrukken. (Een voorbeeld van een dergelijke maatregel is het opnemen van een bepaling in het arbeidscontract waarin de gebruiker verantwoordelijk wordt gesteld voor de acties die onder zijn user-id worden uitgevoerd.)

Als bijzonder risico wordt hier nog genoemd het bekend raken van het bestand met user-id/password-combinaties. Bij de meeste beveiligingssystemen is de toegang tot dit bestand beperkt en zijn de passwords encrypt opgeslagen (via een one-way-functie[3]). Als iemand echter toch toegang kan krijgen tot dit bestand (en bijvoorbeeld bij UNIX is dit bestand - vooralsnog - in beginsel openbaar), en in staat is dit te kopiëren, kan hij op zijn gemak passwords uitproberen totdat de encryptie daarvan overeenkomt met een encrypt password in het bestand. (De inbreker moet hiervoor natuurlijk wel kennis hebben van het encryptie-algoritme, maar dat is vaak openbaar; bij UNIX wordt het password zelf als sleutel gebruikt om het getal nul met het DES[4]-algoritme te encrypten. Het resultaat van deze bewerking is het encrypte password. Om doorbreking van de password-geheimhouding op deze manier te bemoeilijken, wordt door UNIX bij het opvoeren of wijzigen van een password hieraan een getal toegevoegd gebaseerd op de systeemtijd, dat mee wordt encrypt.)

In de praktijk worden bij kritische toepassingen ook wel andere vormen van authenticatie gehanteerd, in aanvulling op of in plaats van de password-authenticatie. Een voorbeeld hiervan is het "challenge/response"-mechanisme; in zijn meest eenvoudige vorm wordt hierbij door het beveiligingssysteem met het user-id geen password, maar een (wiskundige) functie geassocieerd. Bij het aanloggen genereert de computer, na identificatie van de gebruiker, een getal (de "challenge"), waarop de gebruiker moet antwoorden met een "response" (een getal dat wordt berekend op basis van het challenge-getal en de wiskundige functie). Het voordeel hiervan is dat het wachtwoord iedere keer anders is. (Als bij deze vorm van authenticatie een complexe wiskundige functie wordt toegepast, wordt aan de gebruiker een speciale rekenmachine ter beschikking gesteld voor de berekening van het response-getal.)
Tegenwoordig wordt ook wel gebruik gemaakt van authenticatiemechanismen die niet alleen zijn gebaseerd op kennis, maar ook op bezit. De combinatie van een fysiek "token", zoals een magneet- of chipkaart, en een geheime sleutel, bijvoorbeeld een pincode, authenticeert de gebruiker.
Veelal nog in een experimenteel stadium verkeren de biometrische authenticatiemechanismen; hierbij wordt de authenticiteit van het subject vastgesteld op basis van (geautomatiseerde) herkenning van meetbare eigenschappen die specifiek zijn voor levende wezens, zoals vinger- en handpalmafdrukken, het patroon van bloedvaten in het netvlies, stemkenmerken en handschriftkarakteristieken. Dergelijke mechanismen worden echter nog niet op grote schaal (in commerciële omgevingen) toegepast.

Het probleem dat slechts eenzijdig authenticatie plaatsvindt, speelt vooral in netwerkomgevingen, waarbij minder zekerheid bestaat over de vertrouwenswaardigheid van de partij waarmee een verbinding tot stand komt. In normale gevallen vertrouwt het subject erop dat hij aanlogt bij een authentiek computersysteem (via een bekende terminal, die in zekere mate fysiek is beveiligd, en die via vaste bekabeling op het centrale systeem is aangesloten, dat weer voldoende is beveiligd tegen inbrekers en manipulatie door frauduleuze programmeurs).
In situaties dat wederzijdse authenticatie wenselijk is kunnen op encryptie gebaseerde protocollen worden toegepast (bijzondere vormen van het eerder genoemde challenge/response-mechanisme).

Als iemand toegang kan krijgen tot het password-bestand kan hij op zijn gemak passwords uitproberen totdat de encryptie ervan overeenkomt met een encrypt password in het bestand.

Formeel geredeneerd dient het subject zich niet alleen te vergewissen van de authenticiteit van het computersysteem waarop hij aanlogt, maar ook van de overige objecten (programma's, bestanden) waartoe hij toegang verzoekt.
Authenticatiemiddelen zijn in dit geval versie-aanduidingen, hash counts, date/time-stamps en dergelijke. De kracht van deze authenticatiemiddelen is afhankelijk van het gemak waarmee zij kunnen worden gemanipuleerd. In de praktijk wordt er meestal op vertrouwd dat het computersysteem de authenticiteit van de objecten waarborgt, waardoor formele authenticatie niet nodig is.

Autorisatie

Objecten waartoe een subject toegang verzoekt zijn behalve het computersysteem zelf, bestanden, programma's, bibliotheken, etc. Objecten en subjecten kunnen hierbij een rolverandering ondergaan: een programma is in eerste instantie een object waartoe een gebruiker toegang verzoekt, en vervolgens een subject dat toegang vraagt tot een bestand. Ook gebruikers zelf, althans de entiteit gebruiker waarover gegevens zijn opgeslagen, kunnen als object fungeren.

Met betrekking tot de toegangsrechten kunnen verschillende bevoegdheden worden onderscheiden, zoals lezen, schrijven, toevoegen, verwijderen en uitvoeren. Minder voor de hand liggend zijn:

3 *Een one-way-encryptie-functie is een functie waarbij encryptie relatief makkelijk is en decryptie relatief moeilijk.*
4 *Data Encryption Standard, een veel gebruikte encryptiestandaard, opgesteld door het Amerikaanse National Institute of Standards and Technology.*

– toestaan (PERMIT of ALLOW): de bevoegdheid om bovenstaande toegangsrechten aan subjecten toe te kennen;

– eigenaar zijn (OWN): de bevoegdheid om PERMIT-bevoegdheid (soms ook OWN-bevoegdheid) toe te kennen.

Beveiligingssystemen die een (al dan niet toegevoegd) onderdeel vormen van het besturingssysteem bieden een grofmazige beveiliging (op het niveau van wat het besturingssysteem als objecten onderkent, dit zijn in het algemeen volumes, libraries en files). In beveiliging op record- of veldniveau moet echter veelal worden voorzien door andere software-lagen, zoals met name het database managementsysteem.
Beveiligingssystemen vertonen onderling verschillen in de mate waarin zij een toegangsregel ondersteunen als: subject (user-id) mag alleen op bepaalde tijden (kantooruren), maar niet gedurende een bepaalde periode (vakantie), uitsluitend vanaf een bepaalde terminal en via een bepaald programma een bepaald object met bepaalde bevoegdheden benaderen.

Alle groepsleden van de groepen waarvan een subject lid is, beschikken over de groepstoegangsrechten tot de objecten waarvan het subject eigenaar is.

Naast gebruikers met de boven beschreven specifieke toegangsrechten kennen beveiligingssystemen gebruikers met algemene privileges ("special", "super" en dergelijke). Deze geprivilegieerde gebruikers zijn onder andere bevoegd algemene beveiligingsopties in te stellen en toegangsregels te onderhouden.

Om te voorkomen dat voor elke subject/object-combinatie toegangsregels moeten worden gedefinieerd, hetgeen onderhoud in een enigszins grootschalige omgeving vrijwel onmogelijk zou maken, bieden de meeste beveiligingssystemen faciliteiten voor het toekennen van regels op groepsniveau (tussen groepen van subjecten en groepen van objecten).
Veel beveiligingssystemen kennen hierbij een driedeling van subjecten in eigenaar (van een bepaald object), lid van de groep van de eigenaar en behorend tot de rest van de wereld. Bij de toekenning van bevoegdheden levert deze indeling, indien zonder nadere verfijning toegepast, problemen op:

– De bevoegdheid van eigenaars om toegangsregels toe te kennen kan leiden tot een diffusie van bevoegdheden en daarmee tot een onbeheersbare situatie.

– Het is niet mogelijk te differentiëren tussen gebruikersbevoegdheden anders dan tussen eigenaar, groep en wereld. Het is bijvoorbeeld niet mogelijk aan één groep leesbevoegdheid toe te kennen en aan een andere schrijfbevoegdheid.

– Als een subject lid kan zijn van meerdere groepen (onder hetzelfde user-id), ontstaat een moeilijk te beheersen structuur van toegangsregels: alle groepsleden van de groepen waarvan een subject lid is, beschikken over de groepstoegangsrechten tot de objecten waarvan het subject eigenaar is.

– Als een subject slechts lid kan zijn van één groep, leidt dit tot een weinig flexibele structuur van toegangsregels, met als gevolg dat deze in de meeste gevallen te ruim moeten worden vastgesteld. (Als voorbeeld kan worden gedacht aan de salarisadministrateur; deze moet kunnen lezen in het bestand met brutosalarisgegevens (en derhalve lid zijn van de desbetreffende groep) en kunnen schrijven in het bestand met nettosalarisgegevens. Dit maakt het noodzakelijk één groep te definiëren voor de bruto- en de nettosalarisgegevens, hetgeen in de meeste gevallen ongewenst is.)

Een mogelijke oplossing is om aan een subject meerdere user-ids (met bijbehorende groepen) te koppelen. Dit heeft onder meer als bezwaar dat een gebruiker niet tegelijkertijd onder meerdere user-ids kan werken.

De huidige beveiligingssystemen die het groeperingsprincipe van eigenaar-groep-wereld toepassen (meest uitgesproken de besturingssystemen UNIX en VAX/VMS), bieden talloze verfijningen van dit principe, waardoor bovengenoemde problemen zich niet hoeven voor te doen. Eén van deze verfijningen is de mogelijkheid dat een programma wordt uitgevoerd onder de bevoegdheden van de eigenaar van dat programma, en niet onder de bevoegdheden van de gebruiker die het heeft opgestart. Op deze manier kan een gebruiker een bestand benaderen (een bekend voorbeeld is het password-bestand, voor het wijzigen van het password), zonder dat hij rechtstreekse toegang tot dat bestand nodig heeft. Helaas maken deze verfijningen op het eenvoudige indelingsprincipe de werking van deze beveiligingssystemen ook wat ondoorzichtiger.
Overigens bieden VAX/VMS en sommige versies van UNIX ook de mogelijkheid via Access Control Lists (ACL's) toegangsregels te definiëren tussen afzonderlijke subjecten en objecten.

Auditing

Om het mogelijk te maken dat achteraf wordt nagegaan welke acties door subjecten zijn uitgevoerd - en zelfs dat tijdens het uitvoeren van de actie dit kan worden bewaakt - voorzien beveiligingssystemen in audit-faciliteiten, die niet alleen inzicht geven in de status van de toegekende bevoegdheden, maar ook in het gebruik dat daarvan wordt gemaakt.
Van belang hierbij is dat elke actie kan worden herleid tot een individuele gebruiker, hetgeen niet mogelijk is als niet-persoonsgebonden user-ids worden gehanteerd.

Het is in het kader van dit inleidende artikel niet mogelijk dieper in te gaan op de uiteenlopende audit-faciliteiten van de verschillende beveiligingssystemen. Wel kan in het algemeen worden gesteld dat deze faciliteiten van de thans beschikbare beveiligingsprodukten voor verbetering vatbaar zijn.

TE STELLEN EISEN

Aan beveiligingssystemen kunnen bepaalde ontwerpeisen worden gesteld. In de literatuur worden onder meer de volgende ontwerpprincipes onderkend:

→ *Good guest.* Indien het beveiligingssysteem geen standaardfunctie is van het besturingssysteem maar een toegevoegde software-laag, dient dit de integriteit van het besturingssysteem als geheel niet aan te tasten.[5]

→ *Self protection.* Programmatuur en bestanden van het beveiligingssysteem zelf mogen alleen met de geëigende hulpmiddelen worden geïnstalleerd en onderhouden.

→ *Least privilege.* Gebruikers en programma's dienen de beschikking te krijgen over zo min mogelijk bevoegdheden, om de schade van een opzettelijke of onopzettelijke fout zoveel mogelijk te beperken. Dit principe staat ook wel bekend als "need to use" of "need to know".

→ *Complete mediation.* Alle toegangsverzoeken dienen via het beveiligingsmechanisme te lopen, en alle toegangsverzoeken moeten worden gecontroleerd.

→ *Permission-based.* Het beveiligingssysteem moet standaard geen toegang verlenen, tenzij een toegangsregel is gespecificeerd.

→ *Accountability.* Het beveiligingssysteem moet uiteraard voorzien in de drie hoofdfuncties die in de voorgaande paragraaf zijn behandeld (de "triple A" authenticatie, autorisatie en auditing). Deze functies worden wel samengevat als accountability.

– *Open design.* De kracht van de beveiliging moet zo min mogelijk afhankelijk zijn van onwetendheid van potentiële inbrekers. Een open ontwerp is daarnaast bevorderlijk voor onafhankelijk onderzoek.

– *Economy of mechanism.* Een simpel beveiligingssysteem is eenvoudig te testen en wekt vertrouwen op.[6]

– *Easy to use.* Een gebruiksvriendelijk beveiligingssysteem vermindert de kans dat gebruikers zullen trachten het te ontwijken.

Voor een nadere uitwerking van deze begrippen wordt verwezen naar de literatuur (bijvoorbeeld de evaluatiecriteria in [DODE85] en [COTE91]). Overigens zou het strikt doorvoeren van deze principes leiden tot een aanzienlijke belasting van het computersysteem. Zo impliceert consequente toepassing van het accountability-principe dat alle handelingen van alle gebruikers worden geregistreerd; complete mediation houdt in dat bijvoorbeeld elke schrijfactie wordt gecontroleerd, en niet slechts het verzoek om een bestand te openen voor schrijven.

ORGANISATORISCHE EN TECHNISCHE RANDVOORWAARDEN

In het voorgaande is al aangegeven dat de effectiviteit van logische toegangsbeveiliging in belangrijke mate afhankelijk is van de organisatorische inbedding daarvan en van bepaalde fysieke (technische) voorzieningen.

Organisatorische randvoorwaarden

Voor installatie en onderhoud van een beveiligingssysteem dient een groot aantal taken te worden uitgevoerd. Bij de toewijzing van deze taken aan functionarissen moet zorgvuldigheid worden betracht, om te voorkomen dat door een ongewenste combinatie van taken bepaalde functionarissen over te ruime bevoegdheden beschikken. Onderstaand wordt kort ingegaan op de taken die voor het installeren en onderhouden nodig zijn. Hiermee wordt niet gepretendeerd een volledig overzicht te geven van de uit te voeren taken, noch een pasklare oplossing te presenteren voor het toewijzingsprobleem.

– Installatie en onderhoud van het pakket zelf. Dit omvat de eerste installatie van het pakket en van onderhoudswijzigingen en nieuwe releases, alsmede het optimaliseren van input/output, performance tuning, etc.
Deze taken komen voor rekening van de functie systeemprogrammering. Voor systeemprogrammatuur dient een aparte test/acceptatie-omgeving te zijn ingericht, net als voor applicatieprogrammatuur. Het inrichten van een dergelijke omgeving voor beveiligingssystemen is echter problematisch, doordat in de testomgeving niet met de actuele toegangsregels kan worden gewerkt, zoals die in de produktie-omgeving gelden.

– Het definiëren van beveiligingsopties. Het gaat hierbij om de opties en parameters die voor het gehele systeem gelden, bijvoorbeeld al dan niet "permission-based". Dit is de uitwerking van een deel van het algemene beveiligingsbeleid, dat onder verantwoordelijkheid valt van het hoogste management (in de gebruikersorganisatie). Het management zal zich hierbij laten adviseren door beveiligingsdeskundigen uit de automatiseringsorganisatie. (In de praktijk zullen zij de aanzet hebben gegeven tot het installeren van het beveiligingssysteem.)

– Het definiëren van toegangsregels. Deze taak valt onder verantwoordelijkheid van de "eige-

5 *Met name de plaatsen waar communicatie plaatsvindt tussen het besturingssysteem en het beveiligingssysteem vormen vulnerabilities (zie de paragraaf over beveiliging in het algemeen). Als een (frauduleus) gebruikersprogramma zich hier kan nestelen, profiterend van de interface-voorzieningen die het besturingssysteem biedt, zou het alle beveiliging kunnen doorbreken.*

6 *Het is aannemelijk dat beveiligingssystemen die zijn geïntegreerd met het besturingssysteem in dit opzicht in het voordeel zijn. De noodzakelijke communicatie met het besturingssysteem kan eenvoudiger plaatsvinden.*

naars" of "houders" van de te beveiligen objecten. Eigenaars of houders[7] zijn inhoudelijk verantwoordelijk voor de objecten. In de praktijk blijkt het aanwijzen van formele eigenaars voor alle te beveiligen objecten een moeizaam proces te zijn.

– Het implementeren van beveiligingsopties en toegangsregels. Functionarissen die met deze taak zijn belast, worden aangeduid met termen als "security administrators", "security officers", "autorisatiebeheerders", etc. Voor het onderbrengen van deze taak bestaat geen principiële voorkeur voor gebruikersorganisatie of automatiseringsorganisatie; om praktische redenen (technische deskundigheid) is zij vaak bij de laatste ondergebracht.

Het ontbreken van een faciliteit van dubbele sluiting bij beveiligingssystemen leidt tot een ongewenste concentratie van bevoegdheden bij de security administrator.

Bij het muteren van gegevens met een veiligheidsrisico (en daar gaat het hier om), is het wenselijk dat het principe van dubbele sluiting wordt toegepast, zodat twee functionarissen nodig zijn om de gegevens te wijzigen. Helaas bieden de meeste beveiligingssystemen deze faciliteit niet. Het ontbreken van deze faciliteit leidt tot een ongewenste concentratie van bevoegdheden bij één functionaris, die technisch niet eenvoudig kan worden beperkt.

– Het controleren van het gebruik van de bevoegdheden (inclusief het afhandelen van security violations, zoals foutieve aanlogpogingen). Het grootste deel van deze taak kan worden uitgevoerd door de security administrator, met als belangrijkste uitzondering de controle op de verrichtingen van de security administrator zelf. Hiervoor dient een onafhankelijke controlefunctionaris te worden aangewezen. In de praktijk blijkt dit vaak problematisch te zijn en wordt de controle ondergebracht bij een functie die daarvoor minder geëigend is (bijvoorbeeld de interne accountantsdienst c.q. EDP-audit-afdeling, die echter tot taak heeft vast te stellen of de interne controle, waaronder de bevoegdheidscontrole, naar behoren functioneert). Bij de controle op de security administrator is het van belang dat zijn verrichtingen kunnen worden geregistreerd zonder dat hij de mogelijkheid heeft deze registratie te beïnvloeden. Ook in dit opzicht schieten veel beveiligingssystemen te kort. De logging-opties kunnen vaak (deels of indirect) door de security administrator worden gewijzigd. Deze onvolkomen audit-faciliteiten, in combinatie met de eerder genoemde concentratie van bevoegdheden, hebben tot gevolg dat aan de functie security administrator een veiligheidsrisico is verbonden.

In het bovenstaande is afgezien van het proces van selecteren van een beveiligingspakket. Meestal wordt de keuzevrijheid beperkt door de reeds aanwezige hardware; de keuze van een hardwareplatform wordt als regel bepaald door de beschikbaarheid van applicaties of applicatie-ontwikkelomgevingen. Beveiligingsoverwegingen zullen slechts in uitzonderingsgevallen een doorslaggevende rol spelen. Voor zover keuzevrijheid bestaat, geldt voor de taken en verantwoordelijkheden hetzelfde als voor het definiëren van beveiligingsopties.
De functionaliteit van beveiligingssystemen kan, behalve via optie-instellingen, vaak ook worden beïnvloed door coding toe te voegen (met name in IBM-omgevingen, waarbij dergelijke coding die wordt toegevoegd aan systeemprogrammatuur "exit" wordt genoemd). De ontwikkeling en implementatie hiervan zullen, anders dan bij de beveiligingsopties, meestal door de functie systeemprogrammering worden uitgevoerd.

Technische randvoorwaarden

Een essentieel kenmerk van logische beveiliging is dat zij functioneert als proces[8] in het interne geheugen van de computer. De effectiviteit van de logische beveiliging staat of valt met de beveiliging van het interne geheugen. Niet alleen moeten de verschillende gebruikersprocessen die in het interne geheugen actief zijn worden beschermd, maar ook, en met name, het besturings- en beveiligingssysteem.

Om te voorkomen dat gebruikersprogramma's per ongeluk of met opzet delen van het interne geheugen zouden overschrijven die gereserveerd waren voor het besturingssysteem, werden door computerleveranciers al heel vroeg voorzieningen in de hardware ingebouwd die verhinderden dat gebruikersprogramma's dat deel van het geheugen konden adresseren. De huidige generatie computers maakt gebruik van verschillende mechanismen voor de beveiliging van het interne geheugen:

– Het toevoegen van "tags" aan woorden in het interne geheugen. Tags zijn labels bestaande uit één of meer bits die de toegangsrechten tot het geheugenwoord aangeven en alleen door het besturingssysteem kunnen worden gewijzigd. Deze architectuur wordt onder andere toegepast bij Unisys A Serie en IBM AS/400.

– Segmentering. Hierbij worden gegevens en programmadelen in logische delen, segmenten, opgesplitst en wordt het interne geheugen geadresseerd via een segmentnaam en een relatief adres ("offset") binnen dat segment. Alle segmenttabellen worden bijgehouden door het besturingssysteem, dat hierdoor in staat is toegangsverzoeken tot geheugensegmenten te controleren, waarbij het onderscheid kan maken tussen bijvoorbeeld lees- en schrijfbevoegdheid.[9]

– Paginering. Dit is vergelijkbaar met segmentering, maar de segmenten, pagina's, hebben hierbij een vaste omvang, waardoor het interne geheugen efficiënter kan worden benut.
Paginering (in combinatie met segmentering) wordt bij de meeste computersystemen toegepast

7 *Sommigen geven de voorkeur aan de term houder in plaats van eigenaar, anderen geven aan de begrippen een enigszins verschillende inhoud.*

8 *Een proces is in dit verband een computerprogramma in uitvoering.*

9 *Aan segmentering is overigens wel het risico verbonden dat door het kiezen van een offset groter dan het segment, geheugenruimte kan worden benaderd die buiten het toegewezen segment ligt. Het besturingssysteem moet dan ook controleren of de offset binnen het segment valt (dat tijdens de uitvoering van een programma in grootte kan veranderen). Deze controle leidt tot een extra belasting van het besturingssysteem.*

(zoals VAX/VMS van Digital en de S/370- en S/390-architecturen van IBM).

Onafhankelijk van de wijze waarop adressering plaatsvindt dient het besturingssysteem toegang te hebben tot het gehele interne geheugen. Om onderscheid te kunnen maken tussen het besturingssysteem, dat het gehele geheugen rechtstreeks moet kunnen adresseren, en gebruikersprogramma's, die langs de geëigende weg moeten gaan, kent de processor (minimaal) twee "modes": "user mode" en "system mode". Een proces in user mode kan niet buiten het voor het proces bestemde deel van het geheugen komen.

Bij de huidige general purpose, multi-user computers kan men in de meeste gevallen ervan uitgaan dat de combinatie van hardware en besturingssysteem voldoende beveiliging biedt van het interne geheugen. Tot voor kort vertoonden vooral personal computers in dit opzicht tekortkomingen. Een sluitende (software-matige) beveiliging van deze computers was dan ook niet goed mogelijk. PC's met de nieuwste generatie processoren (bijvoorbeeld Intel vanaf 80286) en de nieuwste besturingssystemen (OS/2, Windows) doen in dit opzicht echter niet meer voor de mainframes onder.

STANDAARDISATIE EN CERTIFICERING

Wie tegenwoordig een artikel opslaat over logische beveiliging, treft daarin vrijwel altijd een verwijzing aan naar het "Orange book" ([DODE85] - oorspronkelijk verschenen in 1983, de huidige versie werd gepubliceerd in 1985), of naar andere standaarden voor beveiliging (zoals [COTE91]). Deze standaarden bevatten criteria voor de evaluatie van computersystemen op beveiligingsaspecten. Speciaal daartoe aangewezen of daarvoor ingestelde keuringsinstanties kunnen op basis van een - meestal langdurige - evaluatie certificaten verstrekken volgens de beveiligingscriteria van de standaard.

Wereldwijd het meest gezaghebbend zijn de "trusted computer system evaluation criteria" van het Orange book. Hoewel oorspronkelijk ontwikkeld voor militaire omgevingen, waarin het geheimhoudingsaspect voorop staat, zijn deze criteria inmiddels ook van betekenis geworden voor commerciële omgevingen.

Als belangrijkste algemene (beheersings)doelstellingen van computerbeveiliging worden in het Orange book onderkend:

- Het definiëren en implementeren van een "security policy". Computerbeveiliging is geen absoluut begrip, maar moet nader worden omschreven in termen van de beveiligingsdoelstellingen die ermee moeten worden bereikt en de bedreigingen die ermee moeten worden afgewend. Een security policy is een expliciete uitspraak over deze beveiligingsdoelstellingen, die mede gebaseerd moeten zijn op geldende regelgeving en algemene beleidsuitgangspunten.
- "Accountability". Dit omvat de identificatie en authenticatie van individuele gebruikers, alsmede het (selectief) vastleggen van de handelingen die door hen worden verricht (audit-informatie). De audit-informatie moet beschermd zijn en daarnaast makkelijk toegankelijk ten behoeve van onafhankelijke controle.
- "Assurance". In voldoende mate moet zijn gewaarborgd dat de security policy correct op het computersysteem is geïmplementeerd en dat de beveiligingsdoelstellingen inderdaad worden bereikt.

Deze algemene beheersingsdoelstellingen worden nader uitgewerkt in zes meer concrete eisen en vervolgens in zevenentwintig evaluatiecriteria.

Hoewel oorspronkelijk ontwikkeld voor militaire toepassingen zijn de evaluatiecriteria van het Orange book inmiddels ook van betekenis geworden voor commerciële omgevingen.

In het Orange book worden computersystemen, op basis van de mate waarin zij aan de evaluatiecriteria voldoen, ingedeeld in de volgende klassen:

- D: "minimal protection". In deze klasse vallen computersystemen die niet aan de noodzakelijke criteria voldoen om in een hogere klasse te kunnen worden ingedeeld.
- C: "discretionary protection". Beveiliging moet mogelijk zijn op aanwijzing (volgens de "discretion") van een eigenaar of verantwoordelijke gebruiker. Deze klasse wordt nader onderverdeeld in C1 en C2 (met oplopende vereisten).
- B: "mandatory protection". Beveiliging moet kunnen worden afgedwongen door het gebruik van labels. Binnen deze klasse wordt nader onderscheid gemaakt tussen B1, B2 en B3.
- A: "verified protection". Bij deze klasse moet formeel kunnen worden aangetoond dat althans het ontwerp voldoet aan de gestelde beveiligingseisen. Deze klasse wordt nader onderscheiden in A1 (verifieerbaar ontwerp) en hoger (verifieerbare implementatie, niet nader onderverdeeld in subklassen).

De thans op de markt zijnde beveiligingsprodukten voor mainframe- en minicomputers beschikken meestal over een C2-classificatie. De meeste leveranciers hebben aangekondigd te streven naar het verkrijgen van een B(2)-certificaat, waarin enkele reeds zijn geslaagd. B2-produkten zijn vooralsnog echter vrij kostbaar.
Een toegekend beveiligingscertificaat aan een bepaald computersysteem houdt niet noodzakelijkerwijs in dat een willekeurige installatie aan de eva-

luatiecriteria voldoet, zelfs als hetzelfde model computer en dezelfde versies van de besturingsprogrammatuur worden gebruikt. Veel van de beveiligingsvoorzieningen waarop het certificaat betrekking heeft, moeten via optie-instellingen bij installatie worden geactiveerd. Bij de meeste installaties zullen niet alle beveiligingsopties worden benut. (Daarnaast is het onwaarschijnlijk dat een bepaalde installatie exact overeenkomt met de geëvalueerde installatie - in het bijzonder bij IBM-systemen, met een groot aantal afzonderlijke besturingsprogramma's met elk een eigen versie.)

Hoewel het Orange book en andere standaarden zeker een stimulans hebben betekend voor het proces van bewustwording van het belang van computerbeveiliging, moet hun betekenis (voor commerciële omgevingen) niet worden overschat. Op een aantal punten vertonen de standaarden belangrijke tekortkomingen (zie ook [NGIS90]):

- In de standaarden zijn geen eisen beschreven die afdwingen dat voor bepaalde handelingen meerdere functionarissen nodig zijn. De ongewenste concentratie van bevoegdheden bij de security administrator wordt derhalve door de standaarden niet tegengegaan.

- In het bijzonder het Orange book is sterk georiënteerd op het beveiligingsmodel van Bell en LaPadula (onder andere [BELL73]) dat is gericht op de geheimhouding van gegevens. In commerciële omgevingen is de integriteit van gegevens over het algemeen van groter belang dan de vertrouwelijkheid. Voor zover integriteitsmodellen in de literatuur zijn beschreven (bijvoorbeeld [CLAR87]), hebben zij nog niet geleid tot concrete evaluatiecriteria in de standaarden, al biedt bijvoorbeeld [COTE91] hiertoe wel de mogelijkheid.

Om een indruk te krijgen van de betrekkelijke betekenis van een certificaat volgens het Orange book kan men denken aan het evaluatiecriterium "object reuse". Om te voldoen aan dit criterium moeten geheugenmedia, voordat zij ter beschikking worden gesteld aan subjecten, worden geschoond van eventuele gegevens die er door processen van een ander subject op zijn achtergelaten.

De functionaliteit van commerciële beveiligingsprodukten is in sommige opzichten meer gericht op het verkrijgen van een gunstig certificaat, dan op de beveiligingsbehoeften in het bedrijfsleven.

Gedurende een bepaalde periode had RACF in dit opzicht een achterstand op zijn belangrijkste rivalen, doordat het geen faciliteit ondersteunde voor het wissen van geheugenmedia, hetgeen tot uitdrukking kwam in "slechts" een C1-certificaat.

Voor een C2-certificaat is vereist dat er "system wide" een optie is voor het wissen van geheugenmedia voor hergebruik. Voor commerciële omgevingen is een dergelijke optie, die leidt tot een extra belasting van het computersysteem, in het algemeen niet interessant. Niettemin bood RACF vanaf een bepaalde release de mogelijkheid van "erase on scratch" op systeemniveau (en voldeed daarmee aan de C2-criteria). Pas enige releases later maakte RACF het mogelijk deze optie in te stellen op bestandsniveau (wat voor commerciële omgevingen wel van belang kan zijn).

Het bovenstaande doet vermoeden dat sommige functionaliteit van commerciële beveiligingsprodukten niet zozeer is gericht op de beveiligingsbehoeften in het bedrijfsleven, als wel op het - uit marketingoverwegingen - verkrijgen van een zo gunstig mogelijk Orange book-certificaat.

EDP-AUDIT

In deze paragraaf wordt kort stilgestaan bij de wenselijkheid en de wijze van uitvoering van een (EDP-)audit van logische toegangsbeveiliging. Met deze korte en vereenvoudigde beschrijving zou ten onrechte de indruk kunnen worden gewekt dat een dergelijke audit gemakkelijk is uit te voeren; in werkelijkheid zal hiermee echter een aanzienlijke inspanning zijn gemoeid. Tevens is een diepgaande (technische) kennis vereist van het beveiligingsprodukt en de omgeving waarin het wordt toegepast.

Verschillende omstandigheden dragen ertoe bij dat het wenselijk is dat de implementatie van logische toegangsbeveiliging op gezette tijden door onafhankelijke functionarissen wordt beoordeeld op de mate waarin deze een effectieve bijdrage levert aan de gestelde of te stellen beveiligingsdoelstellingen:

- Inhoudelijk verantwoordelijk voor de beveiliging van de geautomatiseerde gegevensverwerking is het management in de gebruikersorganisatie, maar de uitvoerende taken komen voor een belangrijk deel voor rekening van de automatiseringsorganisatie (bij wijze van gedelegeerde bevoegdheid). Als gevolg van de deskundigheidskloof tussen deze organisaties is de eerste in het algemeen niet goed in staat de betrouwbaarheid van de verantwoordingsinformatie van de tweede te beoordelen.

- De concentratie van bevoegdheden bij de belangrijkste uitvoerder van de logische beveiligingsmaatregelen (security administrator), in combinatie met de gebrekkige (technische) interne-controlemogelijkheden daarop, maakt het noodzakelijk dat de interne controle gericht op zijn functioneren kritisch wordt beoordeeld.

De EDP-audit van logische toegangsbeveiliging zal zijn gericht op de effectiviteit daarvan, dat wil zeggen de mate waarin zij bijdraagt aan het bereiken van de beveiligingsdoelstellingen (in termen van het Orange book: de security policy) van de orga-

nisatie. De beveiligingsdoelstellingen zullen weer een afgeleide zijn van de algemene organisatiedoelstellingen.
Niet altijd zal er een expliciet beveiligingsbeleid door het management zijn geformuleerd. De EDP-auditor kan dan een adviserende bijdrage leveren aan het opstellen van een dergelijk beleid.

Ervan uitgaande dat er een beveiligingsbeleid is geformuleerd, kunnen bij een EDP-audit de getroffen beveiligingsmaatregelen in opzet, bestaan en/of werking worden gecontroleerd. Aandachtspunten zijn in ieder geval de organisatorische beheersstructuur (taakverdelingen, procedures voor het definiëren en implementeren van bevoegdheden, alsmede de controle daarop, en voor het afhandelen van overtredingen, etc.), de technische infrastructuur (bijvoorbeeld de interfaces met andere besturingsprogrammatuur), de algemene optie-instellingen en de feitelijk toegekende bevoegdheden (in het bijzonder de geprivilegieerde bevoegdheden).

Bij een audit van de opzet van de getroffen maatregelen wordt op basis van beschrijvingen en interviews een oordeel gevormd over de mate waarin zij het beveiligingsbeleid ondersteunen. Norm bij deze audit is het beveiligingsbeleid, terwijl de "evidence" bestaat uit handboeken, procedurebeschrijvingen, besprekingsverslagen en dergelijke.

Een audit van het bestaan houdt in dat wordt nagegaan of de maatregelen die zijn beschreven ook daadwerkelijk worden uitgevoerd. Bij een dergelijke audit geldt als norm de opzet (die is getoetst aan het beveiligingsbeleid) en wordt bevestiging gezocht van hetgeen is gesteld of beweerd door middel van directe waarnemingen (bijvoorbeeld bij terminals) en in registraties die als bewijs kunnen dienen, zoals:

- formulieren voor het aanvragen van bevoegdheden, alsmede voorbeelden hiervan die door geautoriseerde functionarissen zijn geparafeerd;
- een overzicht van de ingestelde beveiligingsopties uit het systeem;
- overzichten van toegekende bevoegdheden uit het systeem;
- logging-informatie uit het systeem over het gebruik van toegekende bevoegdheden, alsmede een registratie van de afwerking daarvan.

Voor de beoordeling van de betrouwbaarheid van dergelijk bewijsmateriaal is een zekere deskundigheid vereist.

Bij een audit van de werking wordt het bestaan van de maatregelen niet alleen op een bepaald moment, maar gedurende een zekere periode vastgesteld.

TENSLOTTE

Volgens het Orange book zijn de belangrijkste doelstellingen die met computerbeveiliging moeten worden bereikt: het realiseren van een expliciet beveiligingsbeleid (security policy), identificatie en authenticatie van subjecten, alsmede het registreren van hun activiteiten (accountability) en het afdwingen van de security policy en de accountability (assurance).

Als bezwaar tegen (certificering volgens) deze driedeling kan worden ingebracht dat functionele eisen (security policy en accountability) op één hoop worden gegooid met technische eisen (assurance), maar dit terzijde.

Om de doelstelling van assurance te bereiken zal het beveiligingssysteem aan bepaalde ontwerpeisen moeten voldoen, zoals "complete mediation" en "economy of mechanism".
Voor een geïntegreerd systeem is dit wellicht eenvoudiger te realiseren dan voor een computersysteem met een toegevoegd beveiligingspakket. De praktijk geeft vooralsnog echter geen aanleiding te veronderstellen dat een toegevoegd pakket niet hetzelfde Orange book-certificaat kan krijgen als een beveiligingssysteem dat is geïntegreerd met het besturingssysteem.

Drs. P. Veltman RA
Is sedert 1983 werkzaam bij KPMG Klynveld, thans in de functie van senior EDP-auditor. Zijn audit-ervaring ligt op het terrein van besturingssystemen en beveiligingspakketten, informatiesystemen en automatiseringsorganisaties. Hij heeft een aantal artikelen over deze onderwerpen gepubliceerd.

LITERATUUR

[BELL73] D.E. Bell and L.J. LaPadula, *Secure Computer Systems; A Mathematical Model*, The Mitre Corp., 1973.

[CLAR87] D.D. Clark and D.R. Wilson, *A Comparison of Commercial and Military Security Policies*, Proceedings of the 1987 IEEE Symposium on Security and Privacy.

[COTE91] Commission of the European Communities, Directorate General XIII, Directorate F, *Information Technology Security Evaluation Criteria*, Provisional Harmonised Criteria, Version 1.2, June 1991.

[DODE85] Department of Defense, *Trusted Computer System Evaluation Criteria*, DoD 5200.28-STD, 1985.

[DUYM87] M.C. Duym, *Belangrijke functies van een toegangsbeveiligingspakket*, in Compact 1987/45.

[NGIS90] NGI, Sectie EDP Auditing, Werkgroep beveiligingssystemen, *Beveiligingssystemen - een visie op toegang toegang tot een visie*, Nederlands Genootschap voor Informatica, 1990.

[PFLE89] Charles P. Pfleeger, *Security in Computing*, Prentice-Hall International, Inc., 1989.

[WINK90] Drs.ing. J.C. van Winkel RI, *UNIX-beveiligingsaspecten*, in Compact 1990/1.

[WINK91] Drs.ing. J.C. van Winkel RI, *De relatieve veiligheid van PC-besturingssystemen*, in Compact 1991/2.

Toepassing van CA-ACF2 in de praktijk

Ing. D.J. Huis

**CA-ACF2 is een door Computer Associates geleverd hulpmiddel voor logische toegangscontrole voor MVS-omgevingen.
De auteur geeft vanuit zijn EDP-audit-ervaring een beschrijving van de wijze waarop dit pakket bij de NMB-bank wordt gebruikt en de bijzondere aandachtspunten bij een beoordeling van de effectiviteit ervan.**

INLEIDING

In de afgelopen twee decennia hebben de ontwikkelingen in de automatisering een grote invloed gehad. Naast een meer efficiënte gegevensverwerking en een betere informatievoorziening aan medewerkers en cliënten heeft de toenemende automatisering echter ook een aantal neveneffecten gehad. In het kader van dit artikel wordt volstaan met een beperkte opsomming:

- De gegevensopslag is meer gecentraliseerd, waardoor een steeds grotere afhankelijkheid van de gegevens is ontstaan.

- De bewerkingen op de daadwerkelijke gegevens zijn veel verder van de gebruiker af komen te staan: programmatuur brengt wijzigingen aan op gegevens op voor gebruikers ondoorzichtige wijze. Hierdoor is de kans op ontdekking van bewuste of onbewuste fouten afgenomen.

- De gegevens worden op een zodanige manier opgeslagen dat zij slechts door de machine te lezen zijn: zonder aanvullende beveiligingsmaatregelen is het hierdoor mogelijk kopieën van gegevens te maken of wijzigingen in gegevens aan te brengen, terwijl de gebruiker daar niets van bemerkt. Wijzigingen in bestanden kunnen via computernetwerken en terminals op honderden kilometers afstand van de fysieke opslagplaats van de gegevens worden geïnitieerd.

Hieruit kan worden afgeleid dat de automatisering enerzijds noodzakelijk is voor een efficiënte bedrijfsvoering en voor een tijdige en adequate informatieverstrekking, maar dat anderzijds de automatisering bedrijven ook kwetsbaarder maakt. Vandaar dat een goede beveiliging van gegevens en programmatuur noodzakelijk is. Enerzijds uit deze beveiliging zich in de fysieke beveiliging van computercentra; anderzijds worden door middel van toegangsbeveiligingspakketten logische toegangsbeveiligingsmaatregelen genomen om de gegevens te beschermen tegen ongeautoriseerde manipulaties. In de loop der tijd is de functionaliteit van deze pakketten steeds verder uitgebreid. Van doorslaggevend belang voor het uiteindelijk gerealiseerde beveiligingsniveau zijn echter de technische en vooral de organisatorische implementatie van het beveiligingspakket.

Dit artikel beschrijft de toepassing van het beveiligingspakket CA-ACF2 (van Computer Associates) voor het centrale IBM-mainframe-systeem van de NMB-bank.
Hiertoe wordt eerst ingegaan op de ontwikkelingen binnen de bank met betrekking tot het gebruik van ACF2 sinds de implementatie van het pakket tot heden. Vervolgens wordt globaal aandacht besteed aan de opzet en de technische werking van ACF2. Daarna wordt stilgestaan bij de huidige organisatorische implementatie van ACF2 binnen de NMB-bank. Vervolgens komt de technische implementatie van ACF2 binnen de NMB-bank aan bod. Ten slotte wordt aandacht besteed aan de controleaanpak binnen de NMB-bank met betrekking tot ACF2.

ONTWIKKELINGEN MET BETREKKING TOT ACF2 BINNEN DE NMB-BANK

Zoals bekend mag worden verondersteld, is de NMB-bank in 1989 gefuseerd met de Postbank. Inmiddels is de organisatorische integratie van beide banken vrijwel afgerond. Deze organisatorische integratie zal met het oog op de gewenste synergie-effecten in de (nabije) toekomst ook leiden tot een bezinning omtrent de te hanteren technische hulpmiddelen. Gezien het feit dat Postbank en NMB-bank verschillende pakketten toepassen voor de beveiliging van de mainframe-omgevingen (respectievelijk RACF en ACF2) zal dit ook gevolgen hebben voor het toe te passen beveiligingspakket. Op korte termijn zal hiervoor een keuze worden gemaakt. Om onduidelijkheden en inconsistenties te vermijden is deze problematiek bij de samenstelling van dit artikel geheel buiten beschouwing gelaten. Het artikel refereert derhalve aan de organisatie van de NMB-bank en de technische implementatie van ACF2 zoals deze voor de fusie bestonden.

In 1979 werd door een binnen de NMB-bank ingestelde werkgroep onderzoek gedaan naar de functionaliteit en de werking van een aantal beveiligingspakketten voor IBM-mainframe-systemen:
- RACF;
- SECURE;
- ACF2.

Op grond van afwegingen met betrekking tot onder andere functionaliteit en performance werd op 28 februari 1980 het pakket ACF2 door de NMB-bank aangeschaft. Na uitgebreide acceptatietests werd het pakket op het centrale produktiesysteem ingevoerd. In de loop der tijd werd de functionaliteit van het pakket verder uitgebreid door nieuwe releases en door koppelingen met specifieke, binnen de bank toegepaste programmapakketten. Tevens werd programmatuur ontwikkeld om, uitgaande van de logging van ACF2, een voor de NMB-bank bruikbare rapportage op te leveren omtrent wijzigingen in de autorisaties en pogingen tot overtreding van de beveiligingsregels (security violations).

Een wezenlijk uitgangspunt bij de keuze van het beveiligingspakket was dat de organisatorische eenheid die verantwoordelijk is voor de inhoud van een bestand ook verantwoordelijk is voor dat deel van het autorisatieschema dat op dat bestand betrekking heeft. Deze doelstelling werd echter in eerste instantie, ondanks de technische mogelijkheden die ACF2 hiervoor bood, niet gerealiseerd. Bij de introductie van ACF2 werd het beheer van de beveiligingsstructuur (de security officer-functie) bij gebrek aan alternatieven namelijk geplaatst bij de afdeling Systeemontwikkeling en Onderhoud van de Interne Accountantsdienst. Wel werd hierbij vastgesteld dat deze organisatorische plaatsing minder gelukkig was en dat op termijn naar een betere inbedding van de security officer-functie zou moeten worden gezocht. In februari 1986 werd deze functie derhalve overgeheveld naar een aparte afdeling Informatiebeveiliging (zie verder de paragraaf Organisatorische implementatie ACF2 bij de NMB-bank). Na deze organisatiewijziging werd de decentralisatie van de security officer-functie gerealiseerd. Naast de centraal opererende Master Security Officer werden binnen de bedrijfsonderdelen Restricted Security Officers aangesteld, die verantwoordelijk werden gesteld voor de verstrekking en het beheer van autorisaties met betrekking tot de tot het bedrijfsonderdeel behorende bestanden en gebruikers.

GLOBALE OPZET EN WERKING VAN ACF2

In het bestek van dit artikel wordt globaal ingegaan op de opzet en de technische werking van ACF2. Tevens komt hierbij een aantal belangrijke begrippen aan de orde.

Het doel van een toegangsbeveiligingspakket kan worden omschreven als: het beveiligen van de logische toegangspaden via de computer of via een computernetwerk tot gegevens of andere te beveiligen componenten. Beveiligen heeft hierbij betrekking op het voorkomen dat ongeautoriseerd kennis wordt genomen van respectievelijk invloed wordt uitgeoefend op de te beveiligen componenten. De functie van een toegangsbeveiligingspakket is beperkt tot de logische afscherming van de te beveiligen componenten en houdt dus geen (overigens noodzakelijke) fysieke beveiliging in.

In zijn algemeenheid zijn de functies van beveiligingspakketten naar een drietal gezichtspunten te onderscheiden:

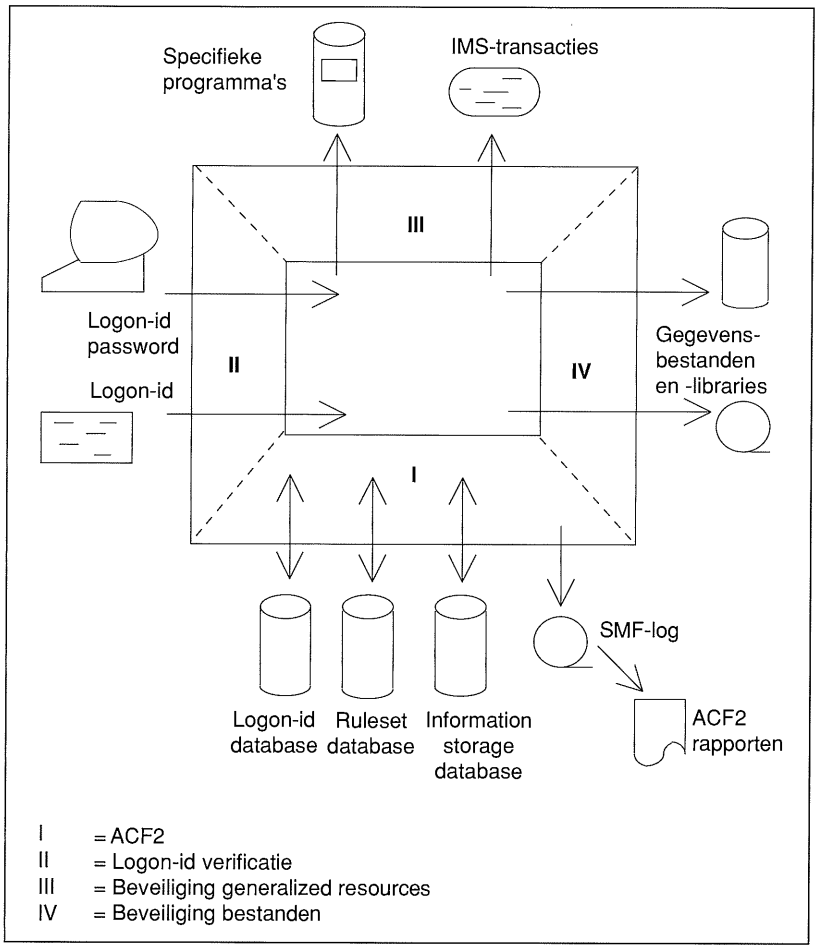
- De *identificatiefunctie:* dit betreft het identificeren van de persoon of het programma dat de beveiligde componenten tracht te benaderen. Het is namelijk noodzakelijk onderscheid te kunnen maken tussen de diverse gebruikers. Hiertoe wordt gebruik gemaakt van unieke gebruikerscodes, in ACF2-terminologie logon-ids genoemd.

- De *authenticatiefunctie:* dit betreft het vaststellen dat de geïdentificeerde persoon degene is voor wie hij zich uitgeeft. Dit gebeurt in zijn algemeenheid door toepassing van passwords.

- De *autorisatiefunctie:* het beveiligingspakket beheert op basis van in het systeem vastgelegde autorisatieregels de toegang tot de beveiligde componenten. In het vervolg van deze paragraaf zal nader worden ingegaan op de wijze waarop deze drie functies binnen ACF2 zijn gerealiseerd (zie figuur 1 op de volgende pagina).
Daarnaast zal worden ingegaan op de technische opbouw van de ACF2 databases en op de technische werking van ACF2.

Identificatiefunctie

De identiteit van een gebruiker wordt vastgelegd door middel van een unieke gebruikerscode, het



Figuur 1. Functies van ACF2.

logon-id. In de NMB-omgeving wordt voor het logon-id gebruik gemaakt van het (unieke) personeelsnummer. Behalve deze identificatie van personen kent ACF2 ook het toewijzen van logon-ids aan jobs en started tasks. Een job is een samenstel van bij elkaar behorende programma's (jobsteps), dat binnen het computersysteem aan de hand van een toegekende jobnaam wordt geïdentificeerd. Started tasks zijn programma's die automatisch dan wel vanaf het master console door operators worden gestart en dan veelal gedurende langere tijd actief blijven. ACF2 biedt dus een fijnmazige identificatie van de verschillende "gebruikers" (in de ruime zin van het woord) van het computersysteem.

Authenticatiefunctie

Om de authenticiteit van de gebruiker van een logon-id vast te stellen, dient de gebruiker bij het aanloggen een password in te toetsen. De passwords worden door ACF2 one-way encrypted opgeslagen, hetgeen inhoudt dat er geen algoritme bestaat om vanuit de opgeslagen geëncrypte passwords het werkelijke password te herleiden. Door middel van ACF2 kan een aantal maatregelen met betrekking tot het gebruik van de passwords worden afgedwongen. ACF2 biedt hiertoe onder andere instelmogelijkheden voor de minimale lengte van het password en de maximum geldigheidsduur van een password. ACF2 biedt daarnaast de mogelijkheid om het gebruik van logon-ids te beperken tot specifieke terminals of (in het geval van jobs of started tasks) tot specifieke paden waarlangs het systeem wordt benaderd. Met name voor jobs en started tasks biedt dit een (beperkte) mogelijkheid voor de vaststelling van de authenticiteit van het logon-id.

Autorisatiefunctie

Autorisaties binnen computersystemen hebben betrekking op de bevoegdheid voor het uitvoeren van specifieke activiteiten binnen het computersysteem. Hierbij zijn meerdere soorten autorisaties mogelijk. Voorbeelden hiervan zijn:

- autorisatie voor het gebruik van monitorprogrammatuur, waardoor vanaf een terminal met de centrale computer kan worden gecommuniceerd. Voorbeelden hiervan zijn IMS/DC, TSO en Roscoe. Dit betreft algemene privileges, die per logon-id kunnen worden verstrekt;

- autorisatie voor het benaderen van bestanden: per bestand of groep bestanden kan worden aangegeven welke gebruikers (personen, jobs of started tasks) bepaalde manipulaties mogen uitvoeren (programma-uitvoering, lezen, schrijven of alloceren);

- autorisatie voor het uitvoeren van specifieke transacties: per transactie kan worden aangegeven welke personen deze kunnen uitvoeren. Het betreft transacties van diverse pakketten, zoals IMS en CICS;

- autoriseren van het gebruik van specifieke programma's: ACF2 biedt mogelijkheden om specifieke risicovolle programma's af te schermen en slechts specifieke logon-id's te autoriseren voor het uitvoeren hiervan.

Technische opbouw van ACF2

Om bovengenoemde functies naar behoren te kunnen uitvoeren, beschikt ACF2 over een drietal databases:
- de logon-id database;
- de ruleset database;
- de information storage database.

Logon-id database
De logon-id database bevat voor ieder logon-id een record. Dit record bevat gegevens van verschillende aard:

- Identificatie: deze velden hebben betrekking op de houder van het logon-id. Voorbeelden hiervan zijn de locatiecode, het telefoonnummer, de afdelingscode, etc.

- Beperkingen: in het logon-id kunnen bepaalde beperkingen met betrekking tot het gebruik van het logon-id worden opgenomen. Zo kan het ge-

bruik worden beperkt tot bepaalde terminals of tot bepaalde uren van de dag.

– Privileges: deze velden geven bepaalde privileges van het desbetreffende logon-id weer. Enerzijds kunnen dit privileges met betrekking tot ACF2 zijn (ten behoeve van het beheer van of de controle op ACF2); anderzijds kunnen deze privileges ook betrekking hebben op het gebruik van specifieke pakketten. Een bijzonder privilege wordt gevormd door het non-cancellable attribuut. Deze logon-ids hebben toegang tot alle bestanden en overige resources; de toegang wordt wel door ACF2 gecontroleerd en gelogd, maar wordt niet onderbroken.

– Statistische gegevens: deze gegevens geven inzicht in het aantal aanlogpogingen, het aantal security violations en dergelijke.

Bij de installatie van ACF2 kunnen naast de standaard opgenomen velden nog installatie-afhankelijke velden worden opgenomen. Hierbij kan voor ieder veld in het logon-id record worden gespecificeerd wie de inhoud daarvan kan inzien of wijzigen. Bij de installatie van ACF2 dient tevens te worden opgegeven hoe de zogenaamde user identification-string (UID-string) is opgebouwd. De UID-string is een veld dat wordt opgebouwd uit een aantal velden uit het logon-id record. De UID-string kan bijvoorbeeld een afdelingscode, een functiecode of een applicatiecode of combinaties hiervan bevatten. De toetsing van de autorisatieregels vindt plaats met de UID-string. Hierdoor behoeven de individuele logon-ids niet afzonderlijk bij de autorisatieregels te worden gespecificeerd, maar kan (door een juiste toepassing van de UID-string) met een meer algemene autorisatieregel worden volstaan.

Ruleset database
De ruleset database bevat alle toegangsregels tot bestanden. ACF2 heeft als eigenschap dat alle bestanden automatisch zijn beveiligd. Dit houdt in dat voor alle (groepen van) bestanden toegangsregels dienen te zijn gedefinieerd. Bestandsnamen bij MVS bestaan uit een aantal delen (qualifiers), gescheiden door punten.
Groepering binnen ACF2 vindt plaats op basis van de eerste qualifier van de datasetnaam. Voor iedere op deze wijze gevormde groep bestanden wordt in ACF2 een ruleset gedefinieerd. Deze rulesets bestaan uit:
- identificatiegegevens: de naam van de ruleset en de naam van de eerste qualifier van de desbetreffende groep bestanden;
- beheerinformatie: hierin wordt vastgelegd welke UID-strings naast de security officer de desbetreffende ruleset mogen wijzigen;
- de toegangsregels: deze regels kunnen per bestand of groep bestanden toegang verlenen aan (groepen van) UID-strings.

Met betrekking tot de toegang tot bestanden maakt ACF2 onderscheid tussen de volgende bevoegdheden:
- exec: de bevoegdheid programma's vanuit het desbetreffende bestand (of de desbetreffende library) uit te voeren (impliceert dus geen leesbevoegdheid);
- read: de bevoegdheid de inhoud van bestanden te lezen (of te kopiëren naar een ander bestand);
- write: de bevoegdheid de inhoud van het bestand te wijzigen;
- alloc: de bevoegdheid bestanden aan te maken, te verwijderen of een andere naam te geven.

Voor elk van deze bevoegdheden kan worden opgegeven of een logging van het gebruik ervan moet plaatsvinden.

Information storage database
Deze database bevat enerzijds de resource-autorisaties (voor andere resources dan bestanden) en anderzijds de centraal beheerde systeemopties (global system options).

De resource-autorisaties zijn vastgelegd in zogenaamde generalized resource rules. Deze rules hebben bijvoorbeeld betrekking op IMS-transacties of op specifieke, risicovolle programma's. Generalized resource rules kunnen ook bij de installatie voor eigen toepassingen worden gedefinieerd. Autorisatieverlening met betrekking tot generalized resources verloopt op gelijke wijze als de autorisatieverlening met betrekking tot bestanden, met dien verstande dat slechts onderscheid wordt gemaakt tussen:
- gebruik toegestaan;
- gebruik toegestaan, maar gelogd;
- gebruik niet toegestaan.

In de global system options worden specifieke zaken met betrekking tot de werking van het pakket als geheel vastgelegd. Deze opties worden beheerd door de centrale security officer. Met behulp van deze opties wordt bijvoorbeeld de minimale password-lengte ingesteld en (bij decentralisatie van de security officer-functie) de taakverdeling over de security officers gespecificeerd.

Een bijzonder privilege wordt gevormd door het non-cancellable attribute. Deze logon-ids hebben toegang tot alle bestanden en overige resources; de toegang wordt wel gelogd maar niet onderbroken.

Audit-faciliteiten

Ten behoeve van de controle op de autorisatieverstrekking biedt ACF2 een aantal standaard audit-faciliteiten. Zo worden standaard alle wijzigingen in de logon-id records gelogd. Bij wijzigingen in de rulesets en bij security violations vindt eveneens een automatische logging plaats. De auditor kan

deze logging via standaard ACF2-rapporten zichtbaar maken. De houder van een logon-id waaraan het audit-privilege is verleend, is in staat kennis te nemen van alle instellingen van ACF2, de inhoud van de logon-ids en de verleende autorisaties. Hij is echter niet in staat zelfstandig traces of specifieke logging op het gebruik van resources aan te zetten. Het audit-privilege wordt verstrekt door de security officer. Het aanzetten van specifieke logging en traces geschiedt eveneens door de security officer.

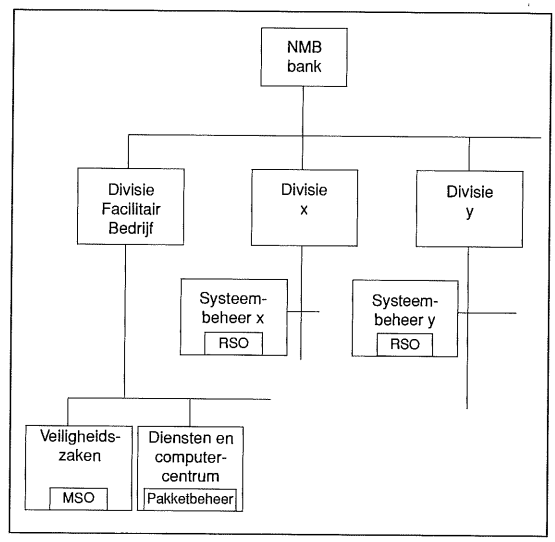
Technische werking ACF2

Het operating system MVS biedt slechts beperkte mogelijkheden voor het aanbrengen van logische toegangsbeveiliging. Door de toevoeging van een beveiligingspakket is een beter beheersbare en meer verfijnde beveiliging van bestanden en overige resources mogelijk. Dit houdt echter wel in dat ACF2 op de momenten dat moet worden beslist of een bepaalde actie doorgang moet kunnen vinden, controle dient te krijgen.

Hiertoe wordt zoveel mogelijk gebruik gemaakt van de structuur die IBM ontworpen heeft voor het aanroepen van het IBM-beveiligingspakket Resource Access Control Facility (RACF). Ook de mogelijkheid om de koppeling met de diverse pakketten ten aanzien van de autorisatieverlening via een eenduidige door IBM ontwikkelde interface, de System Authorization Facility (door middel van SAF-aanroepen), te laten plaatsvinden, wordt hierbij gevolgd. Bij de installatie van een monitorpakket als TSO is vastgelegd dat bij het starten van een sessie het beveiligingspakket dient te worden geraadpleegd. Langs deze weg ontvangt ACF2 controle en wordt de desbetreffende MVS address-space gekoppeld aan een ACF2 UID-string. Wanneer vanuit deze address-space een bestand wordt geopend, wordt door middel van een supervisor call opdracht gegeven aan het besturingssysteem het bestand te openen. In de supervisor call is een aanroep van ACF2 opgenomen, waardoor ACF2 op dat moment kan vaststellen of de gevraagde actie is toegestaan. Indien in ACF2 geen autorisatie voor de desbetreffende actie is opgenomen, vindt een negatieve terugmelding plaats en wordt de gevraagde actie niet uitgevoerd.

ORGANISATORISCHE IMPLEMENTATIE ACF2 BIJ DE NMB-BANK

Bij de binnenlandse vestigingen van de NMB-bank werken ruim 10.000 mensen, verdeeld over een aantal hoofdkantooronderdelen en de kantorenorganisatie (ruim 400 vestigingen). Een groot deel van deze medewerkers maakt gebruik van de centrale computerfaciliteiten van de bank. Daarnaast zijn vele duizenden produktie-jobs in gebruik. Het beheer van de hiervoor benodigde logon-ids en autorisaties is een belangrijke taak, die zorgvuldig dient te worden ondergebracht.
Zoals reeds eerder werd aangegeven, was de mogelijkheid van decentralisatie van de autorisatieverstrekking een belangrijk uitgangspunt bij de selectie van het beveiligingspakket. Dit heeft uiteindelijk geresulteerd in de organisatorische structuur zoals die is weergegeven in figuur 2.



Figuur 2. Vereenvoudigd organisatieschema NMB-bank.

Master Security Officer

De centrale security officer (de Master Security Officer, kortweg MSO) is ondergebracht bij de groep Informatiebeveiliging van de afdeling Veiligheidszaken. Deze afdeling ressorteert rechtstreeks onder de directie van het Facilitaire Bedrijf van de NMB-bank.
Naast de algemene verantwoordelijkheid voor het logisch beheer van het beveiligingspakket en de koppelingen daarvan met andere pakketten en besturingsprogrammatuur, heeft de MSO tevens het beheer van een aantal specifieke autorisaties. In principe worden de autorisaties die betrekking hebben op meerdere bedrijfsonderdelen door de MSO beheerd.
Daarnaast heeft de MSO in het handboek voor de security officers richtlijnen uitgevaardigd voor de bij de bedrijfsonderdelen ondergebrachte gedecentraliseerde security officers (de Restricted Security Officers, kortweg RSO's).

In het handboek voor security officers zijn onder meer procedures opgenomen voor:
- de verstrekking van logon-ids aan personen;
- de verstrekking van logon-ids ten behoeve van jobs;
- het verstrekken van toegang tot bestanden en andere resources;
- het verstrekken van een nieuw password (indien vergeten).

Tevens zijn aanwijzingen opgenomen voor de afhandeling van security violations en ter voorkoming van vervuiling van de ACF2-bestanden.

Voor een goede uitvoering van zijn functie beschikt de MSO onder andere over dagelijkse rapportages met betrekking tot:

- wijzigingen van logon-ids;

- wijzigingen van rulesets (voor bestanden en overige resources);

- gelogde gebeurtenissen met betrekking tot bestandstoegang. Deze logging ontstaat indien een security violation heeft plaatsgevonden, of indien is opgegeven dat toegang alleen gelogd kan plaatsvinden;

- gelogde gebeurtenissen met betrekking tot de logon-ids. Dit heeft met name betrekking op het toepassen van een onjuist password, het aanloggen met een verlopen password, het aanloggen vanaf een ongeautoriseerde terminal, etc.;

- het starten en stoppen van ACF2.

Restricted Security Officers

De RSO's beheren de logon-ids die tot het desbetreffende bedrijfsonderdeel behoren en beheren de autorisaties van de bestanden en overige resources die tot de verantwoordelijkheid van het desbetreffende bedrijfsonderdeel worden gerekend.
ACF2 voorziet erin dat de RSO's tot de logon-ids en rulesets worden beperkt waarvoor zij verantwoordelijk zijn. Het voordeel van de instelling van een decentrale security officer is gelegen in het feit dat deze functionaris dichter bij de desbetreffende gebruikers en toepassingen staat en dus een betere inschatting kan maken van de aanvaardbaarheid van bepaalde aanvragen.
Een nadeel is dat de ACF2-kennis op een groot aantal plaatsen binnen het bedrijf moet worden opgebouwd en onderhouden. Wanneer een gebruiker toegang wenst tot een bestand van een ander bedrijfsonderdeel is hierbij zowel de RSO van zijn eigen bedrijfsonderdeel als de RSO van het bedrijfsonderdeel waartoe het bestand behoort betrokken.

De RSO ontvangt die delen van de rapportages aan de Master Security Officer die van toepassing zijn op zijn bedrijfsonderdeel. Daarnaast ontvangt de RSO maandelijks een vergelijking tussen een aantal velden uit het logon-id record met de vergelijkbare gegevens uit het personeelsinformatiesysteem. Hiermee kan hij de consistentie van deze gegevens vaststellen. Met behulp van deze rapportage kunnen functiewijzigingen van medewerkers die gevolgen hebben voor de autorisatiestructuur worden vastgesteld.

Pakketbeheerder

Naast de MSO en RSO is voor het beheer van specifieke pakketten nog een beperkt aantal pakketbeheerders actief. Deze hebben van de MSO de autorisatie verkregen om specifieke privilegevelden uit het logon-id record, die betrekking hebben op het desbetreffende pakket, te muteren. Deze velden kunnen door de RSO niet worden aangepast. Aanvragen voor het gebruik van deze specifieke pakketten worden door de security officer aan de pakketbeheerder gezonden, die dan de desbetreffende privileges kan toekennen.

TECHNISCHE IMPLEMENTATIE ACF2 BIJ DE NMB-BANK

In principe is ACF2 bij de NMB-bank op een standaardwijze geïmplementeerd. Wel is ten behoeve van de beveiliging van specifieke pakketten naast de standaard door leverancier Computer Associates geleverde koppelingen een aantal zelf ontwikkelde koppelingen gerealiseerd. Daarnaast wordt een beperkt aantal exits toegepast, om ACF2 op de installatie-eisen van de NMB-bank toe te snijden. Bovendien wordt gewerkt aan een koppeling tussen de binnen ACF2 vastgelegde autorisaties en de te verlenen autorisaties op de lokale netwerken (LAN's) binnen de bankkantoren.

Op deze onderdelen wordt in deze paragraaf globaal ingegaan.

Koppelingen met andere pakketten

Binnen ACF2 kunnen koppelingen op verschillende wijzen worden gerealiseerd. Een veelvuldig toegepaste methode is gebruik te maken van op de organisatie toegesneden generalized resource rulesets. Dit wordt onder andere toegepast bij het pakket Spitab, dat algemeen gebruikte tabellen (zoals een rentetarieventabel) beheert. Hierbij wordt vanuit de applicatie Spitab ACF2 geactiveerd, waarbij ACF2 vaststelt of het desbetreffende logon-id toegang heeft tot de desbetreffende tabel. Dezelfde methode wordt binnen de NMB-bank toegepast om het gebruik van filetransfer (FTP) tussen het ontwikkel- en het produktiesysteem te beheersen.
Een andere mogelijkheid wordt gevormd door de toekenning van installatie-afhankelijke velden in het logon-id record. Het geautoriseerd gebruik van de monitoren IMS/DC, TSO en CA-7 wordt op deze wijze afgedwongen. Op deze manier is ook een koppeling gerealiseerd met het database managementsysteem DB2. Binnen ACF2 wordt het logon-id gekoppeld aan één of meer groepen waarbij deze groepen in DB2 toegang krijgen tot bepaalde views, tabellen of databases. Hierdoor kan binnen DB2 eenmalig een autorisatiestructuur worden opgezet, terwijl de koppeling van personen aan de groepen binnen ACF2 (dus zonder technische kennis van DB2) kan worden gerealiseerd.

Exits met betrekking tot ACF2

De huidige release van ACF2 biedt een aantal aanpassingsmogelijkheden (exits) om het pakket "op maat te kunnen snijden" voor de eigen installatie. Het gebruik van exits wordt binnen de NMB-bank tot een minimum beperkt, omdat een onjuiste werking van een exit ernstige gevolgen kan hebben voor het uiteindelijke beveiligingsniveau. Als voorbeeld van een exit die door de NMB-bank wordt gebruikt, kan hier een routine worden genoemd waarbij een aanpassing plaatsvindt in de koppeling tussen dataset-naam en ruleset-naam. Zoals reeds aangegeven, wordt door ACF2 de eerste qualifier van de bestandsnamen gebruikt om verschillende rulesets te onderscheiden. Dit sluit

echter niet goed aan bij de standaardnaamgeving van de bestanden bij de bank. Met behulp van genoemde exit wordt de verdeling van de rulesets toegesneden op de standaardnaamgeving bij de NMB-bank, waar met name de tweede qualifier een belangrijke rol speelt bij het onderscheiden van de verschillende applicatiesystemen.

Koppeling van centrale en decentrale autorisaties

Ten behoeve van de informatievoorziening op de kantoren wordt momenteel veel energie gestoken in werkplekautomatisering. Het ligt in de bedoeling een standaardinfrastructuur op de kantoren aan te bieden waarop alle voor de kantoormedewerkers noodzakelijke toepassingen kunnen worden ondergebracht. Hiertoe is gekozen voor personal computers als werkstations, samengevoegd in een local area network (LAN) per vestiging. Vanuit het LAN zijn verbindingen met het centrale computersysteem aangebracht. Het ontwerp voor deze infrastructuur voorziet in een algemeen autorisatiemechanisme, waarvan alle lokale applicaties gebruik kunnen maken. Hierbij zijn de lokale autorisaties vastgelegd in een autorisatietabel per LAN.

Om inconsistenties met de centrale autorisatiestructuur te voorkomen en voldoende functiescheiding te creëren is gekozen voor een koppeling van het decentrale autorisatiemechanisme met de centraal beheerde autorisatiestructuur.

Om inconsistenties met de centrale autorisatiestructuur te voorkomen en (met name voor de kleine vestigingen) voldoende functiescheiding te creëren tussen de verstrekker van de autorisaties en de gebruikers, is gekozen voor een koppeling van het decentrale autorisatiemechanisme met de centraal beheerde autorisatiestructuur. Concreet betekent dit dat dagelijks een aantal specifieke autorisatiegegevens van de kantoormedewerkers aan de ACF2-database wordt onttrokken. Hierbij zijn met name het logon-id, het kantoornummer en de in ACF2 vastgelegde functiecode van belang. Op basis hiervan en op basis van centraal beheerde beslissingsregels omtrent de toe te kennen autorisaties per functiecode worden dagelijks automatisch autorisatietabellen per vestiging gegenereerd, die vervolgens via het netwerk over de verschillende LAN's worden gedistribueerd.
Tevens wordt gewerkt aan een koppeling tussen de ACF2-database en het centrale personeelsinformatiesysteem. Op deze wijze wordt voldoende zekerheid verkregen dat informatie in ACF2 omtrent het kantoornummer en de functie van de ingebrachte logon-ids juist is.
Door de centraal vastgestelde beslissingsregels, waarbij een medewerker autorisaties ontvangt op basis van zijn functiecode, kan een optimale functiescheiding ten aanzien van applicatiefuncties worden gerealiseerd. Door de frequente hernieuwde opbouw van de lokale autorisatietabel vanuit de centrale ACF2-database wordt vervuiling van de autorisatietabellen beperkt en worden de toegekende autorisaties beter beheersbaar.

CONTROLE-AANPAK MET BETREKKING TOT ACF2

Ten aanzien van de aanpak van de controle op ACF2 kan in principe een drietal gezichtspunten worden onderscheiden:
- de decentrale organisatie met betrekking tot ACF2 (de RSO-functies);
- de centrale organisatie met betrekking tot ACF2 (de MSO-functie);
- de technische implementatie van ACF2.

Controle op de decentrale organisatie

Bij de controle op de RSO-functie wordt zowel de opzet als de werking van de decentrale organisatie beoordeeld.

Beoordeling opzet organisatie
Bij de controle op de opzet van de decentrale organisatie wordt de functiescheiding tussen de security officer enerzijds en de gebruikers en beheerders van de systemen anderzijds beoordeeld, inclusief de voor deze functies opgestelde procedures. De aandacht is daarbij met name gericht op de volgende procedures:
- creëren of muteren van logon-ids voor personen;
- creëren of muteren van logon-ids voor jobs;
- autorisatieverstrekking met betrekking tot bestanden;
- autorisatieverstrekking met betrekking tot overige resources (programma's, IMS-transacties, etc.);
- afhandeling van "vergeten" passwords;
- afhandeling van security violations;
- voorkomen van vervuiling van de autorisaties (door mutaties in de organisatie).

Daarnaast wordt in verband met continuïteitsaspecten aandacht besteed aan het opleidingsniveau en de mogelijke vervanging van de RSO.

Beoordeling werking organisatie
Ter beoordeling van de werking van de organisatie rond de RSO worden naast de werking van de genoemde procedures de volgende onderdelen gecontroleerd:

- de aanvaardbaarheid van de verstrekte privileges. Hiertoe wordt gebruik gemaakt van een inventarisatie van de met betrekking tot de beveiliging belangrijke velden in het logon-id record;

- de aanvaardbaarheid van de verstrekte be-

standsautorisaties. Hierbij wordt de aandacht met name gericht op de beperking van de toegang van persoonlijke logon-ids op produktiebestanden;

– de aanvaardbaarheid van de verstrekte autorisaties voor de overige resources;

– de afhandeling door de RSO van gerapporteerde security violations.

Controle op de centrale ACF2-organisatie

De opzet van de centrale ACF2-organisatie wordt periodiek door de Interne Accountantsdienst beoordeeld. Dit betreft de opzet van de organisatie met betrekking tot de volgende elementen:
- het beveiligingsbeleid;
- de beveiligingsorganisatie;
- de functiescheidingen.

Daarnaast wordt de taakuitvoering van de MSO-functionaris beoordeeld, waarbij de volgende aandachtsgebieden worden onderscheiden:
- organisatie en procedures;
- rapportages;
- verstrekte privileges aan logon-ids;
- verstrekte autorisaties.

Beveiligingsbeleid
Bij de beoordeling van het beveiligingsbeleid wordt uitgegaan van een aantal uitgangspunten. Zo dient er een beveiligingsbeleid te zijn geformuleerd, dat onderschreven wordt door de hoogste leiding in het bedrijf. De aan te schaffen of in gebruik zijnde beveiligingsprogrammatuur zal aan dit beveiligingsbeleid moeten voldoen. Het beleid en de procedures met betrekking tot de aanschaf en ontwikkeling van hard- en software-componenten zullen eveneens op het beveiligingsbeleid moeten aansluiten. Gezien het belang van standaardnaamgeving voor de beheersbaarheid van de autorisaties, dienen hiervoor goede richtlijnen te zijn vastgesteld.

Beveiligingsorganisatie
Gezien de toegepaste decentralisatie van de security officer-functie is de taakverdeling tussen de RSO en MSO en de vastlegging daarvan van groot belang. De beoordeling hiervan betreft met name de functionele bevoegdheden van de MSO ten opzichte van de RSO's en de controle door de MSO op de werkzaamheden van de RSO's.

Functiescheidingen
Een veelheid van functies is betrokken bij het beheer van ACF2 en de te verstrekken autorisaties. Bij de beoordeling worden de volgende functiescheidingen onderzocht:

– functiescheiding tussen ontwikkeling en produktie;

– functiescheidingen tussen de aanvrager, de beschikkende functie en de uitvoerende functie met betrekking tot de creatie of mutatie van logon-ids;

– functiescheidingen tussen de aanvrager, de beschikkende functie en de uitvoerende functie met betrekking tot het beheer van ACF2 rulesets;

– functiescheiding met betrekking tot het operationeel en functioneel beheer van ACF2-programmatuur en exits;

– functiescheiding tussen operationeel en functioneel beheer met betrekking tot systeemparameters en instellingen van ACF2;

– functiescheiding tussen security officers en de beheerder van ACF2-rapportages ten behoeve van de controle op ACF2;

– mogelijke ongewenste combinatie van ACF2-taken en andere taken van de security officers.

Organisatie en procedures met betrekking tot de MSO
Analoog aan die van de RSO richt deze beoordeling zich op de door de MSO gehanteerde procedures en de continuïteit van de MSO-functie. Van groot belang hierbij is de wijze waarop de procedures zijn vastgelegd.

Rapportages ten behoeve van de MSO
In de bespreking van de organisatorische implementatie van ACF2 bij de NMB-bank is reeds ingegaan op de rapportages die beschikbaar zijn voor de security officers. Voor een goede informatievoorziening aan de MSO dient de volgende informatie beschikbaar te zijn:
- overzichten van autorisaties per gebruiker of job;
- overzichten van de geautoriseerde gebruikers per bestand of andere resource;
- overzicht van wijzigingen van de logon-ids;
- overzicht van wijzigingen in de autorisatiestructuur;
- overzicht van geconstateerde security violations;
- overzicht van starten en stoppen van logging van ACF2, MVS en SMF;
- periodiek overzicht van de verstrekte risicovolle privileges;
- trace-mogelijkheden van het systeemgebruik door specifieke logon-ids.

Verstrekte privileges aan logon-ids
Ten behoeve van de beoordeling van de door de MSO verstrekte privileges is een inventarisatie gemaakt van de belangrijke opties en privileges die aan een logon-id kunnen worden toegekend. ACF2 biedt goede mogelijkheden te rapporteren omtrent de houders van deze specifieke privileges. Hierbij wordt beoordeeld of de belangrijke privileges terecht zijn verstrekt.

Verstrekte bestandsautorisaties
De beoordeling van de bestandsautorisaties wordt vanuit twee gezichtspunten uitgevoerd. Enerzijds wordt vastgesteld in hoeverre de door de MSO beheerde bestanden en libraries op adequate wijze worden afgeschermd. Het betreft hier met name de

libraries en databases van ACF2. Anderzijds wordt vastgesteld of de autorisaties tot wijziging van rulesets op een aanvaardbare wijze binnen de organisatie zijn toegekend.

Controle op de technische implementatie van ACF2

Bij de controle op de technische implementatie van ACF2 wordt voornamelijk gebruik gemaakt van de in ACF2 vastgelegde informatie (global system options, etc.). Belangrijkste aandachtsgebieden zijn hierbij:
- organisatie met betrekking tot de technische implementatie van ACF2;
- parameter-settings;
- password-beveiliging;
- logging;
- operating-aspecten;
- ACF2-exits.

Daarnaast wordt aandacht besteed aan een aantal aspecten van het operating system MVS.

Organisatie met betrekking tot de technische implementatie van ACF2
De organisatie rondom de technische implementatie dient gericht te zijn op het voorkomen dat de werking van ACF2 ongeautoriseerd wordt beïnvloed. De werking kan worden beïnvloed door het wijzigen van:
- de ACF2-programmatuur;
- de ACF2-exits en koppelingen met andere pakketten;
- de parameters met betrekking tot de definitie van de velden en het beheer ervan in de logon-id database (het field definition record);
- de parameters die op de werking van ACF2 zijn gericht (de global system options).

Het beheer van deze onderdelen dient derhalve zodanig te zijn opgezet dat slechts geautoriseerde wijzigingen hierop kunnen worden aangebracht.

Parameter-settings
De parameter-settings dienen in overeenstemming te zijn met de binnen de organisatie noodzakelijk geachte functionaliteit. Deze parameters zijn de global system options. Als voorbeeld kan hier worden genoemd dat schijfeenheden kunnen worden gespecificeerd waarvoor geen validatie door ACF2 plaatsvindt. Tevens wordt door middel van deze opties aangegeven of ACF2 bij een security violation de verdere verwerking moet afbreken of alleen een boodschap moet geven.
De global system options worden inhoudelijk gecontroleerd.

Password-beveiliging
Omdat passwords het middel zijn om de authenticiteit van de gebruikers vast te stellen dienen eisen te worden gesteld aan de gebruikte passwords. ACF2 biedt hiervoor diverse faciliteiten. Bij de beoordeling wordt onder andere vastgesteld welke eisen met betrekking tot de minimumlengte en de maximumlevensduur in ACF2 zijn gespecificeerd. Tevens wordt vastgesteld of het aantal mislukte aanlogpogingen dat wordt toegestaan, beperkt is.

Logging
Vastgesteld wordt welke handelingen en gebeurtenissen met betrekking tot ACF2 worden gelogd. Zo dienen ten behoeve van de controle alle wijzigingen in de autorisatiestructuur te worden vastgelegd. Tevens dienen de security violations te worden gelogd. Daarnaast is het zinvol het gebruik van logon-ids met vergaande bevoegdheden te loggen.

Operating-aspecten
Vastgesteld wordt in hoeverre operator-interventies invloed hebben op de goede werking van het beveiligingspakket. Zo dient de operator niet in staat te zijn ongemerkt ACF2 te stoppen. Het opstarten dient automatisch plaats te vinden zo spoedig mogelijk na de start van het operating system.

ACF2-exits
Bij de beoordeling van de ACF2-exits dient de doelstelling ervan te worden vastgesteld. Voor het bestaan van deze exits dient een goede reden te zijn. Daarnaast kan ook een technische beoordeling van deze exits plaatsvinden.

Operating system MVS
De beoordeling van de technische implementatie van ACF2 is niet volledig indien niet enige aandacht is besteed aan de implementatie van het besturingssysteem MVS. Immers, MVS biedt faciliteiten waarmee de werking van het beveiligingspakket volledig ongedaan kan worden gemaakt. Vandaar dat in het kader van de audit op ACF2 tevens aandacht wordt besteed aan enkele wezenlijke componenten van MVS:
- organisatie met betrekking tot wijzigingen in het operating system;
- beveiliging van de MVS-parameter-settings (in de SYS1.PARMLIB);
- beveiliging van APF-authorized libraries;
- toegekende autorisaties in de Program Properties Table;
- beveiligingsaspecten met betrekking tot supervisor calls;
- afhandeling van door IBM aangeleverde wijzigingen (program temporary fixes);
- procedures met betrekking tot de toepassing van het Remote Support Facility (RSF).

TOT SLOT

In dit artikel is ingegaan op de implementatie van het beveiligingspakket ACF2 bij de NMB-bank en op de wijze waarop de controle op de autorisatieverstrekking wordt aangepakt.

Aangegeven is dat een goed beveiligingspakket in een MVS-omgeving noodzakelijk is om op een beheersbare wijze een voldoende beveiligingsniveau te realiseren. Tevens is aangegeven dat het gerealiseerde beveiligingsniveau in grote mate afhangt van de technische en organisatorische implementatie van het beveiligingspakket. In de praktijk blijkt dat grote inspanningen nodig zijn om binnen een groot bedrijf met een complexe automatiseringsomgeving de noodzakelijke beveiliging te realiseren.

Ten aanzien van het pakket ACF2 kan worden gesteld dat door de flexibele mogelijkheden om koppelingen tot stand te brengen met allerlei pakketten de beheersbaarheid van de beveiligingsstructuur relatief groot is. Tevens blijkt dat de filosofie van ACF2, waarbij toegang voor alle gedefinieerde resources bewust verleend moet worden, een voordeel kan inhouden ten opzichte van andere pakketten. De verfijnde mogelijkheden om de autorisatieverstrekking te decentraliseren kunnen voor grote organisaties belangrijke voordelen opleveren.

Ten aanzien van de controleerbaarheid zijn echter verbeteringen mogelijk. Een sluitende controle op de Master Security Officer is, gezien de enorme bevoegdheden waarover deze beschikt, slechts met grote inspanningen te realiseren. Daarnaast blijkt in de praktijk dat een goede beoordeling van ACF2 veel technische kennis en kennis van de organisatie in kwestie vereist.

Ing. D.J. Huis
Is sinds 1985 werkzaam bij de EDP-audit-afdeling van de Interne Accountantsdienst van de NMB-bank (sinds 1990 deel uitmakend van de NMB-Postbankgroep). Zijn audit-ervaring ligt op het technical audit-vlak en varieert van computercentrum-audits tot het beoordelen van grootschalige ontwikkelingen met betrekking tot de technische infrastructuur.

Access control op Unisys A Serie computers

Drs. M.A. Bongers RA en
J-M. van Leerdam

De Unisys A Serie computers worden in Nederland regelmatig aangetroffen bij middelgrote tot grote instellingen en bedrijven. De auteurs, die beiden werkzaam zijn bij een bank die deze computers gebruikt, geven een uitgebreide beschrijving van de beveiligingsmogelijkheden van het standaard-besturingssysteem en van de access control-module InfoGuard. Ook gaan zij in op de specifieke audit-aspecten in deze omgeving.

INLEIDING

Toegangsbeveiliging is een onderwerp dat momenteel bijzonder in de belangstelling staat. Door publikaties over computerinbraken en computerfraude ([CFSB91], [STOL89]) groeit het besef dat adequate beheersing en beveiliging van geautomatiseerde informatievoorziening noodzakelijk is. Het maatschappelijk belang dat aan deze beveiliging wordt toegekend, blijkt uit het wetsvoorstel Computercriminaliteit ([DSDI90]) en bijvoorbeeld het memorandum van De Nederlandsche Bank ([DNBM88]). Mede ook door de toenemende afhankelijkheid van computersystemen zijn interne-controle- en beveiligingsmaatregelen noodzakelijk om verkeerd gebruik (zowel opzettelijk als onopzettelijk) van die systemen te voorkomen. De beheersing van de toegang tot computersystemen is hiervoor een essentiële voorwaarde.

Dit artikel geeft een overzicht van beschikbare controle- en beveiligingsmaatregelen op het gebied van toegangsbeheersing van Unisys A Serie computers. Deze computers worden in Nederland veelvuldig aangetroffen bij middelgrote tot grote organisaties. Voor de Unisys A Serie kan als aanvulling op de standaardmogelijkheden de access control-module InfoGuard worden geleverd. Aangegeven zal worden welke mogelijkheden InfoGuard toevoegt. Het doel van dit artikel is een bijdrage te leveren aan het vergroten van de kennis over access control op Unisys A Serie bij systeembeheerders, security officers en EDP-auditors in Nederland.

Na een korte beschrijving van de fysieke en logische structuur van de A Serie in de volgende paragraaf, wordt ingegaan op wat in dit artikel onder access control wordt verstaan. Hierbij wordt een afbakening van het in dit artikel beschreven onderwerp gegeven. Daarna komen in drie paragrafen de access control-mogelijkheden, ingedeeld naar controle- en beveiligingsdoelstellingen (authenticiteit, geautoriseerdheid en controleerbaarheid) aan de orde. In de laatste paragraaf worden de specifieke toevoegingen van InfoGuard uitgezet tegen de standaardmogelijkheden. Het slotwoord geeft enkele conclusies en een aantal mogelijke aandachtspunten voor de toekomst.

Aan het einde van dit artikel is, in aanvulling op de toelichtingen in de tekst, een woordenlijst opgenomen met de vaak gebruikte (Unisys-)termen en afkortingen.

Wanneer in dit artikel wordt gesproken over een "systeem", wordt een computer of een computerconfiguratie inclusief de daarbij behorende besturings-software en applicaties bedoeld. In dit artikel worden overigens alleen enkelvoudige configuraties beschouwd (dat wil zeggen één A Serie computer met aangesloten terminals). De specifieke consequenties van koppelingen met andere mainframes, netwerken of externe instanties (bijvoorbeeld via inbel-lijnen) komen niet aan de orde.

UNISYS A SERIE COMPUTERS

In deze paragraaf wordt een schets gegeven van Unisys A Serie computers met typen, prestaties, hardware en (besturings-)software. Per organisatie zal de feitelijke systeemconfiguratie uiteraard verschillend worden samengesteld. De hierna volgende introductie is dan ook bedoeld als referentiekader in het bijzonder voor lezers die nog geen of weinig ervaring met Unisys A Serie computers hebben.

Algemeen

De Unisys A Serie bestaat momenteel uit circa 25 modellen, lopend van de Micro A 825-DS tot de A19-664. In Nederland worden Unisys A Serie computers bij ongeveer 150 bedrijven gebruikt, hetgeen overeenkomt met een marktaandeel van circa tien procent. Unisys wordt beschouwd als de derde hardware-leverancier in Nederland.

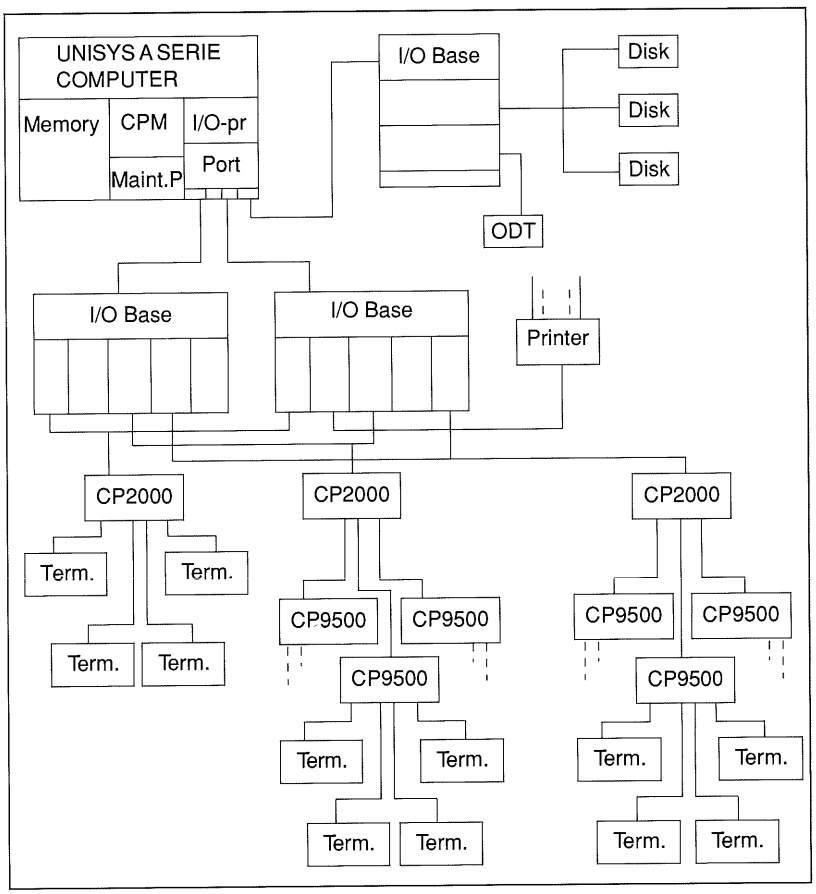
Tabel 1 geeft een overzicht van de krachtsverhoudingen (in "relatieve performance" - een Unisys-maatstaf voor verwerkingscapaciteit) tussen een aantal A Serie modellen en een aantal andere minicomputers en mainframes[1].
Als karakteristiek van de A Serie lijn moet het uniforme operating system worden genoemd. Hierdoor is overgang van een model naar een ander model relatief eenvoudig te realiseren. Ook wanneer meerdere A Serie computers in gebruik zijn binnen een organisatie, kunnen programma's verhoudingsgewijs eenvoudig worden uitgewisseld.

Hardware

Figuur 1 geeft een schematisch overzicht van een specifieke voorbeeldconfiguratie met mogelijke systeemcomponenten. De configuratie is gebaseerd op de structuur van een grotere A Serie computer (A10, A12 of groter). De aantallen componenten kunnen variëren. Gebruikers van het mainframe werken in dit voorbeeld via een netwerk van terminals en CP9500's (CP = Communication Processor), die zijn verbonden met de CP2000's. De CP9500's gedragen zich als minicomputers en verzamelen de input vanaf een aantal terminals. Vervolgens wordt de informatie doorgestuurd naar één van de CP2000's, die de communicatie naar het mainframe verzorgt.
De CP2000's zijn aan de I/O-base(s) (Input/Output-poorten) van het mainframe gekoppeld. Terminals kunnen ook direct op een CP2000 zijn aangesloten. Aan de I/O-base(s) zijn ook de diskdrives, tape-units, ODT's (Operator Display Terminals ofwel operator consoles) en printers gekoppeld. Binnen het mainframe bevindt zich het werkgeheugen, de data processor (CPM - Central Processing Module), de I/O-processor en de maintenance processor. De fysieke configuratie (adressen van printers, terminals, CP's) wordt vastgelegd in de NAU-database (Network Administrative Utility). Systeemprinters en ODT's worden hardware-matig geconfigureerd en liggen niet in de NAU-database vast.

Unisys-modellen	Rel. perf.	Andere merken	Rel. perf.
Unisys MA825-DS	35	DEC Micro VAX 2000	22
Unisys A1-FX	40	IBM SYS38/200	25
Unisys A4-FS	60	Wang VS 100	65
Unisys A6-HS	150	HP 9000/300	75
Unisys A12-211	230	IBM 4381-13	175
Unisys A12-411	500	DEC VAX 8840	550
Unisys A16-61E	1440	Prime 6550	1180
Unisys A19-622	4780	IBM 3090/600E	3570
Unisys A19-664	12010		

Tabel 1. Overzicht van de krachtsverhoudingen.



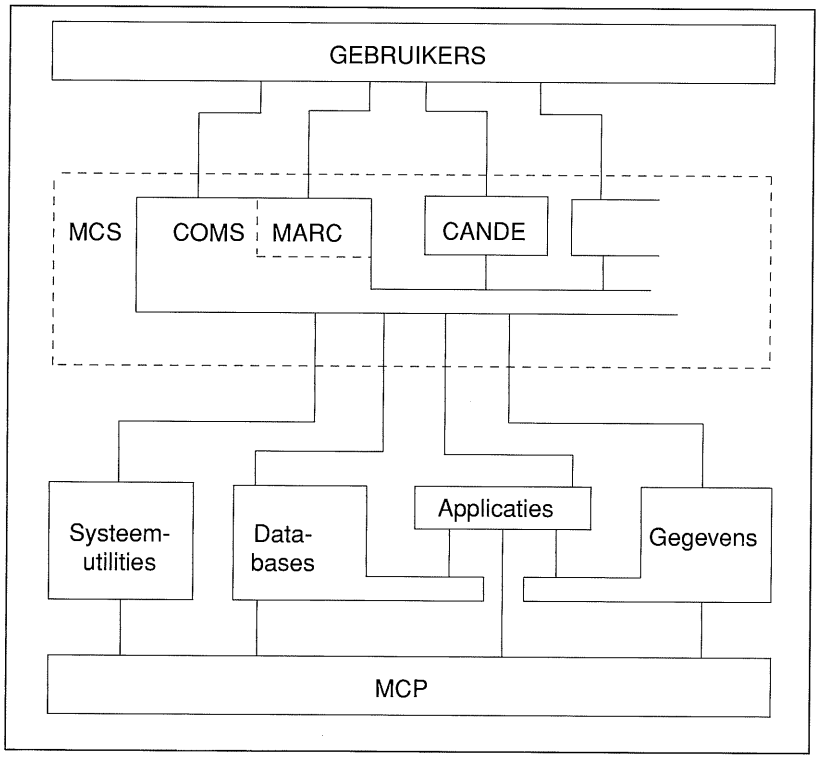
Figuur 1. Voorbeeld hardware-configuratie Unisys A Serie.

Systeem-software

Gebruikers communiceren met het mainframe via één van de aanwezige Message Control Systems (MCS'en). Deze systeemprogramma's verzorgen het versturen en afbeelden van boodschappen. Gebruikelijke MCS'en zijn COMS (COmmunication Management System) en CANDE (Command AND Editor). MARC (Menu Assisted Resource Control) is de menu-handler van COMS. Dit is een programma dat op interactieve wijze commando's van de gebruiker opbouwt en vervolgens aan COMS aanbiedt voor verwerking. Afhankelijk van zijn bevoegdheden heeft de gebruiker een aantal schermen (en daarmee commando's) tot zijn beschikking.

1 *Bron gegevens: Unisys Nederland, afdeling Marketing.*

CANDE en andere MCS'en steunen voor een deel op de door COMS geboden faciliteiten. Zonder het basis-COMS kunnen deze andere MCS'en niet functioneren. Een en ander wordt schematisch weergegeven in figuur 2.



Figuur 2. Logische structuur Unisys A Serie computers.

In COMS worden programma's en andere gebruikte MCS'en aan windows gekoppeld. Een window is een link tussen de gebruiker en het (sub)systeem. Via deze windows wordt zowel de communicatie met als de toegang tot utilities, gebruikersapplicaties en andere MCS'en geregeld. In de COMS-configuration-file is vastgelegd welke windows en terminals voor de verschillende gebruikers beschikbaar zijn.

Binnen de windows kunnen bevoegdheden verder gespecificeerd zijn aan de hand van transaction-codes. Per gebruiker kan worden aangegeven welke transaction-codes hij binnen een window mag gebruiken. Omdat de gevolgen van het gebruik van transaction-codes voornamelijk binnen een applicatie liggen, zal dit artikel verder niet ingaan op deze overigens wel van belang zijnde beheersingsmogelijkheden. Het gebruik van transaction-codes is een alternatief voor het binnen gebruikersapplicaties aanbrengen van functiescheidingen.

Het op vrijwel alle installaties gebruikte databasesysteem bij Unisys A Serie computers is DMSII (Database Management System II), een netwerkdatabase management-systeem. Relaties tussen verschillende datasets worden bijvoorbeeld gedefinieerd door gelijke sleutelvelden in de datasets. DMSII-databases zijn in principe met iedere (derde-generatie-)programmeertaal te benaderen.

Tegenwoordig worden veel applicaties in de vierde-generatie-taal LINC (Logic and Information Network Compiler) ontwikkeld. De ontwikkelde programmatuur wordt door de LINC-compiler vertaald naar een DMSII-database met Cobol-programma's voor het benaderen van die database. In dit artikel wordt niet ingegaan op de extra access control-mogelijkheden die LINC biedt.

Gebruikers kunnen, door middel van de MCS'en, programma's en systeem-utilities opstarten en systeemcommando's geven. Veel gebruikte systeem-utilities zijn bijvoorbeeld:
- PRINTS/REPRINTS - afdrukken van bestanden;
- FILEDATA - opvragen van bestandsgegevens.

De systeem-utilities kunnen ook door applicaties worden gebruikt.

Het MCP (Master Control Program) is het eigenlijke operating system van de A Serie computers. Het operating system verzorgt de uitvoering van jobs, de toewijzing van geheugen en processortijd, etc. Het MCP wordt alleen benaderd door MCS'en, systeem-utilities en programma's. Gebruikers kunnen alleen vanaf de ODT's direct met het MCP communiceren.

ACCESS CONTROL-DOELSTELLINGEN

Interne-controle- en beveiligingsmaatregelen (ICB-maatregelen) zijn in het algemeen gericht op de beheersbaarheid van bedrijfsprocessen (interne controle) en het bevoegd gebruik van de bedrijfsactiva (beveiliging). Een stelsel ICB-maatregelen bestaat uit organisatorische én technische maatregelen.

In dit artikel behandelen wij slechts de technische mogelijkheden voor toegangsbeheersing die door Unisys A Serie computers en InfoGuard worden geboden. Op de organisatorische randvoorwaarden, procedures en eisen die eveneens noodzakelijk zijn, wordt in dit artikel niet ingegaan.

Access control of toegangsbeheersing wordt bereikt door ICB-maatregelen die gericht zijn op met name de authenticiteit, geautoriseerdheid (bevoegd gebruik) en de controleerbaarheid van het gebruik van het systeem. Maatregelen die hoofdzakelijk worden toegepast om andere doelstellingen te bereiken (continuïteit, integriteit, vertrouwelijkheid en efficiëntie) zullen voor zover relevant slechts zijdelings worden behandeld. Een nadere uitwerking van deze doelstellingen is te vinden in *EDP-Auditing in relatie tot management* van prof. M.E. van Biene-Hershey ([BIEN89]).

Toegangsbeheersingsmaatregelen moeten erop zijn gericht de in de ACM vastgelegde bevoegdhedenstructuur zo dwingend mogelijk op het systeem te implementeren. Hierbij wordt er tevens voor gezorgd dat afwijkingen van de bevoegdhedenstructuur (of pogingen daartoe) tijdig worden gedetecteerd.

Authenticiteit

Authenticiteit is de oorspronkelijkheid of echtheid van de persoon, het object of het programma in kwestie. Authenticatie omvat alle maatregelen ter waarborging van die oorspronkelijkheid. De authenticiteit wordt vastgesteld door identificatie en verificatie van die identificatie. Voorbeelden van identificatiemiddelen zijn:
- personeelsnummer;
- naam;
- rekeningnummer;
- terminal-adres.

De echtheid van de opgegeven identificatie moet worden geverifieerd aan de hand van bij de identificatie opgegeven verificatie-informatie. Deze extra informatie, ook wel authenticatiemiddelen genoemd, moet voldoende bewijs van de oorspronkelijkheid van de identificatie in zich dragen. Voorbeelden hiervan zijn:
- persoonlijk wachtwoord;
- handtekening, foto;
- PIN-code;
- hardware-gegenereerde sleutel.

Authenticatiemiddelen kunnen worden onderscheiden in op kennis gebaseerde middelen (wachtwoord, PIN-code, etc.) en op bezit gebaseerde authenticatiemiddelen (zoals smartcard, cardkey of sleutel). Een bijzondere vorm van op persoonlijk bezit gebaseerde middelen zijn persoonskenmerken zoals vingerafdruk en oogkarakteristiek.

Met behulp van identificatie- en verificatiemiddelen is het systeem in staat de authenticiteit van personen, objecten of processen vast te stellen. Zonder deze authenticatie is het niet mogelijk het bevoegde gebruik van het systeem vast te stellen. Authenticatie bij geautomatiseerde systemen kan worden verdeeld in drie gebieden:
- authenticatie van gebruikers;
- authenticatie van bestanden (waaronder gegevens, applicaties, databases en systeem-software);
- authenticatie van systeem-hardware-componenten (terminals, printers, etc.).

Geautoriseerdheid (bevoegd gebruik)

Geautoriseerdheid van het gebruik van een systeem houdt in dat het systeem wordt gebruikt conform de namens het management van de desbetreffende organisatie gestelde delegatie van bevoegdheden. Bij die verdeling van de bevoegdheden of autorisaties moet zijn aangegeven welke taken door welke personen al of niet met behulp van het systeem mogen worden uitgevoerd. De vastlegging van de bevoegdheden kan plaatsvinden in een matrix met als rijen en kolommen respectievelijk gebruikers en objecten (programma's, gegevens, systeemonderdelen). De matrix-elementen bevatten de voor dat object aan de gebruiker toegekende bevoegdheden. Deze vorm van vastlegging wordt ook wel een Access Control Matrix (ACM) of competentietabel genoemd.

De opgestelde ACM moet in het systeem worden afgedwongen door het creëren van omgevingsstructuren, algemene gebruikersprivileges en specifieke toegangsrechten. Samen met het vaststellen van de authenticiteit van gebruikers en objecten, maken de in het systeem vastgelegde autorisatiegegevens het mogelijk geautomatiseerd te bepalen of (aangevraagde) acties al dan niet geautoriseerd zijn en doorgang mogen vinden.

Controleerbaarheid

Controleerbaarheid wordt bereikt door maatregelen die het mogelijk maken om (achteraf) te constateren dat een object of proces aan de gestelde eisen voldoet. Daarvoor moet het systeem, naast authenticatie van gebruikers en objecten en autorisatie van acties, faciliteiten bieden voor het controleren van de verrichte acties. Middelen die in het algemeen worden gebruikt voor de invulling van de controleerbaarheid zijn registraties van informatie over de integriteit van objecten (bijvoorbeeld hash totals voor bestanden) of over de juiste werking van processen (bijvoorbeeld een audit trail of controletotalen). Zonder controleerbaarheid is het niet mogelijk het systeem op een adequate wijze te beheersen. Voorbeelden van acties die in het kader van access control moeten kunnen worden gecontroleerd, zijn: (foute) aanlogpogingen, wijzigingen van systeemparameters, (pogingen tot) toegang tot vertrouwelijke onderdelen van het systeem en wijzigingen in gebruikersbevoegdheden.

Toegangsbeheersingsmaatregelen moeten erop gebaseerd zijn de in de Access Control Matrix vastgelegde bevoegdhedenstructuur zo dwingend mogelijk op het systeem te implementeren.

De hiernavolgende drie paragrafen gaan in op de diverse technische mogelijkheden die Unisys A Serie computers inclusief InfoGuard bieden. Per paragraaf worden de maatregelen besproken die betrekking hebben op één van de drie access control-doelstellingen, te weten: de authenticiteit, de geautoriseerdheid (bevoegd gebruik) en de controleerbaarheid inzake het systeemgebruik. De beschrijvingen in de komende paragrafen zijn gebaseerd op informatie uit de Unisys A Serie handleidingen (met name [UCAN90], [UCOM89], [UDMS89], [USAG89] en [USSF87]).

AUTHENTICITEIT

Authenticiteit wordt bereikt door een authenticatieproces, dat uiteenvalt in twee delen: identificatie en verificatie van de identiteit. Deze paragraaf gaat, voor wat betreft de A Serie mogelijkheden, in

op de onderkende deelgebieden (authenticatie van gebruikers, bestanden en hardware-componenten).

Authenticatie van gebruikers

Gebruikers worden op het systeem geïdentificeerd aan de hand van persoonlijke USERCODES, eventueel aangevuld met ACCESSCODES. De USERCODES en ACCESSCODES kunnen ten behoeve van verificatie worden voorzien van passwords, die versleuteld in het systeem worden opgeslagen.

Onder InfoGuard kan voor passwords van USERCODES password-aging worden toegepast (hierdoor wordt het regelmatig "verversen" van passwords afgedwongen), evenals password-generation (hierdoor worden passwords door het systeem gegenereerd in plaats van door de gebruiker gekozen). Deze maatregelen moeten de risico's van het bekend raken van passwords limiteren. Verder kan onder InfoGuard per gebruiker een lijst met recente passwords worden vastgehouden en een minimale levensduur van de passwords worden ingesteld. Hiermee kan het snel achtereen wisselen tussen twee of meer passwords worden voorkomen.

Het bekend raken van passwords kan worden beperkt door passwords in een "protected" videoveld in te voeren (waardoor de passwords onzichtbaar zijn op het scherm). Onder InfoGuard wordt het gebruik hiervan afgedwongen.

De aanlogprocedure is uit te breiden met een zelf ontwikkelde controleprocedure waarin specifieke additionele controles worden uitgevoerd voor gebruikers die door de normale aanlogprocedure zijn geaccepteerd. Te denken valt aan het toevoegen van een werktijdentabel, of een uitgebreidere aanlogprocedure voor belangrijke gebruikers (de Privileged Users en Security Administrators). De volgende versie van het MCP (begin 1992) zal het gebruik van een werktijdentabel ondersteunen.

Het bekend raken van passwords kan worden beperkt door passwords in een "protected" videoveld in te voeren, waardoor de passwords onzichtbaar zijn op het scherm.

Het is mogelijk op het systeem zogenaamde SUPER-USERSTATIONS te definiëren met behulp van de COMS-configuration-file. Vanaf SUPER-USERSTATIONS zijn commando's te geven alsof de gebruiker een Privileged User (zie verder) is. Op deze stations kunnen gebruikers zich aanmelden met een * (ster). Het systeem kan de gebruiker dan echter niet identificeren. Het gebruik van SUPER-USERSTATIONS is niet noodzakelijk en in een omgeving waar beveiliging belangrijk is, wordt het gebruik dan ook sterk ontraden. Onder InfoGuard is het gebruik van deze stations onmogelijk.

Daarnaast kunnen op de computerzaal enkele ODT's zijn geplaatst waarop aanmelden niet noodzakelijk is (continuous logon). In dit geval is identificatie van de gebruiker eveneens onmogelijk. Vanaf ODT's met een continuous logon zijn alle operator commando's te geven, waaronder bijvoorbeeld het commando voor het activeren en deactiveren van databases. Voor ODT's is het wel mogelijk een logon verplicht te stellen met behulp van de COMS-configuration-file. Hierdoor wordt authenticatie van de gebruiker mogelijk.

Authenticatie van gebruikers van ODT's met continuous logon en van SUPER-USERSTATIONS kan niet door het systeem worden uitgevoerd. De terminals dienen daarom, als ze gedefinieerd zijn, fysiek zodanig te worden afgeschermd dat te allen tijde duidelijk is wie de terminal gebruikt (bijvoorbeeld door ze op te stellen in een apart afgeschermde ruimte of door ze te voorzien van smartcards).

Authenticatie van bestanden

Bestanden (gegevens, applicaties, databases en systeem-software) worden op het systeem geïdentificeerd door een unieke naam in de vorm (UC)DIR1/DIR2/DIR3/../NAAM ON DISKNAAM. Hierin is UC de user-code van de eigenaar van het bestand. (Wanneer aan het bestand geen user-code is toegekend, dan is UC gelijk aan * (ster).) DIR<i> zijn directories in een boomstructuur. NAAM is de naam van het bestand binnen de laatste directory. DISKNAAM geeft aan op welke fysieke schijfeenheid de boomstructuur en het bestand zich bevinden. Binnen het operating system wordt gegarandeerd dat het oorspronkelijk onder deze naam opgeslagen bestand intact blijft zolang er geen expliciete kopieer- of mutatie-opdrachten voor dat bestand worden gegeven.

Van elk bestand wordt vastgelegd wat zijn grootte, bestandstype, aanmaakdatum, laatste wijzigingsdatum en laatste toegangsdatum is. Op deze wijze kan een gebruiker vaststellen of zijn bestanden nog authentiek zijn.

DMSII-databases worden daarnaast bij het opstarten van de database getest op integriteit. In de DMSII-control-file worden onder andere de time-stamps (datum/tijd creatie en datum/tijd laatste wijziging) van de bestanden van de database bijgehouden. Bij het opstarten worden de actuele time-stamps met de geregistreerde waarden vergeleken. Zodra tijdens deze controle een bestand wordt ontdekt waarvan de time-stamp niet overeenkomt met de geregistreerde waarde, zal de database niet worden geactiveerd en wordt een foutmelding gegeven.

Het aanpassen van time-stamps en het ongedetecteerd wijzigen van de DMSII-control-file is op de Unisys A Serie niet mogelijk. Ook het wijzigen van file-attributen in het algemeen kan alleen geschieden met de daarvoor bestemde operaties van het operating system.

Authenticatie van systeemonderdelen

De diverse systeemonderdelen (terminals, printers, CP's, ODT's, etc.) worden op het systeem geïdentificeerd door een uniek toegewezen "adres". Dit adres wordt gebruikt bij de communicatie tussen de verschillende systeemonderdelen. In de NAU-database en de COMS-configuration-file wordt bijgehouden welk onderdeel bij welk adres hoort. De NAU-database bevat de gegevens over de fysieke configuratie; de COMS-configuration-file bevat de gegevens over de logische samenhang tussen de systeemonderdelen.

Binnen het operating system zijn waarborgen aanwezig voor het in stand houden van de relatie tussen adres en systeemonderdeel. Wijzigingen hierin kunnen alleen door een COMSCONTROL gebruiker worden aangebracht (zie bespreking USERDATAFILE in de hiernavolgende paragraaf Geautoriseerdheid).

GEAUTORISEERDHEID

Binnen de Unisys A Serie computers vindt autorisatie op een aantal niveaus plaats. Hierna worden besproken:
- autorisatie in de hardware;
- autorisatie van gebruikers;
- autorisatie van programma- en bestandstoegang;
- autorisatie van database-toegang.

Autorisatie in de hardware

Het geheugen van de Unisys A Serie is opgebouwd uit woorden, die ieder voorzien zijn van een "tag" (een label). Hiermee wordt aangegeven wat voor gegevens zijn opgeslagen. Het operating system voert alleen code uit wanneer die is voorzien van een code-tag. Er zijn geen assemblers voor machinetaal aanwezig, alleen compilers voor hogere programmeertalen. Het schrijven van code-files is alleen toegestaan voor compilers (programma's die compiler-status via het MC-commando (Make Compiler) toegewezen hebben gekregen). Het MC-commando is alleen beschikbaar voor Privileged Users; onder InfoGuard alleen voor Security Administrators (zie verder). Dit mechanisme biedt protectie tegen virussen, omdat normale programma's (code-files) geen andere programma's kunnen aanpassen.

Zodra in een hogere programmeertaal constructies worden gebouwd die als onveilig worden beschouwd, zal de compiler de gegenereerde code markeren. Een voorbeeld van een dergelijke onveilige actie is het uitschakelen van bepaalde categorieën hardware-interrupts (het interrupt-mechanisme verzorgt de uitvoering van operating system-taken, waaronder ook ICB-maatregelen vallen). De gemarkeerde code kan pas worden uitgevoerd wanneer voor dat programma het XP-commando (eXecutable Program) wordt gegeven.

Programma's die gegevens van andere gebruikers moeten benaderen, kunnen evenmin automatisch worden uitgevoerd. Na compilatie moet voor dergelijke programma's het PP-commando (Privileged Program) worden gegeven. Gebeurt dit niet dan treden bij uitvoering van het programma security violations op.

Zonder InfoGuard kunnen het XP-commando en het PP-commando door iedereen die ODT-commando's kan uitvoeren, worden gegeven; onder InfoGuard kan dit alleen door Security Administrators. Op deze wijze wordt het onopgemerkt invoeren van "onveilige" constructies voorkomen.

De memory manager (onderdeel van het MCP) verzorgt de toewijzing van geheugen aan processen. Toegang tot geheugen buiten de toegewezen gedeelten moet worden aangevraagd via een "descriptor". In die descriptor staat alle relevante informatie over het aanvragende proces. De descriptor maakt het voor de memory manager mogelijk de aanvraag vooraf te beoordelen op geautoriseerdheid aan de hand van in het systeem vastgelegde bevoegdheden.

Autorisatie van gebruikers

Gebruikers worden geautoriseerd door het toekennen van bevoegdheden. Indien nodig, kunnen gebruikers de beschikking krijgen over additionele bevoegdheden, die voor het gehele systeem gelden. De Unisys A Serie kent als extra gebruikersbevoegdheden:

- Privileged User: de gebruiker heeft toegang tot alle programma's en normale gegevensbestanden. Daarnaast is hij bevoegd bepaalde systeemcommando's te geven (zoals PP en XP, zie hiervoor). Als InfoGuard is geïnstalleerd, komt de bevoegdheid om deze commando's te geven toe aan de Security Administrator, en heeft de Privileged User geen toegang tot de utilities van de Security Administrator.

- Security Administrator (SA): toegang tot de SA-utilities (MAKEUSER en SECOPT) en SA-bestanden (USERDATAFILE en SUMLOG). De Security Administrator-bevoegdheid is een toevoeging van InfoGuard.

- SYSTEMUSER: toegang tot het systeem alsof de gebruiker op een ODT werkt.

- COMSCONTROLUSER: toegang tot het COMS-utility window, waarmee configuratiewijzigingen worden aangebracht. De toegang tot het COMS-utility window wordt op twee plaatsen geregeld: in de COMS-configuration-file zelf én in de USERDATAFILE. Dit laatste geldt pas onder InfoGuard. De eerste manier geldt slechts totdat InfoGuard op een zeker niveau (S1, zie paragraaf Vergelijking InfoGuard en standaard A Serie access control) is geïnstalleerd.

Combinaties van de genoemde bevoegdheden zijn eveneens mogelijk. Naast deze bevoegdheden kunnen aan een USERCODE één of meer ACCESSCODES

worden toegekend, die toegang verlenen aan bestanden die niet noodzakelijkerwijs onder de desbetreffende USERCODE zijn opgeslagen (zie hierna).

De bevoegdheden van een gebruiker hoeven niet voor alle terminals van het systeem te gelden. In de COMS-configuration-file wordt vastgelegd op welke terminals een gebruiker zich mag aanmelden. Bovendien kan per terminal worden aangegeven of Privileged Users en SYSTEMUSERS daarop van hun ruime bevoegdheden gebruik mogen maken.

Autorisatie van programma- en bestandstoegang

De autorisatie van programma- en bestandstoegang wordt vastgelegd in de file-attributen en guard-files. Via de file-attributen wordt per bestand onder andere vastgelegd: eigenaar, gevoeligheid van de opgeslagen gegevens (sensitivedata; zie verder) en toegangsrecht in het algemeen. De mogelijke algemene toegangsrechten zijn:

- *private.* Alleen de eigenaar heeft lees/schrijf/execute-rechten;
- *public.* Alle gebruikers hebben toegangsrechten volgens het attribuut SECURITYUSE (dit kan zijn lees/execute, schrijf of lees/ schrijf/execute);
- *guarded.* De eigenaar heeft lees/schrijf/execute-rechten, de overige gebruikers hebben rechten zoals die zijn vastgelegd in de door het attribuut SECURITYGUARD genoemde guard-file;
- *controlled.* Alle gebruikers (inclusief de eigenaar) hebben rechten zoals die zijn vastgelegd in de door het attribuut SECURITYGUARD genoemde guard-file.

Een guard-file is een bestand waarin specifieke toegangsregels worden opgenomen die gelden voor de betrokken bestanden (deze regels slaan op USERCODES, ACCESSCODES en/of programma's en verlenen lees-, schrijf- en/of execute-bevoegdheden). Een aangemaakte guard-file is aan ieder willekeurig bestand of programma te koppelen (door het desbetreffende bestand "guarded" of "controlled" te maken). De op het systeem gedefinieerde Privileged Users hebben altijd, ongeacht de inhoud van eventuele guard-files, toegang tot alle bestanden. Alleen de Security Administrator-bestanden (SUMLOG en USERDATAFILE) zijn niet toegankelijk voor Privileged Users.

Op het systeem moet worden aangegeven of programma's vooraf bepaalde privileges bezitten, of dat de privileges afhankelijk zijn van hun aanroeper. Dit wordt met respectievelijk CHECKDECLARER=TRUE en CHECKDECLARER=FALSE ingesteld. Mogelijke bevoegdheden zijn Privileged-status en Security Administrator-status. Het gebruik van de CHECKDECLARER=TRUE wordt aanbevolen. Onder InfoGuard én vanaf de volgende versie van het MCP (begin 1992) is CHECKDECLARER=TRUE verplicht.
Programma's die worden opgestart vanaf een ODT (met continuous logon) of vanaf een SUPERUSERSTATION draaien niet onder een USERCODE (zogenaamde non-user-coded processen) en hebben bevoegdheden die vergelijkbaar zijn met Privileged programma's (met uitzondering van de universele bestandstoegang).

InfoGuard voegt aan de standaard bestandsbeveiliging zoals hierboven beschreven, toe dat ook printerspool-files beschermd kunnen worden. Zonder InfoGuard worden printerspool-files Public opgeslagen onder de USERCODE *. Onder InfoGuard kan worden ingesteld dat printerspool-files (Private) onder de USERCODE van de maker worden opgeslagen (USERCODEDBACKUP=TRUE). Ook andere bestanden zonder USERCODE kunnen Private worden gemaakt (NONUSERFILES=PRIVATE).

Verder kan met InfoGuard een disk-scrubbing verplicht worden gesteld (DISKSCRUBBING=TRUE). Als deze optie actief is, wordt de in gebruik te nemen disk-ruimte overschreven met een patroon dat de oude waarden vernietigt. Op deze wijze komt de inhoud van verwijderde bestanden nooit per ongeluk beschikbaar bij het hergebruik van de oude disk-ruimte. Het gebruik van DISKSCRUBBING heeft invloed op de performance van het systeem doordat disk-ruimte tweemaal beschreven moet worden bij ingebruikneming (eenmaal met een patroon en eenmaal met de nieuwe gegevens).
Zonder InfoGuard is het SENSITIVEDATA-file-attribuut beschikbaar dat per bestand kan worden gezet. In dit geval wordt reeds bij verwijdering van het bestand de vrijgekomen disk-ruimte overschreven met een patroon.
Gebruik van beide opties leidt tot het drie keer overschrijven van opnieuw in gebruik te nemen disk-ruimte (eenmaal bij vrijgave en tweemaal bij ingebruikneming).

Onder InfoGuard kunnen tape-files op een met disk-files vergelijkbare manier worden beveiligd (zie bovenstaande beschrijving). Op deze wijze worden "onbekende" tapes herkend, die vervolgens niet gebruikt kunnen worden zonder dat ze worden geaccepteerd door een gebruiker van een ODT.
Zonder InfoGuard kunnen alleen de tape-units (de machines waarop de tapes worden geplaatst) worden beveiligd, ongeacht de gegevens op de tape in de tape-unit. Printerspool-files en code-files die vanaf een beveiligde unit zijn geladen, kunnen niet afgedrukt respectievelijk uitgevoerd worden voordat ze zijn vrijgegeven door een systeembeheerder (Privileged User; met InfoGuard een Security Administrator).

Autorisatie van database-toegang

De autorisatie van database-toegang wordt eveneens met file-attributen en guard-files geregeld. De detailleringsmogelijkheden zijn echter veel groter dan bij toegang tot gewone bestanden.
In een DMSII-database kunnen meerdere logische databases worden gedefinieerd. Deze logische databases zijn deelverzamelingen van de gehele database. Per logische database kunnen bevoegdheden (lezen, schrijven, verwijderen, etc.) aan gebruikers worden toegewezen. Via guard-files worden de toegangsrechten van gebruikers tot de logische databases vastgelegd.
Bij databases krijgen Privileged Users slechts toegang via de gebruikte guard-file, in tegenstelling tot normale bestanden. Privileged Users hebben echter wel de mogelijkheid de desbetreffende

guard-file te verwijderen. Hierdoor werkt de database alsof er geen guard-file is gedefinieerd en krijgen Privileged Users toegang tot de database.

CONTROLEERBAARHEID

De Unisys A Serie computers leggen in verschillende log-bestanden gegevens vast over op het systeem verrichte acties:

- SUMLOG: log-bestand van het MCP, waarin vrijwel alle acties op het systeem kunnen worden vastgelegd;
- COMS-logging: log-bestand van COMS, waarin onsuccesvolle logon's en toegangspogingen naar niet beschikbare windows en naar het COMS-utility window worden vastgelegd;
- DMSII-audit-file: recovery-bestanden van het DMSII-systeem, die eveneens ten behoeve van controlewerkzaamheden kunnen worden gebruikt.

Naast registratie van gebeurtenissen in deze bestanden bestaat onder InfoGuard de mogelijkheid een Security station in te richten. Op dit station worden alle optredende security violations afgebeeld zodra ze optreden.
Per gebruiker kan, onder InfoGuard, worden opgegeven hoeveel violations hij mag veroorzaken. Zodra dit aantal wordt bereikt, volgt een blokkade van de gebruikerscode.

SUMLOG-bestanden

In de SUMLOG kunnen zo goed als alle acties op het systeem worden vastgelegd (onder andere BEGIN/END OF JOB en BEGIN/END OF TASK). Via het LOGGING-commando is aan te geven welke acties dienen te worden vastgelegd. Zonder InfoGuard is dit commando beperkt tot twee settings, te weten: LOGGING MINIMAL en LOGGING * (wat de default logging instelt). Met InfoGuard zijn alle afzonderlijke events te selecteren. Onder InfoGuard (IG) is het LOGGING-commando alleen beschikbaar voor Security Administrators. Onder andere kunnen de volgende, in tabel 2 opgenomen gebeurtenissen worden vastgelegd.

Het LOGGING-commando geldt voor alle processen op en gebruikers van het systeem. In de USERDATAFILE kan per gebruiker worden aangegeven welke acties van die gebruiker moeten worden gelogd. Daarnaast kan onder InfoGuard met behulp van het LG-commando per programma een afwijkende logging worden ingesteld.

Het benaderen van de aangemaakte SUMLOG-bestanden kan plaatsvinden via een aantal in functionaliteit vergelijkbare tools: LOGANALYZER, SMFII/QUERY (onder InfoGuard) en LOGGER (deze laatste is voornamelijk bedoeld voor het verkrijgen van statistische gegevens). Bij het lezen zijn selecties te maken op alle records of op JOB/TASK-nummer. Selectie op USERCODE/ACCESSCODE is eveneens mogelijk, zij het dat voor LOGANALYZER InfoGuard nodig is om deze selecties te kunnen maken.

MIN	*	IG	Gebeurtenis
•	•	•	Establish identity - bekend maken identiteit van een gebruiker bij overgang naar een ander MCS
•	•	•	BEGIN/END OF JOB/TASK - start- en eindtijden van processen, inclusief informatie over verbruikte resources en identiteit aanroeper
•	•	•	Maintenance records - gegevens over wijzigingen in hardware
•	•	•	Messages - de op de terminals afgebeelde systeemboodschappen (waaronder alle foutmeldingen)
•	•	•	LOGON/LOGOFF - aan- en afmelden van gebruikers
•	•	•	Security violations - optredende violations, zoals verkeerd aanmelden, pogingen tot ongeautoriseerde toegang tot een window en pogingen de USERDATAFILE aan te passen
•	•	•	HALT-LOAD - herstart van het systeem
•	•	•	LOG-RELEASE - openen van een nieuw SUMLOG-bestand
•	•	•	DATE-TIME RESET - opnieuw instellen van de systeemdatum en tijd
	•	•	FILE OPEN/CLOSE - openen en sluiten van bestanden, inclusief informatie over gebruiker en aantal lees- en schrijfoperaties
	•	•	Print requests - printopdrachten
	•	•	POWER-OFF - compleet stilleggen van het systeem
	•	•	USERDATA change/install - respectievelijk vervangen en opnieuw installeren van de USERDATAFILE
		•	START/END FILE PRINT - begin- en eindtijden van het afdrukken van bestanden
		•	Library-operaties - het SL-commando (System Library) voor activeren, deactiveren en bevriezen van programmabibliotheken (stukken code die vanuit applicaties aangeroepen kunnen worden, bijvoorbeeld goniometrische functies of statistische berekeningen)
		•	Database-operaties - openen, sluiten en activeren van databases
		•	COMS-configuration-records - wijzigingen in de COMS-configuration

Tabel 2. Gebeurtenissen die kunnen worden gelogd.

COMS-logging

Als onderdeel van COMS kan een security monitoring worden ingesteld. Daarmee worden onsuccesvolle logon's, toegangspogingen naar niet beschikbare windows en toegangspogingen naar het COMS-utility window vastgelegd in de COMS-logging. Eventueel kunnen alle logon's (ook de

succesvolle) door deze security monitoring worden geregistreerd. Ook wanneer InfoGuard wordt gebruikt en een Security station is gedefinieerd, blijft de COMS-security monitoring beschikbaar.

DMSII-audit-bestanden

Voor de DMSII-databases wordt een history-file aangehouden (de DMSII-audit) die bij calamiteiten reconstructie van de database mogelijk maakt. In deze bestanden liggen alle operaties die op de database zijn uitgevoerd vast. Voor controledoeleinden zijn deze bestanden met PRINTAUDIT te benaderen en kunnen selecties worden gemaakt op tijdsinterval, job-nummer, programmanaam en operatietype (records wijzigen, verwijderen, opnieuw indexeren, etc.). Het gebruik van PRINTAUDIT is onafhankelijk van de eventuele installatie van InfoGuard mogelijk.

Security station

Wanneer InfoGuard wordt gebruikt, bestaat de mogelijkheid een Security station te definiëren. Dit is een terminal en/of printer die alle security-relevante gebeurtenissen meldt, zodra ze optreden. Een Security station maakt het mogelijk direct in te grijpen wanneer de boodschappen daartoe aanleiding geven. Een voorbeeld hiervan is het detecteren van een reeks foute aanlogpogingen vanaf een bepaalde terminal. Deze worden direct op het Security station gemeld, waardoor onmiddellijk actie kan worden ondernomen door bijvoorbeeld de security officer.

Een Security station kan alleen worden bemand door een gebruiker die SECURITYMSGUSER is (dit wordt in de USERDATAFILE vastgelegd). Wanneer een andere gebruiker zich op het Security station aanmeldt, worden de boodschappen niet afgebeeld en functioneert het Security station als een normale terminal.

VERGELIJKING INFOGUARD EN STANDAARD A SERIE ACCESS CONTROL

Deze paragraaf geeft een overzicht van de in dit artikel besproken interne-controle- en beveiligingsmaatregelen in de vorm van een vergelijking van de standaard-ICB-mogelijkheden met de toevoegingen door InfoGuard. Daarna wordt een beschrijving gegeven van de installatieniveaus van InfoGuard. Figuur 3 aan het einde van deze paragraaf laat zien in welke mate de ICB-doelstellingen kunnen worden bereikt zonder en met InfoGuard.

Standaard Unisys A Serie

Zonder installatie van InfoGuard zijn de volgende ICB-faciliteiten op de Unisys A Serie computers aanwezig:

- passwords voor USERCODES en ACCESSCODES;
- programma- en bestandsautorisatie door middel van file-attributen en guard-files;
- database-authenticatie door middel van time-stamp-controle via de DMSII-control-file;
- database-autorisatie door middel van guard-files, ook voor Privileged Users (die echter wel de bevoegdheid hebben de guard-files te verwijderen);
- wijzigen van gebruikersbevoegdheden alleen door Privileged Users;
- wijzigen systeemconfiguratie alleen door COMSCONTROL-users (aangegeven in de COMS-configuration-file);
- logging-faciliteiten voor het systeem, in twee standen in te stellen (respectievelijk minimal en * (= default));
- beveiliging van tapes, maar alleen op tape-unit-niveau;
- op hardware-niveau aanwezige structuren die het als programma uitvoeren van data voorkomen;
- afwezigheid van assemblers, programma's met "gevaarlijke" constructies moeten via XP worden geaccepteerd.

InfoGuard-bijdrage

Afhankelijk van het installatieniveau van InfoGuard worden de standaardmogelijkheden uitgebreid. InfoGuard kent vier installatieniveaus, te weten: U, S0, S1 en S2. Deze instellingen geven een algemene classificatie van het beveiligingsniveau voor InfoGuard. Overeenkomstig de door het Amerikaanse ministerie van Defensie gehanteerde normen ([DODE83]) kan met InfoGuard op niveau S2 de classificatie C2 worden gehaald ([DRIS88] en [DRIS90]). De security manual ([USAG89]) van Unisys geeft in een bijlage het traject dat een organisatie moet volgen om deze C2-classificatie te bereiken.

De (mogelijke) toevoegingen van InfoGuard zijn de volgende:

- Security Administrator (SA). Dit is de via de USERDATAFILE verleende autorisatie aan gebruikers, die het mogelijk maakt:
  - de USERDATAFILE te wijzigen. Hierdoor wordt het toekennen van bevoegdheden, inclusief het invoeren van Privileged Users, SYSTEMUSERS en Security Administrators geconcentreerd bij de Security Administrators;
  - het SECOPT-commando te gebruiken (voor het instellen van beveiligingsopties);
  - het CF-commando te gebruiken (voor het verplaatsen van het Configuratie-bestand);
  - het DL-commando (Disk Location) te gebruiken voor het verplaatsen van de USERDATAFILE en SUMLOG-bestanden;
  - de PP-, XP-, MC- en SL-commando's te gebruiken (het toekennen van meer dan normale bevoegdheden aan programma's en libraries).
- Vereenvoudigde security administration, door het samenbrengen van de beveiligingscommando's

in één systeemcommando (het SECOPT-commando). Dit commando is alleen te gebruiken door Security Administrators. Hieronder vallen onder andere DISKSCRUBBING, NONUSERFILES en USERCODEDBACKUP.

– Password-aging en -generation: het verplicht periodiek vernieuwen van de passwords op het systeem (aging) en het door het systeem laten genereren van een password (generation). De gegenereerde passwords zijn eenvoudig te onthouden combinaties van drie Engelse woorden (bijvoorbeeld LONGLEANTREE of GREENHOUSELAWN).

– Toegang tot COMS-utility window via USERDATAFILE geregeld, in plaats van via COMS-configuration-file.

– Effectievere en efficiëntere logging. De in de paragraaf Controleerbaarheid genoemde SUMLOG-elementen kunnen met InfoGuard individueel worden geselecteerd. Hierdoor is het mogelijk de logging nauwkeurig af te stemmen op de gewenste informatie, waarbij de belasting van het systeem beperkt blijft. Verder is het mogelijk de specifieke logging voor een USERCODE of een programma ruimer in te stellen. Op deze wijze kunnen belangrijke processen gedetailleerd worden gevolgd zonder de performance van het systeem (ernstig) nadelig te beïnvloeden.

- Tape-beveiliging. InfoGuard maakt het mogelijk tape-bestanden te beveiligen op een manier die vergelijkbaar is met de beveiligingsmogelijkheden die standaard alleen voor disk-bestanden worden geboden.

– Afschermen toegang tot SUMLOG-bestanden. Gebruikers die geen Security Administrator (SA) zijn, kunnen geen gegevens opvragen over security-relevante gebeurtenissen (zoals foutieve aanlogpogingen of wijzigingen in de USERDATAFILE).

– Security station: instellen van een terminal als Security station zodat daar alle optredende security violations direct worden gemeld.

Installatieniveaus InfoGuard

De mogelijkheden die InfoGuard biedt zijn in principe willekeurig te gebruiken. Door Unisys is echter een indeling gemaakt van logische mogelijkheden in de vorm van installatieniveaus. De niveaus van installatie die met betrekking tot InfoGuard worden onderkend, zijn:

Niveau U
Dit is de standaardinstelling. Het systeem werkt alsof InfoGuard niet is geïnstalleerd. Alle controle- en beveiligingsmaatregelen die zonder InfoGuard mogelijk zijn, kunnen zonder meer worden toegepast.

Niveau S0
Dit niveau is vergelijkbaar met niveau U, met de toevoeging dat nu alle InfoGuard-opties willekeurig te selecteren zijn. In S0 is elk InfoGuard-feature te gebruiken, zonder dat mogelijkheden verplicht gesteld worden.

Niveaus S1 en S2
Deze niveaus zijn stringentere vormen van respectievelijk S0 en S1. Bij S1 wordt een aantal InfoGuard-opties verplicht gesteld, bij S2 wordt daar nog een aantal verplichte opties aan toegevoegd. Met S1 of S2 kan in één keer een hele reeks maatregelen worden geactiveerd die te zamen een coherente controle en beveiliging opzetten. In beide gevallen blijven de overgebleven InfoGuard-opties beschikbaar voor gebruik. In tabel 3 is aangegeven welke opties de niveaus S1 en S2 verplicht stellen.

S1	S2	Optie
•		Minimaal één password bij elke USERCODE
	•	Eén en hoogstens één password bij elke USERCODE
•	•	NONUSERFILES = PRIVATE
•	•	Tape-beveiliging
•	•	USERCODEDBACKUP = TRUE
•	•	SUPERUSERSTATIONS kunnen niet gedefinieerd worden
•	•	COMS-utility window alleen beschikbaar voor COMSCONTROL-gebruikers (aangegeven via USERDATAFILE)
•	•	Normale programma's kunnen bestaande guard-files niet overschrijven
	•	DISKSCRUBBING

Tabel 3. Beveiligingsopties bij de niveaus S1 en S2.

Overzicht access control

De op de volgende pagina geplaatste schema's geven voor de access control-doelstellingen aan welke middelen voor de controle en beveiliging van de diverse objecten worden gebruikt. Per access control-doelstelling wordt een overzicht gegeven van de afdekking, onderscheiden naar de standaardmogelijkheden, de verbeteringsmogelijkheden door InfoGuard en de mogelijkheden die alleen InfoGuard biedt.

SLOTWOORD

De Unisys A Serie computersystemen beschikken met de standaard-utilities en de besturings-software reeds over een uitgebreide set van mogelijke interne-controle- en beveiligingsmaatregelen op het gebied van access control.
InfoGuard voegt aan die standaardmogelijkheden een aantal belangrijke functionaliteiten toe, die met name de beheersbaarheid en controleerbaarheid van de access control vergroten.
Het bij de A Serie computers van Unisys bereikbare niveau van beveiliging met optimale gebruikmaking van InfoGuard (C2-classificatie DOD) kan op basis van de huidige maatstaven als adequaat worden beschouwd. Dit betekent niet dat men zich ook voor de toekomst tevreden mag stellen met het nu bereikbare controle- en beveiligingsniveau.

Doel: Authenticatie / Middel	Gebruiker	Systeem	Station	MCS	Window	Programma	Bestand	Database	Dataset	Randapp.
Fysieke maatregelen	•									•
Hardware		•	•							•
COMS-systeem-software			•	•	•					
Operating system						•	•	•		
DMS-systeem-software								•	•	
Usercode/password	A									
Access code/password	A									

Legenda:
• = Zowel met als zonder InfoGuard
A = Verbetering door InfoGuard
I = Alleen met InfoGuard

Figuur 3. Access control-doelstelling authenticatie.

Doel: Autorisatie / Middel	Gebruiker	Systeem	Station	MCS	Window	Programma	Bestand	Database	Dataset	Randapp.
Hardware		•								
Aanlogprocedure	A	•	•							
User-privileges	A	•	•		•	•	•			
COMS-configuration	•	•	•	•	•	•		•		•
File-attributen						•	•	•		
Guard-files	•					•	A	•	•	

Legenda:
• = Zowel met als zonder InfoGuard
A = Verbetering door InfoGuard
I = Alleen met InfoGuard

Figuur 4. Access control-doelstelling autorisatie.

Doel: Controleerbaarheid / Middel	Gebruiker	Systeem	Station	MCS	Window	Programma	Bestand	Database	Dataset	Randapp.
SUMLOG	A	•	•	•	A	A	A	•		I
COMS-logging	•		•	•	•	•				
DMS-audit-files								•	•	
Security station	I					I				

Legenda:
• = Zowel met als zonder InfoGuard
A = Verbetering door InfoGuard
I = Alleen met InfoGuard

Figuur 5. Access control-doelstelling controleerbaarheid.

Belangrijke zaken betreffende access control die naar onze mening aandacht behoeven bij de toekomstige nieuwe versies van systeemprogrammatuur en InfoGuard zijn:

– het vereenvoudigen respectievelijk het geautomatiseerd ondersteunen van de controle en het beheer van de technische implementatie van de access control-matrix. De technische maatregelen zijn op dit moment namelijk verspreid over een aantal verschillende onderdelen van het systeem (USERDATAFILE, COMS-configuration-file, guard-files en InfoGuard-opties). Hierdoor is het produceren van overzichten van getroffen maatregelen en het in stand houden van de relatie tussen de logische access control-matrix en de feitelijk geïmplementeerde bevoegdheden vooralsnog een relatief bewerkelijk en grotendeels handmatig proces;

– het introduceren van het functiescheidingsbeginsel voor kritische systeemacties, zoals het toekennen van systeemautorisaties Privileged User en Security Administrator. Ook het toevoegen of verwijderen van essentiële systeemcomponenten zou slechts met behulp van door het systeem afgedwongen functiescheiding gerealiseerd moeten kunnen worden. Met de huidige faciliteiten kunnen te veel verantwoordelijkheden en bevoegdheden aan individuele personen zijn toegekend;

– het integreren van middelen die harde persoonsauthenticatie ondersteunen in de access control-systemen. In de huidige opzet is voorzien in uitsluitend op kennis gebaseerde verificatiemiddelen (met name de passwords). Ook op bezit gebaseerde middelen zoals smartcards en cardkeys zouden toepasbaar moeten zijn, in verband met het belang dat de systemen kunnen vertegenwoordigen voor de desbetreffende organisaties in de huidige maatschappij;

– het nadrukkelijker betrekken van EDP-auditors bij de ontwikkeling van (nieuwe releases van) access control-systemen. Tegenwoordig zijn in Nederland opleidingen van niveau beschikbaar die zich ook richten op de evaluatie van access control-systemen. De expertise van EDP-auditors die bijvoorbeeld afgestudeerd zijn aan post-doctorale EDP-audit-opleidingen, kan goed worden gebruikt in het ontwikkeltraject van access control-systemen.

De hiervoor gedane aanbevelingen zijn overigens niet alleen van toepassing op de Unisys A Serie, maar gelden merendeels voor alle bekende momenteel op de markt beschikbare systemen.

Dit artikel is tot stand gekomen met medewerking van ir. R. Hak van Unisys Nederland en prof. M.E. van Biene-Hershey van de Vrije Universiteit te Amsterdam. Van hun commentaar en opmerkingen bij een concept van dit artikel is dankbaar gebruik gemaakt.

VERKLARENDE WOORDENLIJST

Accesscode
Toevoeging aan een usercode die een gebruiker extra bevoegdheden voor bestandstoegang verleent (via guard-files).

ACM
Access Control Matrix - ook wel competentietabel genoemd, hierin worden van alle gebruikers hun bevoegdheden voor de verschillende objecten vastgelegd.

CANDE
Command AND Editor - MCS voor het schrijven van programma's en het uitvoeren van commando's.

COMS
COmmunications Management System - MCS dat als basis dient voor veel andere MCS'en en de configuratie van het systeem vastlegt.

CP
Communications Processor - knooppunt in het netwerk.

CPM
Central Processing Module - de processor van de Unisys A Serie computers.

DMSII
Database Management System II - een netwerk-database systeem.

Guard-file
Bestand met toegangsregels, die vrij te definiëren zijn. Guard-files kunnen aan bestanden worden gekoppeld, waardoor de vastgelegde regels voor de toegang tot dat bestand gaan gelden.

ICB
Interne Controle en Beveiliging.
Interne Controle : de maatregelen ter beheersing van bedrijfsprocessen. *Beveiliging:* de maatregelen ter voorkoming van misbruik (opzettelijk of onopzettelijk) van bedrijfsactiva.

I/O-base
Aantal Input/Output-poorten.

LINC
Logic and Information Network Compiler - vierde-generatie-ontwikkelomgeving voor Unisys A Serie computers.

MARC
Menu Assisted Resource Control - menugestuurde "schil" om COMS van waaruit de gebruiker COMS-commando's en systeemutilities kan uitvoeren.

MCP
Master Control Program - operating system van de Unisys A Serie computers.

MCS
Message Control System - systeem-software die de communicatie tussen de Unisys A Serie, applicaties en gebruikers verzorgt.

NAU
Network Administrative Utility - onderdeel van het operating system waarin de fysieke configuratie is vastgelegd.

ODT
Operator Display Terminal, de operatorconsole (op de computerzaal).

Usercode
Naam of nummer waarmee een gebruiker zich op het systeem identificeert.

LITERATUURLIJST

[BIEN89] M.E. van Biene-Hershey, *EDP-Auditing in relatie tot management*, M.E. van Biene-Hershey, Abcoude 1989.

[CFSB91] *Computer fraud & security bulletin*, mei 1991, Elsevier Science Publishers Limited.

[DNBM88] *Memorandum omtrent de betrouwbaarheid en continuïteit van geautomatiseerde gegevensverwerking in het bankwezen*, De Nederlandsche Bank N.V., september 1988.

[DODE83] George G. Meade, *Department of Defense, Trusted Computer System Evaluation Criteria*, beter bekend als Orange book, 1983 DOD Fort.

[DRIS88] Datapro reports on Information Security, *Unisys Corporation InfoGuard*, IS52-944 101 t/m 105, juni 1988, Datapro Research Corporation.

[DRIS90] Datapro reports on Information Security, *NCSC Evaluated Operating Systems and Software*, IS50-100 101 t/m 112, mei 1990, McGraw Hill Incorporated.

[DSDI90] Data Security Digest, *Wetsontwerp Computercriminaliteit deel I, II en III*, augustus, oktober en december 1990, Cipher Management B.V.

[STOL89] C. Stoll, *Het Koekoeksei; over krakers en computerspionage*, De Haan 1989.

[UCAN90] *Unisys A Series CANDE Operations Reference Manual*, Release 3.8.1 maart 1990, Unisys Corporation.

[UCOM89] *Unisys A Series Communications Management System (COMS) Operations Guide*, Release 3.8.0 mei 1989, Unisys Corporation.

[UDMS89] *Unisys A Series DMSII Utilities Operations Guide*, Release 3.8.0 mei 1989, Unisys Corporation.

[USAG89] *Unisys A Series Security Administration Guide*, Release 3.8.0 mei 1989, Unisys Corporation.

[USSF87] *Unisys A Series Security Features Operations and Programming Guide*, Release 3.7.0 juli 1987, Unisys Corporation.

Drs. M.A. Bongers RA
Is hoofd EDP-Audit bij de Interne Accountants Dienst van Credit Lyonnais Bank Nederland N.V. Daarnaast is hij lid van de programmacommissie van de EDP-Audit-opleiding aan de Vrije Universiteit te Amsterdam.

J-M. van Leerdam
Is bijna afgestudeerd in de Technische Informatica aan de Technische Universiteit Delft en is in dat kader momenteel werkzaam in het technical EDP-Audit-team van IAD/EDP-Audit van Credit Lyonnais Bank Nederland N.V.

Beveiliging van Tandem-systemen

K.E.A. van Dijk en
M.M.J.A. van Dijk

Tandem-computersystemen worden met name aangetroffen als hulpmiddel voor geautomatiseerde gegevensverwerking waarbij continuïteit een belangrijke rol speelt.
Dit artikel geeft inzicht in de beveiligingsmogelijkheden van de Tandem-besturingsprogrammatuur Guardian en een additioneel pakket hiervoor: Safeguard.
Daarnaast wordt aandacht besteed aan de aspecten die een rol spelen bij de beoordeling van de effectiviteit van de beveiliging van een dergelijke omgeving.

INLEIDING

Logische toegangsbeveiliging kan worden gedefinieerd als het stelsel van maatregelen en procedures (organisatorische en software-matige) dat erop gericht is de toegang tot een computersysteem (gegevens, programma's, randapparatuur, etc.) te beschermen tegen benadering door ongeautoriseerde personen. Over logische toegangsbeveiliging is een betrekkelijk omvangrijke literatuur verschenen. Met betrekking tot het beveiligen van Tandem-systemen (Guardian-systemen) is echter weinig gepubliceerd.
Dit artikel gaat nader in op de logische beveiliging van Tandem-systemen door middel van het toegangsbeveiligingspakket Safeguard (versie C22) in combinatie met de standaardfaciliteiten van het besturingssysteem Guardian (versie C20). Naast Safeguard is voor de logische beveiliging het pakket Onguard op de markt. In dit artikel zal op de functionaliteit van Onguard slechts terloops worden ingegaan.

Allereerst wordt een beschrijving gegeven van de architectuur en systeem-software van Tandem-systemen alsmede een algemene beschrijving van de faciliteiten voor het beveiligen van de toegang tot Tandem-systemen. Vervolgens wordt in hoofdlijnen aangegeven hoe een Tandem-systeem kan worden beveiligd met behulp van Guardian en Safeguard. Tot slot wordt ingegaan op de aspecten die voor de EDP-auditor van belang kunnen zijn bij het beoordelen van het stelsel van maatregelen en procedures ter beveiliging van een Tandem-systeem.

ARCHITECTUUR EN SYSTEEM-SOFTWARE TANDEM-SYSTEMEN

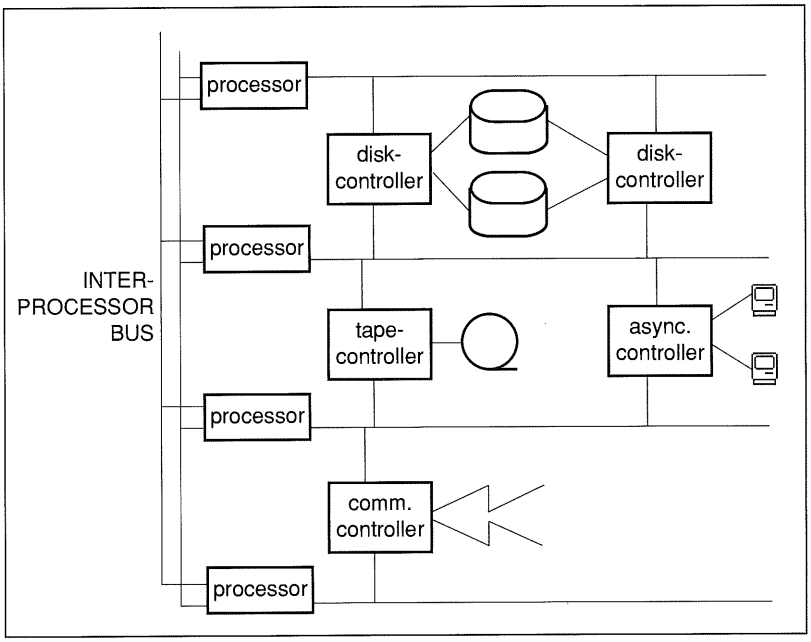
Alvorens nader wordt ingegaan op de logische toegangsbeveiliging, wordt in deze paragraaf een schets gegeven van de architectuur en de systeemsoftware van Tandem-systemen.

Architectuur Tandem-systemen

Tandem-systemen zijn ontworpen voor online-/realtime-toepassingen, bijvoorbeeld een reserveringssysteem voor vliegtuigen. In Nederland worden Tandem-systemen met name gebruikt voor bancaire toepassingen zoals geld- en betaalautomaatsystemen.
Tandem-systemen zijn voor dergelijke toepassingen geschikt vanwege de zogenaamde fout-tolererende (fault tolerant) omgeving. Kenmerkend voor fout-tolererende systemen is dat indien delen van het systeem (hardware of software) defect raken, de werking hierdoor niet nadelig wordt beïnvloed. Dientengevolge is de beschikbaarheid van het systeem groot.
Om dit te bereiken zijn Tandem-systemen modulair opgebouwd en zijn alle noodzakelijke onderdelen dubbel uitgevoerd. Zo zijn er twee of meer tweevoudig aangesloten processor-modules, diskcontrollers, disks, meerdere gedeelde energievoorzieningen, accu's voor backup, etc. (zie figuur 1).
Andere kenmerken van Tandem-systemen zijn dat deze modulair kunnen worden uitgebreid en dat reparatie en herconfiguratie van een gedeelte van het systeem kan plaatsvinden terwijl de rest van het systeem operationeel blijft.
Elk onderdeel voert een (zelf)controle uit. Een processor controleert de status van andere processoren en van zichzelf. Als een processor een fout bij een andere processor constateert, zal deze de als backup gedefinieerde activiteiten overnemen. Constateert een processor een fout bij zichzelf, dan zal hij stoppen, waarna een backup-processor de activiteiten zal overnemen.
Een processor is een zelfstandige verwerkingseenheid, geschikt om alle functies voor gegevensverwerking te ondersteunen. Hiertoe wordt in het geheugen van de processor de noodzakelijke code van het besturingssysteem (Guardian) opgeslagen. De communicatie tussen de processoren onderling verloopt via speciale dubbele high-speed channels (InterProcessor Bus (IPB) of Dynabus). Een processor kan worden geconfigureerd om meerdere verschillende onderdelen te ondersteunen en parallelle verwerking uit te voeren. Dit alles maakt het mogelijk dat een fout in een enkel onderdeel "getolereerd" kan worden door de rest van het systeem.

Systeem-software

Aan de hand van het "logische toegangspad" wordt in deze paragraaf een aantal systeem-software-componenten binnen een Tandem-systeem nader uitgewerkt. Het "logische toegangspad" kan schematisch worden voorgesteld als geschetst in figuur 2 op de volgende pagina.



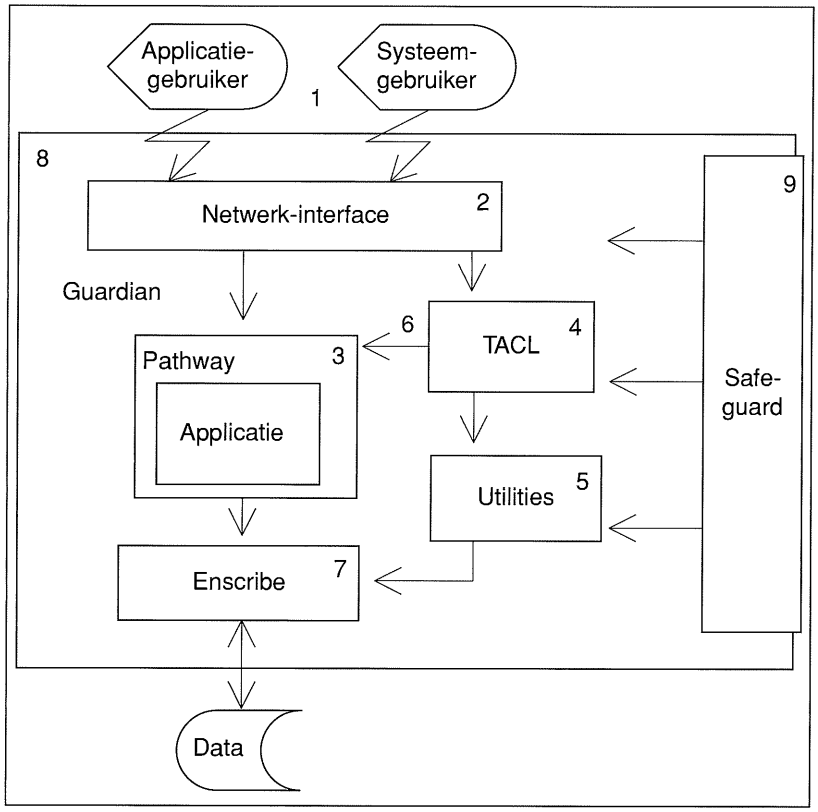
Figuur 1. Architectuur Tandem-systeem.

Systeem	Introductie-jaar	Performance [1]	Capaciteit I/O chann./ IPB (1bus) in Mb/sec	Max. cap. main memory in Mb/p.proc.
NonStop1+	1976	1,0	5,0 / 13,3	2
NS EXT10	1986	1,25	5,0 / 13,3	8
CLX 620	1987	1,12	5,0 / 20,0	12
CLX 720	1989	1,55	3,7 / 20,0	16
TXP EXT25	1986	1,25	5,0 / 10,0	16
VLX	1986	1,45	5,0 / 20,0	96
Cyclone	1989	3,40	10,0 / 20,0	128

Tabel 1. Guardian-systemen.

Tandem-gebruikers kunnen in twee groepen worden ingedeeld: applicatiegebruikers (eindgebruikers) en systeemgebruikers ((systeem)-programmeurs, operators, systeembeheerders) (1). De gebruikers krijgen toegang tot het systeem via netwerk-interface-programmatuur. Te onderscheiden zijn onder andere directe aansluitingen, X25-aansluitingen en Expand-aansluitingen (het netwerk dat Tandem-computers onderling verbindt).
Applicatiegebruikers maken gebruik van toepassingen ontwikkeld met behulp van Pathway (3). Pathway is de omgeving waarbinnen de applicatie wordt uitgevoerd en levert de faciliteiten voor het beheer van de applicatie-omgeving. Via Pathway wordt onder andere de relatie gelegd tussen de applicatiegebruiker en een applicatie.
Systeemgebruikers communiceren rechtstreeks met het besturingssysteem Guardian, waarbij gebruik wordt gemaakt van TACL (Tandem Advanced Command Language) (4), een commandotaal voor systeemontwikkeling, operations en beheer.
De scheiding tussen de applicatiegebruikers en systeemgebruikers kan worden afgedwongen omdat bij iedere toegangspoort tot het systeem moet worden aangegeven of doorleiding dient plaats te vinden naar een Pathway-applicatie of naar TACL. Via TACL kan een groot aantal Tandem-systeem-utilities worden uitgevoerd (5).

1 De performance ratio is een schatting, gebaseerd op door Tandem opgedane ervaring en experimenten. Voorbeeld:
- 1 TXP-processor is 1,25 x krachtiger dan 1 CLX720-processor;
*- 1 VLX-processor is 1,45*1,25*1,55 = 2,8 x krachtiger dan een CLX620-processor.*



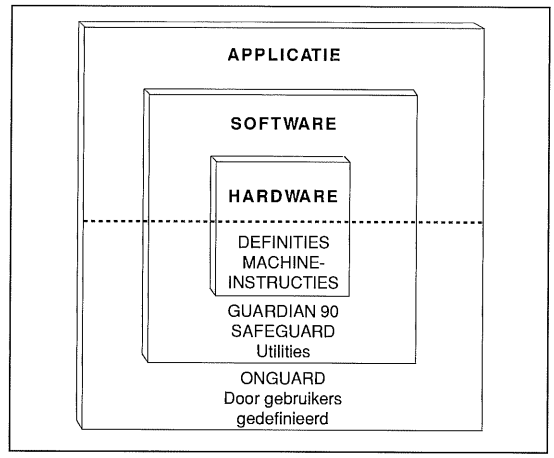
Figuur 2. Logisch toegangspad Tandem.

Eén van de utilities betreft het beheren en monitoren van de Pathway-omgeving (Pathcom) (6). Gezien de mogelijkheid via TACL applicaties te beïnvloeden, dient bij een Tandem-omgeving een fysieke scheiding te worden aangebracht tussen ontwikkeling en produktie. In dit artikel wordt verder uitgegaan van de produktie-omgeving.
De relatie naar de opgeslagen data komt tot stand via Enscribe (7), een onderdeel van het besturingssysteem Guardian.
Het toegangsbeveiligingspakket Safeguard (9) in samenhang met Guardian (8) zal in de loop van dit artikel nog uitvoerig aan bod komen.

BEVEILIGING VAN TANDEM-SYSTEMEN ALGEMEEN

Het besturingssysteem Guardian biedt standaard een aantal faciliteiten. Deze faciliteiten zijn:
- authenticatie van de gebruiker om tot het systeem te worden toegelaten (subjectbeveiliging);
- autorisatie van de handelingen met betrekking tot schijfbestanden (objectbeveiliging).

Het toegangsbeveiligingspakket Safeguard, een produkt van Tandem, is een uitbreiding op de standaardfaciliteiten van Guardian. Safeguard biedt meer mogelijkheden voor het beveiligen van schijfbestanden en voor de authenticatie van gebruikers. Naast schijfbestanden kunnen met behulp van Safeguard ook objecten als schijfruimte,



Figuur 3. Lagen Tandem-systeembeveiliging.

processen en randapparatuur worden beveiligd. Tevens worden audit-faciliteiten geboden voor het vastleggen van pogingen om toegang te krijgen tot beveiligde objecten. In dit artikel wordt nader ingegaan op de beveiligingsfaciliteiten die het pakket Safeguard biedt in combinatie met de standaardfaciliteiten van Guardian.

De toegangsbeveiliging op applicatieniveau, onder andere ter ondersteuning van functiescheiding in de gebruikersorganisatie, dient vooral in de applicatie zelf te worden geregeld. Ook kan gebruik worden gemaakt van het pakket Onguard, dat een vorm van menubeveiliging biedt.

WAT IS SAFEGUARD

In Safeguard wordt onderscheid gemaakt tussen de beveiliging van subjecten en objecten. De beveiliging van subjecten betreft de gebruikers van het systeem en de beveiliging van objecten betreft de systeemcomponenten. Ten opzichte van Guardian biedt Safeguard met name de volgende uitbreidingen:

– Guardian beveiligt de toegang tot slechts één soort object: schijfbestanden. Een eigenaar kan de verschillende bevoegdheden tot zijn bestand toekennen.
Met Safeguard daarentegen kan ook de toegang tot andere soorten objecten worden beveiligd, zoals schijfruimte (volumes en subvolumes), processen en randapparatuur. Met behulp van Safeguard kan de eigenaar van het autorisatie-record behorende bij een object, de bijbehorende Access Control List (ACL) creëren of wijzigen. Met de ACL kan worden aangegeven welke individuele gebruikers en welke specifieke gebruikersgroepen welke bevoegdheden hebben ten aanzien van een bepaald object.

– Met behulp van Safeguard kunnen (gelukte en mislukte) pogingen om aan te loggen alsmede pogingen tot het verkrijgen van toegang tot objecten worden vastgelegd (logging). Guardian biedt deze faciliteit niet.

In dit artikel wordt verder uitgegaan van de beveiliging die met Safeguard in combinatie met Guardian is te realiseren, tenzij anders is vermeld.

Authenticatie van gebruikers

Authenticatie van gebruikers vindt plaats aan de hand van een geldige gebruikersidentificatie in combinatie met een wachtwoord.
Vanaf het moment dat Safeguard is geïnstalleerd, neemt het automatisch het beheer over van de bestaande Guardian-bestanden met gebruikersidentificaties en wachtwoorden (USERID-files). Met Safeguard kunnen gebruiker-records worden uitgebreid met extra opties zoals geldigheidsduur van wachtwoord en/of gebruikersidentificatie, het voor onbepaalde tijd inactief maken van een gebruiker en encryptie van wachtwoorden.
Safeguard creëert een database met authenticatie-records voor gebruikers. Default is de Super-id (zie hierna) eigenaar van deze authenticatie-records. Safeguard biedt de mogelijkheid het eigendom onder te brengen bij een algemene gebruiker; deze gebruiker kan dan worden belast met de functie Security Administrator.

Een Guardian-systeem kent verschillende soorten gebruikers. Classificatie vindt plaats aan de hand van het groepsnummer en het gebruikersnummer (n,n). Guardian maakt onderscheid tussen de volgende typen gebruikers:

- General user (n,n): de standaardgebruikers kunnen aanloggen op het systeem om bepaalde applicaties, bijvoorbeeld een boekhoudprogramma, uit te voeren.

- Group manager (n,255): de zogenaamde group managers zijn verantwoordelijk voor een specifieke groep (klasse) gebruikers op het systeem.

- System operator (255,n): deze groep verricht verschillende systeemfuncties met betrekking tot systeembestanden, disks en andere randapparatuur.

- Super-id (255,255): de Super-id of Super.Super is de hoogste klasse gebruiker met de meeste bevoegdheden. De Super-id-functie heeft toegang tot de bestanden, processen en randapparatuur van het gehele systeem zonder enige restrictie.

De laatste drie typen gebruikers worden ook wel "privileged users" genoemd.

Naast voornoemde typen gebruikers kent Guardian ook speciale gebruikers, zoals de Network User voor op afstand (remote) gekoppelde systemen. Network Users kunnen gegevens transporteren of hebben toegang tot gegevens verspreid over het netwerk.
De gebruikersidentificatie van een Network User is voor alle betrokken systemen identiek. Voor de toegang tot een systeem op afstand heeft de Network User naast zijn gebruikersidentificatie ook een zogenaamd remote password nodig. Hiermee kan hij aanloggen vanaf een ander Tandem-systeem.

Autorisatie

Aan gebruikers wordt autorisatie verleend ten aanzien van schijfbestanden, schijfruimte, processen en randapparatuur (objecten). Autorisatie vindt plaats met behulp van de eerder genoemde Access Control Lists (ACL's). Een ACL is een toegangstabel van subjecten (gebruikers) in relatie tot een object en geeft aan welke gebruiker toegang heeft tot een bepaald object en welke bevoegdheden hij heeft.
Door middel van niveaus wordt aangegeven welke gebruikers toegang hebben. De volgende niveaus worden in Guardian onderscheiden:
- O (local owner): alleen de eigenaar van het object op het lokale systeem kan het object benaderen;
- U (network owner): alleen de eigenaar van het object op het lokale systeem of in het netwerk kan het object benaderen;
- G (local group): de gebruikers op het lokale systeem, die horen tot de groep van de eigenaar van het object, kunnen het object benaderen;
- C (network group): de gebruikers op het lokale systeem of in het netwerk, die horen tot de groep van de eigenaar van het object, kunnen het object benaderen;
- A (any local user): elke gebruiker op het lokale systeem kan het object benaderen;
- N (any user): elke gebruiker op het lokale systeem of in het netwerk kan het object benaderen;
- - (local Super-id): alleen de lokale Super-id kan het object benaderen.

De bevoegdheden die in Safeguard aan een gebruiker worden toegekend - Read, Write, Execute, Purge, Create en Owner - geven de functies aan die ten aanzien van dat object mogen worden uitgevoerd.

In tabel 2 staat aangegeven welke toegangsbevoegdheden per object kunnen worden toegekend.

Tabel 2. Objecten en toegangsbevoegdheden in Safeguard.

Soort object	R	W	E	P	C	O
Bestanden	×	×	×	×	×	×
Schijfruimte:						
- volume	×	×	×	×	×	×
- subvolume	×	×	×	×	×	×
Randapparatuur:						
- devices	×	×	–	–	–	×
- subdevices	×	×	–	–	–	×
Processen:						
- proces	×	×	–	×	×	×
- subproces	×	×	–	–	–	×

Voorbeeld:
Een (R,W,P,C,O)-autorisatie voor gebruiker A ten aanzien van een beveiligd proces houdt in dat gebruiker A is geautoriseerd om:
- een proces te openen voor invoeractiviteiten (Read);
- een proces te openen voor uitvoeractiviteiten (Write);
- een nieuw proces te creëren (Create);
- een proces te stoppen (Purge);
- het autorisatie-record behorende bij het proces te lezen of te veranderen (Owner).

Safeguard beveiligt objecten niet automatisch. Een hiervoor in de organisatie verantwoordelijk gestelde functie dient de beveiliging van objecten te implementeren. Hieraan vooraf zal eerst moeten worden vastgesteld waar in de organisatie de verantwoordelijkheden (eigenaarschap) ten aanzien van deze te beveiligen objecten liggen. Dit laatste is vaak een langdurig en moeizaam proces.
Voor het toekennen van bevoegdheden wordt per object een autorisatie-record toegevoegd aan de object-database. Nadat een ACL is gedefinieerd, zijn de voor het desbetreffende object geldende Guardian-beveiligingsopties overgenomen door Safeguard.

Auditing

Safeguard bevat opties voor het vastleggen van pogingen om aan te loggen, om toegang te krijgen tot een met Safeguard beveiligd object en om Safeguard-beveiligingsparameters te wijzigen. Deze vastleggingen kunnen worden gebruikt voor onder andere audit-werkzaamheden.
Pogingen om de Safeguard-configuratie te wijzigen of om commando's uit te voeren met betrekking tot vastleggingen (audit service) of de beveiliging van terminals (Terminal Commands), worden altijd vastgelegd. Voor de overige opties moet expliciet worden aangegeven of en zo ja, welke vastlegging moet plaatsvinden.
Om de door Safeguard gegenereerde vastleggingen voor controlewerkzaamheden te kunnen gebruiken, zijn automatische hulpmiddelen nodig. Zonder deze hulpmiddelen is de informatie moeilijk toegankelijk. Hiervoor zijn speciale pakketten op de markt, bijvoorbeeld Auditview, die aan de hand van de vastleggingen de gewenste overzichten kunnen genereren.

Internationale toetsing/certificering

Het German Information Security Agency (GISA) heeft in 1988 richtlijnen ontwikkeld voor het beveiligen van geautomatiseerde systemen. De criteria zijn opgesteld naar analogie van het Orange book uit de Verenigde Staten. De C20-versie van Guardian in combinatie met Safeguard is in 1990 succesvol getoetst door het GISA. De toetsing heeft plaatsgevonden op het niveau van de IT-standaard kwaliteitsklasse Q3 voor de functionaliteitsklassen F2 en F7 (F2/Q3 is vergelijkbaar met C2 van het Orange book, F7 heeft betrekking op beschikbaarheid en kent geen Orange book-equivalent).
Dezelfde versie van Guardian is aangeboden voor een C2-evaluatie bij het Amerikaanse National Computer Security Center (NCSC).

BEVEILIGING MET BEHULP VAN GUARDIAN/SAFEGUARD

In deze paragraaf wordt in hoofdlijnen aangegeven hoe een Tandem-systeem met behulp van Safeguard/Guardian kan worden beveiligd. Achtereenvolgens wordt ingegaan op de installatie van Safeguard, instellen van systeemparameters, beveiligen van objecten, toegangscontrole, geprivilegieerde programma's en auditing.

Installatie

Tandem-systeem-software wordt geleverd via een System Image Tape (SIT). Deze wordt gebruikt voor de initiële cold load. Safeguard is geen onderdeel van de SIT (maar wordt geleverd via een Site Update Tape). Om er zeker van te zijn dat Safeguard altijd aanwezig is op het systeem verdient het aanbeveling Safeguard als onderdeel van het operating system te installeren. Hiertoe dient Safeguard te worden gespecificeerd als een system process tijdens de systeemgeneratiefase van de installatie.
Safeguard dient daarna onder beheer van de security administrator te worden gebracht.

Instellingen Safeguard

De volgende stap na de installatie is het activeren van een aantal systeemparameters binnen Safeguard, en het wijzigen van de default-instellingen van Safeguard. Het betreft hierbij system wide-parameters (configuratieparameters genoemd).

Instellingen als het gebruik van een password, gebruik van password-encryptie, periodiek wijzigen van een password, het tegengaan van hergebruik van een password en de minimumlengte van het password dienen te worden geactiveerd. Verder zal moeten worden aangegeven welke ACL's van de verschillende soorten objecten door Safeguard moeten worden gebruikt.
Een mogelijke optie is de "clearonpurge-diskfile". Deze optie biedt de mogelijkheid de inhoud van een verwijderd bestand met nullen te overschrijven. Het gebruik van deze optie heeft echter een nadelige invloed op de performance. Deze optie kan beter op bestandsniveau voor bestanden met vertrouwelijke gegevens worden ingesteld.
De audit-mogelijkheden die Safeguard biedt dienen te worden ingesteld.

Een Tandem-systeem wordt standaard geleverd met een tweetal gebruikers die vergaande bevoegdheden hebben, de Super.Super en de Null.Null.
De Super.Super heeft onbeperkte bevoegdheden op het systeem. De Super.Super kan het best worden bevroren (optie FREEZE in Safeguard) en als ge-

bruik noodzakelijk is, worden ontdooid (optie THAW). Voor dit ontdooien dienen procedures te worden ontworpen. Daarnaast biedt Safeguard de mogelijkheid de toegang van Super.Super tot objecten uit te sluiten (deny-parameter). Dit dient echter per object te worden aangegeven.
De Null.Null wordt geleverd zonder password en wordt alleen voor testdoeleinden gebruikt. Hij is niet nodig op een produktiesysteem en kan daarom eveneens het best worden bevroren. Bevriezen heeft de voorkeur boven verwijderen, om te voorkomen dat de user-id weer wordt opgevoerd.

Beveiliging van objecten

De ACL is het basismechanisme om objecten met behulp van Safeguard te beveiligen. Via een ACL wordt aangegeven welke gebruikers toegang mogen hebben tot een object en welke bevoegdheden deze gebruikers met betrekking tot dat object hebben.

Safeguard beveiligt objecten niet automatisch. Dit dient door de security administrator te gebeuren. De eerste stap bij het beveiligen van objecten is de beveiliging van objecttypen. Objecttypen betreffen de beveiligingsgegevens met betrekking tot een object (meta-gegevens).
Een autorisatie-record voor een objecttype kent twee toegangsbevoegdheden: creëren en eigenaarschap.
Het toekennen van objecttypebevoegdheden dient door de security administrator te worden gedaan.

Hierna kan de beveiliging worden ingesteld van de objecten zoals:
- kritische bestanden; systeembestanden uitgeleverd door Tandem, bestanden voor utilities en applicaties, databestanden en TACL-macro's;
- kritische processen;
- volumes en subvolumes; (sub)volumebeveiliging brengt minder onderhoud met zich mee dan bestandsbeveiliging. Subvolumebeveiliging zorgt er tevens voor dat elk bestand dat op dat subvolume wordt gecreëerd, beveiligd is. Het biedt echter minder flexibiliteit;
- terminals.

Toegangscontrole

Safeguard biedt de mogelijkheid de toegang tot het systeem te controleren. Hiertoe wordt voor iedere gebruiker een authenticatie-record aangemaakt. Dit record bevat de user-id, logon-naam, wachtwoord en een aantal security-attributen welke voor die gebruiker zijn gedefinieerd.
Bij installatie zijn alleen de Super.Super en de Null.Null als gebruikers op het systeem aanwezig. De security administrator dient de overige gebruikers daarna aan het systeem bekend te maken en de benodigde beveiligingsparameters binnen het authenticatie-record te activeren.
Bij het opzetten van een beveiligingsstructuur is de eerste stap het definiëren van gebruikersgroepen en de tweede stap is het toevoegen van gebruikers aan deze groepen.

Het verdient aanbeveling de default-beveiliging voor gebruikersbestanden in te stellen op "OOOO", zodat alleen de eigenaar bevoegdheden met betrekking tot het bestand heeft.
Binnen Safeguard zijn met betrekking tot bovengenoemde beveiliging twee niveaus te onderkennen: algemene Safeguard-instellingen, geldend voor elke gebruiker en specifieke instellingen voor een individuele gebruiker.

Safeguard beveiligt objecten niet automatisch. Een hiervoor in de organisatie verantwoordelijk gestelde functionaris dient de beveiliging van (alle) objecten expliciet te implementeren.

Safeguard kent nog een aantal tekortkomingen met betrekking tot de beheersing van de toegang tot het systeem. Het betreft onder andere:
- het password wordt op het scherm vertoond bij het intypen;
- geen automatische logoff na een bepaalde tijdsperiode;
- de Super-id kan remote aanloggen.

Via afzonderlijke programma's (TACL's) dient in bovengenoemde tekortkomingen te worden voorzien. Deze programma's zijn onder andere ontwikkeld door de ITUG (International Tandem Users Group).

Prog-id en licensed programma's

Binnen Guardian wordt een tweetal faciliteiten geboden die een risico inhouden met betrekking tot de beveiliging. Het betreft het "licensed" en "prog-id" maken van programma's.
Een licensed programma krijgt de mogelijkheid privileged instructies uit te voeren. Privileged instructies zijn de instructies die het besturingssysteem gebruikt voor de communicatie met de hardware. Door een programma als "licensed" te definiëren, ontvangt het de bevoegdheden van het besturingssysteem. Een licensed programma kan derhalve data binnen het gehele systeem modificeren. Als algemene regel kan worden gehanteerd: geen enkel gebruikersprogramma licensed maken.
Het licensed maken van een gebruikersprogramma is een optie die alleen met behulp van de Super-id kan worden uitgevoerd.
Prog-id programma's zijn programma's die draaien onder de bevoegdheden van de programma-eigenaar en niet onder de bevoegdheden van degene die het programma uitvoert. Het programma verkrijgt dus ook de toegang tot de objecten waar de programma-eigenaar toegang toe heeft. In de normale situatie wordt alleen gewerkt volgens de bevoegdheden van de gebruiker.
Het ondoordacht ontwikkelen van prog-id programma's kan grote leemtes in de beveiliging veroorzaken.

Prog-id programma's kunnen worden gebruikt om gebruikers te dwingen uitsluitend via bepaalde programma's gegevens te benaderen.

Instellen auditing-parameters

Om van de audit-mogelijkheden van Safeguard gebruik te kunnen maken, kan worden aangegeven welke "gebeurtenissen" moeten worden vastgelegd. Daartoe dient in Safeguard de audit-service te worden geconfigureerd. De audit-service betreft het bestandsbeheer en de beveiliging van de Safeguard audit-records.
De security administrator dient de bestanden te specificeren die moeten worden gebruikt om de audit-records op te slaan. Tevens dient hij aan te geven welke recovery-acties moeten worden uitgevoerd indien de auditing wordt onderbroken.
Naast de security administrator kan de systeem-operator audit-service-commando's uitvoeren. Hij kan echter geen wijzigingen in de configuratie aanbrengen.
Alle commando's die door de security administrator dan wel de systeem-operator worden verricht worden gelogd, ongeacht de instellingen.

Een gemis binnen Safeguard is het ontbreken van rapportages aan de hand van audit-bestanden. Programmatuur hiervoor dient zelf te worden ontwikkeld. Wel kan gebruik worden gemaakt van door derden geleverde pakketten, zoals Auditview.
Als "gebeurtenissen" worden altijd opgeslagen: audit-service-wijzigingen en de wijzigingen in de Safeguard-configuratie. De overige "gebeurtenissen" zijn optioneel. Onderscheiden worden: user-authenticatiegebeurtenissen (logon, wijzigingen in het authenticatie-record), object-autorisatiegebeurtenissen (toegang tot objects, wijzigingen in het autorisatie-record van het object) en objecttype-autorisatiegebeurtenissen (wijziging beveiligingsparameters). Daarnaast wordt onderscheid gemaakt tussen "global auditing" (via configuratieparameters, system wide) en "individual auditing"-parameters (via user-authenticatie-record of het object-autorisatie-record).
De gespecificeerde configuratieparameters zijn aanvullend op de individual parameters. De individual parameters zijn leidend.

AUDIT VAN SAFEGUARD IN COMBINATIE MET GUARDIAN

Gelet op het belang van Safeguard/Guardian voor de beveiliging van de geautomatiseerde gegevensverwerking, bestaat bij veel organisaties behoefte de implementatie en het beheer ervan te laten beoordelen door een onafhankelijke of althans onpartijdige deskundige. In verband met de benodigde deskundigheid zal deze beoordeling door een technisch geschoolde EDP-auditor dienen plaats te vinden.
De audit van Safeguard in combinatie met Guardian kan in een aantal stappen worden uitgevoerd:

- beoordelen organisatie en procedures;
- toegangsbeveiliging op systeemniveau;
- toegangsbeveiliging op applicatieniveau.

Onderstaand wordt in hoofdlijnen aangegeven hoe een audit volgens bovengenoemde stappen eruit kan zien.

Beoordelen organisatie en procedures

Dit onderdeel van de audit richt zich met name op de plaats en functie van de security administrator (voldoende onafhankelijk) en zijn rol in de beheersing van het Tandem-systeem. Zo zullen onder andere procedures aanwezig dienen te zijn voor het verkrijgen van toegangsautorisatie en storingsprocedures (ontdooien van de Super.Super).
Voorts moet aandacht worden besteed aan de wijze waarop het gebruik van verleende bevoegdheden wordt gecontroleerd (met behulp van auditrapportages).
In het voorgaande werd in dit verband reeds gerefereerd aan het pakket Auditview. Auditview is een pakket waarmee op eenvoudige wijze rapportages uit de audit-bestanden van Safeguard kunnen worden verkregen.
De volgende audit-rapporten zijn hierbij onder andere mogelijk:

- overzicht mislukte aanlogpogingen;
- overzicht gelukte en mislukte aanlogpogingen te specificeren naar gebruiker (user-id);
- overzicht van alle wijzigingen op Safeguard;
- overzicht van belangrijke bestanden die zijn benaderd en door wie.

Bijzondere aandachtspunten in dit kader zijn de afwikkeling van security violations en de bewaartermijnen van de audit-bestanden.
Gezien het karakter van Tandem-systemen (online/realtime) kan ook worden gedacht aan het direct monitoren van security violations. Faciliteiten zijn beschikbaar waarbij Safeguard-boodschappen worden uitgefilterd en doorgeleid naar een daarvoor gedefinieerde terminal.

Toegangsbeveiliging op systeemniveau

De audit zal zich richten op de implementatie van de Guardian/Safeguard-beveiliging. Uitgangspunt bij deze beoordeling vormt het "need to know"-principe, dat wil zeggen dat de toegekende bevoegdheden zodanig zijn dat een gebruiker niet meer bevoegdheden ter beschikking heeft dan uit hoofde van zijn functie nodig is.
Bij deze beoordeling dienen onder andere de volgende aspecten aan bod te komen:

- Beoordelen van de Guardian/Safeguard-configuratie. Vaststellen dat de basisinstellingen voldoen aan hetgeen in de paragraaf Beveiliging met behulp van Guardian/Safeguard is beschreven en welke de redenen zijn als hiervan wordt afgeweken. Tevens dient te worden vastgesteld dat de system wide-instellingen inzake de systeemgebruikers niet zijn gewijzigd. Dit betekent dat de EDP-auditor van alle systeemgebruikers het authenticatie-record dient te beoordelen.

– Beoordelen van alle gebruikersauthenticatie-records. Hierbij onder andere letten op de default-bestandsbeveiliging en het bevroren zijn van de gebruikers Super.Super en Null.Null. Vaststellen dat alleen daartoe geautoriseerde gebruikers (operators, systeembeheerders) toegang op systeemniveau (TACL) krijgen.

– De toereikendheid van de instellingen van de TACL-configuratieparameters (automatisch afloggen, geen wachtwoord op het scherm, etc.).

– Vaststellen welke programma's met de optie licensed en welke met de optie prog-id zijn en waarom. Het beoordelen van de documentatie en de goedkeuring van deze programma's. Het beoordelen van de toegang tot deze programma's. Deze programma's dienen tot het noodzakelijk gebruik beperkt te zijn.

– Beoordelen van de objectbeveiliging. Volume en subvolume beveiliging en bestandsbeveiliging onder Safeguard (via de ACL's) en de bestandsbeveiliging onder Guardian voor zover niet met Safeguard beveiligd.

– Afscherming van de systeembestanden.

– Vaststellen dat de objectcodebestanden voor alle programma's en utilities een "execute"-bevoegdheid hebben voor de gebruiker die het programma moet uitvoeren (applicatiegebruiker) en "read"- en "write"-bevoegdheden voor degene die de code moet kunnen onderhouden (systeembeheer).

– Vaststellen dat de databestanden alleen benaderbaar zijn voor de gebruikers-id waaronder de applicatie draait.

– Toegang van de zogenaamde remote users beoordelen.

– Vaststellen welke software er wordt gebruikt naast Guardian en Safeguard ter ondersteuning van de beveiliging (bijvoorbeeld Auditview) en de installatie en instellingen van deze software beoordelen.

Voor ieder van bovengenoemde stappen is het mogelijk de nodige output uit het systeem te verkrijgen. Dit betreft dan zowel overzichten via Safeguard en Auditview als overzichten vanuit Guardian. Het verkrijgen van laatstgenoemde overzichten dient via de Super-id plaats te vinden.

Toegangsbeveiliging op applicatieniveau

Zoals in het voorgaande reeds aangegeven, is de Guardian/Safeguard-beveiliging met name gericht op de toegang tot het Tandem-systeem en de toegang tot bestanden. De toegangsbeveiliging op applicatieniveau, onder andere om functiescheidingen te realiseren, dient met name in de applicatie zelf te worden geregeld. Ter ondersteuning kan gebruik worden gemaakt van het pakket Onguard dat een vorm van menu-beveiliging ondersteunt.
Als onderdeel van de beoordeling van de toegangsbeveiliging op applicatieniveau dient de Pathway-configuratie te worden beoordeeld. Zo zullen de instellingen in de "Pathway control-file" moeten worden beoordeeld. Hierin is onder andere de relatie aangegeven tussen de terminalpoort en de applicatie. Ook wordt aangegeven welk initieel scherm een eindgebruiker krijgt gepresenteerd. Tevens wordt aangegeven welke bestanden en randapparatuur door de applicatie worden gebruikt. De EDP-auditor dient te beoordelen of het hier door de gebruiker geaccepteerde applicaties betreft.

De toegang tot de applicatiebestanden en programmatuur dient op systeemniveau voldoende te zijn afgeschermd. De EDP-auditor dient dit te beoordelen aan de hand van de Safeguard-ACL's, de Guardian-bestandsbeveiliging en de wijzigingsprocedures die hiervoor gelden.
Met behulp van Pathway-output kan worden vastgesteld wie de eigenaar van de Pathway-omgeving is; dit dient de eigenaar van de applicatie te zijn. De EDP-auditor dient vast te stellen dat de eindgebruikers geen TACL-commando's kunnen uitvoeren ("exclusive on" in de Pathway-instellingen).

Bovenstaande activiteiten die de EDP-auditor moet uitvoeren bij de audit van de toegangsbeveiliging op een Tandem-systeem geven aan dat een dergelijke audit een gecompliceerde zaak is. Bij de beveiliging speelt een groot aantal systeem-software-componenten een rol, die alle in het totale toegangspad een plaats innemen. De EDP-auditor zal zich bewust dienen te zijn van de samenhang tussen de componenten en risico's bij het onjuist gebruik van bepaalde componenten.

NAWOORD

Algemeen kan worden gesteld dat Guardian in combinatie met Safeguard voldoende voorzieningen biedt om een adequate toegangsbeveiliging te realiseren.
Dit blijkt onder andere uit de succesvolle toetsing door het GISA.
Het implementeren en onderhouden van de toegangsbeveiliging met behulp van Guardian/Safeguard is bewerkelijk. Doordat verschillende systeem-software-componenten een rol spelen in de totale toegangsbeveiliging kan het geheel ondoorzichtig worden. Het optimaal benutten van de geboden faciliteiten staat of valt met een goede organisatie.
De EDP-auditor dient zich bij zijn audit bewust te zijn van de afhankelijkheden tussen de verschillende componenten en de relatie met de organisatie om tot een adequaat oordeel te komen.
Een gemis van Guardian/Safeguard betreft het ontbreken van functionaliteit met betrekking tot het produceren van audit-rapporten. Bij een volledig toegangsbeveiligingspakket dienen faciliteiten met betrekking tot vastlegging en signalering van overtredingen betreffende ongeautoriseerde benadering van computer-resources aanwezig te zijn.

K.E.A. van Dijk
Is werkzaam als EDP-auditor bij de BankGiroCentrale. In 1991 heeft hij zijn AMBI-opleiding voltooid. Zijn auditervaring ligt op het gebied van automatiseringsorganisaties en informatiesystemen, besturingssystemen en beveiligingspakketten (Tandem).

M.M.J.A. van Dijk RA/CISA
Is sinds 1987 werkzaam bij de Accountantsdienst, afdeling EDP Audit van de Rabobank Nederland. Hij heeft zijn post-doctorale studie EDP Auditing voltooid aan de VU te Amsterdam. Hij heeft meerdere EDP-audit-onderzoeken verricht in de Tandem-omgeving bij de Rabobank.

RACF als access control software voor MVS-omgevingen

Ing. G.H.M. Meijer

Resource Access Control Facility is een hulpmiddel voor logische toegangscontrole voor VM- en MVS-omgevingen.
De auteur, die geldt als bij uitstek deskundig op dit gebied, geeft een beschrijving van de functionaliteit van dit pakket, alsmede van de specifieke elementen die van invloed zijn op de effectiviteit ervan.
Tevens gaat hij in op de beoordeling van de implementatie van dit pakket.

INLEIDING

Het besturingssysteem Multiple Virtual Storage (MVS) van IBM heeft slechts zeer beperkte mogelijkheden tot toegangscontrole van gebruikers en beveiliging van resources. Om deze elementen op een adequaat niveau te brengen is een aanvullend programmaprodukt nodig. In de praktijk veel toegepaste programmaprodukten voor logische toegangsbeveiliging in de MVS-omgeving zijn CA-ACF2 en CA-Top Secret van Computer Associates en Resource Access Control Facility (RACF) van IBM.

Dit artikel vormt een beschrijving van het pakket RACF en aspecten die een rol spelen bij de beoordeling ervan. De beschrijving van de functionaliteit en technische implementatie is gebaseerd op de meest recente versie van RACF: versie 1, release 9. Hierbij wordt uitsluitend ingegaan op RACF voor MVS. Het pakket is ook geschikt voor de beveiliging van een VM-omgeving. Deze omgeving blijft in dit artikel buiten beschouwing.

Allereerst zullen in dit artikel de belangrijkste functies van het pakket alsmede de technische implementatie worden beschreven. Vervolgens wordt ingegaan op de beheersing van de RACF-database en op de audit-aspecten. Hierbij zal ook aandacht worden besteed aan de hulpmiddelen ten behoeve van de uitvoering van een audit van RACF.

Als in dit artikel wordt geschreven over een systeem dan wordt daarmee bedoeld één MVS-omgeving met al haar subsystemen en resources. Gevolgen voor de implementatie van RACF door het toepassen van communicatie tussen meerdere systemen zullen in dit artikel buiten beschouwing blijven.

FUNCTIES VAN RACF

De belangrijkste functies die door RACF in het kader van de logische toegangsbeveiliging worden geboden, zijn het identificeren, authenticeren en autoriseren van gebruikers. Daarnaast biedt RACF een aantal faciliteiten voor het beheer van de RACF-database en het registreren van gebeurtenissen in het systeem.

Identificatie en authenticatie

Elke gebruiker heeft in RACF een unieke user-id en is in de RACF-database gedefinieerd met behulp van een "user profile". In deze user profile is een algemene beschrijving opgenomen van de user-id. Deze user-id kan de representatie zijn van een eindgebruiker (individu), maar ook van een started task of een batch-job. Tijdens het aanloggen dient de gebruiker het bij de user-id behorende password op te geven. Met behulp van dit mechanisme wordt de authenticiteit van de gebruiker bepaald.

Gebruikers kunnen in groepen worden ingedeeld. Hiertoe dienen in RACF eerst groepen te worden gedefinieerd, met behulp van een "group profile". Een gebruiker kan lid zijn van meerdere groepen. Hij dient echter lid te zijn van minimaal één groep: de "default group". Deze default group is aangegeven in de user profile van de gebruiker. De relatie van de gebruiker met eventuele andere groepen wordt gedefinieerd met behulp van "connect profiles".

De groepsstructuur is met name van belang voor het autorisatiemechanisme van RACF en het beheer van de RACF-database. Tijdens het aanloggen dient door de gebruiker te worden opgegeven tot welke groep hij (op dat moment) behoort. Dit moet een groep zijn waar hij lid van is, dus óf zijn default group, óf een groep waarmee hij via een connect profile is geassocieerd.

Autorisatie

Nadat van een gebruiker de identiteit en de authenticiteit zijn vastgesteld, kan deze worden geautoriseerd tot het gebruiken van bepaalde resources.
Voorbeelden van resources zijn:
- subsystemen;
- applicaties;
- transacties;
- programma's;
- datasets;
- terminals.

RACF maakt bij resources onderscheid tussen datasets (bestanden) en de overige resources, general resources genoemd. Datasets worden gedefinieerd in "dataset profiles", general resources in "general resource profiles". Als in dit artikel verder over een resource profile wordt gesproken, dan wordt daarmee zowel de dataset profile als de general resource profile bedoeld.

Met behulp van een access list in de resource profile wordt aangegeven wie toegang heeft tot de desbetreffende resource. In de access list kunnen zowel group-ids als user-ids zijn opgenomen. Als in de access list een group-id is opgenomen, hebben alle members van de groep de desbetreffende autorisatie.
De autorisatie in de access list kan aan bepaalde condities worden gekoppeld. In dat geval is er sprake van een conditional access list. Een voorbeeld van zo'n conditie is de tijdsspanne (bijvoorbeeld alleen tijdens kantooruren) waarbinnen de autorisatie van toepassing is.

Naast autorisatie met behulp van de access list in de resource profiles, kent RACF ook autorisatie met behulp van security categories en security levels. Op deze faciliteiten, waarvan in de praktijk weinig gebruik wordt gemaakt, zal in dit artikel niet inhoudelijk worden ingegaan.

TECHNISCHE IMPLEMENTATIE

Deze paragraaf gaat in op de technische implementatie van RACF. Welke essentiële elementen dienen op welke wijze te worden geïmplementeerd alvorens de access control software operationeel kan worden?

Profiles

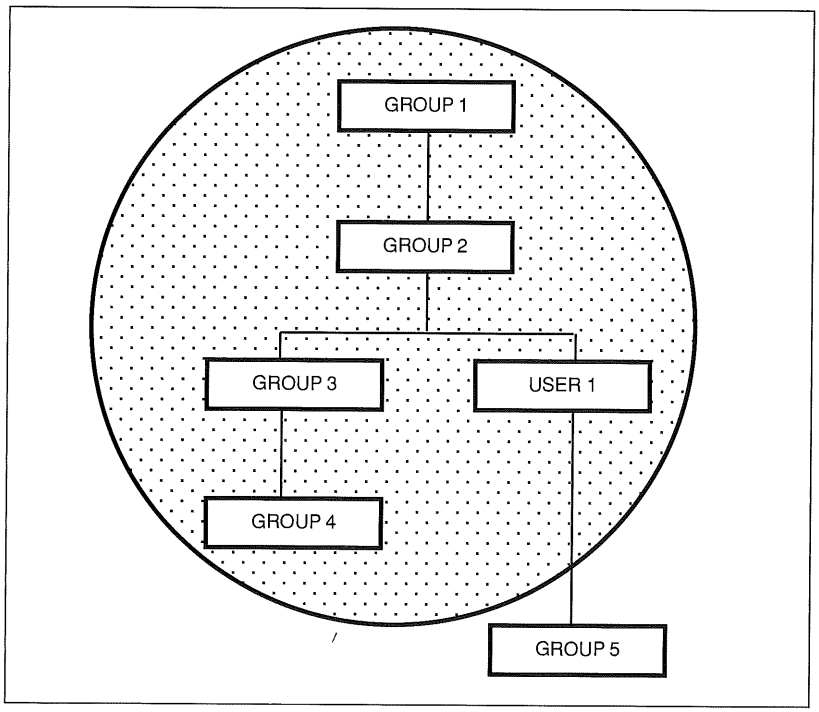
In het voorgaande is beschreven dat RACF vijf typen profiles kent: user, group, connect, dataset en general resource profiles. Onderstaand wordt kort ingegaan op de inhoud van de verschillende soorten profiles.

User profile
Een RACF user profile dient ter definiëring van een (mogelijk fictieve) gebruiker in een MVS-omgeving en kent drie segmenten: een RACF-, een TSO- en een DFP-segment, waarvan de laatste twee optioneel zijn.

In het RACF-segment staat de algemene definitie van de gebruiker zoals de user-id, de naam van de gebruiker, de owner van de user-id (dit kan een group-id of een andere user-id zijn), de default group en de autorisatie van de gebruiker binnen die default group. Ook staan in het RACF-segment de eventuele speciale autorisaties ("attributes") die aan de user zijn toegekend. Deze speciale autorisaties kunnen system wide gelden of alleen binnen een groep. Dit betekent dat in het eerste geval de gebruiker de autorisatie die hij vanwege het attribute ontvangt over het hele systeem kan gebruiken, in het tweede geval kan dat alleen binnen de "scope" van de desbetreffende groep. System wide attributes worden toegekend via de user profile. Group attributes worden toegekend via de connect profile waarmee de gebruiker met de groep is geassocieerd.

Bepalend voor de reikwijdte van group attributes

is de scope van de groep. Alle resources die eigendom zijn van de groep respectievelijk subgroep of subsubgroep etc., vallen binnen de scope van de groep. Indien echter de user-id eigenaar is van een onderliggende groep of user-id, vallen de resources die eigendom zijn van die group of user-id buiten de scope. Volgens het voorbeeld van figuur 1 vallen de resources die eigendom zijn van user 1 nog wel binnen de scope van group 1, maar de resources die eigendom zijn van group 5 vallen erbuiten.



Figuur 1. De scope van een groep.

Onderstaand volgen de belangrijkste user-attributes.

CLAUTH. Dit staat voor CLass AUTHority. Het CLAUTH-attribute wordt per resource-type toegekend aan een gebruiker, hetgeen inhoudt dat de gebruiker profiles voor de desbetreffende resource class kan definiëren. Dit attribute kan alleen op system wide-niveau worden toegekend.

SPECIAL. Een gebruiker met het SPECIAL-attribute kan alle RACF-commando's uitvoeren (afgezien van bepaalde opties binnen commando's die te maken hebben met het genereren van audit-informatie), en heeft volledige controle over alle RACF-profiles. Het SPECIAL-attribute kan worden toegekend op systeem- of groepsniveau. Op groepsniveau betekent dit dat de gebruiker volledige controle heeft over de profiles binnen de scope van de groep. Er is echter één restrictie: deze gebruiker kan niet zonder meer nieuwe user profiles definiëren (zie verder de paragraaf Het beheer van de RACF-database).

AUDITOR. Een gebruiker met het AUDITOR-attribute heeft de bevoegdheid om audit-opties in te stellen. Deze opties kunnen system wide gelden maar ook voor specifieke resources of gebruikers; zij leiden ertoe dat audit-informatie wordt geregistreerd. Ook het AUDITOR-attribute kan zowel op systeem- als op groepsniveau worden toegekend.

OPERATIONS. Een gebruiker met het OPERATIONS-attribute heeft volledige toegang tot alle door RACF beschermde resources van de classes datasets, disk volumes en tape volumes. Deze vergaande bevoegdheid gaat echter niet op indien de desbetreffende gebruiker of de groep waarvan hij deel uitmaakt, is opgenomen in de access list van de profile, of indien de autorisatieregels volgens de principes van security classification of security label checking de toegang verhinderen. Het OPERATIONS-attribute kan zowel op systeem- als op groepsniveau worden toegekend.

REVOKE. Dit attribute geeft aan dat de desbetreffende user-id op non-actief is gesteld. Dit kan zowel op systeem- als op groepsniveau. REVOKE op groepsniveau houdt in dat de gebruiker niet als lid van die groep kan opereren.

Zoals gesteld zijn het TSO- en het DFP-segment in de user profile optioneel. Het TSO-segment dient voor de definitie van TSO-gebruikers en wordt toegepast indien geen gebruik wordt gemaakt van de SYS1.UADS dataset.
In het DFP-segment (Data Facility Product) van de user profile worden data en storage management-karakteristieken van de door de gebruiker aangemaakte datasets vastgelegd.

Group profile
Een group profile in RACF bevat een RACF-segment en een optioneel DFP-segment. Het DFP-segment is vergelijkbaar met het DFP-segment in de user profile. In het RACF-segment van de group profile is onder meer opgenomen de group name (dit is de group-id), de owner van het group profile en de superior group.

Connect profile
De connect profile wordt aangemaakt met behulp van het CONNECT-commando. Hiermee worden user-ids lid gemaakt van een groep (anders dan van hun default group). In de connect profile staat onder meer aangegeven welke autorisaties de user-id binnen de groep heeft. Deze autorisaties zijn:

USE. De user-id kan als lid van de groep opereren en kan resources benaderen waartoe de groep bevoegd is.

CREATE. Deze omvat tevens de USE-autorisatie. Verder kan de user-id group datasets aanmaken en dataset profiles van de desbetreffende groep wijzigen.

CONNECT. Deze omvat tevens de USE- en de CREATE-autorisaties. Bovendien kan de user-id reeds gedefinieerde andere user-ids lid maken van de desbetreffende groep.

JOIN. Deze omvat tevens de USE-, de CREATE- en de CONNECT-autorisaties. Daarnaast kan de user-id

nieuwe gebruikers definiëren en group attributes toekennen aan de gebruikers binnen de groep. Het definiëren van nieuwe gebruikers kan echter niet zonder dat de user-id tevens het CLAUTH-attribute voor de user class heeft (dit staat in zijn user profile).

Een gebruiker kan dus op groepsniveau een aantal attributen (bijvoorbeeld REVOKE, SPECIAL, OPERATIONS en AUDIT) en een aantal autorisaties (USE, CREATE, CONNECT en JOIN) hebben meegekregen.

Dataset en general resource profiles
RACF kent twee soorten datasets: user dataset en group dataset. Een user dataset is een dataset waarvan de high level qualifier een RACF user-id is; een group dataset is een dataset waarvan de high level qualifier een RACF group-id is.

De bevoegdheidscontrole door RACF ten aanzien van toegang tot datasets en general resources geschiedt zoals eerder aangegeven op basis van profiles die voor deze datasets zijn gedefinieerd. Hierbij kan onderscheid worden gemaakt tussen discrete profiles, die gelden voor afzonderlijke datasets en generic profiles, die in beginsel betrekking hebben op een groep van datasets. Het is echter mogelijk generic profiles dusdanig op maat te snijden dat zij toch betrekking hebben op één specifieke dataset. Er is dan sprake van een "fully qualified generic profile". De dataset en general resource profiles bevatten onder meer de volgende informatie:

- Owner. Hiermee wordt de eigenaar van de profile aangegeven. Deze kan een group-id of een user-id zijn. De eigenaar kan de inhoud van de profiles wijzigen en kan de profile verwijderen. Indien een groep eigenaar is van de profile betekent dit niet dat automatisch alle leden van de groep de profiles kunnen wijzigen. Hiertoe hebben zij het CREATE-attribute binnen de groep nodig.

- Access list. Hierin staan de bevoegdheden van user-ids en/of group-ids ten opzichte van de desbetreffende resource.

- Universal access. Dit geeft de bevoegdheid aan die de gebruikers hebben ten opzichte van de resource indien zowel de gebruiker als de groep waartoe hij op dat moment behoort niet is opgenomen in de access list van de resource profile (een soort minimale toegang voor alle gebruikers).

- Audit options. Deze opties stellen de eigenaar en de gebruikers met het AUDIT-attribute in staat bepaalde logging-informatie met betrekking tot het gebruik van de resource te laten genereren.

In de access list van de resource profiles kunnen de volgende bevoegdheden worden opgenomen:

- NONE. De gebruiker heeft geen enkele toegang tot de data. Het toekennen van deze "bevoegdheid" aan een gebruiker is bijvoorbeeld zinvol om gebruikers met het OPERATIONS-attribute toegang tot de resource te ontzeggen (zij hebben normaal gesproken immers toegang tot alle datasets alsmede disk en tape volumes).

- EXECUTE. De gebruiker heeft slechts toegang voor het uitvoeren van programma's.

- READ. De gebruiker mag de data lezen, kopiëren en programma's laden.

- UPDATE. De gebruiker mag de data wijzigen.

- CONTROL. Deze bevoegdheid is in de meeste gevallen gelijk aan UPDATE.

- ALTER. De gebruiker mag de dataset weggooien. Voor discrete profiles levert dit de gebruiker ook volledige controle over de profile op.

Systeemparameters voor RACF

De werking van RACF wordt in belangrijke mate bepaald door een aantal opties of parameters (stuurgegevens) op system wide-niveau, die in het algemeen alleen kunnen worden gewijzigd door óf gebruikers met het system-SPECIAL-attribute óf gebruikers met het system-AUDIT-attribute. Het wijzigen van deze parameters geschiedt met behulp van het SETROPTS-commando (set RACF options), waaraan bepaalde parameters kunnen worden meegegeven. Onderstaand worden de belangrijkste parameters beschreven:

- PASSWORD. Hiermee worden regels met betrekking tot het gebruik van passwords vastgelegd. Het betreft hier onder meer de lengte, samenstelling en geldigheidsduur van de passwords.

- INACTIVE. Met behulp van deze parameter wordt het aantal dagen gespecificeerd dat een gebruiker zijn user-id ongebruikt mag laten zonder dat deze user-id automatisch op non-actief wordt gesteld.

- GRPLIST/NOGRPLIST. Bij NOGRPLIST worden tijdens de autorisatiecontrole door RACF alleen de bevoegdheden van de groep geëvalueerd waarvan de user-id op dat moment deel uitmaakt. Dit kan de default group van de gebruiker zijn, of een groep waarmee hij via een connect profile is geassocieerd. Bij GRPLIST worden de bevoegdheden van alle groepen waarvan de gebruiker deel uitmaakt geëvalueerd.

- RVARYPW. Met behulp van deze parameter worden de passwords voor het activeren/deactiveren van RACF respectievelijk het switchen tussen de primary en secondary RACF-database gedefinieerd. De operator heeft deze passwords nodig om de genoemde functies te kunnen uitvoeren.

- CLASSACT. Met behulp van deze parameter wordt de beveiliging van de general resource classes geactiveerd. Iedere resource class dient individueel te worden geactiveerd.

- GLOBAL. Hiermee wordt de global access checking geactiveerd (zie verder de paragraaf Overige belangrijke faciliteiten van RACF).

worden uitgevoerd, hetgeen bijvoorbeeld resulteert in een supervisor call.

Via de MVS router exit en de RACF router tables kan dus invloed worden uitgeoefend op het beveiligingsmechanisme van RACF.
Reeds is gesteld dat resource managers van MVS het beveiligingsmechanisme via SAF aanroepen. Het is echter de vraag of programmaprodukten van andere leveranciers, maar ook programmaprodukten van IBM, deze "standaard" wel altijd volgen. Dit kan een inbreuk betekenen op de effectiviteit van de logische toegangsbeveiliging.

OVERIGE BELANGRIJKE FACILITEITEN VAN RACF

RACF biedt een aantal faciliteiten om het produkt aan te passen aan de specifieke omstandigheden van een bepaalde installatie en ten behoeve van een vereenvoudigde toegang tot gemeenschappelijk benaderbare resources. Deze paragraaf beschrijft de belangrijkste van deze faciliteiten.

Naming Convention Table

RACF biedt de mogelijkheid een Naming Convention Table (NCT) te definiëren. Deze tabel stelt een installatie in staat namen van datasets ten behoeve van autorisatie-evaluatie (virtueel) te converteren naar andere namen die dan door RACF voor autorisatie-evaluatie worden gebruikt. Hierdoor kan de RACF-database worden ingericht volgens een door de organisatie ingestelde naamgevingsstandaard, terwijl de werkelijke naamgeving van de datasets hier (nog) niet aan voldoet. Deze optie wordt met name gebruikt in overgangssituaties of in geval van door programmatuur afgedwongen dataset-naamgeving die niet past in de standaard van de organisatie.

De bewaking van het gebruik van de Naming Convention Tabel is van groot belang. In de praktijk wordt hieraan vaak onvoldoende aandacht besteed; ook bij audits wordt deze tabel nogal eens gemist.

De NCT is een load-module die in de MVS-systeemdataset SYS1.LPALIB dient te worden geplaatst. De tabel wordt gedefinieerd en onderhouden met behulp van de RACF-macro ICHNCONV en kan tot maximaal vierhonderd entries bevatten. Per tabelentry dient te worden gedefinieerd:

- define-macro; betekent het begin van een nieuwe naming convention entry en de start van het proces;
- select-macro; beschrijft de condities op basis waarvan de in deze entry beschreven conversie dient te worden uitgevoerd. Als de situatie niet aan de hierin beschreven condities voldoet, wordt de action-macro niet uitgevoerd en wordt de volgende entry in de tabel verwerkt. Indien geen select-macro is gespecificeerd, zal RACF onvoorwaardelijk de action-macro uitvoeren;
- action-macro; legt de feitelijke conversie-activiteiten vast;
- end-macro; stopt het proces voor deze entry.

Het moge duidelijk zijn dat het gebruik en de inhoud van de NCT zeer goed moeten worden gedocumenteerd. Immers, door alleen af te gaan op de inhoud van de profiles aan de ene kant en de naamgeving van de datasets aan de andere kant kan een onjuist beeld over de feitelijke beveiliging ontstaan.

Door het technisch karakter van deze faciliteit van RACF, te weten een macro en een exit, schuilt in het gebruik nog een ander risico. Het beheer van deze tabel dient, net als alle andere beveiligingsdefinities (de gehele RACF-database) te worden toebedeeld aan een beveiligingsfunctionaris. In de praktijk blijkt echter dat de voor het onderhoud van de NCT benodigde kennis meer op het terrein van functies als systeemprogrammering ligt dan op het terrein van de beveiligingsfunctionaris. De bewaking van het gebruik van de NCT is voor de effectiviteit van de beveiligingsdefinities van groot belang. In de praktijk blijkt vaak dat aan het beheer van deze tabel onvoldoende aandacht is besteed; ook bij audits van RACF wordt de tabel nogal eens gemist.

Global Access Checking

Bij het evalueren van een autorisatieverzoek wordt door RACF een algoritme toegepast, waarbij de profiles in de volgorde van meest specifiek naar meest generiek worden doorzocht. In beginsel dienen deze profiles allemaal vanuit de RACF-database te worden geladen in de RACF address space, hetgeen betekent dat bij iedere autorisatie-evaluatie door RACF een I/O dient te worden gepleegd. De generic profiles worden echter in het interne geheugen van de computer vastgehouden, zodat na verloop van tijd steeds minder I/O nodig is.

Voordat RACF echter gaat zoeken naar de bij de resource behorende profiles, zal (afhankelijk van de waarde van bepaalde SETROPTS-parameters) eerst het Global Access Checking (GAC)-mechanisme worden geactiveerd. Dit is een mechanisme op basis waarvan RACF zeer snel kan bepalen of een gebruiker toegang heeft tot de resource. Deze bepaling geschiedt aan de hand van een tabel in het interne geheugen, waarin algemene toegangsregels, bedoeld voor alle gebruikers, zijn vastgelegd. Op basis van deze tabel kan echter alleen toegang worden verleend; er kan geen toegang worden ontzegd. Indien geen entry in de GAC-tabel is opgenomen op basis waarvan de gebruiker toegang kan worden verleend, zal RACF verder de autori-

satie-evaluatie uitvoeren aan de hand van de inhoud van de profiles.

Authorized Caller Table

De RACINIT-macro heeft als doel het (laten) uitvoeren van de user-identificatie en -authenticatie. Bij positief resultaat zal een address space voor de desbetreffende user-id worden opgebouwd. In deze address space is een Access Control Environment Element (ACEE) opgenomen. Dit is een control block dat onder meer wordt gebruikt ten behoeve van het autorisatiemechanisme van RACF. Hierbij wordt de user-informatie uit de ACEE vergeleken met de access list in de profile voor de resources waar de gebruiker om vraagt.

Het ACEE vervult dus een cruciale rol in het mechanisme voor het checken van de autorisatie. Het is echter "manipuleerbaar" door aan de RACINIT-macro "verkeerde" parameters mee te geven. Op deze wijze kan een gebruiker een andere gebruiker simuleren en kunnen er beveiligingsmaatregelen worden doorbroken. Om deze reden mag de RACINIT-macro alleen worden aangeroepen door daartoe geautoriseerde programma's. Autorisatie in deze zin betekent dat het programma draait:
- in APF-mode, of
- met system-key 0-7, of
- in supervisor state.

RACF biedt echter de mogelijkheid om programma's die niet aan deze criteria voldoen toch te autoriseren voor het aanroepen van de RACINIT-macro. Dit wordt gedaan met behulp van de Authorized Caller Table (ACT). Indien een programma in de ACT is opgenomen, is dit geautoriseerd de RACINIT-macro aan te roepen mits het afkomstig is uit een APF library (maar dus niet noodzakelijk met Authorization Code = 1).

De programma's die zijn opgenomen in de ACT zijn tevens geautoriseerd tot het aanroepen van de RACLIST-macro. Deze macro zorgt ervoor dat in het interne geheugen van de computer (in de RACF address space) kopieën worden opgebouwd van de profiles uit de RACF-database.

HET BEHEER VAN DE RACF-DATABASE

De inrichting van de RACF-database is in belangrijke mate bepalend voor de complexiteit van het beheer ervan. RACF biedt de mogelijkheid van vergaande delegatie van beheersmogelijkheden. Beheersmaatregelen zijn in dit verband het definiëren en onderhouden van gebruikers-, groeps- en resource-definities. Deze delegatie kan op verschillende manieren technisch worden geïmplementeerd.
Bij een ondoordachte technische implementatie bestaat het risico dat de uiteindelijke technische delegatiestructuur niet (meer) aansluit op de organisatorische, bijvoorbeeld doordat onvoldoende rekening is gehouden met de betrekkelijk ruime bevoegdheden van (technische) eigenaars.

In deze paragraaf wordt ingegaan op de wijze waarop de beheersorganisatie kan worden ingericht en de invloed hiervan op de technische implementatie.

Toevoegen en wijzigen van user profiles

Uit het oogpunt van beheersbaarheid kan het van belang zijn de controle over profiles te decentraliseren, of bijvoorbeeld een scheiding aan te brengen tussen de bevoegdheid user-ids te mogen definiëren en user-ids te mogen wijzigen.

Het definiëren van nieuwe user-ids gebeurt met behulp van het ADDUSER-commando. Dit commando kan worden uitgevoerd door gebruikers met één van de volgende (combinaties van) bevoegdheden:
- system-SPECIAL;
- owner van de default group van de nieuw te definiëren gebruiker én het CLAUTH-attribute;
- owner van de default group én het JOIN authority;
- group-SPECIAL voor de default group én het CLAUTH-attribute.

Met behulp van het ALTUSER-commando kan de user profile van een gebruiker worden gewijzigd, inclusief de user attributes en authorities. In de meeste gevallen heeft het ALTUSER-commando alleen tot gevolg dat de user profile wordt gewijzigd. In een aantal gevallen heeft het gebruik van dit commando echter tot gevolg dat óf de desbetreffende group profile óf de desbetreffende connect profile wordt gewijzigd.
De RACF-gebruiker met het system-SPECIAL-attribute kan alle attributes en authorities van de RACF-gebruikers veranderen, behalve de UAUDIT/NOUAUDIT-attributes (hiermee wordt bepaald of de activiteiten van de gebruiker al dan niet dienen te worden gelogd). De RACF-gebruiker met het group-SPECIAL-attribute heeft meer beperkingen. Deze kan het commando slechts gebruiken binnen de scope van zijn groep en is overigens niet in staat SPECIAL-, AUDIT-, OPERATIONS- en UAUDIT/NOUAUDIT-attributes toe te kennen aan andere gebruikers. Ook aan andere gebruikers staat het ALTUSER-commando, met een beperkte scope en/of een beperkt aantal opties, beschikbaar.

Bij een ondoordachte technische implementatie bestaat de kans dat de uiteindelijke technische delegatiestructuur niet aansluit op de organisatorische.

Door nu bijvoorbeeld, naast de system-SPECIAL, group-SPECIAL-gebruikers te definiëren voor bijvoorbeeld verschillende werkmaatschappijen, zon-

der dat de group-SPECIAL-gebruikers worden voorzien van het CLAUTH-attribute voor de user class, kunnen de user-ids alleen centraal worden gedefinieerd maar kunnen ze wel decentraal worden gewijzigd.

Een ander voorbeeld is het door de system-SPECIAL laten definiëren en onderhouden van een administratieve en een functionele groepsstructuur. Door vervolgens decentrale gebruikers te voorzien van het CONNECT-attribute kunnen, zonder dat de user en resource profiles inhoudelijk worden gewijzigd, veranderingen worden aangebracht in de bevoegdheden van gebruikers.
Voordeel van deze methode is dat het beheer van bevoegdheden relatief eenvoudig te regelen is. Indien een gebruiker van functie verandert hoeft zijn user profile slechts onder een andere functionele groep te worden geplaatst (via de functionele groep worden dus de bevoegdheden verkregen).
Een voordeel van het niet in de access list opnemen van user-ids is dat bij verwijdering of verandering van de user-id niet alle resource profiles behoeven te worden gecontroleerd. Via een listing van de desbetreffende user-id is wel te achterhalen in welke groepen deze is opgenomen. Er is echter via deze lijst niet te achterhalen of en zo ja, in welke access lists de user-id voorkomt. Door toch user-ids op te nemen in access lists van resource profiles wordt de onbeheersbaarheid van de RACF-database vergroot.

Toevoegen en wijzigen van resource profiles

Het definiëren van profiles voor datasets gebeurt met behulp van het ADDSD-commando. Met betrekking tot het al dan niet mogen gebruiken van dit commando wordt door RACF onderscheid gemaakt in group en user datasets.
User datasets kunnen worden beschermd door de gebruiker zelf (dus als zijn user-id gelijk is aan de high level qualifier van de dataset) of door de gebruikers met het system-SPECIAL en group-SPECIAL (alleen binnen de scope van hun groep). Bij group datasets echter kunnen ook de gebruikers met CREATE-authority en het OPERATIONS-attribute dit commando gebruiken.

Een duidelijk onderscheid tussen het aanmaken en wijzigen van profiles is bij datasets niet te maken. Hierbij dient te worden gelet op het feit dat dataset profiles in een aantal gevallen ook automatisch door RACF kunnen worden gegenereerd. Het wijzigen van een dataset profile gebeurt met behulp van het ALTDSD-commando.

Op soortgelijke wijze zijn de definitie en de wijziging van general resource profiles geregeld met behulp van de RDEFINE- en de RALTER-commando's.

HULPMIDDELEN VOOR DE AUDIT

Bij een audit van de effectiviteit van de logische toegangsbeveiliging kan onderscheid worden gemaakt tussen:

- beoordelen van de opzet en het bestaan van de organisatorische maatregelen en procedures;

- beoordelen van de opzet en het bestaan van de beveiligingsarchitectuur (de ondersteuning van de organisatorische maatregelen en procedures met de juiste parameterinstellingen, gebruikersbevoegdheden en andere relevante componenten);

- vaststellen van de werking van de maatregelen en procedures.

Organisatorische maatregelen en procedures

Het vaststellen van de opzet en het bestaan van de organisatorische maatregelen en procedures wordt in dit artikel buiten beschouwing gelaten. Dit zal in grote lijnen overeenkomen met wat in andere omgevingen ten aanzien van deze aspecten geldt.

Beveiligingsarchitectuur

RACF biedt de auditor een aantal hulpmiddelen voor het vaststellen van de opzet en het bestaan van de beveiligingsarchitectuur. De belangrijkste hulpmiddelen hiervoor zijn:
- lijst van de actuele SETROPTS-parameters;
- Data Security Monitor (DSMON)-rapportage;
- lijst van (een deel van de) user, group en resource profiles.

Voor bijvoorbeeld informatie over de inhoud van exits en tabellen (zoals de Naming Convention Table) dient op MVS-hulpmiddelen, zoals print- en punch-utilities, te worden gesteund.

SETROPTS-parameters
Met behulp van een uitdraai van de SETROPTS-parameters kan de auditor vaststellen welke waarde aan kritische systeemparameters is toegekend. Een dergelijke uitdraai kan worden verkregen door het commando SETROPTS LIST te geven. De LIST-optie kan zowel door een system- als een group-AUDITOR worden gegeven.

DSMON-rapportage
De DSMON-rapportage bestaat uit een aantal vaste onderdelen en kan volledig of op onderdelen worden uitgedraaid. De gebruiker die dit rapport wil laten genereren, heeft het AUDIT-attribute nodig.
De functies van de DSMON-rapportage en de naar aanleiding daarvan opgeleverde informatie zijn:

- SYSTEM. Dit resulteert in een lijst met een aantal algemene gegevens over het systeem, zoals identificatie en modelnummer van het processor-complex, naam, versie en release van het besturingssysteem, de naam van het system residence volume, de system identifier voor SMF en het versie- en release-nummer van RACF.

- RACGRP. Group Tree Report. Dit is een overzicht waarmee de RACF-groepsindeling zichtbaar wordt gemaakt. De hoogste groep in de hiërarchie is SYS1. Dit is een door IBM geleverde groep. Alle

door de installatie gedefinieerde groepen zijn hiërarchisch ondergeschikt aan SYS1.

- SYSPPT. Program Properties Table van MVS.
- RACAUT. Authorized Caller Table.
- RACCDT. Class Descriptor Table.
- RACEXT. RACF Exits Report: een overzicht van de in het systeem actieve RACF exits.
- RACGAC. Global Access Checking Report.
- RACSPT. Started Procedures Table Report: een overzicht van de aan RACF gedefinieerde started-procedures en onder welke user-id en group-id deze procedures draaien.
- RASUSR. Selected User Attribute Report: een overzicht waarmee zichtbaar wordt gemaakt welke user-ids welke attributes hebben en op welk niveau (system of group).
- SYSSDS. Selected Data Sets Report: een overzicht van kritieke datasets. Kritieke datasets zijn onder meer: Linklist datasets, APF libraries, catalogs, RACF primary en backup database, etc. Het Selected Data Sets Report bestaat uit een aantal onderdelen dat apart dient te worden opgegeven bij het genereren van de DSMON-rapportage.

User, group en resource profiles
Met een lijst van de SETROPTS-parameters en een DSMON-rapport heeft de auditor al een redelijk beeld verkregen van de bestaande beveiligingsarchitectuur. Belangrijk hierbij is echter ook dat deze beveiligingsarchitectuur niet zomaar kan worden doorbroken. Hiertoe dienen de essentiële componenten adequaat te zijn beveiligd. Voorbeelden van deze componenten zijn onder meer de RACF-database en kritische MVS-systeemdatasets.

De auditor heeft de beschikking over de LSTUSER-, LSTGRP-, LSTDSD- en RLIST-commando's voor het kennis nemen van de inhoud van respectievelijk user, group, dataset en general resource profiles (de informatie uit de connect profiles wordt bij het genereren van een LSTUSER-commando opgenomen in de listing van de user profiles).
Met behulp van deze informatie kan worden vastgesteld of de in het kader van de logische toegangsbeveiliging kritieke systeemcomponenten voldoende beveiligd zijn.

Overige van belang zijnde informatie
In dit artikel is een aantal elementen van RACF en MVS beschreven dat van bijzondere invloed is op de effectiviteit van RACF. Zo kunnen bijvoorbeeld worden genoemd:
- de MVS router exit;
- de Naming Convention Table;
- de Authorized Caller Table (is reeds opgenomen in de DSMON-rapportage).

Om een gefundeerd oordeel te kunnen geven over de effectiviteit van de beveiliging, dient kennis te worden genomen van de inhoud van de MVS router exit en de Naming Convention Table. Voor een beoordeling van de Naming Convention Table is geen diepgaande MVS-kennis vereist. Beoordeling is mogelijk aan de hand van de load module van deze tabel, dan wel aan de hand van de macro met behulp waarvan deze is opgebouwd, mits kan worden gewaarborgd dat de versies van de macro en de opgebouwde tabel overeenkomen.

Op interview-basis kan inzicht worden verkregen in de functionaliteit van exits. Niet alleen de MVS router exit, maar alle RACF exits zijn in dit kader van belang. Voor een inhoudelijke beoordeling van exits is kennis van Assembler een vereiste.

Werking maatregelen en procedures

Bij het vaststellen van de werking van de maatregelen en procedures is het van belang te bepalen welke audit-informatie benodigd is. Deze auditopties dienen namelijk eerst te worden ingesteld via het SETROPTS-commando of via de commando's voor het wijzigen van de user, group en resource profiles.

De logging van RACF wordt opgebouwd via het System Management Facility (SMF) van MVS. Met behulp van de RACF report writer kunnen de aldus verkregen gegevens worden geanalyseerd en kan worden gecontroleerd of richtlijnen en procedures worden gevolgd.

TOT SLOT

In dit artikel is de functionaliteit alsmede de technische implementatie en werking van RACF aan de orde geweest. Duidelijk is geworden dat de grote flexibiliteit die RACF biedt met betrekking tot de inrichting van de beheersorganisatie een zeker risico inhoudt, omdat bij ondoordachte implementatie mogelijk de technische delegatiestructuur niet (meer) aansluit op de organisatorische. Hierdoor kan een onjuist beeld over de effectiviteit van de beveiliging ontstaan.

Voorts is gebleken dat er een aantal addertjes onder het gras zit. Via speciale exits en tabellen die misschien niet direct onder het aandachtsgebied van de beveiligingsfunctionaris vallen, kan vergaande invloed worden uitgeoefend op de effectiviteit van de beveiliging.

Ing. G.H.M. Meijer
Is sinds 1985 werkzaam bij KPMG Klynveld EDP Auditors. In de afgelopen jaren heeft hij zich beziggehouden met opdrachten uit de algemene EDP-audit-praktijk, alsmede opdrachten met de specifieke aandachtsgebieden besturingssystemen (MVS) en beveiligingspakketten (RACF, ACF2, Top Secret). Hij publiceerde reeds eerder over de beveiliging van MVS-systemen.

Implementatie van een beveiligingspakket

J.H. Diekema

Het implementeren van een beveiligingspakket is een gecompliceerd scala van activiteiten. De auteur heeft in een coördinerende rol het implementatieproces van begin tot eind meegemaakt en geeft in dit artikel zijn ervaringen weer. Hierbij besteedt hij ruim aandacht aan de voorbereidingen die moeten worden getroffen en de mogelijke hindernissen op de weg naar een goed beheersbare logische toegangscontrole.

INLEIDING

Dit artikel geeft de ervaringen weer die werden opgedaan bij de implementatie van een beveiligingspakket.
De implementatie vormde de afsluiting van een complex proces dat bestond uit beleidsvorming, inrichting van de organisatie, opstellen van procedures en implementatie van de techniek. Implementatie van de techniek omvat de software-installatie van het pakket en de implementatie van het pakket. Onder implementatie van een beveiligingspakket wordt verstaan het doen functioneren van beveiliging door de functies te gaan gebruiken.
De ervaringen werden opgetekend door een beveiligingsfunctionaris bij een grote centrale IBM-mainframe-configuratie, voorzien van het beveiligingspakket Top Secret van Computer Associates.
Omwille van de beknoptheid blijven in deze bijdrage onder meer de decentrale verwerking, netwerkbeveiliging en performance-aspecten van beveiliging buiten beschouwing.
Deze beveiligingsfunctionaris vervulde in het proces een coördinerende rol en gaf mede vorm aan de inrichting van de beveiliging.

Gebleken is dat er verschillen zijn tussen implementatie van een beveiligingspakket en de implementatie van andere "beheers-software", en wel:
- de werking van een beveiligingspakket oefent invloed uit op alle faciliteiten die de geautomatiseerde gegevensverwerking aan gebruikers biedt. Deze brede werking is uniek voor een beveiligingspakket;
- beveiliging moet in staat zijn a tempo de ontwikkelingen in de beveiligde omgevingen bij te houden. Hierdoor moet de inrichting van het beveiligingspakket dynamischer zijn dan andere software die veelal kan volstaan met een beperkte "wijzigingenorganisatie";
- automatisering is er sinds jaar en dag op gericht nuttig te zijn voor de gebruiker. Het moest en kon sneller, goedkoper en vriendelijker. Hierdoor liggen de "push" van de automatisering en de "pull" van de gebruiker in één lijn. Deze "push/pull-werking" ligt anders als het om beveiliging gaat.

Er zijn ook overeenkomsten geconstateerd:
- het implementeren van een beveiligingspakket is niet moeilijker. Implementatie van bijvoorbeeld accounting en job-scheduling heeft ook eigenschappen waardoor de implementatie moeilijk kan zijn;
- implementatie van een beveiligingspakket en van andere beheers-software zal voor elk bedrijf een weinig voorkomend, zo niet uniek gebeuren zijn. De gelegenheid om in deze implementatie ervaring op te doen zal zich weinig voordoen.

In dit artikel komen de volgende onderwerpen aan de orde:
- keuze van de implementatiestrategie;
- architectuur van het security-programma en de security-file;
- het object van beveiliging;
- de relatie tussen beveiliging, interne controle en systeembeheer.

IMPLEMENTATIESTRATEGIE

De implementatiestrategie moet het bedrijf zelf bepalen. Deze staat niet in de manuals en wordt niet meegeleverd. Dit kan niet van de leverancier worden verwacht omdat bedrijfskenmerkende omstandigheden hiervoor bepalend zijn.
In deze paragraaf worden mogelijke uitgangsposities beschreven. Het terrein wordt verkend en de belangrijke factoren worden genoemd. Vervolgens komen de strategiekeuze en -toepassing aan de orde.

Koude start

Invoeren van beveiliging in een computersysteem waarin zich nog geen produktieprocessen afspelen biedt een comfortabele uitgangspositie. De zwaarste afstellingen die het pakket kent kan men aanbrengen terwijl minimale bevoegdheden worden verleend. Deze gelegenheid kan zich voordoen bij conversies of bij het (op)nieuw inrichten van automatisering.
Er zit wel een aantal haken en ogen aan.
De "beveiliging" moet herkenbaar en bereikbaar zijn. Niet alleen dienen daartoe organisatorische en procedurele maatregelen te zijn genomen, maar deze moeten ook bij de andere installateurs bekend zijn.
De beveiligingsfunctionaris dient voorbereid te zijn op de acties die hij neemt als gevolg van de gekozen "harde afstellingen". Aanpassen van de afstellingen en mogelijk ongegrond uitreiken van bevoegdheden kunnen de beveiliging aantasten. Het is verstandig ook in een comfortabele uitgangspositie de criteria duidelijk te hebben. Toch lijkt een koude start te verkiezen boven een warme start, als er tenminste iets te kiezen valt.
Bij een koude start luidt het devies: "Zachte heelmeesters maken stinkende wonden".

Warme start

Bij een warme start staat de beveiligingsfunctionaris voor de taak het beveiligingspakket te implementeren terwijl het bedrijf in volle produktie is. In de praktijk blijkt dat een warme start, of een koude start die in een warme start overgaat, vaak voorkomt. Volle produktie houdt in dat gebruikers online met de systemen werken, de batch-processen draaien, externe datacommunicatie gebruik maakt van de systemen en er dagelijks wijzigingen zijn als gevolg van onderhoud aan de systemen. De implementatie van beveiliging mag uiteraard geen bedreiging voor de continuïteit van de gegevensverwerking vormen.
In deze uitgangspositie luidt het devies: "Voorzichtigheid is de moeder van de porseleinkast".

Terrein verkennen

Het terrein waar de implementatie zich afspeelt bestaat uit "omgevingen" die overeenkomen met de functies die de automatisering kent: produktie, systeemontwikkeling en systeemondersteuning.
Voor de werking van de beveiliging is deze indeling niet van belang, maar voor het bereiken van een werkende beveiliging wel. Elke omgeving vereist een andere implementatie, hetgeen voornamelijk wordt veroorzaakt door de verschillende risico's.
In elke omgeving staan aan gebruikers en beheerders faciliteiten ter beschikking. Deze zijn bijvoorbeeld time-sharing, teleprocessing en batch-gewijze verwerking. De faciliteiten stellen hen in staat de resources te benaderen.
De indeling van het terrein in omgevingen, faciliteiten, gebruikers, beheerders en resources is min of meer hiërarchisch. Helaas maakt dit niet zonder meer een top-down of bottom-up aanpak of een aanpak per applicatiesysteem mogelijk. Behalve verticale relaties bestaan er talloze horizontale relaties die dit belemmeren. Enkele voorbeelden:

- De "produktie-omgeving" en de "ontwikkelomgeving" maken gebruik van resources die voorkomen in de "besturingssysteemomgeving". Vanuit beide omgevingen wordt immers een beroep gedaan op ondersteuning van besturingsprogramma's die systeemdata benaderen.

- Het kan voorkomen dat een bepaalde faciliteit gemeenschappelijk in verschillende omgevingen wordt gebruikt. De produktie van informatie vindt batch-gewijs plaats, maar ook ontwikkelaars en systeembeheerders starten batch-jobs.

- Het komt voor dat een faciliteit wel naar verschillende omgevingen te onderscheiden is maar uitgaat van een gemeenschappelijke verzameling resources. Eindgebruikers kunnen bijvoorbeeld met een teleprocessing-faciliteit werken, terwijl ontwikkelaars een eigen teleprocessing-faciliteit hebben. Hierdoor is deze verwerking op het niveau van omgeving goed te beveiligen, maar het besturingssysteem en daarmee het beveiligingspakket beschouwt in dit geval de teleprocessing-resources als één verzameling.

Koester niet de gedachte dat het ooit "af" is.
Roep ook dat beeld bij anderen niet op.
Een beveiligingspakket is in deze zin vergelijkbaar met elk ander informatiesysteem, het blijft zeer onderhoudsgevoelig.

Omdat de werking van de faciliteiten en de benadering van resources niet altijd eenduidig tot de grenzen van een omgeving beperkt blijven, is het omgevingsgewijs implementeren vrijwel onmogelijk.
Het kan voorkomen dat in het verleden reeds beveiligingsmaatregelen in faciliteiten en in programma's zijn aangebracht. Deze kunnen worden overgenomen door of worden aangesloten op het beveiligingspakket of eenvoudig worden genegeerd.

Bovengenoemde indelingen en de aangebrachte beveiligingen vormen de "inrichting van de automatisering" die in dit kader relevant is. Deze inrichting kan per bedrijf verschillen. Om een goede implementatiestrategie te bepalen is het belangrijk deze inrichting te kennen.

De automatiseringsdiscipline die in het verleden is betracht, is eveneens een bepalende factor bij de keuze van de implementatiestrategie.
Als niet consequent een standaard voor de naamgeving van bestanden en transacties is gehanteerd, zal de implementatie veel hinder ondervinden.
Als systemen niet zijn gestructureerd in logische functies zijn deze niet te scheiden en bevoegdheden niet selectief aan gebruikers uit te reiken.
Als de inhoud van bestaande beveiligingstabellen is "vervuild", mogen deze geen basis vormen voor de inrichting van de security-file.
Beveiliging volgt de automatisering. Een slechte automatisering is niet goed te beveiligen.

Het blijkt belangrijk de uitgangspositie en het terrein te kennen om de strategie te bepalen. De betrachte automatiseringsdiscipline en de beschikbare hulpmiddelen zijn hierin ook van essentieel belang.

Een derde belangrijke factor die de implementatiestrategie bepaalt is de ondersteuning die wordt genoten.
Een goed beveiligingspakket helpt bij de implementatie door het beschikbaar stellen van afstellingen die de pijn verzachten. Hiermee is het mogelijk via een "administratief stadium" en via een "waarschuwingsstadium" te komen tot een afstelling waarbij de beveiliging volledig operationeel werkt en dus niet-toegestane gebeurtenissen stopt. Door deze afstellingen selectief per faciliteit toe te passen vormen ze een nuttig hulpmiddel.
Het gebruik van deze afstellingen houdt echter ook een risico in. De implementatiestadia van pakketten zijn afstellingen van de beveiliging, niet van de mogelijkheden van de gebruikers. Het kan voorkomen dat een gebruiker handelingen uitvoert die hij niet mag maar wel kan. Als de gebruiker werkt in het "waarschuwingsstadium" krijgen hij en de security administrator een melding. Als de gebruiker in het "administratieve stadium" werkt genereert het pakket geen waarschuwing. De gebruiker mag niets maar kan alles.

Gekozen strategie (Bottom-up)

De strategie die in dit artikel zal worden gevolgd, bestaat uit het per faciliteit implementeren van beveiliging. Bijvoorbeeld eerst de teleprocessing, dan de batch-verwerking, enz. Dit houdt in dat gelijktijdig in alle omgevingen deelbeveiliging wordt aangebracht, alleen voor een bepaalde soort activiteit. Bottom-up dus.
Per faciliteit is dit een top-down strategie, die volledig kan worden uitgevoerd als de resources voor de faciliteit uniek zijn en dus niet door middel van andere faciliteiten ook worden gebruikt. Ten gevolge van het bestaan van deze relaties kunnen gemeenschappelijke resources niet eerder worden beveiligd dan nadat alle faciliteiten zijn behandeld. Een verstoring van de werking van de andere faciliteiten kan het gevolg zijn als bevoegdheden op gemeenschappelijke resources niet goed zijn uitgegeven.

Toepassen van de strategie

Het implementeren per faciliteit betekent:
1 – beveiliging aanbrengen daar waar zij nog niet was of
2 – beveiliging door het pakket aanvullend implementeren op reeds bestaande beveiliging of
3 – overnemen van beveiliging door het pakket, hetgeen de bestaande beveiliging van de faciliteit uitschakelt.

1 Beveiliging van de eerste soort is het eenvoudigst. Daar heeft het pakket vrij spel. Het implementeren bestaat uit twee fasen: het inrichten van de security-file (zie verder de paragraaf Architectuur van de security-file) en de aanwezigheid van een extern beveiligingspakket kenbaar maken aan de faciliteit. Het eerste is een zaak van de beveiligingsfunctionaris; het tweede een zaak van systeemprogrammeurs die de communicatie moeten activeren.

2 Aanvullend implementeren van beveiliging is vaak lastiger. Vooral als de software van de faciliteit en van het pakket niet "uit dezelfde stal" komen. De volgende situaties onderscheiden zich van elkaar:

– De beveiliging van het pakket en de bestaande beveiliging zijn zich van elkaars bestaan niet bewust en communiceren dus niet met elkaar. Dit houdt in dat twee lagen van beveiliging bestaan, hetgeen storend is voor gebruikers (dubbel aanloggen, meerdere passwords, andere spelregels). Het beheer van meerdere tabellen levert meer werk op.

– De bestaande beveiliging wikkelt zelf voor die faciliteit de beveiliging af maar raadpleegt daarbij wel het centrale beveiligingspakket. Bij deze categorie spelen de communicatiemogelijkheden van het beveiligingspakket en de faciliteit een belangrijke rol. Het beveiligingspakket heeft soms nauwelijks grip op wat de faciliteit vraagt en wat deze met het antwoord doet. Deze communicatie speelt zich af op de grens van de mogelijkheden van het beveiligingspakket en kan lekken in de beveiliging opleveren. Uit oogpunt van gebruikersvriendelijkheid en beheer is dit echter een elegante en goedkope implementatie.

Het overnemen van de beveiliging van de faciliteit in het beveiligingspakket biedt in het algemeen een goede beveiliging, zo goed namelijk als het pakket dat kan waarmaken. Het is gebruikersvriendelijk

omdat beveiliging "één gezicht" vormt en goedkoop omdat het specifieke tabelbeheer voor de faciliteit vervalt. De ervaring is dat vaak wel de technische mogelijkheden aanwezig zijn, omdat de software uit dezelfde stal komt of omdat de ontwerpers met elkaar rekening hebben gehouden.
Ook in deze situatie geldt dat de security-file moet zijn gevuld en de communicatie geactiveerd. Een verschil met de voorgaande situatie is echter dat tevens een laag van beveiliging verdwijnt. Als de communicatie niet goed werkt of de security-file niet correct is gevuld, kan de beveiliging wegvallen of de werking van de faciliteit verstoord raken.

Ervaring leert dat "implementeren van beveiliging daar waar zij nog niet was" bovenaan de prioriteitenlijst van de implementatie mag staan. Niet alleen omdat dit direct een tastbare bijdrage levert aan beveiliging, maar ook omdat deze eerste stap het eenvoudigst is en tevens ervaring voor de volgende stappen oplevert. Neem alleen goede systemen op in het beveiligingspakket.
Voor het bepalen van de prioriteit voor de andere faciliteiten geldt de afweging of de werking en de beveiliging van deze faciliteiten stabiel en van voldoende niveau zijn.

Het is aan te bevelen alleen faciliteiten in het beveiligingspakket op te nemen die reeds in alle opzichten een goede kwaliteit bezitten. De verwachting gelijk met het opbouwen van beveiliging een "schoning" uit te voeren loopt waarschijnlijk op een teleurstelling uit. Ga één op één "linea recta" over en pas niets aan.
Denk na over de "weg terug" en neem maatregelen die dit mogelijk maken. Niet dat dit iets aan beveiliging toevoegt, maar door de nood gedwongen kan er wel eens bij een "warme start" geen keus zijn. Door kleine stappen te nemen bij de implementatie valt de "pijn van een stap terug" mee.

Stoppen

Bij het implementeren van beveiliging blijkt dat er geen mechanisme bestaat dat aangeeft wanneer beveiliging goed genoeg is. De steun die bij deze afweging kan worden verwacht van risico-analyse en kostenbeheersing is beperkt.
Risico-analyse gaat uit van een verzameling onderkende risico's. De neiging zal bestaan om deze verzameling zo groot mogelijk te doen zijn ter wille van de compleetheid. Het besluit om van alle onderkende risico's bepaalde zaken niet te beveiligen is moeilijk te beargumenteren. De opzet van de beveiliging zal derhalve tenderen naar over-kill.
Het hanteren van kostenbeheersing om de grenzen van de beveiliging aan te geven is een verplaatsing van het probleem. De afweging wat een bedrijf voor beveiliging over heeft is dezelfde als de afweging waar de beveiliging stopt.

Ervaring leert dat het uitvoeren van een test door een onafhankelijke partij goed inzicht geeft in de vraag of de aangebrachte beveiliging toereikend is. Het probleem verplaatst zich daarmee in feite naar de inschatting van de professionaliteit van de testers. Hiervan is in het algemeen eenvoudig een goed beeld te krijgen. Op deze wijze testen vormt, voor zover bekend, het enige bruikbare instrument om te bepalen wanneer met het implementeren van beveiliging verantwoord kan worden gestopt.

Hoe diep men de beveiliging moet doorvoeren, de mate van detaillering of fijnmazigheid, hangt nauw samen met de eisen die in het beveiligingsbeleid zijn gesteld ten aanzien van de mate waarin de beveiliging de interne controle en het systeembeheer moet ondersteunen. De eerder genoemde automatiseringsdiscipline bepaalt de mogelijkheden om te volstaan met een grovere beveiliging.
Een grotere fijnmazigheid betekent niet een betere beveiliging. Wel meer werk. Stop zodra het "goed genoeg" is, want eenmaal aangebrachte fijnmazigheid is niet eenvoudig terug te draaien.

Als alle omgevingen, faciliteiten, resources, beheerders en gebruikers zijn gedefinieerd in de security-file, sluit men dit proces af door het activeren van de afstellingen op pakketniveau. Dit heeft tot gevolg dat de beveiliging volledig operationeel werkt.

ARCHITECTUUR VAN HET SECURITY-PROGRAMMA

In deze paragraaf wordt beschreven "hoe het beveiligingsprogramma werkt" en waarom dit inzicht voor de beveiligingsfunctionaris belangrijk is. Aandacht wordt besteed aan het belang van parameters.

Behalve te volgen "hoe het werkt" is het zinvol er voortdurend kritisch bij stil te staan "hoe het eigenlijk zou moeten werken" en de bevindingen eventueel met de leverancier te bespreken.

Algoritme

De architectuur van het programma is alleen van belang voor zover het zich functioneel manifesteert aan de beveiligingsfunctionaris en de gebruikers. Uit de manuals is hiervan in het algemeen een goed beeld te krijgen en als de pakketselectie naar behoren is uitgevoerd, zijn de geboden functies duidelijk en toereikend.

De beveiligingsfunctionaris dient vertrouwd te zijn met de "denkwijze" van het security-programma. Als het programma beoordeelt of een bepaald verzoek van een gebruiker is toegestaan, doorloopt het programma een "zoek- en evaluatie-algoritme". Dit gebeurt in een bepaalde volgorde aan de hand van informatie uit de security-file, parameters en informatie die het verzoek vergezelde. Om te kunnen bepalen of het programma tot de gewenste besluitvorming zal komen, is het nodig dat het op het juiste moment de juiste informatie ontvangt, waarbij bekend moet zijn hoe het programma deze informatie verwerkt. Dit komt niet altijd even duidelijk in de manuals tot uiting. Raadpleeg de leverancier of stel testgevallen met "uitvoerverwachtingen" op.

Parameters

Parameters besturen de werking van het programma. Met deze parameters regelt de beveiligingsfunctionaris de "intelligentie" van de beveiliging en de wijze waarop zij moet reageren op bepaalde gebeurtenissen.
Met parameters regelt men bijvoorbeeld het functioneren van de beveiliging ("aan" of "uit"), de password-spelregels, hoe het besturingssysteem verzoeken van gebruikers moet afhandelen als de beveiliging niet actief is en hoe het security-programma de prioriteit in aangetroffen bevoegdheden moet afhandelen. Ook kan men het gebruik van ongewenste passwords, bijvoorbeeld de namen van de maanden, door het programma laten weigeren.
Parameters regelen niet alleen de werking van de beveiliging maar beschrijven ook de eigenschappen van de computerfaciliteiten voor het beveiligingspakket. Het is belangrijk dat deze beschrijvingen met de werkelijkheid overeenstemmen.
De betekenis van de parameters en hun waarden moet volledig duidelijk zijn voordat men de beslissing neemt hoe de afstellingen dienen te zijn. Vaak is het raadzaam bij de implementatie voorlopig de standaardafstelling van de leverancier te volgen. Soms wijkt men daarvan af, waarbij zorgvuldig documenteren belangrijk is.

Sommige parameters worden direct actief: "on the fly". Andere parameters worden eerst actief nadat het besturingssysteem opnieuw is opgestart of worden bij hernieuwde opstart vervangen.

Functies

Een beveiligingsprogramma biedt twee soorten functies:

- de beveiligingsfuncties, bijvoorbeeld het beveiligen van het aanlogproces of van een resource-type;

- de beheersfuncties. De security administration gebruikt deze functies. Ze dienen om het gebruik van de beveiligingsfuncties mogelijk te maken. De beheersfuncties ondersteunen de beveiligingsfuncties. Als "terminals" een resource-type is waarvoor beveiliging wordt geïnstalleerd, is beheer nodig van de terminal-identificaties en moeten de bevoegdheden op terminals worden beheerd.

De ervaring leert dat de inrichting van de beheersfuncties van een pakket in belangrijke mate bepalend is voor de kosten die aan security administration zijn verbonden. Slechte beheersfuncties kunnen ook aanleiding zijn tot het maken van fouten bij security administration. Beveiligen doen alle pakketten wel, maar ook het bieden van goede mogelijkheden tot security administration is belangrijk voor kwalitatief goede beveiliging.

Om te voorkomen dat, bijvoorbeeld ten gevolge van storingen in een bepaalde faciliteit, de security-file niet meer toegankelijk is voor beheer, is het aan te bevelen ten minste twee toegangen tot de security-file en de parameters te implementeren.

Deze toegangen (bijvoorbeeld de teleprocessing-monitor, de batch-verwerking of de time-sharing-faciliteit) dienen regelmatig afwisselend te worden gebruikt, om verzekerd te zijn van continuïteit in security administration.

Het is aan te bevelen de beveiligings- en beheersfuncties te implementeren en te gebruiken zoals deze zijn bedoeld; zeker zolang de implementatie loopt en niet is aangetoond dat beveiliging of beheer ontoereikend is.

Encryptie

Passwords mogen alleen encrypt worden vastgelegd. (Omdat netwerkbeveiliging in dit artikel niet wordt behandeld, wordt geen aandacht besteed aan het transporteren van passwords.) Het beveiligingsprogramma beschikt over een encryptie-algoritme en een sleutel.

Als de pakketselectie naar behoren is uitgevoerd, beschikt het pakket over een toereikend algoritme. Bij implementatie hoeft de beveiligingsfunctionaris zich dan ook geen zorgen te maken over de "kraakbaarheid" van dit algoritme.

Het verdient wel aanbeveling te onderzoeken of andere programma's ook zorgvuldig met het encrypten van passwords omgaan. Het is niet altijd zo dat zodra een gebruiker zijn password ingeeft, dit direct onder beheer van het beveiligingsprogramma is. Het kan voorkomen dat passwords in leesbare vorm worden opgeslagen of van programma naar programma worden doorgegeven. Het is niet uitgesloten dat hierdoor iemand die de weg weet erin slaagt passwords te achterhalen.

Bij installatie van het pakket wordt de encryptiesleutel meegegeven. Deze sleutel is op het moment van installatie uiteraard leesbaar. De beveiligingsfunctionaris dient deze leesbare opslag van de sleutel na installatie te verwijderen en samen met het password van de "super-security administrator" veilig in een kluis op te bergen.

ARCHITECTUUR VAN DE SECURITY-FILE

In deze paragraaf wordt de rol van de security-file behandeld, alsmede de reden waarom de inrichting van dit bestand belangrijk is. Aan de orde komt de wijze waarop de toegangsregels tot stand komen. Voor de architectuur van de security-file staat de organisatie van het bedrijf model.

Inrichting

De security-file is een bestand waarin alle gebruikersdefinities (en passwords), resource-definities en toegangsregels (access control rules) zijn opgeslagen. Het is een belangrijk bestand, zodat het de moeite waard is de toegang te beveiligen en te zorgen voor de nodige backup- en herstelmogelijkheden.

Bij de implementatie van beveiliging komt de vraag aan de orde welke inrichting de security-file moet hebben. Voor een deel bepaalt de wijze waarop het pakket werkt deze inrichting. Maar voor een belangrijk deel zal de beveiligingsfunctionaris zelf dit "inrichtingsvraagstuk" moeten oplossen.

De keuzes die men maakt zijn niet van invloed op de werking van de beveiliging. Het pakket blijft zijn werk doen ongeacht de structuur die de security-file heeft. Een ontoereikende inrichting van de security-file heeft echter verstrekkende gevolgen voor de inrichting van het beheer, de security administration. De besluitvorming ten aanzien van centraal of decentraal beheer dient haar grondslag te vinden in de inrichting van de file. Zaken als hoe gebruikers zijn gegroepeerd in afdelingen of in systemen, zijn bepalend voor de inrichting van het beheer: als systeembeheer (dus systeemgericht) of als organisatorisch beheer (dus afdelingsgericht). Het gebruik van systemen hoeft niet tot de grenzen van een afdeling te zijn beperkt, zodat deze indeling niet altijd voor de hand ligt.
Waar hoort de batch-verwerking: bij de systemen (als systeembeheer) of bij het Rekencentrum waar de verantwoordelijkheid rust voor de correcte verwerking van batch-jobs? Op het eerste gezicht mag dit soort beslissingen wat speelruimte bieden aan creatieve geesten, maar de gevolgen zijn verstrekkend. Een gekozen inrichting is niet gemakkelijk aan te passen.

Toegangsregels

Een toegangsregel (access control rule; ACR) is een beschrijving van de bevoegdheden van een gebruiker. ACR's komen in twee vormen voor:

- als papieren vastlegging van de communicatie tussen gebruikers, systeemhouders en security administration;

- als geautomatiseerde vastlegging in de security-file.

Beide verschijningsvormen dienen uiteraard inhoudelijk gelijk te zijn. ACR's komen in het algemeen niet als losse regels voor maar zijn verzameld tot een functie. Deze verzameling kan men zich voorstellen als een "functieprofiel". Dit profiel wordt uitgereikt aan de gebruiker die de functie vervult. Een gebruiker krijgt die bevoegdheden die hij voor het uitoefenen van zijn functie nodig heeft. Dit principe staat bekend als: "need-to-use". Dit is een eenvoudig en daardoor bijna vanzelfsprekend goed uitgangspunt.

De praktijk wijst uit dat het niet eenvoudig is om wat technisch onder functies wordt verstaan (dit treft men aan in het functioneel ontwerp van de applicatie) overeen te laten komen met wat in de zin van de administratieve organisatie onder functies wordt verstaan. Om het langdurige en kostbare proces van zoeken naar de juiste indeling in organisatorische en technische functies met de bijbehorende bevoegdheden te vermijden, kan worden uitgegaan van de dagelijkse werkelijkheid. In deze aanpak wordt ervan uitgegaan dat "wat de gebruiker doet" overeenkomt met "wat de gebruiker nodig heeft". De inrichting die op deze wijze ontstaat wordt achteraf bekrachtigd en eventueel geschoond. Met deze "reverse-engineering"-achtige

Test en laat testen.
Er is geen betere manier om er achter te komen of de beveiliging goed genoeg is dan door een onafhankelijke derde erop los te laten.

aanpak wordt voorkomen dat een eventueel ontbreken van een pasklare vastlegging van organisatorische en technische functies met de benodigde bevoegdheden een struikelblok wordt voor het implementeren van beveiliging. Er dient echter voor te worden gewaakt dat "vervuiling" op deze wijze de kans krijgt zich te verheffen tot geformaliseerde vastlegging in de security-file. Het voert in het kader van dit artikel te ver om aan te geven welk instrumentarium de beveiligingsfunctionaris hiervoor ten dienste staat.
Het probleem kan zich voordoen dat gebruikers meerdere functies vervullen die bevoegdheden bevatten die in combinatie met bevoegdheden uit andere functies tot ongewenste vermengingen leiden. De kans is tevens aanwezig dat het aantal functies groot wordt. Zodanig zelfs dat bijna elke gebruiker zijn eigen functie heeft en men het uitgangspunt "need-to-use" geweld aandoet.
Het verdient aanbeveling te waken voor het verschijnsel van de voortdurend uitdijende security-file. Gebruikers vragen in het kader van hun functie bevoegdheden aan maar zullen minder geneigd zijn deze bevoegdheden weer te laten vervallen. De beveiligingsfunctionaris heeft tot taak te voorzien in een "clean-up"-procedure, omdat er geen natuurlijk mechanisme is dat hierin voorziet.

Organisatie

In het algemeen is het aan te bevelen de security-file zoveel mogelijk conform de opzet van de organisatie in te richten, omdat hierdoor het beheer kan worden vereenvoudigd. Bepalend is "wie" verantwoordelijk is voor "wat" en "wie" moet "wat" gaan beheren en niet "wat hoort logisch bij elkaar". Dit heeft tot gevolg dat gebruikers bij een afdeling horen en niet bij het applicatiesysteem dat zij gebruiken, ook al lijkt de indeling van "systemen met hun gebruikers" heel plausibel.

Op het vlak van de organisatie en procedures moet zijn geregeld tot wiens bevoegdheid het behoort om te bepalen "wat mag". Er zijn vele oplossingen mogelijk: de lijnchefs, de beveiligingsfunctionaris of de systeemhouder. Een opzet waarbij de lijnchef aanvraagt, de systeemhouder goedkeurt en de beveiligingsfunctionaris controleert en aanbrengt blijkt in de praktijk te werken. De controle van de

beveiligingsfunctionaris betreft de formele goedkeuring van de aanvraag en de vaststelling dat bevoegdheden alleen binnen de spelregels worden uitgegeven. Een systeemontwikkelaar bijvoorbeeld heeft geen bevoegdheden op produktiegegevens en aangevraagde bevoegdheden mogen niet strijdig zijn met reeds bestaande bevoegdheden. Tevens moet inhoud worden gegeven aan onafhankelijke controle op de verrichtingen van de beveiligingsfunctionaris.

OBJECT VAN BEVEILIGING

Behandeld wordt de wijze waarop bepaald wordt wat het voorwerp van beveiliging zal zijn. Er worden kanttekeningen geplaatst bij aanlogprocessen, de reikwijdte van de beveiliging en bij de volledigheid van de beveiliging.

Beveiligingsbeleid

Bij aanvang van de implementatie dient duidelijk voor ogen te staan wat men met beveiliging nastreeft. Dit dient vast te liggen in het beveiligingsbeleid en zal in grote lijnen neerkomen op het beveiligen van:
- de aanlogprocedure (gebruikersidentificatie en -authenticatie);
- de toegang tot resources;
- het gebruik van faciliteiten, programma's en schijfcapaciteit.

Aanlog

Het is aan te bevelen de bestaande aanlogprocedure kritisch onder de loep te nemen. Het is niet onwaarschijnlijk dat hieruit de conclusie naar voren komt dat het aanlogproces verschilt per omgeving en per faciliteit. Hierbij kunnen wisselende spelregels worden gehanteerd, bijvoorbeeld ten aanzien van de opbouw en geldigheidsduur van passwords.
De volgende aanlogprocedures kunnen voorkomen:
- aan netwerk- en terminal-besturings-software;
- aan een session-manager;
- aan systeem-services (bijvoorbeeld databasepakketten, time-sharing-pakketten en teleprocessing-monitoren);
- aan gekochte en zelf gemaakte applicaties.

In de meeste gevallen tikt de gebruiker zijn user-id en password in en wordt dit gecontroleerd aan de hand van verschillende tabellen.
Het is aan te bevelen ook de aanlogprocedures zoveel mogelijk te laten afwikkelen door het centrale pakket en niet door "lokale" software. In de subparagraaf Encryptie is aangegeven waarom dit belangrijk is.

Resources

Het beveiligingsbeleid dient aan te geven welke resource-typen de moeite waard zijn om beveiligd te worden. In het algemeen zal het beveiligingspakket een groot aantal te beveiligen resource-typen standaard leveren. De verleiding is groot om deze allemaal te gebruiken, maar enige beperking is aan te bevelen. Overdaad schaadt. De noodzaak om voor al het mogelijke beveiliging te bieden zal niet altijd aanwezig zijn.
Een goed pakket biedt de mogelijkheid resource-typen toe te voegen, zodat de beveiliging op maat kan worden gemaakt.
Gangbare resource-typen zijn:
- bestanden;
- programma's;
- jobs;
- schijfruimte;
- terminals.

In de situatie dat het beleid voorschrijft dat bestanden beveiligd dienen te zijn tegen ongeoorloofde benadering, komt de vraag naar voren of dit voor alle bestanden het geval moet zijn. (Dit is een ander probleem als de "fijnmazigheid" die in de paragraaf Implementatiestrategie is behandeld.) Het is denkbaar dat bestanden aanwezig zijn die de moeite van het beveiligen niet waard zijn. In deze situatie ligt het min of meer voor de hand te kiezen voor selectieve resource-beveiliging, maar hier schuilt een addertje onder het gras.
In de eerste plaats blijkt het zeer moeilijk de verantwoordelijkheid voor de selectie te dragen. Wie geeft aan welke bestanden niet beveiligd hoeven te worden?
In de tweede plaats brengt het beheer van selectief beveiligde resources veel werk met zich mee.
De praktijk wijst uit dat integrale resource-beveiliging van een bepaald type veel eenvoudiger is en daardoor te verkiezen boven selectieve beveiliging.

In dit verband wordt de aandacht gevestigd op de reikwijdte van de beveiliging van een resource-type. Resources zijn beveiligd als ze in de security-file als zodanig zijn vastgelegd. De gebruiker mag en kan datgene wat hem is toegekend. De resources die niet in de security-file zijn vastgelegd, dus niet zijn beveiligd, kan de gebruiker niet benaderen omdat zijn bevoegdheden limitatief zijn. Hij kan alleen wat hij mag.

Er ontstaat een andere situatie als het beveiligingspakket op de volgende wijze met de resource-beveiliging omgaat.
Als de bevoegdheden niet limitatief bepalend zijn, betekent dit dat alle niet-beveiligde resources vrijelijk te benaderen zijn. De gebruiker kan wat hij mag en heeft verder onbeperkte toegang tot alles wat niet beveiligd is.

De ene situatie is niet beter dan de andere. Het verschil heeft echter wel gevolgen.
In de eerste situatie, waarbij dus de resource-beveiliging zodanig is dat de bevoegdheden limitatief zijn, betekent dit dat alle resources benoemd en uitgegeven moeten zijn. Ook als die voorkomen in de omgeving van systeemontwikkeling.
In de tweede situatie, waarbij alles wat niet gedefinieerd is vrij toegankelijk is, bestaat er een voortdurende zorg voor de volledigheid van de beveiliging. Dit stelt hoge eisen aan de werking van de

change-procedure. Resources die worden toegevoegd aan een applicatiesysteem, bijvoorbeeld bij onderhoud aan dat systeem, zijn niet eerder beveiligd dan nadat ze tevens in de security-file zijn opgenomen.

De mogelijkheid om resources te beveiligen die (nog) niet bestaan lijkt handig bij de implementatie. Het betekent echter dat er geen directe relatie is tussen de "werkelijk te beveiligen" resources en de definities in de security-file. Om vervuiling van de security-file te voorkomen zullen goede procedures voor het change-proces in het bedrijf aanwezig moeten zijn.

BEVEILIGING, INTERNE CONTROLE EN SYSTEEMBEHEER

In deze paragraaf wordt aandacht geschonken aan de vraag hoe men beveiliging kan hanteren ter ondersteuning van interne controle in systemen en van het beheer van systemen en wat voor deze relatie bepalende factoren zijn.

Beveiliging en interne controle

Beveiligen van een systeem is het beschermen tegen onheil. Dit onheil kan van buiten en van binnen dat systeem komen. Bij het beschermen van een systeem tegen van binnen komend onheil wordt de effectiviteit onder meer bepaald door de mate waarin beveiliging de interne controle kan ondersteunen. In een ongunstig geval kan het zo zijn dat de interne controle dermate slecht is opgezet dat de beveiliging onvoldoende ondersteuning kan bieden. Dit is een probleem van interne controle en niet van beveiliging.
Een voorbeeld. Als een systeem verschillende functies kent kan het nuttig zijn hiertussen scheiding aan te brengen. Of dit nodig is, wordt bepaald door aspecten van interne controle en niet van beveiliging. Als dit nodig en mogelijk is kan het beveiligingspakket de interne controle ondersteunen door de scheiding te realiseren. De scheiding hoeft dan niet "procedureel" te worden geregeld maar het beveiligingspakket dwingt dit af.
Beveiliging en interne controle dienen hetzelfde belang: het handhaven van een goed werkend systeem. Beveiliging en interne controle kunnen elkaar ondersteunen, maar ook danig in elkaars vaarwater zitten.

Als het om zuivere beveiligingszaken gaat moet van het pakket worden verwacht dat het in beveiliging conform de richtlijnen voorziet. Als het gaat om aspecten van interne controle kan de werking van het pakket alleen ondersteunend zijn. Er mag van worden uitgegaan dat de interne controle van het systeem goed is opgezet en correct wordt beheerd. Daaraan kan een beveiligingspakket geen bijdrage meer leveren.

In een ideale situatie moeten alle functies en alle resources van een systeem voor het beveiligingspakket herkenbaar zijn. Tevens moet de werking van de beveiliging zich ook daadwerkelijk uitstrekken tot het voorkómen van ongeoorloofde acties. Het mag niet zo zijn dat het systeem het beveiligingspakket slechts als adviseur raadpleegt en zelfstandig beslist wat met de mening van het beveiligingspakket wordt gedaan.
In een ideale situatie kan het beveiligingspakket naadloos voorzien in ondersteuning van de interne controle. Dit is afhankelijk van de discipline die bij de opzet van de interne controle is betracht.
Bij de implementatie van een beveiligingspakket moet worden stilgestaan bij de vraag of en in hoeverre beveiliging de interne controle moet en kan ondersteunen.

Beveiliging en systeembeheer

Onder "systeembeheer" wordt in dit verband verstaan het "beheer van de te beveiligen systemen". Niet te verwarren met het beheer van het beveiligingspakket zelf, ook wel aangeduid met "security administration".

Overeenkomstig de situatie in de vorige subparagraaf kan er sprake zijn van een "territoriaal" conflict tussen beveiliging en systeembeheer, hetgeen erop neerkomt dat moet worden uitgevochten "wie" verantwoordelijk is voor "wat".

In de security-file is informatie vastgelegd die onder meer betrekking heeft op gebruikers, afdelingen en systemen. Tevens neemt het beveiligingspakket in de technische infrastructuur een centrale plaats in, waardoor het in het algemeen een goede communicatiefaciliteit biedt voor andere software en applicaties.

Een bruikbaar beveiligingsbeleid, waarin onder meer staat wat het object van beveiliging en de grenzen van beveiliging moeten zijn, is onmisbaar.

Het beheer van de beveiliging (security administration) kan met zijn centrale en decentrale opzet een in het bedrijf herkenbare en stabiele rol vervullen.
Door deze aantrekkelijke factoren kunnen het beveiligingspakket en security administration worden ingezet voor bedrijfsdoelstellingen die niet op beveiliging maar zuiver op beheer zijn gericht.

Voorbeeld
De mogelijkheid is aanwezig om bij de gebruikersgegevens in de security-file tevens gegevens op te nemen over de account-code, de postcode en het printer-adres van de gebruiker. Via de bestaande procedure (security administration) kan tevens het change-management van deze gegevens worden uitgevoerd. De accounting-, de nabewerkings- en de spooler-software raadplegen de security-file door middel van de standaard met het beveili-

J.H. Diekema
Is sedert 1985 werkzaam bij de Kas-Associatie N.V. te Amsterdam. Hij was belast met de implementatie van beveiliging in het DOS/VSE- en MVS-besturingssysteem. Momenteel is hij verantwoordelijk voor de coördinatie en het beheer van de geautomatiseerde gegevensbeveiliging. Hij is lid van de sectie Beveiliging van het NGFI.

gingspakket meegeleverde of de zelf geschreven communicatieprogramma's. Het betreft geen gegevens die uit het oogpunt van beveiliging belangrijk zijn, maar het gaat om stuurgegevens. Het beheer van deze stuurgegevens maakt echter deel uit van security administration.

Of het uitoefenen van deze oneigenlijke taak nu wenselijk is of niet, is aan elk bedrijf zelf ter beoordeling. Het management zal hierover beslissingen moeten nemen. Bij het implementeren van een beveiligingspakket moet het vraagstuk "wat wel" en "wat niet" de beveiliging zal betekenen en waar de grenzen liggen, duidelijk zijn.

TOT SLOT

In het voorgaande is een indruk gegeven van de ervaringen die werden opgedaan bij de implementatie van een beveiligingspakket.
Behalve kennis van de werking van het beveiligingspakket is het belangrijk dat een diepgaand inzicht bestaat in de inrichting van de automatisering van het bedrijf.
Een bruikbaar beveiligingsbeleid, waarin onder meer staat wat het object en de grenzen van beveiliging moeten zijn, is onmisbaar.
Het succes van de implementatie is echter niet alleen hiervan en van de geleverde inspanning afhankelijk. Slechte automatisering is namelijk niet goed te beveiligen. Ook de kwaliteit van de bestaande automatisering blijkt een bepalende factor.

Of een falende implementatie van beveiliging (mede) haar oorzaak zou kunnen vinden in een gebrekkige automatisering en of, anderzijds, aan succesvolle implementatie een indruk is te ontlenen over de kwaliteit van de automatisering, laat ik gaarne ter overweging aan de lezer over.

EDP AUDITORIUM

In Europa worden de krachten gebundeld om te komen tot een eigen - en beter toepasbare - versie van de Amerikaanse beveiligingsstandaarden van het Orange book. Besproken wordt de in juni van dit jaar verschenen "ITSEC"-standaard versie 1.2, die twee jaar op proef zal worden gebruikt. (Wederzijdse) authenticatie in netwerkomgevingen levert vaak problemen op; door het Massachusetts Institute of Technology is in samenwerking met IBM en DEC een produkt ontwikkeld dat hiervoor een oplossing kan bieden en dat reeds wordt toegepast in UNIX-omgevingen.
Al sinds de introductie van de DES-standaard voor cryptografische beveiliging is scepsis geuit over de "onbreekbaarheid" van deze beveiliging. Ingegaan wordt op enkele recente krante-artikelen en andere ontwikkelingen, en de betekenis hiervan voor DES-gebruikers.
Tot slot wordt in deze rubriek een korte samenvatting gegeven van de oraties van de twee pas benoemde hoogleraren EDP-auditing, prof. H.B. Moonen RA en prof. drs. H.C. Kocks RA. Laatstgenoemde geeft nog een korte reactie op de samenvatting van zijn rede.

ITSEC - WAT DOEN WIJ ERMEE?

J. Brinkman

In juni 1991 is versie 1.2 van de Europese Information Technology Security Evaluation Criteria (ITSEC) beschikbaar gekomen.
In het kader van dit themanummer wordt kort ingegaan op de waarde van dit document en de bruikbaarheid in het EDP-audit-vakgebied.

Inleiding

ITSEC zijn criteria op basis waarvan de beveiliging van produkten en systemen van Informatietechnologie (IT) kan worden geëvalueerd. Beveiliging heeft betrekking op de integriteit, geheimhouding en beschikbaarheid van informatie.
Zowel IT-produkten als IT-systemen kunnen onderwerp van evaluatie zijn. Een IT-produkt is een pakket hard- en/of software dat geschikt is voor het gebruik in IT-systemen. Onder een IT-systeem wordt in dit verband een specifieke IT-installatie met haar operationele omgeving bedoeld. Hieronder vallen naast alle technische maatregelen ook de met het IT-systeem samenhangende fysieke, personele en procedurele maatregelen. Het voordeel van een dergelijke benadering is dat de opname van gecertificeerde IT-produkten in een te certificeren IT-systeem kan leiden tot een versnelde en vereenvoudigde certificering.
In het ITSEC-document wordt onderscheid gemaakt tussen een drietal instanties, waarvan ook de verantwoordelijkheden zijn vastgelegd:
- de sponsor van het evaluatieproces (dit is de instantie die het IT-produkt of IT-systeem ter evaluatie aanbiedt);
- de ontwikkelaar (*developer*) van het IT-produkt of IT-systeem;
- de instantie belast met de evaluatie (*evaluator*).

De met het IT-produkt of IT-systeem gewenste beveiliging dient voor aanvang van een evaluatie te worden vastgelegd in een *security target*. Dit is een door de ontwikkelaar en/of sponsor opgesteld document waarin het volgende is vastgelegd:

- een beveiligingsstrategie (*security policy*) voor het IT-systeem of een beveiligingsdoelstelling (*product rational*) voor het IT-produkt;
- een specificatie van de vereiste beveiligingsfuncties (*security functions*) waarmee de beveiliging wordt afgedwongen (het *claims document*);
- eventueel een vastlegging van de vereiste beveiligingsmechanismen (*security mechanisms*);
- een claim voor het evaluatieniveau;
- een claim voor de minimumsterkte van de mechanismen.

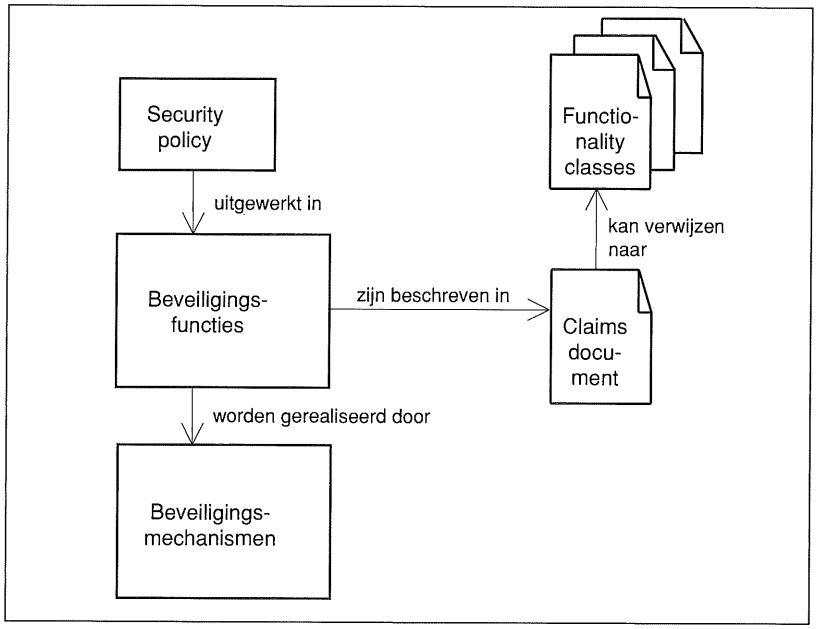
De evaluatie vindt uiteindelijk plaats door vast te stellen dat de claims van de laatste twee punten terecht zijn. De vijf elementen van de security target worden hieropvolgend nader toegelicht.

Beveiligingsstrategie
De beveiligingsstrategie beschrijft hetgeen met de beveiliging moet worden bereikt en hoe dat kan worden bereikt. Dit wordt ook wel de technical *security policy* genoemd. Eventueel kan een formeel beveiligingsmodel worden gebruikt. Voorbeelden hiervan zijn:

- het Bell-LaPadula-model voor toegangsbeheersing bij produkten of systemen waaraan hoge vertrouwelijkheidseisen worden gesteld;
- het Clark- en Wilson-model voor commerciële transactieverwerkende systemen waarbij hoge eisen worden gesteld aan de integriteit van informatie.

Beveiligingsfuncties
De beveiligingsfuncties zijn de diensten die door het IT-produkt of IT-systeem worden geboden om de beveiligingsdoelstelling te realiseren. Belangrijk hierbij is de zekerheid te hebben dat deze functies (of diensten) de beveiligingsdoelstelling afdwingen. Deze functies worden vastgelegd in het claims document.

Beveiligingsmechanismen
Beveiligingsmechanismen zijn de onder de func-



Figuur 1. Het security target.

ties liggende technieken en mechanismen die worden gebruikt om de beveiligingsfuncties te realiseren.

Evaluatieniveau
De instantie die is belast met de evaluatie, zal moeten vaststellen of het evaluatieniveau overeenkomt met de claim in de security target. Dit wordt ook wel met de correctheid van de beveiliging aangeduid.

Minimumsterkte van de mechanismen
Ook hier zal de instantie die is belast met de evaluatie moeten vaststellen of de sterkte van de mechanismen overeenkomt met de claim. Dit wordt de effectiviteit van de beveiliging genoemd.

Historie ITSEC

De ITSEC zijn ontstaan doordat Engeland, Frankrijk, Duitsland en Nederland besloten op het gebied van evaluatie van de beveiliging van IT te gaan samenwerken en te streven naar geharmoniseerde criteria voor het certificeren van beveiligingssystemen. Drie redenen hebben hiertoe bijgedragen:

- het grote voordeel dat bundeling van de in verschillende landen aanwezige schaarse expertise zou opleveren;

- de industrie die aangaf niet in elk land met andere beveiligingscriteria te willen worden geconfronteerd;

- de overeenstemming die reeds bestond tussen de verschillende basisconcepten en ideeën in de verschillende landen.

Deze samenwerking resulteerde in mei 1990 tot ITSEC-versie 1.0. ITSEC is gedeeltelijk gebaseerd op standaarden die reeds in de deelnemende landen beschikbaar waren.
Het initiatief is hierna overgenomen door de Europese Commissie, die op haar beurt in het kader van de Europese eenwording streeft naar uniforme criteria voor IT-security.

In september 1990 is een conferentie gehouden waarop ITSEC-versie 1.0 door ongeveer vijfhonderd experts is besproken. Het commentaar van deze experts leidde in januari 1991 tot ITSEC-versie 1.1. Deze versie was bedoeld als een interimversie, waarin reeds de belangrijkste commentaren waren verwerkt.
Momenteel is ITSEC-versie 1.2 beschikbaar. In deze versie zijn ruim vijfhonderd geschreven commentaren op versie 1.1 verwerkt. Deze versie zal twee jaar op proef worden gebruikt, waarna een evaluatie van de bruikbaarheid van het ITSEC-document is gepland.

Claims document

Centraal in de evaluatie staat de *Target of Evaluation* (TOE). Deze TOE bevat alle hardware, programmatuur en gegevens die verantwoordelijk zijn voor het in stand houden van de beveiliging. De functionaliteit van deze TOE wordt exact omschreven in het claims document. Hiervoor is een formele taal ontwikkeld, die aan een in het ITSEC-document voorgeschreven syntax moet voldoen, maar zich laat lezen als gewone taal (claims language).

In dit document moeten de te beschrijven claims onder de volgende rubrieken vallen:
- *identification and authentication* (identificatie en authenticatie van gebruikers);
- *access control* (toegangsbeheersing van gebruikers en processen);
- *accountability* (vastlegging van beveiligingsrelevante gebeurtenissen zodat deze tot de gebruiker kunnen worden herleid);
- *audit* (vastlegging van de overige beveiligingsrelevante gebeurtenissen);
- *object reuse* (hergebruik van objecten zonder aantasting van de beveiliging);
- *accuracy* (integriteit van gegevens tijdens overdracht binnen het IT-systeem);
- *reliability of service* (beheersing van tijdkritische processen);
- *data exchange* (gegevensuitwisseling). Data exchange is conform de OSI-standaarden weer onderverdeeld in:
  - authentication;
  - access control;
  - data confidentiality;
  - data integrity;
  - non-repudiation.

De mogelijkheid bestaat in een claims document te refereren aan één of meer standaardverzamelingen van claims. Zulke standaardverzamelingen worden functionality classes genoemd. In het ITSEC-document is een aantal voorbeelden van dergelijke functionality classes opgenomen. Deze voorbeelden zijn zowel ontleend aan de klassen die genoemd zijn in de *Trusted Computer System*

Evaluation Criteria (TCSEC, ook bekend als Orange book) van het Amerikaanse Department of Defense als aan enkele additionele klassen. Onderstaand worden deze kort toegelicht:

– *Example Functionality Classes F-C1, F-C2, F-B1, F-B2, F-B3:* afgeleid van de overeenkomstige TCSEC-klassen, waarbij F-B3 een combinatie is van B3 en A1 van TCSEC.

– *Example Functionality Class F-IN:* in het leven geroepen voor TOE's met hoge integriteitsvereisten (*INtegrity*). Vooralsnog zijn hierin slechts de eisen met betrekking tot de *accountability* verder uitgewerkt.

– *Example Functionality Class F-AV:* stelt hoge eisen aan de beschikbaarheid van de TOE (*AVailability*). Met name de eisen ten aanzien van de *reliability of service* zijn in deze klasse uitgewerkt.

– *Example Functionality Class F-DI:* hoge eisen aan de TOE ten aanzien van de integriteit van gegevens (*Data Integrity*) tijdens transport. Eisen in deze klasse hebben vooral betrekking op het onderdeel *data integrity* van de rubriek *data exchange* en de rubriek *accountability*.

– *Example Functionality Class F-DC:* bedoeld voor TOE's waaraan hoge eisen worden gesteld ten aanzien van de geheimhouding van gegevens (*Data Confidentiality*) tijdens transport. Hierin is het onderdeel *data confidentiality* van de rubriek *data exchange* nader uitgewerkt.

– *Example Functionality Class F-DX:* bedoeld voor TOE's met eisen aan zowel de integriteit als de geheimhouding van gegevens tijdens transport (*Data eXchange*). Deze klasse is een combinatie van de klassen F-DI en F-DC.

De onderlinge relatie tussen beveiligingsstrategie, beveiligingsfuncties, beveiligingsmechanismen, claimsdocument en functonality classes is weergegeven in figuur 1.

Evaluatiecriteria - correctheid

De beveiligingsfuncties zijn de diensten die door de TOE worden geboden om de beveiligingsdoelstelling te realiseren. Men kan zich hierbij afvragen of de functies deze doelstelling afdwingen. Dit wordt door de ITSEC de correctheid van de zekerheid (*Assurance - correctness*) genoemd. Voor de mate van correctheid worden zeven evaluatieklassen (E0 tot en met E6) onderscheiden. In figuur 2 is aangegeven welke specifieke eisen gelden voor de genoemde evaluatieklassen. De karakteristieken van deze klassen kunnen als volgt worden omschreven:

– E0: dit niveau geeft aan dat er onvoldoende bewijs aanwezig is.

– E1: op dit niveau dient er een security target te zijn en een informele beschrijving van de beveiligingsarchitectuur. Functionele tests zullen moeten aantonen dat de TOE voldoet aan de security target.

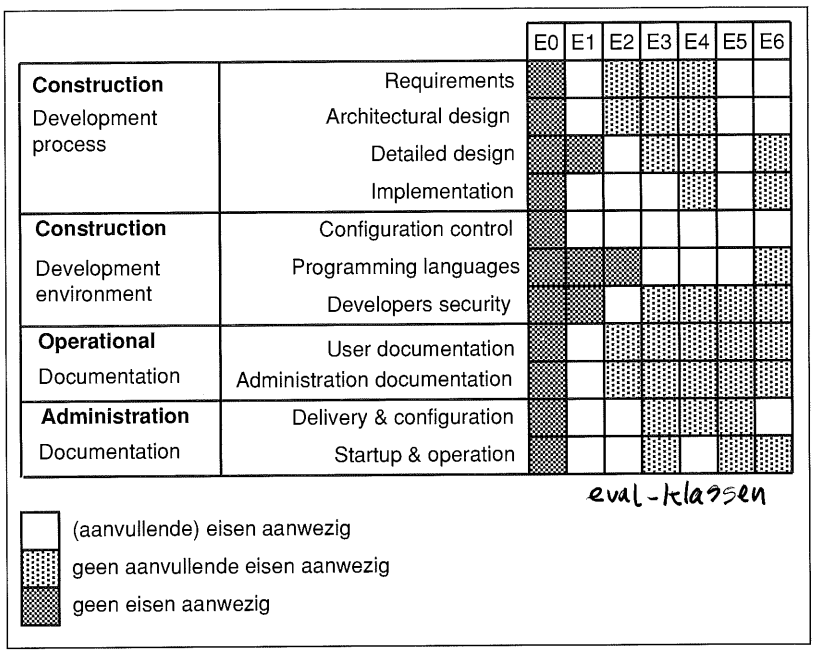
– E2: aanvullend op E1 dient er een informele beschrijving van het detailontwerp te zijn. Er dient bij de ontwikkeling een configuratiebeheersingssysteem te worden gebruikt en er moet een goedgekeurde distributieprocedure zijn.

– E3: ook de broncode van de programmatuur en/of de hardware-tekeningen die corresponderen met de beveiligingsmechanismen worden geëvalueerd. Bewijsstukken met gegevens over de test van deze mechanismen worden tevens in de evaluatie betrokken.

– E4: op dit niveau dient tevens een formeel model van de ondersteunde beveiligingsstrategie aanwezig te zijn. De functies die de beveiliging afdwingen, het architectuurontwerp en het detailontwerp moeten in een semi-formele stijl zijn gespecificeerd.

– E5: dit niveau vereist dat er een nauwe overeenkomst bestaat tussen het detailontwerp en de broncode van de programmatuur en/of de hardware-tekeningen.

– E6: de beveiligingsfuncties en het architectuurontwerp moeten in een formele stijl worden gespecificeerd, en moeten consistent zijn met het gespecificeerde model van de beveiligingsstrategie.



Figuur 2. Eisen met betrekking tot de Assurance - correctness.

Voor elk van de in figuur 2 aangegeven aspecten wordt in het ITSEC-document vermeld wat de vereisten zijn voor de inhoud, presentatie en op te leveren bewijs; daarnaast wordt vermeld welke activiteiten de evaluator moet ondernemen.

Evaluatiecriteria - effectiviteit

Nadat de correctheid is geëvalueerd, vindt een evaluatie plaats van de kracht van de voor de TOE gebruikte beveiligingsmechanismen. Deze kracht wordt in het ITSEC-document de effectiviteit van de zekerheid (*Assurance - effectiveness*) genoemd en wordt aan de hand van de volgende aspecten bepaald:

– de geschiktheid van de beveiligingsrelevante functies om de bedreigingen zoals vastgelegd in de security target te weerstaan;

– de mogelijkheid van de beveiligingsrelevante functies om elkaar wederzijds aan te vullen en te versterken zodat een geïntegreerd en effectief geheel ontstaat;

– de mogelijkheid van de beveiligingsmechanismen om een directe aanval te weerstaan;

– het feit of de bekende beveiligingszwakheden *in de constructie* van de TOE in de praktijk de beveiliging van de TOE kunnen aantasten;

– de garantie dat de TOE niet kan worden geconfigureerd of gebruikt op een manier die niet veilig is, maar een security administrator of gebruiker de indruk geeft wel veilig te zijn;

– het feit of de bekende beveiligingszwakheden *tijdens de werking* van de TOE in de praktijk de beveiliging van de TOE kunnen aantasten.

Het ITSEC-document maakt onderscheid tussen een basis (*basic*), gemiddelde (*medium*) en hoge (*high*) minimale sterkte van de kritieke mechanismen. Onderscheidend is de weerstand van het mechanisme tegen een opzettelijke aanval:

– *Basic.* De minimumsterkte van een mechanisme wordt als basic geclassificeerd indien het tegen onopzettelijke inbreuken is beschermd. Het is echter mogelijk dat het mechanisme niet tegen een opzettelijke aanval is beschermd.

– *Medium.* Indien het mechanisme bescherming biedt tegen aanvallers met beperkte mogelijkheden of hulpbronnen, wordt een classificatie medium toegekend.

– *High.* Deze classificatie is van toepassing als het mechanisme bescherming biedt tegen aanvallers met een hoge kennisgraad en uitgebreide mogelijkheden of hulpbronnen. Een succesvolle aanval kan worden gekarakteriseerd als iets wat normaal gesproken niet voorkomt.

Figuur 3. Eisen met betrekking tot de Assurance - effectiveness.

		B	M	H
Construction	Suitability of Functionality			
	Binding of Functionality			
	Strength of Mechanisms			
	Construction vulnerability Assessment			
Operation	Ease of Use			
	Operational vulnerability Assessment			

(aanvullende) eisen aanwezig
geen aanvullende eisen aanwezig
geen eisen aanwezig

Toepasbaarheid ITSEC

Wat heeft een EDP-auditor nu aan de ITSEC? ITSEC kan in twee situaties bruikbaar zijn:
1. bij de audit van een onderzoeksobject waarvan IT-systemen of IT-produkten met een ITSEC-certificaat deel uitmaken;
2. bij het beoordelen van IT-produkten of IT-systemen waarbij gebruik kan worden gemaakt van (delen van) de ITSEC.

Ad 1.
Wanneer de auditor IT-systemen of IT-produkten beoordeelt die een IT-certificaat hebben gekregen, kan hij nuttig gebruik maken van dit certificaat. Hierbij is echter inzicht in het claims document noodzakelijk. De evaluatie heeft immers betrekking op de in het claims document gestelde beweringen. Het is heel wel mogelijk dat een gunstig certificaat (E6/high) wordt gegeven aan een TOE met een zeer beperkte functionaliteit. Het is dus noodzakelijk zowel het certificaat als het claims document te kennen voordat de waarde van het certificaat kan worden bepaald.

Ad 2.
Delen van de ITSEC zijn zeker bruikbaar voor de EDP-auditor. Hierbij valt te denken aan het gebruik van de claims language voor het vastleggen van de normstelling. Een waarschuwing is hierbij echter op zijn plaats. Het gebruik van (delen van) de ITSEC kan tot gevolg hebben dat bij de opdrachtgever verwachtingen worden gewekt die door de EDP-auditor niet kunnen worden waargemaakt.
Voor certificering volgens ITSEC is het namelijk noodzakelijk inzicht te hebben in het ontwikkelingsproces, zodat de ontwikkelaar bij het evaluatieproces betrokken moet zijn. Dit is een situatie die zich bij de gemiddelde EDP-audit niet vaak zal voordoen.
Daarnaast is een aanzienlijke hoeveelheid expertise en mankracht voor een evaluatie vereist, en moet rekening worden gehouden met een aanmerkelijke tijdsduur van de evaluatie. Hoewel het moeilijk is hier enige indicatie te geven, is een tijdsduur van tien manjaar en een doorlooptijd van één jaar of meer voor een evaluatieproces geen uitzondering.

Conclusies

De ITSEC zijn een grote verbetering ten opzichte van de reeds langer (1985) beschikbare TCSEC. In de ITSEC wordt - in tegenstelling tot de TCSEC - een helder onderscheid gemaakt tussen kwaliteit

van de beveiligingsfuncties en de kracht van de beveiligingsmechanismen.
Het ITSEC-document biedt tevens de mogelijkheid om voor commerciële bedrijven aantrekkelijker beveiligingsmodellen te gebruiken dan het in de structuur van de TCSEC ingebakken - specifiek op geheimhouding gerichte - Bell-LaPadula-model.
Deze verbetering is het gevolg van de ontwikkelingen in het vakgebied en de daaruit voortvloeiende actuelere visie op de evaluatie van beveiliging.
De overeenkomsten en verschillen tussen beide evaluatiecriteria zijn in figuur 4 uiteengezet.

TCSEC	ITSEC	
	Functionality class	Evaluation level
D	-	E0
C1	F-C1	E1
C2	F-C2	E2
B1	F-B1	E3
B2	F-B2	E4
B3	F-B3	E5
A1	F-B3	E6

Figuur 4. De relatie tussen TCSEC en ITSEC.

De functionality classes in het ITSEC-document zijn - afgezien van de uit het Orange book afkomstige functionality classes - nog slechts zeer beperkt uitgewerkt. Tevens is inhoudelijk over deze functionality classes nog geen overeenstemming bereikt. Dit heeft tot gevolg dat het nut van het gebruik van deze klassen momenteel beperkt van aard is. Tevens kan worden getwijfeld aan de volledigheid van de in de functionality classes opgenomen beschrijvingen. Het is jammer dat de voor de commerciële omgeving interessante F-IN momenteel nog onvoldoende is uitgewerkt; met name de rubriek integrity heeft nog geen uitwerking gekregen. Naar verwachting zullen de functionality classes in de toekomst verder worden ingevuld en daarna gestandaardiseerd.

De structuur en opbouw van het ITSEC-document is gedegen en doordacht. Derhalve zou deze structuur als uitgangspunt voor soortgelijke documenten kunnen dienen.

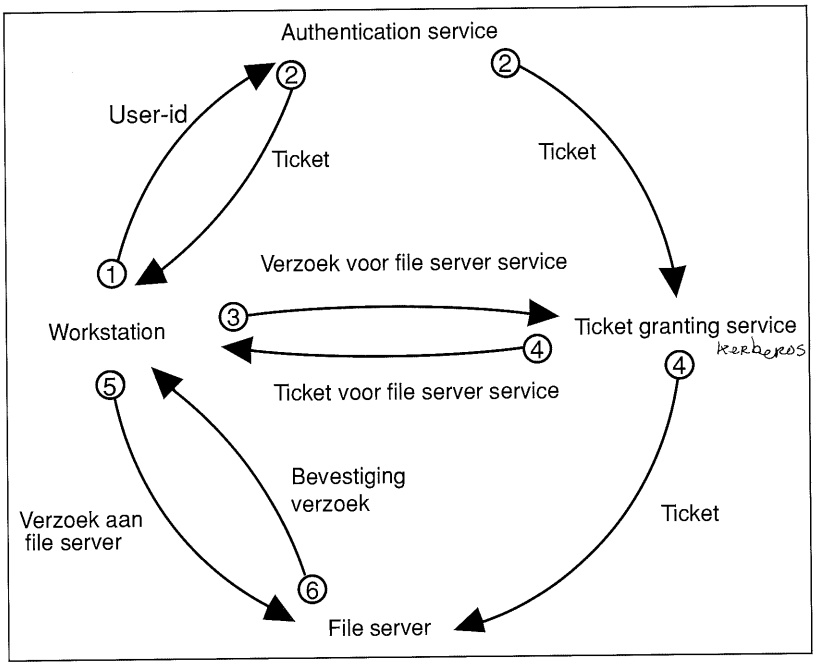
Resumerend kan worden gesteld dat de ITSEC - die in de huidige vorm voor twee jaar ter evaluatie beschikbaar zijn - een significante verbetering zijn ten opzichte van de bestaande evaluatiecriteria. Met name de flexibiliteit in de te kiezen security policy draagt bij tot een grote flexibiliteit van de ITSEC-standaarden.
Dit impliceert dat ITSEC ook in de toekomst de evaluatie van systemen en produkten mogelijk maakt, onafhankelijk van de dan prevalerende beveiligingsmodellen.

AUTHENTICATIE IN EEN NETWERK

P. Kornelisse

Authenticatie van gebruikers in een netwerkomgeving is moeilijk. Hoe weet een server zeker dat een gebruiker inderdaad is wie hij zegt dat hij is? En omgekeerd, hoe weet een gebruiker dat een server inderdaad de server is die hij wil benaderen?

In het begin van de tachtiger jaren beschikte het Massachusetts Institute of Technology (MIT) over vele workstations en servers, die via een netwerk met elkaar in verbinding stonden. Door de toename van het aantal computers werd het steeds moeilijker deze betrouwbaar te authenticeren. Een oplossing bleek noodzakelijk: het MIT ontwikkelde samen met IBM en DEC het authenticatieprotocol Kerberos.
Ten behoeve van Kerberos wordt in het netwerk een server geplaatst, die de correcte authenticatie van gebruikers en servers garandeert. Deze server verstrekt tickets (toegangskaartjes) aan gebruikers en servers: alleen met een geldig ticket mag een gebruiker vervolgens een server benaderen. Op het moment dat een gebruiker een ticket voor het benaderen van een server aanvraagt, ontvangt de server hiervoor ook een ticket. Elk van de twee tickets (voor de gebruiker en voor de server) bevat versleuteld een session-key. Met behulp van deze session-key kunnen de twee via vercijferd berichtenverkeer met elkaar communiceren.
Onderstaand wordt een voorbeeld gegeven van een sessie waarbij een gebruiker inlogt op een workstation, en vervolgens een (file) server benadert (figuur 1).



Figuur 1. Verstrekking van tickets bij een sessie.

De gebruiker identificeert zichzelf bij een willekeurig (vertrouwd) workstation in het netwerk, waarbij hij behalve zijn user-id ook zijn password

invoert. Authenticatie vindt vervolgens plaats door over het netwerk aan de authentication service van Kerberos de user-id te versturen (1). De authentication service, die beschikt over de tabel met user-id/password-combinaties, stuurt vervolgens een ticket terug naar het workstation, versleuteld met het password van de gebruiker (2). Het workstation zal daarna met het ingevoerde password van de gebruiker het ticket ontcijferen.
Tegelijkertijd wordt door de authentication service een ticket naar de ticket granting service van Kerberos gestuurd, versleuteld met het password van de ticket granting service. Via de beide tickets wordt een session-key voor de gestarte sessie aan beide partijen doorgegeven.
Op een bepaald moment zal de gebruiker bestanden van de file server willen benaderen. Hiervoor dient eerst een ticket te worden verkregen: het workstation stuurt een versleutelde boodschap aan de ticket granting service, waarbij het verzoekt de file server te mogen benaderen (3). Dit verzoek wordt versleuteld met de session-key verstuurd.
De ticket granting service controleert de autorisatie, en stuurt na akkoordbevinding aan het workstation een ticket voor het benaderen van de file server (4). Tegelijkertijd wordt aan de file server een ticket verstuurd (versleuteld met de key van de file server) waarmee de gebruiker van het workstation wordt geautoriseerd tot het benaderen van de file server. In de versleuteld verstuurde tickets is een file service session-key opgenomen, die wordt toegepast voor de sessie tussen het workstation en de file server.
Via de verkregen file service session-key benadert het workstation de file server (5). Bij gebruik van de correcte file service session-key zal de file server geoorloofde verzoeken van het workstation honoreren (6).

Met het Kerberos-protocol is het dus mogelijk met wederzijdse authenticatie volledig versleuteld transport toe te passen. Indien men voor een service (file, mail, printer) Kerberos wil benutten, dient dit voor elke service afzonderlijk te worden geïmplementeerd; hierbij dient het besturingssysteem te worden aangepast. Kerberos wordt reeds toegepast bij een aantal UNIX-varianten (onder andere Ultrix van DEC), andere zullen tot toepassing overgaan (onder andere OSF/1).
De Kerberos-server moet volledig fysiek en logisch worden afgeschermd. De betrouwbaarheid van Kerberos wordt uiteindelijk begrensd door de mate van beveiliging van de workstations, waarop inloggen plaatsvindt.

DES GEKRAAKT?

Drs. T. de Vries

Begin oktober 1991 meldden de New York Times en de Daily Telegraph dat het op grote schaal door voornamelijk banken en financiële instellingen gebruikte encryptie-algoritme "Data Encryption Standard" (DES) zou zijn gebroken.

DES is rond 1974 ontwikkeld door IBM en sinds die tijd algemeen aanvaard als één van de meest bruikbare vercijferingsalgoritmen.
Gedurende de gehele levensloop van DES zijn regelmatig artikelen verschenen die structurele zwakheden in het algoritme bespraken. Tevens werd kritiek uitgeoefend op het feit dat de ontwikkelcriteria niet openbaar waren gemaakt.
Voor zover bekend is het echter niet gelukt DES te kraken. De enige bekende aanvallen berusten op de methode van slim proberen totdat de gebruikte sleutel is gevonden (exhaustive search). Deze methode neemt echter onevenredig veel tijd in beslag.

Op de conferentie Securicom '90 toonde de bekende Israelische wiskundige professor Adi Shamir dat hij in staat is, met behulp van een PC, de sleutel te vinden indien hij kan beschikken over gekozen klare tekst en bijbehorende vercijferde tekst (choosen plaintext attack).
Hij deed dit echter voor een afwijkende DES die slechts zes iteraties uitvoerde, terwijl de standaard-DES uit zestien iteraties bestaat. Algemeen bekend is dat bij toename van het aantal iteraties de benodigde zoektijd exponentieel oploopt. Het kraken van een DES met zestien iteraties werd dan ook als te tijdrovend gezien.

Naar verluidt zijn Adi Shamir en dr. Bli Biham er nu in geslaagd deze aanval op DES met de volledige zestien iteraties succesvol af te ronden. Een beschrijving van de gevolgde methode zal op een later tijdstip door hen worden gepubliceerd.
Momenteel is (in de wandelgangen) van de methode bekend dat zij berust op een choosen plaintext attack en gebruik maakt van de zogenaamde "differentiële crypto-analyse". Dit houdt in dat door het leggen van statistische verbanden, een reductie van het aantal zoekpogingen kan worden bereikt. Deze reductie zou echter van beperkte omvang zijn, waardoor DES slechts in beperkte mate gevoeliger wordt voor exhaustive search-aanvallen.

In dit verband is het aardig om te vermelden dat Adi Shamir de medeontwerper is van het bekende asymmetrische encryptie-algoritme RSA (Rivest Shamir Adleman) en belangen heeft in een bedrijf dat het RSA-algoritme commercieel aanbiedt.

Er is geen aanleiding voor de DES-gebruiker om onmiddellijk in paniek te geraken. Hij zal zich echter wel moeten beraden of in de nabije toekomst moet worden overgegaan op het zogenaamde triple-DES. Met triple-DES wordt een verlenging van de tijdsduur benodigd voor een exhaustive search-aanval bereikt van circa zeventig procent.
Tevens kan het frequenter wisselen van belangrijke encryptie-sleutels de gevoeligheid voor een dergelijke aanval beperken.

Op langere termijn zal zeker een nieuwe standaard voor een encryptie-algoritme worden ingevoerd. Momenteel is echter niet aan te geven wanneer de invoering van een dergelijk algoritme is te verwachten.

KWALITEITSNORMEN BIJ EDP-AUDITING: EEN KRITISCHE BESCHOUWING

Drs. M.W. van Aalst

Op 27 september 1991 aanvaardde H.B. Moonen het ambt van hoogleraar EDP-auditing aan de Katholieke Universiteit Brabant. De inaugurele rede had als titel: *Kwaliteitsnormen bij EDP-auditing: een kritische beschouwing.* In zijn rede ging Moonen in op het verantwoord gebruik door EDP-auditors van kwaliteitsnormen als toetsingsmiddel. Hieronder volgt een samenvatting.

EDP-auditing anno 1991

De EDP-auditor verricht waarnemingen op het gebied van de informatievoorziening en de informatietechnologie en toetst deze aan de op dat gebied bestaande normen, de kwaliteitsnormen. Binnen deze kwalificatie constateert Moonen dat de kwaliteitstoetsing door de EDP-auditor niet eenduidig plaatsvindt door het ontbreken of onjuist hanteren van kwaliteitsnormen en doordat algemeen aanvaarde uitvoeringsstandaarden ontbreken. Bij veel uitgevoerde EDP-audits overheerst de persoonlijke visie van de EDP-auditor, zonder dat deze zich altijd verantwoordt voor de gekozen uitgangspunten en het hierbij gehanteerde normenstelsel. Debet aan de overheersende rol van het subjectieve deskundigheidselement bij de uitvoering van een EDP-audit, zijn de problemen met de voor de EDP-auditing noodzakelijke kwaliteitsnormen en uitvoeringsstandaarden. De EDP-auditors van nu realiseren zich nog onvoldoende dat zij moeten werken met kwaliteitsnormen die door de opdrachtgevers worden herkend en geaccepteerd.

Kwaliteit en kwaliteitsnormen

In een rekenkundige analyse komt Moonen tot de volgende definitie van het begrip kwaliteit: kwaliteit is het produkt van effectiviteit en efficiency. Met andere woorden, kwaliteit is de resultante van de mate waarin de beoogde resultaten worden gerealiseerd in relatie tot de mate waarin beoogde offers worden gebracht.

De kwaliteit van de EDP heeft betrekking op de in een EDP-omgeving aan de gebruikers geboden EDP-produkten en op de EDP-processen inclusief de aangewende hulpmiddelen die deze EDP-produkten opleveren. Zowel voor de aanbieder als voor de gebruiker van EDP-produkten wordt de kwaliteit van de EDP bepaald door het relateren van vooraf vastgestelde effectiviteits- en efficiency-normen aan de gemeten effectiviteit en efficiency.
Voor het beoordelen van de kwaliteit van de EDP is het daarom noodzakelijk om een methode ter beschikking te hebben waarmee de waarde van de effectiviteit en de efficiency objectief kan worden vastgesteld. Ten aanzien van de effectiviteit is het niet eenvoudig de waarde van een EDP-produkt in geld uit te drukken, omdat de aan de gebruikers aangeboden produkten zich daarvoor moeilijk lenen. Ook het rechtstreeks meten van de kwaliteitsattributen is een moeilijke zaak. Daarom zal de meetactiviteit in de meeste gevallen gericht worden op de kwaliteitssubattributen.
Ten aanzien van efficiency zijn de meetproblemen in principe minder groot. Het gebruik van activa kan worden gemeten en vertaald in geld.

In het kader van het vaststellen van kwaliteitsnormen worden de volgende normbepalingen onderkend: objectief, subjectief, wettelijk bepaald en aangedragen.

De bewaking van de kwaliteitsnormen voor EDP-processen en hulpmiddelen vindt primair plaats bij en door de organisatie en het management waar het EDP-proces plaatsvindt. Daarnaast kan de kwaliteitsnorm voor EDP-processen ook worden bepaald door anderen, zoals bijvoorbeeld de overheid en de ISO. Andere objectieve kwaliteitsnormen voor EDP-processen ontbreken nog. Deze zouden in beginsel kunnen worden ontleend aan gezaghebbende literatuur op dit gebied.
In vergelijking met de kwaliteitsnormen voor EDP-processen zijn de kwaliteitsnormen voor EDP-produkten in zijn algemeenheid eenvoudiger te bepalen. De gebruiker van een EDP-produkt geeft aan wat hij wil hebben geleverd en daarmee is de norm als toetssteen voor het door de EDP geleverde produkt gemaakt. Ook voor EDP-produkten kunnen de kwaliteitsnormen wettelijk worden bepaald of door anderen worden aangedragen. Objectief vastgestelde kwaliteitsnormen voor EDP-produkten ontbreken vooralsnog.

Normalisatie en standaardisatie worden met betrekking tot de informatietechnologie veelal ten onrechte in één adem genoemd met objectieve kwaliteitsnormen. Op het gebied van informatietechnologie is er vooral sprake van zogenaamde functionele normalisatie. Het doel van de standaardisatie is dat technieken en hulpmiddelen op meer plaatsen voor dezelfde functies bruikbaar zijn. Gezaghebbende standaarden kunnen bij gebrek aan normen in de praktijk goed worden gebruikt voor regelgeving op het gebied van begrippen, definities en kenmerken: een eerste voorwaarde voor normgeving.

De doelstelling van iedere EDP-audit in relatie tot het object van EDP-audit is bepalend voor de kwaliteitsnorm die wordt aangelegd bij de oordeelsvorming. Indien de kring van belanghebbende vooraf bekend is, kan de toetsingsnorm worden toegespitst op de specifieke situatie van de belanghebbende. In het geval de opdrachtgever voor de EDP-audit de enige belanghebbende is, zal de kwaliteitsnorm door hem worden bepaald. De ervaring van de EDP-auditor kan worden ingezet om de aangereikte kwaliteitsnormen op hun consistentie te toetsen en op basis daarvan aanpassingen en aanvullingen voor te stellen. Het kan niet de bedoeling zijn dat de EDP-auditor door de kwaliteitsnorm te bepalen op de stoel van de opdrachtgever gaat zitten. Er is in dit verband dus geen sprake van het gebruik van vaste uitgekristalliseerde normen, omdat het hier om normen

gaat waarmee de uitvoering van beleid moet worden getoetst. Beleid is per definitie subjectief. Indien de resultaten van een EDP-audit bedoeld zijn voor anderen dan de opdrachtgever, zullen objectieve kwaliteitsnormen moeten worden gehanteerd. Indien deze er niet zijn moet door de EDP-auditor worden volstaan met het meten en kwantificeren van de diverse kwaliteitsaspecten. In zijn rapportering verstrekt de EDP-auditor in dit geval de meetresultaten zonder een kwaliteitsoordeel op basis van kwaliteitsnormen te geven. Volgens Moonen kan de EDP-auditor in deze situatie niet toetsen met de door hem opgestelde kwaliteitsnormen. De reden hiervoor is dat dan de subjectieve kwaliteitsnorm van de EDP-auditor wordt verheven tot een algemeen aanvaarde, objectieve kwaliteitsnorm.

De praktijk van vandaag

De hierboven beschreven theorie wijkt volgens Moonen af van de praktijk van vandaag. Volgens hem wordt er te weinig aandacht geschonken aan de kwaliteitsnormen op het gebied van de EDP. Snelheid is hierbij vereist in verband met een aantal recente, voor de EDP-auditing belangrijke ontwikkelingen. Deze ontwikkelingen leveren een bijdrage of kunnen een bijdrage gaan leveren aan algemeen geaccepteerde of te hanteren kwaliteitsnormen. Daarnaast zijn er ontwikkelingen die de noodzaak van deze kwaliteitsnormen verduidelijken, respectievelijk urgenter maken. Moonen signaleert de volgende ontwikkelingen: certificatie, de Wet Persoonsregistraties, het Wetsvoorstel Computercriminaliteit, het memorandum van De Nederlandsche Bank, normalisatie van het beveiligingsbeleid van de leden van de Vereniging Computer Service- en Software Bureaus (COSSO), NIVRA-geschrift 26 waarin de problematiek die verband houdt met een door een accountant af te geven mededeling met betrekking tot betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking wordt behandeld, NIVRA-geschrift 53 waarin de accountant wordt geadviseerd via een risico-analyse een samenvatting te geven van de sterke en zwakke punten, EDP-contracten, computerfraudeverzekering en beroepsaansprakelijkheid.

Conclusie

In steeds toenemende mate worden EDP-auditors geconfronteerd met opdrachten waarbij zij hun persoonlijke visie geven als referentiekader. Niet alleen het ontbreken van een eenduidig normenstelsel voor de kwaliteit van de informatievoorziening en de informatietechnologie maakt toetsing van een gegeven situatie moeilijk, ook speelt het probleem dat de evaluatie zelf vaak problematisch is. Beide aspecten versterken het risico van interpretatieverschillen bij het uitvoeren van soortgelijke EDP-audits door verschillende EDP-auditors. In die gevallen dat subjectieve normstelling door de opdrachtgever niet wordt gewenst of aangereikt, wordt de waarde van het oordeel ontleend aan het gezag van de betrokken EDP-auditor. Dit geeft aan diens beroepsuitoefening een ouderwets persoonlijk karakter, maar laat tevens zien dat het beroep van EDP-auditor nog niet echt volwassen is.
Het belang van objectieve kwaliteitsnormen ligt zowel bij de EDP-auditor als bij de gebruikers van EDP-audit-rapporten. Deze laatste categorie wordt steeds groter getuige de ontwikkelingen op het gebied van de wetgeving, het toenemende belang van beheersbare informatievoorziening en informatietechnologie en de groeiende vraag naar certificering en het afgeven van keurmerken.
In veel gevallen zijn objectieve kwaliteitsnormen een verondersteld uitgangspunt bij het beoordelingsproces van de EDP-auditor. Ten onrechte dus, zoals Moonen heeft proberen aan te geven.

Aanbevelingen

Moonen komt tot de volgende aanbevelingen ten aanzien van de door hem geconstateerde problemen rond de kwaliteitsnormering voor de informatietechnologie:

– Het ontwikkelen van objectieve kwaliteitsnormen dient een gezamenlijke actie te worden van EDP-auditors en informatiekundigen. Er moet niet worden gestreefd naar kwaliteitsnormen die elke situatie voor honderd procent afdekken, maar naar richtinggevende, objectieve kwaliteitsnormen voor informatievoorziening en informatietechnologie.

– Objectieve, meetbare kwaliteitsnormen zijn nodig voor huidige en toekomstige gebruikers en aanbieders van EDP-produkten en EDP-processen. Door objectieve kwaliteitsnormen worden verantwoordingen controleerbaar. Dat geeft maatschappelijke zekerheid voor alle belanghebbenden.

– Ten slotte zou een beroepsorganisatie van EDP-auditors een belangrijke bijdrage kunnen leveren tot het verder ontwikkelen en uitdragen van uitvoeringsstandaarden voor onder meer het gebruik van kwaliteitsnormen bij het uitvoeren van EDP-audits.

"EDP-AUDITING TENEINDE ..... OF ZWART SCHAAP MET VIJF POTEN"

Drs. R. Schenk

Op 24 oktober jl. aanvaardde prof.drs. H.C. Kocks RA zijn ambt als bijzonder hoogleraar aan de Erasmus Universiteit Rotterdam met het uitspreken van de rede: *"EDP-auditing teneinde ..... of zwart schaap met vijf poten"*.

Kocks constateert dat velen hebben getracht door middel van definities een antwoord te geven op de vraag wat EDP-auditing is, maar dat niemand zich publiekelijk heeft afgevraagd waarom het vakgebied EDP-auditing bestaat. Vervolgens stelt hij vast dat het vreemd is, dat het vakgebied EDP-auditing, dat als zeer belangrijk wordt beschouwd,

geen zelfstandig gevestigde beroepsbeoefenaren kent voornamelijk onder de vlag van register-accountants of organisatie-adviseurs wordt uitgevoerd. Bovendien zijn de initiatieven om te komen tot een beroepsorganisatie afkomstig van afgestudeerden van de post-doctorale opleidingen en niet van de beroepsbeoefenaren zelf.

EDP-auditing worstelt kennelijk met een identiteitscrisis. Om te voorkomen dat de EDP-auditor verwordt tot een zwart schaap, vanwege de miskenning en het ondergeschikt blijven aan andere disciplines, met vijf poten (organisatiekunde (1), informatiekunde (2), administratieve organisatie inclusief bedrijfseconomie (3), automatisering/informatietechnologie (4) en auditing (5)), zal hij aan het bedrijfsleven en maatschappelijk verkeer duidelijk moeten maken wat het vakgebied inhoudt en waarom het vakgebied waarde toevoegt. In zijn oratie tracht Kocks met de ontwikkeling van het vakgebied als leidraad een antwoord op deze vragen te geven.

Geschiedenis

EDP-auditing is ontstaan als een specialisme binnen de accountancy. De accountant miste de kennis inzake de invloed van de automatisering op de interne controle/administratieve organisatie en de controle-aanpak. Accountants die zich specialiseerden op het gebied van de automatisering, legden de basis voor EDP-auditing. Het bestaansrecht bestond dus ten gevolge van leemten in de opleiding voor registeraccountant. Door aanpassing van de accountancy-opleiding en het plegen van een inhaalslag zou deze leemte kunnen worden opgevuld. EDP-auditing zou dan niets meer zijn dan een tijdelijk verschijnsel.

Een positief gevolg van deze ontwikkelingen was echter dat deskundigen (EDP-auditors) beschikbaar kwamen, die over kennis en kunde beschikten op het gebied van automatisering en administratieve organisatie. Deze groep werd echter geplaagd door de volgende problemen:

– EDP-auditing werd en wordt geassocieerd met accountancy en het daarbij behorende imago.

– EDP-auditing werd en wordt geassocieerd met het technische aspect van automatisering en niet met het organisatorische.

– EDP-auditing kon en kan haar toegevoegde waarde niet of onvoldoende verkopen.

Diverse deskundigheden met betrekking tot kwaliteit (van informatie), beveiliging, risico-analyse en juridische aspecten van automatisering werden daarom aangegrepen om zich als zelfstandig vakgebied te profileren. De duidelijkheid ten opzichte van het maatschappelijk verkeer was echter bij het bewandelen van deze zijwegen niet gebaat.
Niet gespeend van zelfkritiek constateert Kocks dat in zijn eigen definitie van EDP-auditing zoals geformuleerd bij de aanvang van de post-doctorale opleiding aan de EUR in 1989, de "waarom"-vraag eveneens onbeantwoord bleef.

EDP-auditing anno 1991

Op basis van een analyse van de ontwikkeling van het vakgebied concludeert Kocks dat het op oneigenlijke gronden is ontstaan, maar dat het zich door middel van het zich voortdurend aanpassen aan de omstandigheden, staande heeft weten te houden. Het "teneinde ..." is echter nog steeds niet ingevuld.

Kocks introduceert daarom de definitie van de Rotterdamse school. EDP-auditing is het vakgebied dat zich bezighoudt met
- normondersteuning ten aanzien van
- beoordelen van
- adviseren over

aspecten van *objecten* die zijn gerelateerd aan de (organisatie van de) informatievoorziening in een *omgeving* waar gebruik wordt gemaakt van automatisering
TENEINDE - in dit kader -
kwalitatief en/of kwantitatief een *optimale* bijdrage te kunnen leveren aan de realisatie van een adequate organisatie van de informatievoorziening in het kader van de doelstelling(en) van de opdrachtgever.

Het moge duidelijk zijn dat in tegenstelling tot de oude definities in deze definitie wordt getracht het waarom aan te geven. Binnen het vakgebied kunnen twee richtingen worden onderscheiden: EDP-auditing-inhoudelijk en EDP-auditing-beheersmatig. EDP-auditing-inhoudelijk heeft betrekking op de *materiekennis* met betrekking tot één of meer aspecten ten aanzien van één of meer objecten. EDP-auditing-beheersmatig daarentegen heeft betrekking op functionele kennis van de materie alsmede materiekennis zowel ten aanzien van maatregelen ter beheersing van ... als die beheersing zelf.
Met name de EDP-auditing-inhoudelijk ondervindt veel concurrentie van andere disciplines. De concurrenten richten zich op een specifiek deelgebied en zijn daarom beter in staat deze kennis en kunde te onderhouden.
De toegevoegde waarde van de EDP-auditing ligt, aldus Kocks, met name op het gebied van EDP-auditing-beheersmatig. Deze combinatie van kennis en kunde is thans uniek en kan daarom als het bestaansrecht van EDP-auditing worden beschouwd.

Toch voorziet Kocks dat op (de lange) termijn dit vakgebied weer zal worden overgenomen door de disciplines waar het thuis hoort. De *invloed van automatisering op* zal in de toekomst vervallen als automatisering als een normaal verschijnsel wordt beschouwd. Automatisering zal volledig zijn opgenomen in de vakpijlers organisatiekunde, informatiekunde en administratieve organisatie. Voor EDP-auditing-beheersmatig is dan geen plaats meer.

Conclusie

Voorlopig is er volgens Kocks nog plaats voor het zelfstandige vakgebied EDP-auditing. De vakgebieden organisatiekunde, informatiekunde en administratieve organisatie zullen zich in de nabije

toekomst nog niet gaan richten op beheersbaarheidsaspecten. Ontwikkelingen dienaangaande zullen echter in het oog moeten worden gehouden.

De EDP-auditor zal echter aan het maatschappelijk verkeer duidelijk moeten maken wat naast de kwalitatieve meerwaarde de kwantitatieve meerwaarde van een onderzoek is.

Commentaar

In deze oratie heeft Kocks op een heldere wijze getracht aan te geven wat het bestaansrecht van EDP-auditing zou kunnen zijn. Zijn betoog wordt echter doorkruist door de verhandeling over de verschillende zijpaden die door EDP-auditors zijn bewandeld. Hierdoor kan de lezer de rode draad van het betoog uit het oog verliezen.

Het antwoord op het "teneinde ..." is ons inziens slechts ten dele geslaagd. Zijn theoretisch betoog beperkte zich hoofdzakelijk tot de aanbodzijde van het bestaansrecht van EDP-auditing. De vraagzijde van het bestaansrecht van EDP-auditing komt, zoals Kocks overigens zelf in zijn samenvatting aangeeft, niet in deze oratie aan bod. Het antwoord op de vraag of er in het maatschappelijk verkeer behoefte bestaat aan oordelen met betrekking tot informatievoorziening blijft hij ons dus voorlopig nog schuldig.

Reactie prof.drs. H.C. Kocks RA

Geconfronteerd met het commentaar op mijn inaugurele rede voelde ik vooral behoefte te reageren op het punt als zou ik mijn scope te beperkt hebben gehouden door slechts de aanbodzijde aan de orde te stellen. Deze reactie begrijp ik. Het leek mij beter deze weg te kiezen dan vanuit de vraagkant te redeneren. Dan zou ik namelijk niet de behoefte aan EDP-auditing ter discussie dienen te stellen maar de (maatschappelijke) behoefte aan auditing en wellicht daarna - als subset - EDP-auditing.
Ik heb echter de aansluiting gezocht met de moderne marktbenadering door uit te gaan van het feit dat door de juiste produkten door middel van de juiste PR aan de markt aan te bieden de vraag wordt geschapen. Het punt is dan ook in mijn betoog dat EDP-auditing als produkt niet eenduidig is en derhalve niet aan de markt kan worden aangeboden.
De vraagzijde kan dan evenmin worden ingevuld. Om in moderne termen te spreken: de produkt/markt-combinatie is niet duidelijk of ontbreekt. Door nu de beroepsgroep *registerauditors* te onderkennen kan elke *auditor* zijn/haar produkt - met de juiste PR - aanbieden aan de markt die wordt gezien.

CUMULATIEF

Overzicht van eerder verschenen artikelen in Compact

Een selectie van geactualiseerde artikelen uit de 121/2 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.

49 16e jaargang 89/2 zomer 1989

Beveiliging, noodzaak?
J.L.H. Kooijman RA

Beveiligingsbeleid formuleren
drs. R. Schenk

Informatiebeveiliging in het kader van automatisering
drs. H.C. Kocks RA en drs.ing. H.A.J.M. Spape RA

De keuze van beveiligingsmaatregelen in een geautomatiseerde omgeving
drs. J. Kuipers RA

De praktische methode voor de analyse van risico's bij automatisering
ing. C.J.M. Gielen

Organisatorische beveiliging van de geautomatiseerde gegevensverwerking
J.C. Boer RA

Fysieke beveiliging
J.F.C. van Epen CISA

Beveiligingsaspecten van computernetwerken
drs.ing. H.A.J.M. Spape RA

Logische toegangsbeveiliging
J. Brinkman

Beveiliging van de informatie in geautomatiseerde personeelsregistratiesystemen
J.F.C. van Epen CISA

50 16e jaargang 89/3 winter 1989

De gevolgen van toepassing van informatietechnologie voor banken
ir. S. Lelieveldt

Electronic Data Interchange (EDI) en Elektronisch Betalingsverkeer
M. Groesz

Vernieuwing geautomatiseerd verwerkingsproces van het betalingsverkeer bij de Postbank
drs. C.P. Aland RA en A.H. Kuijlaars RA

Mogelijkheden tot standaardisatie van de beveiliging van geautomatiseerd giraal betalingsverkeer
drs. A. Hemelaar RA

Geautomatiseerd uitgaand geldverkeer en het frauderisico
drs. H.C. Kocks RA

Cryptografische beveiliging van elektronisch berichten- en betalingsverkeer
drs. T.P. de Vries

S.W.I.F.T. en Controle
drs. P.M. Knuvers en ing. G.H.M. Meijer

Met ingang van 1990 wordt Compact uitgegeven in samenwerking met Samsom BedrijfsInformatie. In Compact nieuwe stijl verschenen de volgende artikelen:

1 17e jaargang 90/1 lente 1990

De audit van operating systems
drs. P. Veltman RA

Het Virtual Machine concept van IBM
A.A.J. Breed

Betrouwbaarheid en beveiliging van het MVS-besturingssysteem
ing. G.H.M. Meijer

UNIX-beveiligingsaspecten
drs.ing. J.C. van Winkel RI

Aandachtsgebieden bij een AS/400 security audit
ing. J.F. Kuperus

Beveiligingsaspecten van VAX/VMS-systemen
mw. G.J.C. Heikamp

2 17e jaargang 90/2 zomer 1990

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

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

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

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

3 17e jaargang 90/3 herfst 1990

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

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

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

An approach to Data Centre Efficiency Auditing
D. Hall

4 17e jaargang 90/4 winter 1990

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

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

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

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

Strafbaarstelling van computermisbruik
R.A. s'Jacob

1 18e jaargang 91/1 lente 1991

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

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

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

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

Computercriminaliteit in Nederland
mr. V.A. de Pous

2 18e jaargang 91/2 zomer 1991

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

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

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

Detectie en bestrijding van computervirussen
J. Brinkman

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

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

3 18e jaargang 91/3 herfst 1991

Beveiligingsbeleid geautomatiseerde informatievoorziening
mw. D. Jansen Heijtmajer

Geautomatiseerde produktiebesturing
E.J.M. Ridderbeekx

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

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

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