COMPACT

TIJDSCHRIFT EDP-AUDITING

PLATFORMEN

1998/1

Compact ®
Jaargang 25, nummer 1
Een uitgave van KPMG EDP Auditors NV en ten Hagen & Stam BV.
Het blad verschijnt 6 x per jaar.
Redactie
Prof. A.W. Neisingh RE RA (hoofdredacteur)
J.C. Boer RE RA
Ir. J.A.M. Donkers RE
Drs. R.G.A. Fijneman RE RA
J.C. van Praat RE RA
Ir.drs. J. van der Vlugt
Adviesraad
Mr. P. van Dijken
G. van Essen RA
Prof.mr. H. Franken
Dr. K.J. Mollema RA
Prof. H.B. Moonen RE RA
Prof.dr.ir. R. Paans RE
Uitgeefassistent
C.M.A. van Houtum, ten Hagen & Stam, Postbus 34, 2501 AG Den Haag
Tel.: 070 – 304 57 52
Fax: 070 – 304 58 17
e-mail: c.houtum@wkths.nl
Vormgeving
Bureau Karakter, Delft
Opmaak
AlphaZet bv, Waddinxveen
Abonnementen
f 165,- per jaar incl. BTW.
Losse nummers f 45,- incl. BTW.
Studentenabonnement f 95,- 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.: 0172 – 466 800
Fax : 0172 – 475 933
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.
Overdrukken artikelen
Overdrukken van artikelen kunnen worden aangevraagd bij de uitgeefassistent. Prijs per overdruk per artikel (inclusief omslag) f 5,-.

Uitgever
Dr. J.H. Elich

Nederlandse uitgeversverbond
Groep vaktijdschriften

Lid van de Nederlandse organisatie van tijdschriftuitgevers NOTU

ISSN 0920 – 1645

INHOUDSOPGAVE

REDACTIONEEL

Het blad wil een bijdrage leveren aan de ontwikkeling van het vakgebied EDP-auditing door het publiceren van actuele artikelen op deelterreinen van EDP-auditing en advies, zoals:
• beoordeling automatiseringsorganisaties en -systemen • risicobeheersing • telecommunicatie-adviezen • beveiligingsonderzoeken • quality assurance • opleidingen en trainingen • privacywetgeving • computercriminaliteit en nieuwe regelgeving.

Behalve voor EDP-auditors kan dit blad ook interessant zijn voor IT-deskundigen en gebruikers van informatiesystemen. De in dit tijdschrift weergegeven meningen mogen niet worden gezien als officiële zienswijze van KPMG EDP Auditors NV.

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, KPMG EDP Auditors, noch de redacteuren persoonlijk, noch uitgeverij ten Hagen & Stam BV, 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 de uitgeef-assistent verkrijgbaar is.

Ondanks dat in de IT-wereld de aandacht voor de Jaar 2000- en europroblematiek de laatste tijd (gelukkig) enorm is toegenomen, zetten op andere fronten bestaande vernieuwingen in de techniek zich door. Sterker nog, juist die megaprojecten (wat ze in vrijwel alle organisaties zijn) stimuleren de vernieuwing; slechts zelden blijkt het aantal benodigde aanpassingen zo beperkt dat er geen aanpassing van de technische infrastructuur nodig is.

Gegeven de noodzaak tot vernieuwing van de infrastructuur, komt de vraag naar het wat en hoe naar voren. Op dat punt blijkt dan, dat de vernieuwing nogal eens betekent dat allerlei innovaties die zich tot nu toe beperkten tot proef- of kleinschalige implementaties, plotseling op grote schaal en/of voor bedrijfskritieke toepassingen (moeten) worden ingezet. En dan ontbreekt de ervaring of diepgaande kennis van de aspecten die voor een beheerste implementatie en het beheer van de infrastructuur nodig zijn. Deze Compact probeert bij te dragen aan de oplossing van dit knelpunt.

In het eerste artikel wordt de opzet en inhoud van de Common Criteria behandeld. Deze in wereldwijd verband ontwikkelde criteria betekenen een integratie en implementatie van een aantal reeds bekende en ook internationaal als maatgevend erkende stelsels evaluatiecriteria. Deze moeten in de wereld van de informatietechnologie duidelijkheid gaan bieden in de spraakverwarring over wat de veiligheid van systemen inhoudt en met name welke producten nu aan bepaalde verzamelingen evaluatiecriteria voldoen.

Al of niet uitgaande van dergelijke criteria zou de keus zeer wel op een Unix-(gebaseerd) systeem kunnen vallen. Hoewel daar in kringen van systeembeheerders zeker wel kennis over beschikbaar is, levert de ondoorzichtigheid van de beveiligingsstructuur van Unix voor andere betrokkenen wel eens problemen op bij de beveiligingsaudits. Terwijl daar, bijvoorbeeld met behulp van de OTB-standaard Unix van het Overlegorgaan Technische Beveiligingsstandaarden, op een overzichtelijke wijze aan tegemoet te komen is.

Een ander operatingsysteem dat de laatste tijd sterk in de belangstelling staat, Windows NT, kent een aantal overeenkomsten met Unix (flexibiliteit, technisch van aard) en een aantal verschillen (de naam onveilig te zijn, qua beheerfunctionaliteit gericht op eindgebruikers). Temeer daar NT nogal eens in plaats van of naast Unix in netwerkomgevingen wordt ingezet, is het belangrijk inzicht te hebben in de beveiligingsaspecten die daarbij een rol spelen.

Hoewel de aandacht van de media er de laatste tijd net wat minder op is gericht, blijft Novell NetWare, zeker met de vernieuwde Internet-connectiviteit, een zeer belangrijke speler in de markt. Voorwaar een reden voor een auditor om er, meer dan in wezen tot nu toe het geval was, aandacht aan te besteden. En dat betekent een behoefte aan vaktechniek, die echter voor dit 'uitgerijpte' platform tot ieders bagage zou moeten behoren.

Ziedaar een scala van beheer- en beveiligingsaspecten rond ICT-platformen. Alleen al deze aspecten overziend, is duidelijk dat de toekomst van het vakgebied nog veel interessants zal bieden.

Ir. drs. J. van der Vlugt

Common Criteria voor evaluatie van beveiliging van IT-producten

Dr. ir. P.L. Overbeek en ir. G.N. Nelemans

De Common Criteria biedt een verzameling internationaal erkende criteria voor de evaluatie van de beveiliging van IT-producten en -systemen. Op den duur zal de CC huidige criteria zoals het Orange Book en de ITSEC vervangen. De opbouw en inhoud van de CC worden uiteengezet, met telkens uitleg en aanwijzingen voor nuttig gebruik.

INTRODUCTIE

Het besef van het belang van informatiebeveiliging is groeiende, maar hoe kan men nu weten welke beveiliging is te verwachten van een softwareproduct, en waar het vertrouwen in zo'n product op te baseren is? Evaluatiecriteria voor softwarebeveiliging bestaan reeds lange tijd. Er is nu een internationale set criteria voor de evaluatie van de beveiliging van IT-producten, de zogenaamde *Common Criteria*. De Common Criteria wordt ontwikkeld als opvolger van de Europese ITSEC en het Amerikaanse Orange Book. De Verenigde Staten, Canada, Frankrijk, Engeland, Duitsland en ook Nederland werken eendrachtig samen om te komen tot internationaal erkende criteria en evaluaties op basis van deze criteria. Aanleiding voor dit artikel is het verschijnen van versie 2.0 van de Common Criteria.

Een evaluatie van de beveiliging van een IT-product is een formeel onderzoek naar de beveiligingskwaliteiten van dat IT-product. Naast losse IT-producten worden ook IT-systemen geëvalueerd. Onder een systeem wordt in deze context verstaan een combinatie van verschillende IT-producten inclusief de operationele omgeving waarin deze producten actief zijn. Er zijn drie doelgroepen voor beveiligingsevaluaties:

– *Gebruikers*. Gebruikers van IT-producten willen weten of een geëvalueerd product aan hun beveiligingseisen voldoet. Hiervoor kunnen de evaluatieresultaten worden gebruikt. Ook kunnen de criteria worden gebruikt om de beveiligingseisen van de gebruikers vast te leggen. Op basis van die vastlegging kunnen vervolgens producten worden gebouwd. Voor de specificatie van de beveiligingseisen kan een zogenaamd *Protection Profile* (PP) worden gebruikt. De structuur van een PP wordt hierna behandeld.

– *Product- en systeemontwikkelaars*. De bedoeling van evaluatiecriteria is om ook de ontwikkelaars van IT-producten te ondersteunen, vooral waar het gaat om producten die zullen worden geëvalueerd. De criteria helpen de ontwikkelaars in het 'bouwen voor evaluatie', zodat het evaluatieproces zelf geen onverwachte resultaten oplevert en de inspanningen van de ontwikkelaars tijdens de evaluatie beperkt kunnen blijven (denk bijvoorbeeld aan eventueel benodigde aanvullende documentatie). De duidelijke structuur van criteria voor het definiëren van beveiligingsbehoeften helpt de ontwikkelaar of producent om het eigen product beter te kunnen positioneren. Bovendien leggen de criteria de taken en verantwoordelijkheden van de ontwikkelaars tijdens het evaluatieproces vast. De criteria beschrijven de activiteiten die van de ontwikkelaar worden verwacht en de op te leveren producten (documentatie, testresultaten) ten behoeve van de evaluatie.

– *Beoordelaars van IT-producten of -systemen*. De beoordelaar vindt de evaluatie-eisen in de criteria, met een nauwkeurige beschrijving van de activiteiten die door de beoordelaar tijdens een evaluatie moeten worden uitgevoerd. Tevens is in de criteria aangegeven op welke wijze van deze activiteiten verslag moet worden uitgebracht.

Tussen bovengenoemde doelgroepen voor evaluatiecriteria bestaat een zeker spanningsveld. Een natuurlijke tegenstelling bestaat tussen de doelgroepen gebruikers en product- en systeemontwikkelaars. Daarnaast is er echter nog een 'doelgroep' voor de evaluatiecriteria, die van de beoordelaars zelf. De beoordelaar moet voor het uitvoeren van een evaluatie in een onafhankelijke positie ten opzichte van de hiervoor genoemde groepen gebruikers en product- en systeemontwikkelaars verkeren. De beoordelaar dient immers de belangen van beide groepen te dienen.

De criteria moeten de beoordelaar in staat stellen om te verklaren of het te evalueren product al dan niet de geclaimde beveiliging biedt. Door het gebruik van de criteria tijdens de evaluatie kunnen verklaringen worden afgegeven over:
- het voldoen aan de gestelde beveiligingsbehoeften en -eisen met de voor het product gespecificeerde beveiligingsfuncties;
- de correcte implementatie van de beveiligingsfuncties;
- de effectiviteit van deze functies in het licht van de bedreigingen tegen het product.

De criteria bieden dus een *meetlat* voor IT-beveiliging; een meetlat die kan worden gebruikt door zowel producenten als consumenten van (beveiligings)producten. De beoordelaar moet de meetlat aanleggen: objectief, herhaalbaar, controleerbaar en tegen redelijke kosten.

In dit artikel worden het gebruik en de globale inhoud van evaluatiecriteria beschreven aan de hand van de *Common Criteria for Information Technology Security Evaluation versie 2.0* ([CC98]).

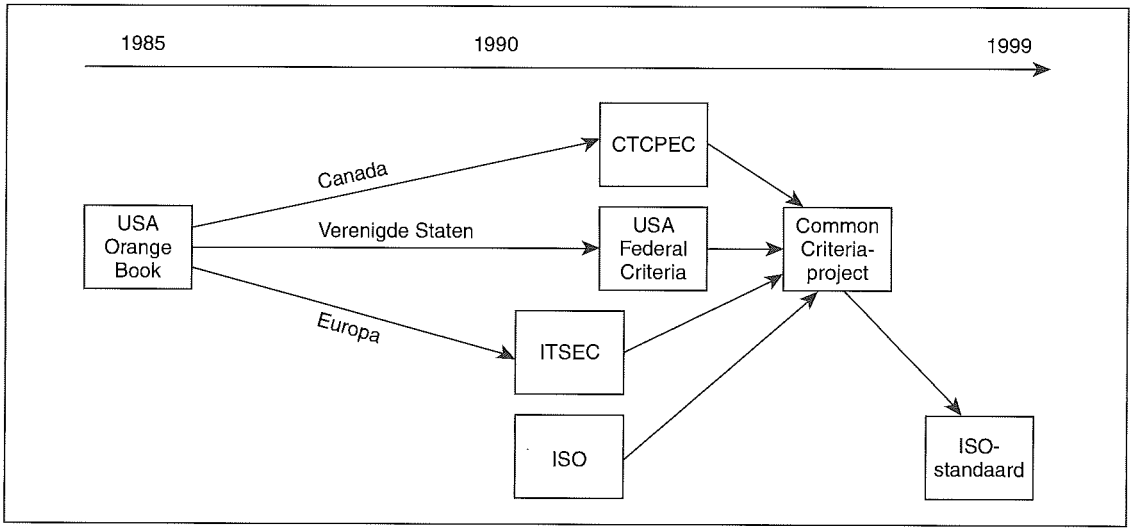
DE COMMON CRITERIA

De Common Criteria (CC) wordt ontwikkeld door de Verenigde Staten, Canada, Frankrijk, Duitsland, Engeland en Nederland. De doelstelling is om de volgende generatie criteria voor de evaluatie van beveiliging in IT-producten te ontwikkelen. De CC is gebaseerd op de volgende 'oude' criteria: ITSEC, USA New Federal Criteria (inclusief de TCSEC ofwel Orange Book) en de Canadese CTCPEC. Deze criteria zullen op den duur geheel verdwijnen ten gunste van de CC. Overigens blijven evaluaties tegen de 'oude' criteria gewoon geldig en kunnen voorlopig probleemloos evaluaties tegen bijvoorbeeld de ITSEC worden uitgevoerd: de CC zal die evaluaties erkennen. Voor wat betreft de opbouw van de CC is tevens gebruikgemaakt van materiaal van ISO SC27 Werkgroep 3 'Evaluatiecriteria'. Tijdens de ontwikkeling van de CC worden nauwe contacten met de ISO onderhouden omdat de CC uiteindelijk een ISO-standaard moet worden, mogelijk op een termijn van een of twee jaar.

De CC biedt een basis voor de wederzijdse erkenning van evaluaties tussen verschillende landen. In het verleden is gebleken dat het ontbreken van zo'n structuur voor internationale erkenning handelsbelemmeringen oplevert. Zo worden in Europa tegen de ITSEC geëvalueerde producten niet als zodanig erkend in de Verenigde Staten.

Het ontstaan van de Common Criteria

De historie van evaluatiecriteria begint onopvallend ergens in de jaren zeventig, toen de eerste ideeën rond het *Orange Book* ([TCS85]) ontstonden. Het Orange Book werd gepubliceerd in 1985 en was lange tijd de enige officiële set criteria. Als zodanig heeft het Orange Book een enorme stimulerende invloed gehad op beveiliging van IT-producten. Sinds 1990 is het 'criterialandschap' aanzienlijk veranderd. In Europa kwamen verschillende landen met eigen criteria uit. Deze zijn geharmoniseerd in wat uiteindelijk de ITSEC ([ITSE91]) is geworden. De ITSEC is in 1991 uitgekomen en vond binnen de doelgroep een brede erkenning in Europa. In ISO-verband werd in 1991 begonnen met de ontwikkeling van een internationale versie van de ITSEC. In Canada zag de CTCPEC ([CTC93]) in 1993 het licht en, eveneens in 1993, ontstond in de Verenigde Staten onder aanvoering van het NIST de eerste versie van de New Federal Criteria ([FC93]), als vervanger van het Orange Book. Deze historie van evaluatiecriteria is weergegeven in figuur 1.



Figuur 1. Historie van evaluatiecriteria.

Veranderingen op het gebied van beveiligingsevaluaties

Het werd duidelijk dat de drijvende krachten en motieven voor beveiligingsevaluaties aan het veranderen zijn. Hiermee veranderden ook de wensen uit de markt op het gebied van evaluaties. Enkele van die veranderende factoren zijn:

– In het verleden werden beveiligingsevaluaties meestal uitgevoerd in opdracht van overheidsorganisaties. Steeds vaker vragen IT-producenten zelf om evaluatie van hun producten. De motivatie van een IT-producent (aanbieder) verschilt natuurlijk sterk van die van een overheidsorganisatie (doorgaans optredend namens de gebruikers binnen de overheid). Voor producenten spelen argumenten een rol als: toegang tot bepaalde markten voor geevalueerde producten, productverbetering en de commerciële waarde van een certificaat (reclamewaarde). Bovendien is het voor een leverancier van belang dat het evaluatieproces synchroon kan lopen met de productontwikkeling en aansluit bij het normale ontwikkelproces en de opleveringstermijnen.

– De ontwikkelingen in de informatietechnologie gaan steeds sneller. Hiermee neemt de behoefte aan flexibiliteit in de criteria toe. Neem als voorbeeld de beveiligingsbehoeften in open, gedistribueerde systemen ([Over93]) zoals in gebruik in het Internet. De grenzen van wat wel en wat niet bij het systeem hoort, zijn niet op voorhand te trekken omdat deze systemen worden opgebouwd uit subsystemen. De vraag is dan: hoe kunnen subsystemen worden ontwikkeld.(en geëvalueerd) die samen met andere *mogelijke* subsystemen een veilig systeem vormen?

– Ook de toepassing van de informatietechnologie verandert. Hierdoor ontstaan nieuwe beveiligingsbehoeften, bijvoorbeeld op het terrein van de *'safety'*- en *'mission critical'*-systemen of de behoefte aan systemen met *Privacy Enhanced Technology*. Bij deze systemen ligt een zwaarder accent op beveiligingseisen als betrouwbaarheid en continuïteit.

– De markt vraagt om evaluaties die internationaal toepasbaar zijn. De reden hiervoor is dat de grootgebruikers van IT-producten zelf internationaal opereren.

– Eén van de hoofddoelen van evaluatiecriteria is de IT-beveiliging in producten te stimuleren en te verbeteren, in het belang van producenten en gebruikers. Dit is alleen te bereiken binnen een beperkte financiële bandbreedte. Of, anders gezegd, evaluaties moeten betaalbaar blijven.

Al deze factoren vragen om een bredere, wereldwijde benadering van beveiligingsevaluaties, hetgeen de belangrijkste reden is voor de ontwikkeling van de Common Criteria for Information Technology Security Evaluation.

REIKWIJDTE VAN DE COMMON CRITERIA

De verwachtingen rond de CC zijn hooggespannen in de wereld van beveiligingsevaluaties. Met de CC wordt natuurlijk geen wondermiddel geboden, maar wat biedt de CC dan wel? Voorop staat dat de CC in de eerste plaats een harmonisatie is van de bestaande evaluatiecriteria. Hierdoor kan verdere wildgroei worden voorkomen. Een afgeleid maar niet minder belangrijk doel is om evaluerende partijen bij elkaar te brengen en kennis te laten maken met elkaars evaluatiecultuur en werkmethoden. Verder helpt de CC in het opheffen van handelsbelemmeringen, immers één van de doelstellingen is de evaluatieresultaten internationaal te erkennen. De CC moet dus ook worden gezien in het belang van de vrije handel tussen landen, zoals gestimuleerd in de World Trade Organisation (WTO), sinds enkele jaren de opvolger van de GATT.

Binnen het aandachtsgebied van de CC vallen:
- evaluatie van de beveiliging in IT-producten of -systemen;
- bescherming van informatie tegen menselijke of andere bedreigingen. De CC onderkent beveiligingsmaatregelen gericht op het bewaren van vertrouwelijkheid, integriteit, beschikbaarheid en controleerbaarheid van de informatie en de IT-middelen;
- technische aspecten van beveiliging;
- gebruik van en interfacing met cryptografische functies (niet de algoritmen zelf).

Buiten het aandachtsgebied van de CC vallen:
- evaluatie van niet-technische beveiliging. Organisatorische, procedurele en fysieke maatregelen vallen buiten de CC *tenzij* ze direct aan een technische maatregel verbonden zijn (bijvoorbeeld functiescheiding);
- evaluatie van in- en uitstralingsbeveiliging (Tempest);
- cryptografische algoritmen;
- de *methodologie* voor evaluaties. Om internationaal tot vergelijkbare evaluatieresultaten te komen is het ook nodig om gelijkwaardige evaluatiemethoden te gebruiken. Zo is er bij de Europese ITSEC een methodologie ontwikkeld, de ITSEM ([NGI95]), die door alle beoordelaars wordt gebruikt. De ontwikkeling van de 'Common ITSEM' is inmiddels in volle gang.

ELEMENTEN VAN DE CC

De CC is zowel geschikt voor IT-producten als -systemen; het is meestal niet nodig een onderscheid te maken. In de CC wordt dan ook de term *Target of Evaluation* (TOE) gebruikt. Onder de TOE wordt dan het IT-product of -systeem verstaan dat het onderwerp van evaluatie is.

De belangrijkste elementen waaruit de CC is opgebouwd, zijn *Security Functional Requirements* (functionaliteit) en *Security Assurance Requirements* (zekerheid).

Security Functional Requirements (functionaliteit)

De beveiligingsfuncties voorzien in de beveiligingsbehoeften van een TOE. Die functies zorgen samen voor het gewenste 'beveiligingsgedrag'. De CC bevat een catalogus met alle beveiligingsfuncties. Hieruit kan de beveiligingsfunctionaliteit worden geselecteerd die in een bepaalde situatie nodig is. Zo'n selectie heet een *Functional Package* (vergelijkbaar met de ITSEC *Predefined Functional Package*). Dit ondersteunt zowel de producenten in de ontwikkeling van producten, als de afnemers in de specificatie van hun beveiligingseisen en de selectie van producten. Omdat de techniek niet stilstaat wordt de mogelijkheid geboden om nieuwe vormen van beveiligingsfunctionaliteit toe te voegen. Voorwaarde is hierbij dat de nieuwe functies ook evalueerbaar moeten zijn. Tabel 1 geeft de *Functionality Classes*. Dit is het hoogste niveau voor de functionaliteitsbeschrijving. De codering voor de Functionality Classes begint steeds met een 'F', gevolgd door twee letters uit de naam (F-AU, voor Functionality Class '*Au*dit'). De Functionality Classes zijn zelf opgebouwd uit steeds fijnere elementen: allereerst de *Families*, en vervolgens de *Components*.

Security Assurance Requirements (zekerheid)

Assurance (zekerheid of verzekering) is de eigenschap van een TOE die de gebruiker het vertrouwen moet geven dat de TOE inderdaad veilig is ofwel daadwerkelijk de gewenste beveiligingsfunctionaliteit biedt. De zekerheid wordt onder andere ontleend aan de kennis van het ontwerp en de ontwikkeling van de TOE, in het licht van het bedoelde gebruik van de TOE. De vereiste maatregelen die het vertrouwen in de beveiliging moeten verzorgen, worden de Security Assurance Requirements genoemd. Deze Security Assurance Requirements zijn gegroepeerd in *Assurance Classes*. Een *Assurance Level* representeert de diepgang waarmee de evaluatie wordt uitgevoerd. Beide termen zullen hieronder nader worden toegelicht.

Assurance Classes

Waarop kan het vertrouwen in een product worden gebaseerd? Hoe kan er in mindere of meerdere mate worden zekergesteld dat het product precies die functionaliteit biedt die benodigd is en dat er geen onverwachte gaten in de beveiliging zitten? De CC onderkent hiervoor verschillende groepen maatregelen, de zogenaamde Assurance Classes. Deze Assurance Classes zijn opgenomen in tabel 2. De Assurance Classes zijn zelf weer opgedeeld in fijnere componenten, zodat een flexibel raamwerk ontstaat waaruit passende maatregelen voor de zekerheid kunnen worden geselecteerd. De al genoemde Assurance Levels zijn samengesteld uit deze componenten. Veel van de Assurance Classes zijn gerelateerd aan kwaliteitsaspecten en zijn ook terug te vinden in ISO 9000-stelsels. De codering voor de Assurance Classes begint steeds met een 'A', gevolgd door twee letters uit de naam (A-CM, voor Assurance class Configuration Management).

Assurance Levels

Een Assurance Level biedt een bepaald niveau van zekerheid dat de geclaimde beveiliging in een product (of systeem) ook daadwerkelijk wordt geboden en niet meer dan die geclaimde functionaliteit (dat zijn immers de gaten in de beveiliging). De As-

Tabel 1. Functionality Classes in de Common Criteria.

Functionality Class	Toelichting
FAU Security Audit	Deze klasse bevat criteria voor de alarm- en incidentenaudit waaronder de registratie van en reactie op beveiligingsrelevante incidenten.
FCO Communication	Bevat momenteel alleen criteria voor functies voor non-repudiation: bescherming tegen het ontkennen van datacommunicatie en communicatie tussen applicaties (onloochenbaarheid).
FCS Cryptographic Support	Bevat criteria voor sleutelbeheer en cryptografische functies, al dan niet op basis van standaardalgoritmen.
FDP User Data Protection	Bescherming van gebruikersdata: onder andere toegangsbeheersing, controle en authenticatie van informatiestromen alsmede import en export van data.
FMT Security Management	Management van beveiligingsfuncties en -attributen, management van beveiligingsrollen en bijbehorende rechten en plichten.
FPR Privacy	Bescherming van de persoonlijke levenssfeer waaronder anonimiteit.
FIA Identification and Authentication	Identificatie en authenticatie van personen en/of programma's die een persoon representeren.
FPT Protection of the TOE Security Functions	Bescherming van de beveiligingsfuncties van het systeem of product zelf.
FRU Resource Utilisation	Gebruik en beheer van middelen: onder andere quota's en prioriteiten, maar ook foutbestendigheid.
FTA TOE Access	Toegang tot de TOE (dit is het systeem of product) zelf, waaronder het opzetten, blokkeren en afsluiten van sessies.
FTP Trusted Path / Channels	Deze klasse bevat criteria voor functies die een vertrouwd pad moeten bieden voor bescherming van de communicatie tussen de gebruiker en de TSF[1] of tussen TSF's onderling.

1 TSF staat voor Trusted Security Functions: de beveiligingsfuncties. De TSF vormt de 'opvolger' van het Orange Book-concept van de TCB (Trusted Computing Base). De TCB vormde één geheel, de TSF kan gepartitioneerd zijn of gedistribueerd. Bovendien kunnen meerdere TSF'en samen weer een geheel vormen.

Assurance Classes	Toelichting
ACM Configuration management	Bevat voornamelijk criteria betreffende de kwaliteit van het configuratiebeheer tijdens de productontwikkeling.
ADO Delivery and operation	Bevat criteria betreffende de veiligheid tijdens distributie naar de afnemers, installatie, systeemgeneratie, opstarten en overdracht.
ADV Development	Het beveiligingsmodel en de architectuur, de functionele specificatie, het globaal en gedetailleerd ontwerp alsmede de implementatie.
AGD Guidance documents	Criteria ter ondersteuning van gebruikers en beheerders betreffende het veilige gebruik van de TOE.
ALC Life cycle support	Criteria betreffende de veiligheid in de ontwikkelomgeving, het melden en verhelpen van fouten en storingen en de procedure rond de introductie van nieuwe versies.
ATE Tests	Criteria betreffende het testen van de TOE: welk gedeelte is getest, met welke diepgang en methode, en zijn er ook onafhankelijke tests uitgevoerd.
AVA Vulnerability assessment	Criteria voor de analyse van zwakke punten, verborgen kanalen (covert channels), mogelijkheden voor misbruik en de sterkte van de gebruikte mechanismen.
APE Protection Profile evaluation	Criteria betreffende de documentatie waar de evaluatie op kan worden gebaseerd. In de klasse APE zijn evaluatiecriteria voor vorm en inhoud van Protection Profiles opgenomen.
ASE Security Target evaluation	Idem voor Security Targets.

Tabel 2. Assurance Classes in de Common Criteria.

surance Levels zelf zijn samengesteld uit de zojuist beschreven vertrouwenwekkende of zekerheidsverhogende maatregelen. De Assurance Levels zijn genummerd, waarbij een hoog Assurance Level een hogere zekerheid biedt dan een lager genummerd Assurance Level. De Assurance Levels zijn opgenomen in tabel 3.

Nieuw ten opzichte van oudere criteria is het EAL1-niveau dat een laag instapniveau biedt en meer mogelijkheden heeft voor leveranciersverklaringen *(vendor assurance)*. In het Orange Book is *assurance* impliciet meegenomen, er bestaan geen aparte niveaus.

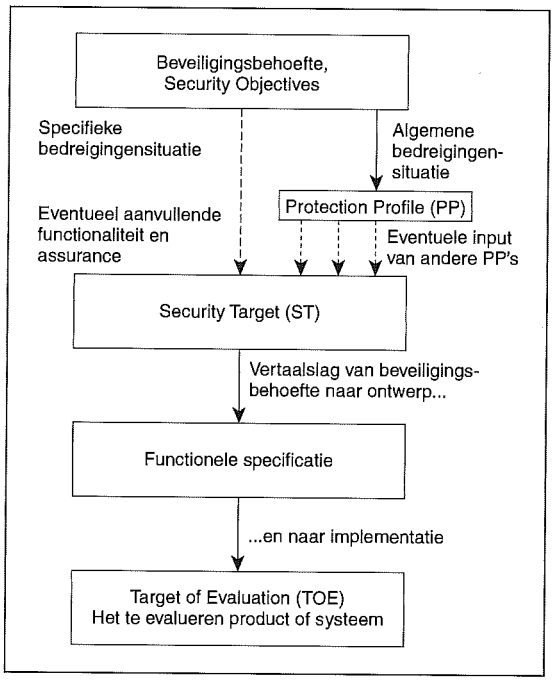
DE TOE EN ZIJN BEVEILIGING

Een TOE zal worden ontwikkeld in de verwachting dat het in de beveiligingsbehoefte voorziet van de beoogde gebruikers. Deze gebruikers zijn uiteraard zelf verantwoordelijk voor het onderkennen van hun beveiligingsbehoefte. De gebruikers kunnen deze behoefte bijvoorbeeld ontlenen aan een risicoanalyse maar deze behoefte kan ook worden ontleend aan een *'security baseline'*. Dat is een minimumniveau aan beveiliging dat binnen een organisatie of voor een specifieke toepassing als ondergrens wordt aangenomen. De Code voor Informatiebeveiliging ([CVI94]) geeft hiervoor een raamwerk. In beide gevallen is er sprake van een specificatie van de bedreigingen voor de informatie en de informatieverwerkende omgeving, het zogenaamde bedreigingenscenario. Ook een productontwikkelaar voert zo'n analyse uit voor zijn product, waarbij aannames worden gedaan over de bedreigingen in de beoogde verwerkingsomgeving. Het bedreigingenscenario wordt gebruikt om de beveiligingsdoelstelling voor de TOE op te stellen.

De CC gebruikt de term *Security Objectives* (SO) voor de beveiligingsdoelstelling van de TOE. De Security Objectives zijn het resultaat van een risicoanalyse, al dan niet als onderdeel van een security baseline. De Security Objectives worden opgesteld naar aanleiding van de analyses van de omgeving van de TOE,

Assurance Level	Beschrijving
EAL0	Dit Assurance Level biedt geen zekerheid. De evaluatie is mislukt.
EAL1	De functionaliteit is eenvoudig getest.
EAL2	De functionaliteit is op structurele wijze getest.
EAL3	Volgens een vaste methodiek getest. Tevens beperkte eisen aan het ontwerp.
EAL4	Als AL3, maar voor het ontwerp is een vaste methodiek gebruikt.
EAL5	Semi-formeel beveiligingsmodel, ontwerp en specificatie.
EAL6	Als AL5 maar met uitgebreidere evaluatiemethode voor testen van het model, het ontwerp en de specificatie.
EAL7	Het hoogste Assurance Level, vereist een formeel beveiligingsmodel, ontwerp en specificatie.

Tabel 3. Assurance Levels in de Common Criteria.

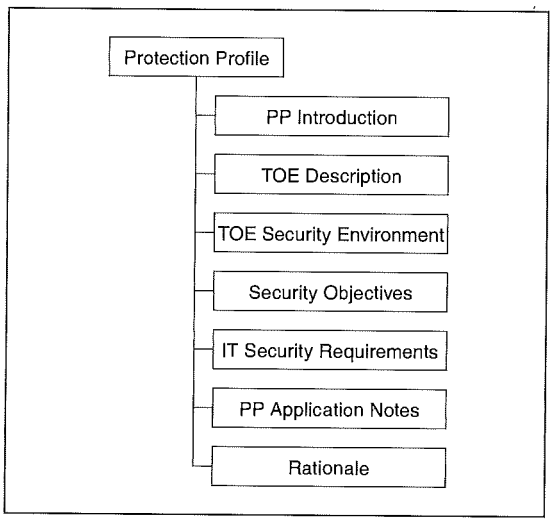


Figuur 2. Bouwstenen van de Common Criteria.

het beoogde gebruik, de bedreigingen die de TOE aan moet kunnen en eventueel een referentie naar toepasbare externe richtlijnen (zoals wetten of beleid). Aan de onderkende bedreigingen worden de hierboven beschreven Security Functional Requirements en Assurance Requirements ontleend. Voor dit proces, dat van iets abstracts als een bedreigingenomgeving naar een specifieke en geëvalueerde TOE leidt, gebruikt de CC een aantal bouwstenen. De CC kent als belangrijkste bouwstenen *Protection Profile, Security Target* en *Security Functional Specification*. Deze bouwstenen zullen hierna worden toegelicht. Figuur 2 toont de samenhang tussen de bouwstenen.

Protection Profile

Een Protection Profile (PP, protectieprofiel) is een definitie van de beveiligingsbehoefte in een algemene bedreigingenomgeving. In de PP wordt beschreven wat de beoogde gebruikersomgeving is, welke bedreigingen daar gelden en welke beveiligingsdoelen in die omgeving worden gesteld (waarom bescherming nodig is). In het gedeelte van de PP met de eisen wordt vervolgens gedefinieerd welke beveiligingsfuncties nodig zijn om die doelen te bereiken (welke functionaliteit is nodig voor de bescherming die nodig is). Tevens wordt met een Assurance Level aangegeven welke zekerheid wordt vereist dat de functionaliteit ook echt en continu wordt geboden.



Figuur 3. De structuur en inhoud van een Protection Profile.

Onderstaand worden enkele voorbeelden van mogelijke PP's weergegeven:
- de vroegere Orange Book-klassen C1, C2, B1, B2, B3 en A1 voor beveiliging van besturingssystemen zijn voorbeelden van PP's. Door deze klassen op te nemen ontstaat tevens een groeipad voor Amerikaanse (en Canadese) gebruikers;
- hetzelfde als voor de Orange Book-klassen geldt voor de huidige ITSEC Predefined Functionality Classes;
- momenteel wordt gewerkt aan een aantal voorbeeld-PP's, bijvoorbeeld voor *firewalls* en enkele besturingssystemen;
- van standaarden zoals de GSS-APIS, de POSIX security interfaces en de ANSI-standaarden voor de bankwereld kunnen PP's worden ontwikkeld.

Er kunnen echter ook veel bredere PP's worden gemaakt. Hierbij kan worden gedacht aan profielen voor privacygevoelige applicaties, de medische omgeving, de *mission-* of *safety critical*-omgeving of voor het elektronisch zakendoen met EDI of elektronische post.

Het idee is dat een PP wordt ontwikkeld door een groep belanghebbenden, bijvoorbeeld een gebruikersgemeenschap of een groep aanbieders. Het PP wordt eerst geëvalueerd en daarna via een register toegankelijk gemaakt voor alle gebruikers.

Structuur en inhoud van een Protection Profile

Figuur 3 toont de vaste structuur van een PP. De verschillende onderdelen van een PP worden hieronder beschreven.

- *PP Introduction.*
Deze bevat de *PP identification* waarmee iedere PP uniek te identificeren is en een korte beschrijving van het doel van deze PP in het *PP overview*.

- *TOE Description.*
Bevat een algemene beschrijving van de TOE zelf.

- *TOE Security Environment.*
Deze bestaat uit de paragrafen *assumptions, threats* en *policies*.

- De *assumptions*. Deze paragraaf bevat de aannames over het beoogde gebruik en de toepassing van de TOE alsmede de aannames over de organisatorische, fysieke, personele en technische inbedding in de omgeving. Tevens bevat deze sectie aannames over de 'waarde' van de te beschermen informatie voor de organisatie en de beveiliging buiten de TOE.

- *Threats* bevat de bedreigingen die de TOE het hoofd moet bieden. Dit onderdeel bevat een be-

schrijving van de bedreigingen in de omgeving zoals die hierboven is beschreven. Er zijn bedreigingen die door de TOE worden afgedekt en bedreigingen die buiten de TOE moeten worden afgedekt. In een bedreigingenscenario moet ook aandacht zijn voor (opzettelijke) aanvallen op de beveiliging en daarbij spelen onderstaande elementen een rol:

- *gelegenheid*: de omgeving zal voor een groot deel bepalen of een aanvaller al dan niet in de gelegenheid is om een aanval op te zetten. Het tijdsaspect speelt hier ook een rol;
- *expertise, kennis:* welk kennisniveau heeft een aanvaller nodig en welke specifieke kennis van de TOE is benodigd om een succesvolle aanval uit te voeren;
- *hulpmiddelen en bronnen*: welke inspanning moet de aanvaller leveren en welke hulpmiddelen moeten de aanvaller daarbij ten dienste staan;
- *motivatie*: wat zouden de voordelen voor de aanvaller kunnen zijn, wat levert een succesvolle aanval eventueel op.

- In de *policies*-paragraaf worden de algemene beleidsuitgangspunten en eventuele wettelijke kaders met betrekking tot de TOE of de doelgroepen beschreven.

- *Security Objectives.*

De beveiligingsdoelstelling van de TOE en de doelstellingen die in de omgeving van de TOE verwezenlijkt moeten zijn. De Security Objectives worden gebaseerd op de hierboven genoemde assumptions, threats en policies.

- *IT Security Requirements.*

Deze zijn opgebouwd uit de volgende twee gedeelten:

- TOE Security Requirements: specificatie van de requirements voor functionaliteit en zekerheid.
  - *functionaliteit*: functional requirements voor de TOE. De beschrijving van de functional requirements verloopt van algemeen naar specifiek via de structuur: class (zeer algemeen, bijvoorbeeld *TOE-entry*), family (gericht op een functie, bijvoorbeeld *Session-locking*) naar component (specifiek, bijvoorbeeld *Automatic terminal locking after inactivity*). In een PP kan het fijnste niveau voor de specificatie van functionaliteit, het componentniveau, desgewenst achterwege blijven. Onder deze kop kan zo nodig ook het gebruik van specifieke beveiligingsmechanismen of -technieken worden voorgeschreven. Vanwege de flexibele structuur is het overigens mogelijk functies toe te voegen die (nog) niet in de CC zijn opgenomen;
  - *zekerheid*: Assurance Requirements voor de TOE, doorgaans in de vorm van een Assurance Level, al dan niet met aanvullende Assurance Components.

- Security Requirements voor de IT-omgeving.

- *PP Application Notes.*

Omvat aantekeningen met betrekking tot het gebruik van deze PP. Hieronder valt eventuele aanvullende informatie over de bouw, de evaluatie of het gebruik van de TOE. Er kan bijvoorbeeld worden verwezen naar gerelateerde PP's of een waarschuwing voor het beheer kan worden gegeven.

- *Rationale.*

Hierin wordt uitgelegd hoe de objectives tot stand zijn gekomen en hoe de geselecteerde requirements voorzien in de beveiligingsbehoefte.

Security Target

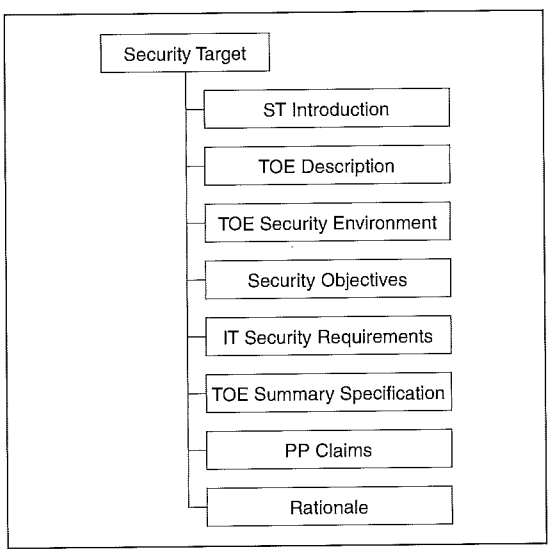
Een Security Target (ST) bevat de definitie van de beveiligingsfuncties en het Assurance Level van een TOE. Een ST is qua opbouw vrijwel gelijk aan een PP, maar een ST is specifiek voor een bepaalde TOE en een bepaalde gebruikersomgeving. In de PP wordt nog veel aangenomen of verondersteld. In een ST is dat niet het geval: alle keuzen zijn gemaakt en ook alle components zijn geselecteerd. Op basis van de ST wordt de evaluatie uitgevoerd. De ST bevat dan ook een TOE-specifiek gedeelte.

Er zijn duidelijke relaties tussen Protection Profiles en Security Targets. Een producent kan een PP nemen en op basis daarvan een product ontwikkelen. De producent stelt dan zijn ST op waarin hij beschrijft hoe de PP in zijn product is geïmplementeerd. In het evaluatieproces wordt eerst onderzocht of de ST inderdaad overeenstemt met de PP (zoals de producent stelt) en vervolgens wordt het product tegen de ST geëvalueerd.

Het is niet noodzakelijk dat een ST wordt afgeleid uit één of meer PP's. Als een TOE 'gewoon' een implementatie is van een PP, dan is de ST een simpele conformiteitsclaim. Is het een geheel nieuwe TOE, of voegt de TOE ten opzichte van bestaande PP's functionaliteit toe, dan wordt de ST op een vergelijkbare manier geëvalueerd als een PP. Het idee is natuurlijk dat nieuwe PP's kunnen worden afgeleid van dit soort ST's (als de producent dat ook wil) en aan de gebruikers ter beschikking kunnen worden gesteld.

Structuur en inhoud van een Security Target

Figuur 4 toont de vaste structuur en inhoud van een ST. Zoals gezegd is het belangrijkste verschil met een PP dat een ST specifiek is voor een bepaalde TOE in een specifiek veronderstelde omgeving en daarom een gedeelte bevat dat specifiek op de TOE betrekking heeft. Alleen de nog niet beschreven onderdelen worden hierna beschreven.



Figuur 4. Opbouw Security Target.

– *TOE Summary Specification.*
De ST bevat de eerste nadere verfijning van het requirementsniveau. Deze verfijning bestaat bijvoorbeeld uit de functionele specificatie voor de beveiliging en een definitie van de maatregelen voor assurance. De beschrijving moet eenduidig het verband tonen tussen de requirements (ofwel: de behoeften) en de functies (ofwel: de wijze waarop in de behoeften wordt voorzien). Voor de hogere evaluatieniveaus is een semi-formele of zelfs formele specificatie vereist. In de ST moet ook duidelijk worden gemaakt welke beveiligingsmechanismen en technieken worden gebruikt in de TOE en in welke functies deze worden ingezet.

– *PP Claims.*
Waar nodig wordt een interpretatie en een verfijning voor de ST gegeven van de gebruikte PP's, bijvoorbeeld waar de PP's keuzemogelijkheden geven. Ook wordt al het nodige gespecificeerd waar in de PP nog aannames worden gedaan. Dit betreft onder andere de specificatie van de omgeving waarin de TOE zal worden gebruikt, de bedreigingen in die omgeving alsmede het gebruik en de toepassing van de TOE.

Security Functional Specification

Op het niveau van PP en ST wordt beschreven *waarom* bescherming nodig is in een algemene (PP) of een specifieke (ST) bedreigingenomgeving. Het PP/ST-niveau beschrijft ook *welke* functionaliteit nodig is om die bescherming te bieden. In de Security Functional Specification (functionele specificatie) is gedefinieerd *welke* precies de functies zijn waarmee de gewenste functionaliteit wordt geboden en *hoe* die functionaliteit wordt geboden. De Security Functional Specification is hiermee tevens de eerste stap in het Assurance-gedeelte van de CC, variërend van informele specificatie tot semi-formele en formele specificatie. Zoals bij de beschrijving van de ST al is vermeld, is het mogelijk de Security Functional Specification in de ST zelf op te nemen.

GEBRUIKSMOGELIJKHEDEN VAN EVALUATIECRITERIA

Met de komst van de Common Criteria is een belangrijke stap vooruit gezet op het gebied van evaluaties van IT-producten en -systemen. Er is een natuurlijk groeipad vanuit de huidige criteria (vooral ITSEC in Europa en Orange Book in de Verenigde Staten) naar de Common Criteria. Huidige en toekomstige investeringen in evaluaties tegen huidige criteria zijn beschermd daar deze evaluaties worden erkend in de Common Criteria. Eén van de belangrijkste winstpunten is dat er nu eindelijk een internationaal erkende basis voor evaluaties kan komen en daaropvolgend internationale erkenning van evaluatieresultaten. Een leverancier hoeft zijn product dan niet meer in bijvoorbeeld de Verenigde Staten én Europa te laten evalueren. Ook in de geest van de vrijhandel (WTO) is de komst van de Common Criteria een groot pluspunt.

Echter, het onderwerp 'beveiligingsevaluaties' is niet altijd los te zien van zaken als nationale veiligheid en landsbelang. Er is daarom meer nodig dan een goed stelsel criteria. Er is ook de politieke wil en durf nodig om tot een werkelijk internationale aanpak te komen. In Europa is dat proces reeds in volle gang met de ITSEC.

De Common Criteria kent ook een aantal beperkingen. Zo is de aanpak complex te noemen, tijdsintensief en voor een nieuwkomer niet direct toegankelijk. Ook ontslaat het de gebruiker niet van de verplichting zelf het gezonde verstand te blijven gebruiken en keuzen te maken uit de in de Common Criteria gedefinieerde functies of zelfs additionele functies te definiëren. Een niet mis te verstane beperking is voorts dat de acceptatiegraad van de Common Criteria nog bijzonder laag is. Een reden hiervoor is dat producenten en gebruikers huiverig staan tegenover een product dat nog (steeds!) in ontwikkeling is.

DE EDP-AUDITOR EN DE COMMON CRITERIA

De vraag is op welke wijze de EDP-auditor gebruik kan maken van de Common Criteria voor zijn werkzaamheden. Bij het uitvoeren van een EDP-audit wordt onder andere onderzoek gedaan naar de beveiliging van applicaties of systemen. In termen van de Common Criteria zijn dit de TOE's. Het EDP-onderzoek betreft doorgaans zowel het systeem of de applicatie zelf als de wijze waarop de mensen in een organisatie ermee omspringen. Voor de beoordeling van een applicatie of systeem zijn de Common Criteria bij uitstek als inspiratiebron te gebruiken; daar zijn ze namelijk precies voor gemaakt. De EDP-auditor kan hierbij met name gebruikmaken van de criteria die zijn gedefinieerd voor functionaliteit en zekerheid.

Ook voor het beoordelen van het gebruik van een TOE binnen een organisatie biedt de Common Criteria aanknopingspunten. Veelal stellen criteria bijvoorbeeld eisen aan documentatie, waarbij kan worden gedacht aan documentatie van de randvoorwaarden waarbinnen een geconstateerd beveiligingsniveau geldt. Deze randvoorwaarden zijn er in drie soorten: fysieke randvoorwaarden, applicatie- of systeemgerichte randvoorwaarden (bijvoorbeeld installatieopties) en organisatorische randvoorwaarden (bijvoorbeeld: scheiding van bevoegdheden eist maatregelen om te voorkomen dat men elkaar het eigen wachtwoord vertelt). De beoordeling van de organisatie als zodanig valt niet binnen het toepassingsgebied van de criteria, evenmin als de fysieke beveiliging.

De EDP-auditor zal ook namens een gebruikersgroep of een productontwikkelaar betrokken kunnen zijn bij de ontwikkeling van Protection Profiles.

Een meetlat

Wil men de mate van beveiliging 'meten', dan is de Common Criteria een geschikte leidraad. De CC bevat immers per beoordelingscriterium een schaal van 'slechte' naar 'goede' beveiliging. Per criterium wordt dus een meetlat aangeboden. De verzameling

meetwaarden van alle individuele criteria tezamen is de volledige meting. De EDP-auditor kan en moet (veelal op basis van de *Corporate Security Policy*) zijn eigen eisen aanleggen ten aanzien van wat hij als minimale meetwaarde wil zien voor elk individueel criterium. De EDP-auditor hoeft zich dus in principe niet veel aan te trekken van Protection Profiles of Security Targets, tenzij deze een erkend niveau van beveiliging geven. Wel kunnen de Protection Profiles worden gebruikt als een eenvoudig gemeenschappelijk referentiekader (bijvoorbeeld in het spraakgebruik).

TOT SLOT

De Common Criteria legt een goede basis om te komen tot een internationale set criteria voor de evaluatie van beveiliging van IT-producten en -systemen. Het voordeel hierbij is dat evaluaties tegen reeds bestaande criteria (zoals het Orange Book of de ITSEC) hun waarde niet verliezen daar ze door de Common Criteria worden erkend. Het erkennen van de Common Criteria als internationale basis voor evaluaties alsmede het internationaal erkennen van evaluatieresultaten tegen de Common Criteria is echter een proces dat enige tijd vergt daar elementen als nationale veiligheid en landsbelang een rol spelen.

Het nadeel van de huidige versie van de Common Criteria is dat de aanpak complex is, hetgeen de toegankelijkheid niet bevordert. De omvang van de criteria, bijna 700 bladzijden, speelt hierbij tevens een rol. Ook de theoretische insteek en het nogal formalistische taalgebruik bevorderen een snelle acceptatie niet. Desalniettemin omvat de Common Criteria vele beveiligingsfuncties die zeer nuttig en interessant zijn voor functionarissen die in mindere of meerdere mate betrokken zijn bij beveiliging. Met name voor EDP-auditors vormen evaluatiecriteria (met in het bijzonder de Common Criteria) een onderwerp dat op de agenda hoort te staan.

LITERATUUR

[CC98] *Common Criteria for Information Technology Security Evaluation*, (parts 1-3), versie 2.0, december 1997 / april 1998.

[CTC93] *Canadian Trusted Computer Product Evaluation Criteria* (CTCPEC), version 3.0, CSSC, CSE, januari 1993.

[CVI94] *Code voor Informatiebeveiliging – een leidraad voor beleid en implementatie*, NNI/Ministerie van Economische Zaken, 1994.

[FC93] *Federal Criteria for Information Technology Security* (FC), draft 1.0, NIST/NSA, januari 1993.

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

[NGI95] P.L. Overbeek (red.), *Evaluatiecriteria voor IT-beveiliging*, NGI, 1995.

[Over93] P.L. Overbeek, *Towards secure open systems*, 2e uitgave, juli 1993.

Dr. ir. P.L. Overbeek
Is als EDP Audit Manager werkzaam binnen de business unit Technical Auditing van KPMG EDP Auditors. Hij heeft ervaring met een breed scala van advies- en auditopdrachten op de gebieden informatiebeveiliging en risicomanagement van informatie en -technologie.

Ir. G.N. Nelemans
Is als EDP-auditor werkzaam bij KPMG EDP Auditors met als aandachtsgebied de ontwikkeling van normenstelsels voor onder andere informatiebeveiliging. Daarnaast is hij specialist op beheer en audit van OpenVMS en van fault-tolerant systemen.

Beheer en beveiliging van Unix-omgevingen

Ir. P. Kornelisse RE

De OTB Unix-beveiligingsstandaard biedt een systematische vertaling van gebruiks- en vooral beheernormen naar functionele beheervereisten. Daaraan koppelt de OTB-standaard de detailmaatregelen van technische en organisatorische aard, in een opzet die stoelt op 'goed huisvaderschap'.

INLEIDING

De afgelopen jaren zijn op verschillende terreinen van Unix verschuivingen opgetreden. De verschuivingen betreffen met name de standaardisatie van de inrichting, de wijze van het gebruik en het beheer van Unix-omgevingen. Navolgend komen deze verschuivingen nader aan de orde.

De EDP-auditor zal in de dagelijkse praktijk met de invloeden van deze verschuivingen te maken hebben. De voornaamste consequentie van de verschuivingen is de veranderende auditbenadering.
Bij de normstelling zal de EDP-auditor meer dan vroeger kunnen steunen op normstellingen binnen de organisatie (beveiligingsstandaarden), of anders ondersteuning bieden door deze normen op te stellen in de vorm van bijvoorbeeld een beveiligingsstandaard.
Bij de audit van de techniek zal een checklistbenadering minder efficiënt kunnen zijn, en mogelijk zelfs niet effectief, als gevolg van respectievelijk het specifieke gebruik of de specifieke beheerorganisatie van Unix.

BEVEILIGINGSSTANDAARD

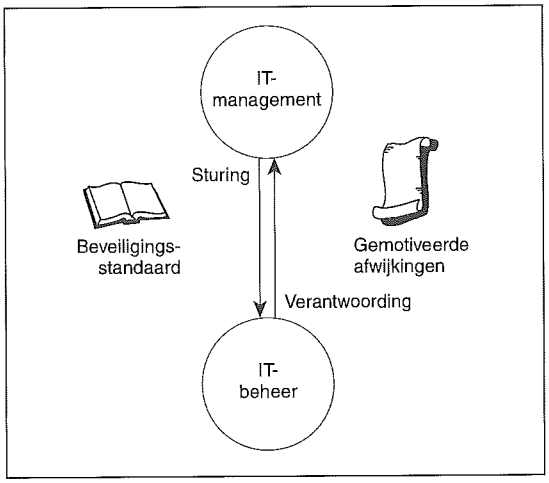
Het Overlegorgaan Technische Beveiligingsstandaarden (OTB) heeft OTB Unix uitgebracht, een beveiligingsstandaard voor de implementatie van Unix-omgevingen.

De normen voor zowel de IT-organisatie als de EDP-auditor worden in een beveiligingsstandaard aangegeven. Voor het IT-management dient de standaard als sturingsinformatie naar de beheerders; de beheerders kunnen de standaard gebruiken als hulpmiddel bij de inrichting van een Unix-omgeving, en bij het verstrekken van verantwoordingsinformatie, door gemotiveerd afwijkingen te rapporteren (zie figuur 1).

In de praktijk zal de EDP-auditor verder moeten kijken dan een checklist of een beveiligingsstandaard lang is. Enerzijds is het de vraag of het voldoen aan een checklist voldoende is, anderzijds kan het voldoen aan een checklist overdaad aan beveiligingsmaatregelen impliceren. Door het veranderende gebruik van Unix en de verschillen in aanwezige beheerorganisaties, evenals de diversiteit van IT-omgevingen, zal de EDP-auditor de aan een Unix-omgeving te stellen eisen steeds weer dienen aan te passen. Het aanpassen van de eisen aan de Unix-omgeving heeft daardoor weer gevolgen voor de eisen die moeten worden gesteld aan application en user controls.

GEBRUIK VAN UNIX

De aard van het gebruik van Unix is aan wijzigingen onderhevig. Oorspronkelijk werd Unix toegepast op basis van terminaltoepassingen. Intussen is veelal sprake van client-servergebruik. De op Unix gebaseerde computers fungeren hierbij als database- of applicatieserver. Daarnaast wordt Unix nu ook frequent toegepast als besturingssysteem voor firewallapplicaties.
Een belangrijke implicatie van de verschuiving in gebruik van Unix is het opheffen van browsemogelijkheden voor de eindgebruiker, waardoor het zoeken naar bijvoorbeeld lekken in Unix van binnenuit sterk wordt bemoeilijkt. Zo kan een eindgebruiker niet meer zoeken binnen het file system naar bestanden die voor eenieder lees- en schrijfbaar zijn. Ook kunnen passwordbestanden niet meer worden ingezien. Publiek beschikbare programmatuur zoals Cops (deze programmatuur zoekt beveiligingslekken binnen Unix) kan door eindgebruikers bijgevolg niet meer worden toegepast. Het opheffen van browsemogelijkheden voor eindgebruikers kan de aan de interne beveiliging van Unix te stellen eisen beperken.
Als uitzondering hierop kan worden geconstateerd dat bij een aantal Internet service providers nog wel een Unix-account ter beschikking wordt gesteld aan eindgebruikers. In dit geval beschikken eindgebruikers nog wel over de gevaarlijk te noemen browsemogelijkheden. Dit betekent dat aan de interne beveiliging van Unix nog steeds hoge eisen dienen te worden gesteld.



Figuur 1. Sturing en verantwoording bij beveiligingsstandaarden.

BEHEER VAN UNIX

Het beheer van Unix vraagt om degelijk ingerichte organisaties met betrouwbare beheerders, in grote maar ook in middelgrote en kleine organisaties.

Beheerorganisaties

Een aantal jaren geleden vond bij veel organisaties de invoering plaats van Unix. Vaak geschiedde dit door de realisatie van een pilotproject. Een klein team werd hiertoe samengesteld, de bestaande beheerorganisatie voor bijvoorbeeld de mainframeomgeving bleef ongewijzigd gehandhaafd.
Een beheerorganisatie voor mainframecomputers kan worden gekenmerkt als professioneel en sterk uitgekristalliseerd. Voor de verschillende beheertaken zijn verschillende medewerkers aangesteld, elk gespecialiseerd op een deelterrein. Tussen de medewerkers worden veelal gewenste functiescheidingen geïmplementeerd.
De oorspronkelijke beheerorganisaties voor Unix-computers verschillen wezenlijk van die voor mainframecomputers. In eerste instantie zijn deze beheerorganisaties als pilot opgericht, waarbij kenmerkend is dat de verschillende betrokken medewerkers over wezenlijke deskundigheid van Unix in de breedte beschikken. De omvang van de beheerorganisatie voor Unix kan sterk verschillen. In de praktijk is sprake van deeltijdbeheerders (bijvoorbeeld de boekhouder die het operationeel beheer van de Unix-computer verzorgt), kritieke applicaties die door een of twee medewerkers uit een projectorganisatie worden verzorgd, tot een opgetuigde organisatie waarin alle vereiste beheerdisciplines met adequate functiescheidingen zijn geïmplementeerd. Samengevat kan worden gesteld dat de beheerorganisatie van een Unix-omgeving veelal wordt gekenmerkt door een klein team, waarbij elk lid van het team een brede en hoge mate van deskundigheid heeft van Unix.

Vertrouwen in de beheerder

Voor adequaat beheer kan worden gesteund op de integriteit en de persoonlijke kwaliteiten van een individuele systeembeheerder. Daarnaast kan als uitgangspunt worden genomen dat de beheerder niet

is te vertrouwen en per definitie fouten zal maken. In de praktijk zal een middenweg worden gekozen. Hiertoe zijn de volgende beveiligingsmogelijkheden aanwezig, waarbij elke mogelijkheid een versterking van de kwaliteit van beveiliging biedt:
- vertrouwen in de beheerder;
- controle achteraf;
- beheerhulpmidelen;
- vierogenprincipe.

Vertrouwen in de beheerder
In elk geval zal als uitgangspunt een zekere mate van vertrouwen in de beheerder moeten bestaan. Hoe anders kan het vertrouwen er zijn dat de beheerder een zekere mate van inzet toont, in het bijzonder bij het optreden van calamiteiten.
Voor het hebben van vertrouwen is ten minste de waarborg van authenticiteit van de beheerder noodzakelijk. Aangezien passwords door Unix in cleartext over het netwerk worden verzonden, dient te worden afgedwongen dat toegang als root (met hoogste privileges) alleen mogelijk is via het console van de Unix-computer.

Bij grote beheerorganisaties kan doorgaans zwaar op EDP-controls worden gesteund.

Controle achteraf van logginginformatie en integriteit van de Unix-omgeving
Een andere medewerker dan de beheerder zal in staat moeten zijn logginginformatie te controleren op ongeoorloofde activiteiten. Overigens dient logginginformatie juist ook ter opsporing van incidenten zonder het oogmerk van frauduleuze handelingen, hetgeen betekent dat juist de beheerder zelf ook toegang dient te behouden tot deze logginginformatie. Het is van belang er rekening mee te houden dat de beheerder als root alle gegevens binnen de eigen Unix-omgeving ongezien kan wijzigen. Daarom dienen zekerheden te worden verkregen betreffende de integriteit van logginginformatie en dient een loghost te worden geïmplementeerd.
Ter controle van de integriteit van de Unix-omgeving dient periodiek te worden vastgesteld dat alle vaste bestanden en alle permissiebits ongewijzigd blijven. Hiertoe dienen zogenaamde ist/soll-vergelijkingen plaats te vinden door gebruikmaking van checksums (bijvoorbeeld MD5).
Bij het optreden van problemen dient direct een alarm te worden afgegeven.

Beheerhulpmiddelen ter beperking van de privileges van individuele beheerders
Gebruikmakend van beheerhulpmiddelen kunnen aan verschillende beheerders taken worden toegekend, waarbij gewenste functiescheidingen worden geïmplementeerd. Hiertoe kunnen geïntegreerde beheerhulpmiddelen worden ingezet, maar ook bijvoorbeeld *sudo*, een specifieke Unix-voorziening waarmee voor verschillende beheerders kan worden aangegeven welke Unix-commando's onder het rootprivilege mogen worden uitgevoerd. Volgens deze constructie kan tevens worden voorkomen dat een beheerder rootprivileges misbruikt om logginginformatie ongeautoriseerd te wijzigen.

Toepassing van het vierogenprincipe
Door het opsplitsen van een password, bijvoorbeeld van de beheerder root, is het mogelijk af te dwingen dat te allen tijde twee beheerders aanwezig zijn tijdens het verrichten van kritieke handelingen.

Kleine en middelgrote beheerorganisatie

In gevallen dat er sprake is van een beheerorganisatie van beperkte omvang (één à twee beheerders) kan niet worden verwacht dat voor het verkrijgen van een adequate functiescheiding zonder meer een voldoende aantal beheerders kan worden ingezet. In dat geval zou een inefficiënt beheer kunnen plaatsvinden, hetgeen in de praktijk uitmondt in het opheffen van deze functiescheiding.

Men dient er bij kleine en middelgrote organisaties rekening mee te houden dat niet kan worden gesteund op EDP-controls voor waarborgen betreffende de integriteit, vertrouwelijkheid en beschikbaarheid van binnen de Unix-omgeving verwerkte gegevens. In dat geval dient te worden gesteund op user controls.

Grote beheerorganisatie

Als sprake is van een beheerorganisatie die bestaat uit meerdere medewerkers voor de te onderscheiden functies binnen een verwerkingsorganisatie, dan wordt het mogelijk zwaar te steunen op EDP-controls. Voor een Unix-omgeving is het echter niet voldoende alleen functiescheidingen te realiseren. Door gebruikmaking van technische voorzieningen ten behoeve van beheer kan een hoog niveau van beveiliging worden gerealiseerd. Deze technische voorzieningen zijn reeds genoemd:

- Periodieke ist/soll-vergelijkingen dienen geautomatiseerd plaats te vinden, opdat ongeautoriseerde wijzigingen efficiënt kunnen worden gedetecteerd.

- Een loghost dient te zijn geïmplementeerd. Dit is een computer die binnen een netwerk bijvoorbeeld via syslog (een netwerkservice voor transport van logginginformatie) logginginformatie ontvangt en opslaat.

- Controle van logging dient direct plaats te vinden, waarbij geautomatiseerde controle de voorkeur heeft.

- Alarms dienen direct bij de beheerder te worden ontvangen. Het tegengaan van alarmmeldingen dient te worden gedetecteerd, bijvoorbeeld door de Unix-computer met een hoge frequentie timestamps te laten afgeven aan de loghost.

Naast deze specifieke technische voorzieningen verdient het tevens aanbeveling de toepassing van beheerhulpmiddelen nader te onderzoeken.

Beheerhulpmiddelen

Unix zelf beschikt voor de verschillende bestaande Unix-versies over veelal dezelfde voorzieningen voor beheer als enkele jaren geleden. Daarnaast zijn op de markt aanvullende beheerhulpmiddelen verschenen die nog relatief weinig worden toegepast.

Op de markt zijn diverse beheerhulpmiddelen aanwezig, die de kwaliteit van het operationeel beheer kunnen verhogen, en tevens de efficiëntie van het operationeel beheer vergroten. Hierbij kan worden gedacht aan geïntegreerde beheerhulpmiddelen zoals Tivoli van IBM, CA-Unicenter van Computer Associates, HP-Openview van Hewlett Packard en Patrol van BMC. Daarnaast zijn diverse beheerhulpmiddelen met gespecialiseerde functionaliteiten beschikbaar.
Ook zijn compliancehulpmiddelen op de markt die de kwaliteit van de geïmplementeerde beveiliging verifiëren. Hierbij kan worden gedacht aan Cops, Omniguard, X-audit van Xirion, DECinspector en dergelijke.

Een organisatie zal een bewuste keuze moeten maken per beheerdiscipline (bijvoorbeeld change, performance en operations management) betreffende de wijze waarop het beheer wordt ingevuld. Per beheerdiscipline dienen prestatie-indicatoren te worden gedefinieerd, waarmee het gewenste niveau van beheer kan worden aangegeven. Vervolgens dient op basis van een kosten-batenanalyse te worden bezien of handmatige, zelf ontwikkelde, gespecialiseerde of geïntegreerde beheerhulpmiddelen moeten te worden toegepast.

DE VOOR- EN DE ACHTERDEUR VAN UNIX, EN DE TUIN EROMHEEN

Het huis van de Unix-infrastructuur biedt diverse toegangswegen.

De voordeur

Over de voordeur van Unix, het inlogscherm, is al veel geschreven, waarbij als voornaamste zwakte het passwordgebruik onder Unix wordt onderkend.

In vele artikelen wordt ingegaan op het gebruik van passwords, waarbij versleutelde opslag op basis van het DES-algoritme aan de orde komt. Bij diverse Unix-implementaties bestaat de mogelijkheid versleutelde passwords in shadow- of gelijksoortige bestanden beter beveiligd dan in `/etc/password` op te slaan. Daarnaast is het veelal mogelijk eisen te stellen aan passwords, bijvoorbeeld betreffende de lengte, de syntax en de geldigheidsduur.

Preventief kunnen eisen worden gesteld aan de door gebruikers toe te passen passwords. Detectief kan de beheerder zelf passwords controleren op eenvoud, door gebruikmaking van het public domain-programma Crack. Dit programma onderzoekt aan de hand van de versleutelde passwords volgens de brute force- en de dictionary-methode of triviale passwords worden toegepast, waarna gebruikers kunnen worden gewaarschuwd.

De achterdeur

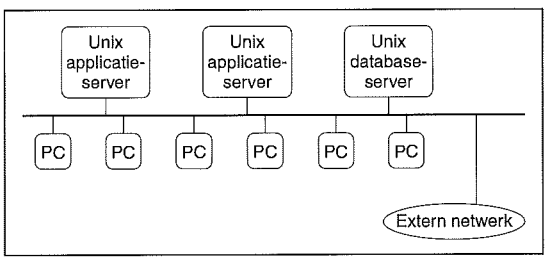
De achterdeur van Unix wordt feitelijk gerepresenteerd door de netwerkservices van Unix, en de trustrelaties tussen verschillende Unix-computers.

In het bestand `/etc/inetd.conf` wordt aangegeven welke netwerkservices zijn toegestaan. Dit betreft bijvoorbeeld services zoals ftp (file transfer), smtp (e-mail) en rlogin (remote login). Door het aantal services in `/etc/inetd.conf` te beperken tot de services die strikt noodzakelijk zijn voor het functioneren van de toegepaste applicaties onder Unix, kan de beveiliging sterk worden verbeterd. Overigens kan gebruik worden gemaakt van een hulpmiddel zoals het public domain-programma TCP-wrapper, waarbij filtering en logging van netwerkservices in detail kunnen worden geparametriseerd.
Daarnaast mogen trustrelaties tussen verschillende Unix-computers alleen onder bijzondere omstandigheden oogluikend worden toegestaan. Trustrelaties maken het immers mogelijk vanaf een computer onder Unix in te loggen, zonder een password in te voeren. Authenticatie wordt in dat geval niet verzorgd door de Unix-computer waarop wordt ingelogd, maar door de computer vanaf welke de gebruiker doorlogt. Feitelijk vindt dus alleen identificatie plaats van de computer vanaf welke de gebruiker doorlogt, hetgeen betekent dat wordt gesteund op de integriteit van IP-nummers van computers. Dit vertrouwen is echter ongegrond, omdat op eenvoudige wijze IP-nummers kunnen worden veranderd.

De tuin

Een huis staat niet op zich maar staat in een omgeving, bijvoorbeeld een tuin. Om deze tuin kan een hek staan met een poortwachter, of de tuin kan overgaan in de straat. In het laatste geval dient geheel te worden gesteund op de beveiliging van het huis zelf.

In een netwerkomgeving kan een analoge situatie worden onderkend. Figuur 2 representeert een huis (Unix-computers en PC's) in een tuin zonder poortwachter. Vanaf het externe netwerk kunnen ongeautoriseerd alle hosts op het netwerk worden aangevallen.

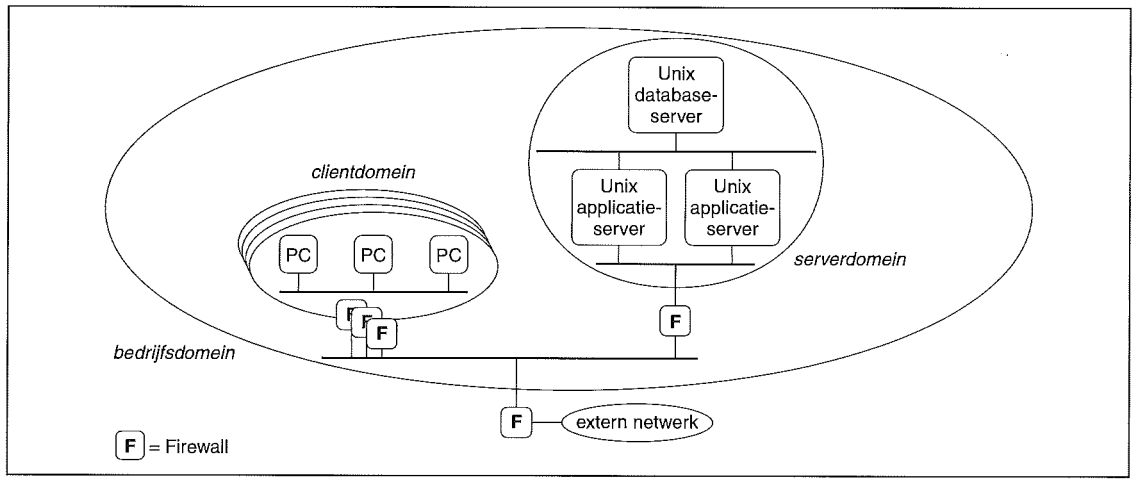


Figuur 2. Zwakke netwerkbeveiliging.

Deze zwakke netwerkbeveiliging geeft aan dat de balans tussen host- en netwerkbeveiliging geheel is doorgeslagen naar de hostzijde.

Het is ook mogelijk de tuin en de buitenwereld te scheiden met een hek en een poortwachter, zoals in figuur 3 voor een netwerk is weergegeven. Feitelijk kunnen serverdomeinen en clientdomeinen worden onderkend. Elk domein is afgeschermd met een firewall, in de praktijk bijvoorbeeld een router, die een aantal toegangsregels hanteert:
- spoofing van hosts binnen het domein door hosts buiten het domein is niet toegestaan;
- alleen toegestane hosts mogen van buiten het serverdomein worden benaderd;
- alleen toegestane hosts mogen berichten naar buiten het domein versturen;

Figuur 3. Sterke netwerkbeveiliging.



- alleen toegestane netwerkservices mogen worden toegepast;
- elke overtreding van één van de bovenstaande regels leidt tot een alarmmelding.

Op deze wijze wordt de beveiliging van Unix minder afhankelijk gemaakt van beveiliging op hostniveau, want ook op beveiliging op netwerkniveau kan nu worden gesteund.

Het interieur

Als het huis eenmaal in een adequaat beveiligde omgeving is opgenomen, wordt het zinvol tevens het huis intern te beveiligen.

De binnenkant van Unix richt zich met name op onderwerpen als file permissies, de wijze van implementatie van applicaties en dergelijke.

AUDIT VAN EEN UNIX-OMGEVING

In vergelijking met enkele jaren geleden benutten EDP-auditors verbeterde checklisten, controleprogramma's, en wordt ook meer complianceprogrammatuur toegepast ter verkrijging van waarborgen voor het bestaan van een voldoende beveiligde Unix-omgeving. Daarnaast is bij technische audits de focus verschoven van met name de technische implementatie van een Unix-omgeving naar zowel techniek als beheer.

De audit van een Unix-omgeving kan dan ook de volgende stappen doorlopen:

1. *Verkenning*
Eerst wordt de scope van de audit vastgesteld: de te onderkennen Unix-computers en de gebruikers-PC's, en de bijbehorende netwerkomgeving. Hierbij wordt ook de aard van het gebruik van Unix vastgesteld, bijvoorbeeld database- of applicatieservices.

2. *Normstelling*
Op basis van de aard van het gebruik van Unix worden normen bepaald voor het beheer en de technische implementatie van de Unix-omgeving.
De EDP-auditor kan hierbij de binnen de cliëntorganisatie toegepaste beveiligingsstandaard als uitgangspunt nemen. Indien een standaard nog niet aanwezig is, kan de normstelling door de EDP-auditor een hulpmiddel voor de cliëntorganisatie zijn om deze standaard nader in te vullen.

3. *Audit van het beheer*
Vervolgens komt het beheer van de Unix-omgeving aan de orde. Inzicht dient te worden verkregen in de beheerorganisatie: de systeemeigenaar, de beheerder, de operator en andere betrokkenen. Voor de te onderkennen beheerdisciplines (change management, operations management, availability management en dergelijke) dient te worden vastgesteld op welke wijze deze zijn ingevuld.

4. *Audit van de techniek*
Rekening houdende met de aard van het gebruik van de Unix-omgeving en de bijbehorende beheerorganisatie wordt de technische implementatie van Unix onderzocht. Hierbij dienen expliciet technische voorzieningen ten behoeve van het beheer te worden betrokken.

5. *Evaluatie en rapportage*
Rekening houdende met de verstrekte opdracht worden de bevindingen en aanbevelingen gerapporteerd. Hierbij is het van belang aan te geven waarom hoge of juist lage eisen zijn gesteld aan de implementatie van de Unix-omgeving.

CONCLUSIES

De toegevoegde waarde die de resultaten van een EDP-audit kunnen leveren, betreft met name de risico-inschatting aangaande het object van onderzoek. In het geval van een Unix-omgeving dient de EDP-auditor zich terdege bewust te zijn van deze toegevoegde waarde. De werkzaamheden behoren te worden gericht op de voornaamste risico's waarover informatie kan worden geboden aan de opdrachtgever.

In Open Omgevingen dient de EDP-auditor bij aanvang van de werkzaamheden niet zonder meer een checklistbenadering te kiezen, maar mag worden verwacht dat een bewuste afweging wordt gemaakt van de uit het gebruik van de Unix-omgeving voortkomende te stellen eisen, de mogelijkheden die de beheerorganisatie kan bieden en de

technische infrastructuur waarbinnen de Unix-computer functioneert. Mede rekening houdende met de ontwikkelingen in de markt kan worden verondersteld dat de aandacht steeds vaker zal liggen bij de beveiliging van de voor- en de achterdeur van de Unix-omgeving, evenals bij technische voorzieningen van preventieve en detectieve aard ten behoeve van beheer.

BIJLAGE

AANDACHTSPUNTEN VOOR EEN BEVEILIGINGSSTANDAARD VOOR UNIX

In deze bijlage wordt een voorbeeld gegeven van onderdelen die in een beveiligingsstandaard kunnen worden opgenomen. Een systeembeheerder dient volgens deze richtlijnen een Unix-omgeving in te richten; afwijkingen van de richtlijnen dienen te worden toegelicht.

De opgenomen richtlijnen zijn grotendeels generiek toepasbaar voor verschillende op de markt zijnde Unix-versies.

Beleid

De volgende beleidsuitgangspunten worden gehanteerd:
- Elke gebruiker dient uniek te worden geïdentificeerd op basis van adequate authenticatiegegevens.
- Elke gebruikersactiviteit dient herleidbaar te zijn tot een unieke gebruiker.
- Toegang is niet toegestaan, tenzij hiertoe expliciet autorisatie is verleend.

De voordeur

Gebruikersaccounts

Voor gebruikersaccounts gelden de volgende regels:
- Elk Unix-account, gedefinieerd in `/etc/password`, dient te beschikken over een unieke user-id (UID).
- Een beheerder dient naast het `root`-account tevens te beschikken over een persoonlijk gebruikersaccount.
- Het `root`-account mag alleen worden benaderd na eerst te zijn ingelogd via een persoonlijk gebruikersaccount.
- Passende maatregelen dienen te worden getroffen opdat alleen geautoriseerde gebruikers kunnen doorloggen naar `root`, door gebruikmaking van bijvoorbeeld `root.allow` en `root.deny` files, lidmaatschap van gebruikersgroepen zoals `wheel`, `system`, etc.
- Alleen via het console mag direct inloggen onder `root` plaatsvinden, door gebruikmaking van `/etc/ttytab`, `/etc/ttys` of de `wheel`-groep.
- Passwordrestricties dienen te worden toegepast: minimumlengte: zes, maximumperiode van geldigheid: drie maanden, de shadow password file dient te zijn geactiveerd, de syntaxregels voor passwords dienen af te dwingen dat als onderdeel van het password ten minste één cijfer wordt opgenomen, initieel toegekende passwords mogen geen triviale betekenis hebben.
- Een time-outmechanisme dient te worden geactiveerd na vijftien minuten van inactiviteit van een gebruiker.
- Gebruikers dienen direct naar de applicatie te worden geleid, de commandoshell van Unix mag door gebruikers niet te benaderen zijn.
- Gebruikersgroepen dienen zorgvuldig te worden ingericht via `/etc/group`, opdat toegang tot shared files beperkt blijft. Eindgebruikerrs mogen geen lid zijn van systeemgroepen zoals `wheel`, `sys`, etc.

De achterdeur

Netwerk
- Alle niet-noodzakelijke netwerkservices zoals gespecificeerd in `/etc/inetd.conf` dienen te worden gedeactiveerd, door een '#' te plaatsen op de eerste positie van de regel waarin de service is vermeld.
- Als de service `ftp` beschikbaar wordt gesteld, dan dient in `/etc/ftpusers` te worden aangegeven welke gebruikers deze service niet mogen benutten.
- Het gebruik van trusted hosts is niet toegestaan, daarom mogen de volgende bestanden niet bestaan, of anders dienen deze files leeg te zijn: `~/.rhosts` (in de homedirectories van alle gebruikers), `/etc/hosts.equiv`, `~/.netrc`.

De tuin

- De productiecomputer dient te worden gekoppeld aan het netwerkbackbone via een afzonderlijk netwerksegment. Alle communicatie tussen de Unix-computer en de netwerkomgeving dient te worden gefilterd, bijvoorbeeld via een router of een softwarefilter zoals TCP-wrapper. Alle verkeer dat niet is toegestaan, dient direct te leiden tot een alarm.

Het interieur

File system
- Alle gebruikersaccounts dienen gebruik te maken van een `umask` met waarde 077, opdat nieuw gecreëerde files en directories alleen kunnen worden gelezen en gewijzigd door degenen die de files en directories hebben gecreëerd.

LITERATUUR

[OTB97] Overlegorgaan Technische Beveiligingsstandaarden, *OTB Unix*, 1997.

Ir. P. Kornelisse RE
Is senior manager binnen de business unit Technical Auditing van KPMG EDP Auditors, vestiging Amstelveen, en coördinator van de productontwikkelingsgroep Open Omgevingen.
Naast zijn werk als algemeen EDP-auditor heeft hij zich ook gericht op specialistische werkgebieden zoals Internet, TCP/IP-netwerken en Unix-omgevingen. Als opdrachtleider en uitvoerende heeft hij daarin ervaring opgedaan met een breed scala van audit- en adviesopdrachten op het gebied van informatietechnologie.

- Het zoekpad (`path`) van een gebruiker dient dusdanig te zijn opgebouwd, dat een programma eerst wordt gezocht in system- en applicatiedirectories. De directory '.' (huidige directory) mag geen onderdeel uitmaken van het zoekpad, in het bijzonder geldt dit voor het `root`-account.
- Geen enkele file of directory mag wereldschrijfbaar zijn.
- Het sticky bit dient te zijn geset voor de `/tmp`-directory.
- De HOME directories van gebruikers dienen als eigenaar de gebruiker zelf te hebben. De directorypermissies dienen gelijk te worden gesteld aan 700.
- Een limiet dient te worden gezet voor de maximale diskruimte per gebruiker.
- File permissies voor devices (in `/dev`) dienen te worden beperkt; group- en world-toegang mogen alleen worden toegekend indien dit strikt noodzakelijk is voor het functioneren van het desbetreffende device.
- Alle system files en directories dienen een systeemaccount (bijvoorbeeld `root` of `bin`) als eigenaar te hebben. Deze files mogen alleen door de beheerder kunnen worden gewijzigd.
- Dagelijks dient een back-up te worden gemaakt van alle system files die zijn gewijzigd.

Applicaties
- Applicaties dienen op dusdanige wijze te worden geïnstalleerd, dat alle bijbehorende bestanden en directories in één subboom van directories zijn opgenomen.
- Voor elke applicatie dient een eigen gebruikersaccount te worden gedefinieerd, dat dient als eigenaar van alle applicatiebestanden en -directories. Onder dit account mag niet worden ingelogd, hetgeen dient te zijn afgedwongen door dit via de password-file onmogelijk te maken.
- Set-UID (SUID)-bits mogen alleen aan programma's worden toegekend in het geval dat gegevens via de applicatie moeten en niet direct bijvoorbeeld via een commandoregel mogen worden benaderd.
- Als batchjobs worden toegepast voor een applicatie, dient hiertoe een afzonderlijk batchscript (at of crontab) te worden toegepast.

Beheer van het huis

Audit trails, logging en rapportages
- Logging dient ten minste voor de volgende gebeurtenissen te worden geactiveerd:
  - succesvol en niet-succesvol inloggen en uitloggen;
  - via commandoregels, cron, at of andere shell-scripts (`/etc/rc`, `/etc/shutdown`) uitgevoerde commando's;
  - systeemmeldingen, naar `messages`, `syslog` en `sulog`.

- Housekeeping dient plaats te vinden op logginginformatie:
  - Dagelijks, wekelijks en maandelijks dient logginginformatie naar archiefbestanden te worden verplaatst; hiertoe dient `cron` te worden toegepast.
  - Archieven dienen elke maand te worden opgeschoond van alle informatie die ouder is dan zes maanden.

- Dagelijks dienen controles plaats te vinden:
  - Checksums dienen te worden berekend voor alle stabiele files. Deze checksums dienen te worden vergeleken met de de voorgaande dag berekende checksums.
  - Waarden van permissiebits van alle files en directories dienen te worden vergeleken met de de voorgaande dag geldende permissiebits.
  - Afwijkingen bij controle van checksums en permissiebits dienen te worden gerapporteerd.
  - Bij aanvang van de dag dient te worden vastgesteld welke gebruikers op niet-reguliere tijden actief waren.
  - Dagelijks en na wijziging van beveiligingsgevoelige parameters dient een compliancehulpmiddel te worden toegepast ter controle van het gerealiseerde niveau van beveiliging.

- Maandelijks dient door de beheerder een rapportage beschikbaar te worden gesteld, waarin betreffende de Unix-omgeving ten minste de volgende onderwerpen worden geadresseerd:
  - geïmplementeerde gebruikers en autorisaties, evenals een lijst van niet-actieve gebruikers;
  - applicaties in productie;
  - performanceontwikkeling, bijvoorbeeld via `sar` (system activity reporting);
  - resterende diskruimte;
  - beveiligingsincidenten;
  - gebruik van root-privileges;
  - wijzigingen in de Unix-omgeving sinds de laatste rapportage.

- Een registratie dient te worden bijgehouden van alle SUID- en SGID-programmatuur. Elke wijziging in SUID- en SGID-programmatuur en het bestaan van alle aanwezige SUID- en SGID-programmatuur dient te zijn toegelicht.

NT en (veilig) netwerken

Ir. drs. J. van der Vlugt

Een aantal technische elementen van Windows NT heeft invloed op diverse aspecten van de beveiliging. Een aparte categorie daarvan betreft de netwerktechniek. De specifieke risico's en tegenmaatregelen verdienen blijvende aandacht.

INLEIDING

Windows NT begint zich langzamerhand te vestigen als operatingsysteem voor met name netwerkomgevingen. Aanvankelijk richtte de inzet zich vooral op het bieden van file- en printservices door NT Servers. Daarmee concurreerde (en concurreert) het onder andere met Novell NetWare. Tevens bood en biedt NT Workstation een stabiel alternatief voor Windows '95 (en '98?) op client-machines.
Zo langzamerhand breidt het gebruik van Windows NT zich flink uit; de feitelijke serverfunctionaliteit wordt in een snel toenemend aantal toepassingen gebruikt om client-serverapplicaties te ondersteunen. Tezamen met de zich snel ontwikkelende multi-userfunctionaliteit (Citrix WinFrame, Microsoft Hydra en erop gebaseerde systemen) begint NT zo langzamerhand van alle markten thuis te worden. Na Apple Macintosh, Novell NetWare en Netscape is zo langzamerhand ook de onderkant van de Unix-markt in beeld gekomen om aan de palmares toe te voegen. Alhoewel de slag op dat terrein pas werkelijk kan worden geleverd wanneer NT zich aanzienlijk verder ontwikkeld heeft. De Lamborghini is nog geen DAF truck.

Vooralsnog zal alle aandacht uitgaan naar het verder ontwikkelen van de losse eindjes die er nog zijn aan Windows NT. Dat NT zo in de belangstelling staat, is een nadeel omdat het gezien de relatieve 'versheid' van het product haast niet anders kan dan dat er allerlei onvolkomenheden opduiken die, nu over het Internet informatie zoveel sneller en uitgebreider de wereld rondgaat dan voorheen bij de ontwikkeling van andere operatingsystemen, het beeld vestigen dat NT kwalitatief achterblijft bij concurrenten.
Het is tevens een nadeel omdat afgunst over het in een zo korte periode veroveren van zulke enorme aandelen op diverse markten een deel van de ingewijden de (gif)pijlen op NT doet richten. De argumenten die over en weer worden gehanteerd, blijken dan ook niet altijd even zuiver te zijn; feiten en emoties lopen nogal eens door elkaar.

Een voordeel van deze aandacht en afgunst is echter dat de feitelijke ontwikkeltijd inclusief de leerschool van de praktijk zo veel korter lijkt te gaan worden dan voor andere systemen. Degenen die Microsoft verwijten zelfs nog te traag te reageren op marktontwikkelingen en de voortgang van verbeteringen aan NT te langzaam vinden gaan, zullen toch moeten onderkennen dat NT binnen relatief zeer korte tijd een op zijn minst zeer redelijk kwaliteitsniveau heeft bereikt. Ook op beveiligingsgebied.

Het doel van dit artikel is tweeledig. Enerzijds zal een deel van de techniek achter Windows NT (versie 4.0) worden toegelicht, voorzover die relevant is voor de beveiliging van de netwerkaspecten van NT. Dit betekent dat een aantal zaken die relevant zijn voor beveiliging in bredere zin, ongenoemd zal blijven. Hierbij valt met name te denken aan beheeraangelegenheden als het gebruik van domains en groups, continuïteitsmaatregelen en stabiliteit (van applicaties en operatingsysteem).

Anderzijds zal specifiek worden ingegaan op de architectuur van de netwerkcomponent die NT in

zich bergt. Daarbij zal de technische kant worden uiteengezet en zullen de voornaamste risico's de revue passeren. De risico's zullen wel worden belicht, maar simpele afdoende oplossingen zijn uit de aard van de problemen niet zomaar te geven. Helaas geeft de praktijk van de inzet van NT een zo grote schakering aan implementaties dat zo'n overzichtelijk checklistje met wat parameterinstellingen die een veilige NT-omgeving opleveren, niet mogelijk is. Per geval zullen de betrokken deskundigen (waaronder de EDP-auditor) een situatiespecifieke beveiliging moeten opstellen, implementeren en handhaven.

NT-STRUCTUUR

De structuur van Windows NT kent vier belangrijke aspecten: het logische beveiligingsmodel, de technische structuur van het operatingsysteem, het inlogproces en de uiteindelijke toegang tot objecten.

Logisch beveiligingsmodel

NT is opgebouwd naar de essentiële functie van een operatingsysteem: gebruikers toegang verschaffen tot gegevens. Subjecten vertegenwoordigen in dit model gebruikers, in de processen die de gebruikers laten uitvoeren. Objecten zijn systeemresources zoals CPU-tijd en files met gegevens. Dit is weergegeven in figuur 1.
(Subjecten zijn in strikte zin ook objecten met eigen kenmerken en gedrag, maar dat is voor de beveiliging van NT minder relevant.)

Een goed geconfigureerd NT-systeem maakt al hetgeen nodig is om bij de gewenste gegevens te komen, transparant voor de gebruiker. Alle onderdelen van NT zijn erop gericht deze transparantie te handhaven; de beveiliging bestaat uit het toestaan van toegang van precies de juiste subjecten (niet meer en niet minder) tot de voor ieder van hen juiste objecten (niet meer en niet minder).

De centrale component die de toegang van subjecten tot objecten bewaakt, is de Local Security Authority (LSA). Deze module maakt gebruik van een aantal hulpmodules voor de identificatie-, authenticatie- en autorisatiecontroles. Eén van de belangrijkste hiervan is de Security Reference Monitor die hieronder wordt beschreven.

De LSA en andere processen gebruiken de Registry waarin vrijwel alle configuratiegegevens zijn opgeslagen; zowel die van de objects als die van de gebruikersaccounts, in de SAM-database. De Registry is een enorm geheel met vele honderden parameters – waarvan een groot deel beveiligingsgerelateerd is.

In de logging kunnen alle gewenste en ongewenste acties van alle lopende processen worden vastgelegd, tot het niveau van detail van in principe iedere call van iedere thread[1]. Tevens kunnen allerlei toegangspogingen tot objecten worden gelogd, waaronder gelukkig ook inzake het Registry-object.

Technische structuur van NT

In figuur 2 staat de basisstructuur van het Windows NT 4.0 operatingsysteem weergegeven, met de beveiligingsrelevante elementen in grijs.

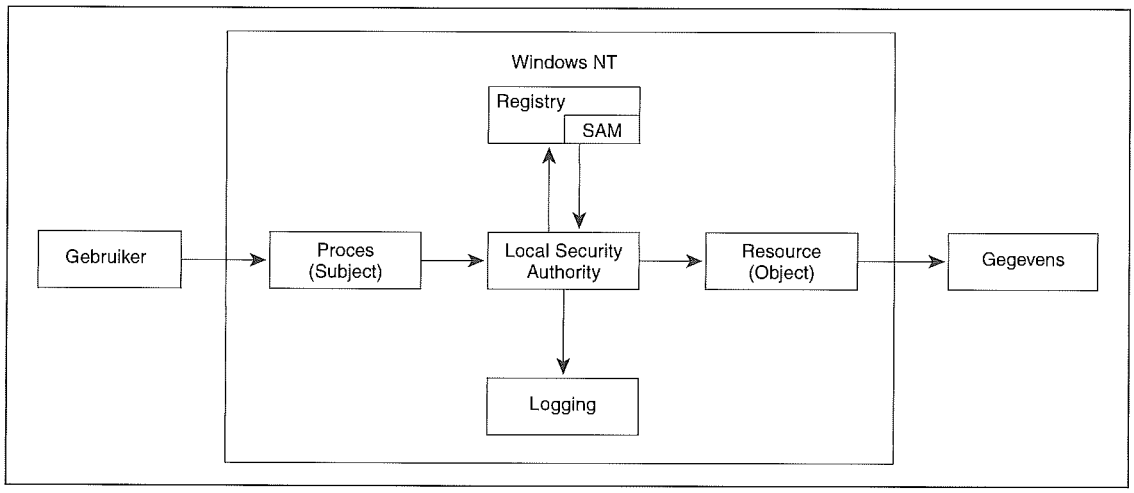
NT kent twee verschillende modes waarin processen kunnen draaien: de user mode en de kernel mode. Alle (deel)processen communiceren door middel van calls.

In de kernel mode draaien de processen die in onderlinge samenwerking het operatingsysteem (NT Executive) vormen. Daar deze processen elkaar onderling vertrouwen, behoeft de onderlinge communicatie geen uitgebreide beveiliging. De onderlinge communicatie en beveiliging wordt afgehandeld door de Local Procedure Call Facility.

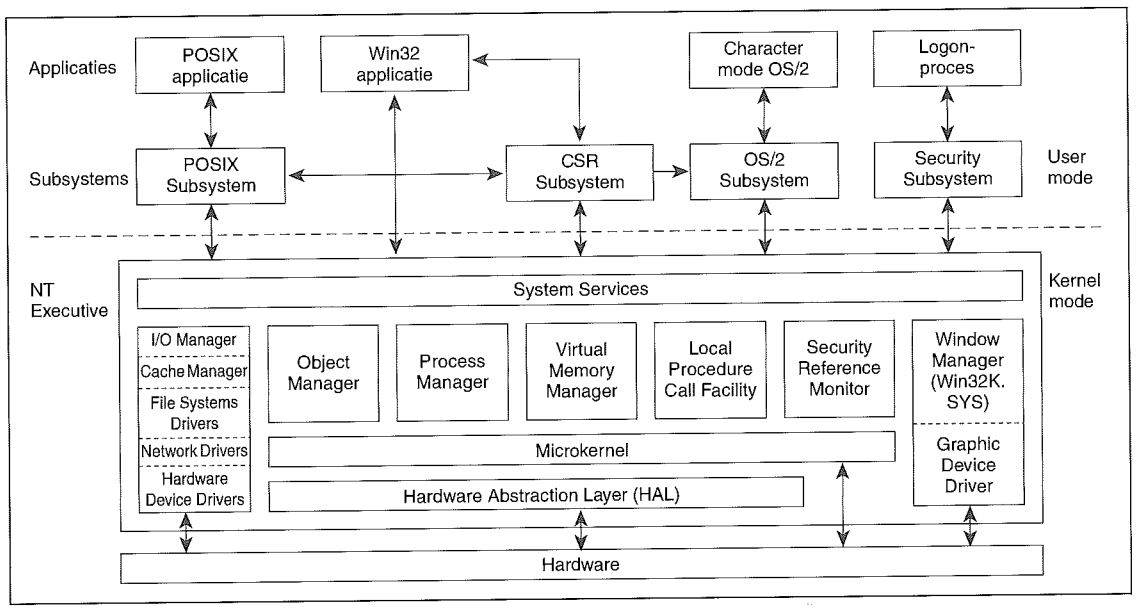
In de user mode draaien de overige processen. Daar ze minder worden vertrouwd, worden bij ontvangst van een call uit een user mode- naar een kernel-modeproces door de Security Reference Monitor meer controles uitgevoerd op de integriteit en autorisatie van het aanroepende proces dan wanneer de call van het ene naar het andere kernel-modeproces wordt gedaan. Alle processen in user mode hebben de beschikking over proces-eigen geheugenruimte die geen toegang biedt aan andere processen.

De in figuur 2 aangegeven hardware omvat de CPU, RAM-geheugen en dergelijke, maar ook beeldscherm en toetsenbord. De grafische randapparatuur (conso-

1 In Windows NT is een thread een deelproces van een hoofdproces; een (hoofd)proces heeft een eigen afgeschermde geheugenruimte, threads binnen een proces delen alle het gebruik van dit geheugen.



Figuur 1. Logische structuur van Windows NT.



Figuur 2. Structuur Windows NT.

le-beeldscherm, muis, etc.) wordt aangestuurd door de Graphics Device Driver in het Win32K subsysteem; netwerkkaarten, harddisks en dergelijke randapparatuur worden aangestuurd door de I/O Manager met behulp van device drivers.

De Hardware Abstraction Layer (HAL) is in opzet het enige element dat hardwareafhankelijk zou zijn. De HAL had als doelstelling juist hardwarespecifieke verschillen tussen bijvoorbeeld Intel- en RISC-architecturen op te vangen, zodat de microkernel en andere NT-elementen op alle platformen op dezelfde virtuele machine zouden kunnen werken. Doordat de I/O Manager en het Win32K subsysteem toch directe toegang tot hardware nodig hadden is dit idee steeds minder van toepassing.

De microkernel bevat een beperkt aantal subroutines die te allen tijde beschikbaar moeten zijn. Microsoft heeft zovéél mogelijk elementen uit de kernel gehaald en in aparte modules ondergebracht, met de doelstelling deze later te kunnen (laten) vervangen door betere implementaties.
De Object Manager creëert, stopt en beheert alle objecten (files, processen, threads, etc.). Alle calls die daarop betrekking hebben, zullen aan de Object Manager gericht zijn die voor de afhandeling zorg draagt. De Process Manager start, stopt en beheert processen (*actieve* objecten), waaronder het beheer van calls uit de user-modeprocessen.

De Virtual Memory Manager (VMM) beheert het interne en externe geheugen (de pagefile). Windows NT isoleert de geheugens van alle processen van elkaar; er is geen sprake van gezamenlijke geheugenallocaties. Alle aanroepen van geheugen worden door de VMM gecontroleerd op autorisatie. Hiermee wordt behalve de exclusiviteit ook de integriteit van de processen bewaard.

Doordat calls van kernel-modeprocessen enerzijds vertrouwd zijn en anderzijds vaak snel moeten worden afgehandeld, worden er minder controles op uitgevoerd. Omwille van de snelheid is de afhandeling ondergebracht in de Local Procedure Call (LPC) Facility.

De I/O Manager beheert alle communicatie met randapparatuur en andere systemen, en bevat de implementaties van de protocol stack. Deze wordt hieronder nader uiteengezet. Zoals uit de structuur van NT in figuur 2 is te herleiden, kunnen I/O-drivers die in kernel mode draaien dus zonder nadere beveiligingsmaatregelen netwerken en dergelijke aanspreken. Dit betekent dat driversoftware met fouten of onvolkomenheden een risico oplevert voor de beveiliging van de server als geheel.

De Security Reference Monitor (SRM) beheert de beveiliging van aanvragen om toegang tot objecten die vanuit de user-modeprocessen en kernel-modeprocessen worden gedaan. De SRM geeft tevens auditberichten af die door het Security Subsystem (ook wel aangeduid als Local Security Authority, LSA) worden gelogd.

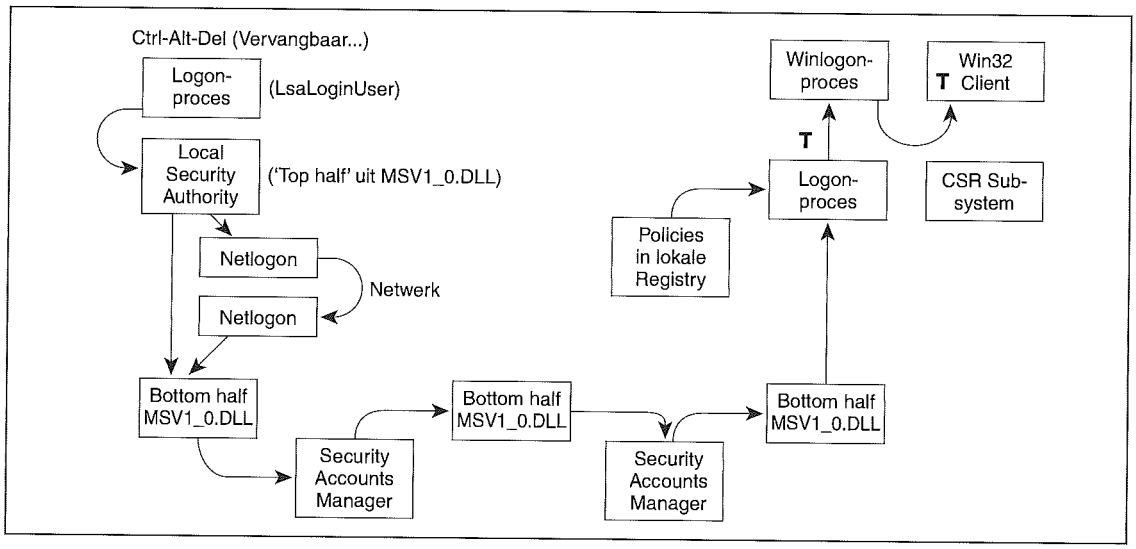
Ten opzichte van Windows NT 3.51 en eerdere versies heeft een verschuiving plaatsgevonden. De onderdelen Window Manager, Graphics Interface en de Graphics, die tot en met versie 3.51 onderdeel uitmaakten van het Win32 subsysteem, zijn overgebracht naar het kernel-modeproces Win32K Executive. Slechts de Console Services uit het 'oude' Win32 subsysteem zijn in het Win32 subsysteem in user mode achtergebleven; het Win32 subsysteem is omgedoopt tot Client/Server Runtime (CSR) subsysteem.

Het Security Subsysteem en het logon-proces worden hieronder besproken.

De POSIX- en OS/2-subsystemen zijn processen die virtuele machines bieden voor POSIX-compliante en OS/2 character mode-programmatuur.
De POSIX-, Win32- en character mode OS/2-applicaties zijn in figuur 2 alleen voor de volledigheid weergegeven; ze maken uiteraard geen onderdeel uit van het operatingsysteem als zodanig.

De System Services ten slotte betreffen de aan de user-modeprocessen beschikbaar gestelde services; ze zijn vergelijkbaar met de in Unix-systemen gebruikelijke deamon-processen. Voorbeelden zijn

Figuur 3. Logon-proces.



print spoolers en netwerkdiensten op het niveau van de presentatie- en applicatielaag.

Inloggen

Het logon-proces verloopt als volgt (zie figuur 3):

1. De gebruiker die wil inloggen, toetst Control-Alt-Delete. Dit start het Logon-proces (in casu het LsaLoginUser-proces). Dit proces vraagt de gebruiker om gebruikersnaam, password en domein om op in te loggen.

2. Het Logon-proces hasht de gebruikersnaam, password en domeininformatie in zowel LAN Manager (DES) als Windows NT (RSA MD4) algoritme en doet een call naar de Local Security Authority (in casu de zogenaamde 'top half' van het NT-authenticatiepakket MSV1_0 uit MSV1_0.DLL). Indien de domeinnaam in de lokale SAM-database staat ('lokaal' inloggen), wordt op dezelfde machine ook de 'bottom half' van MSV1_0 uitgevoerd, die een call doet met de gebruikersgegevens naar de Security Accounts Manager (SAM). Indien de domeinnaam niet in de lokale SAM-database staat, wordt een call gedaan naar de netlogon-service, die het verzoek aan de bottom half op de server geeft.

3. (Indien de netlogon-service wordt gebruikt, selecteert deze het domein en de server om het verzoek aan door te geven, versleutelt de hashes met een sessiesleutel, zet een secure channel op[2] met de server en verstuurt het authenticatieverzoek. De netlogon-service op de server ontsleutelt de gegevens met de sessiesleutel en geeft ze door aan de bottom half van MSV1_0.)

4. De bottom half van MSV1_0 controleert de inloggegevens door op basis van de opgehaalde gebruikersgegevens dezelfde hashes uit te voeren als het Logon-proces. Indien dat in orde is, haalt de SAM de Security ID's (SID's)[3] van alle groepen van het account op en geeft die aan de MSV1_0 bottom half. Deze geeft een remote procedure call return met de SID's etc. direct terug (aan het netlogon-proces op de client-machine indien van toepassing, die ze doorgeeft) aan de MSV1_0 top half. Deze geeft ze weer verder aan LsaLoginUser.

5. LsaLoginUser zoekt in de lokale policy database (die in een beveiligde registry key staat) de lokale groepen met SID's gelijk aan de opgehaalde, en zoekt op basis daarvan in de local policy database de user rights op bij de account(s), groepen en lokale SID's.

6. LsaLoginUser creëert nu een access token met het user rights mask en alle SID's. Dit access token wordt nu doorgegeven aan het Winlogon-proces.

7. Het Winlogon-proces start een nieuw proces dat een gebruikers-shellproces start, en geeft het access token aan dat shellproces. Alle processen die vervolgens uit dit proces worden opgestart, erven het access token. Vanaf dit moment zijn domains en groups voor NT minder relevant; met het access token zijn alle relevante toegangsgegevens van een gebruiker voor NT bij de hand als die met de toegangspermissies van een object moeten worden vergeleken.

Risico's van het inlogproces

Voor het inlogproces wordt het Server Message Block (SMB)-protocol gebruikt. Hieraan kleven bezwaren, zoals de SMB Downgrade-aanval (zie de appendix). Vanaf Service Pack 3 is een gewijzigde versie van het SMB-authenticatieprotocol opgenomen, bekend als het Common Internet File System (CIFS)-protocol.

De Ctrl-Alt-Del-combinatie wordt de Security Attention Sequence (SAS) genoemd. Alle logon-componenten zijn samengevoegd in LSASS.EXE en MSGINA.DLL (GINA voor Graphical Identification and Authorization). Door deze te veranderen kan, anders dan wel eens wordt beweerd, de SAS wel degelijk worden gewijzigd en kan bijvoorbeeld een ander logon-systeem worden geïntroduceerd.

Met Passfilt.dll kan het gebruik van niet-triviale passwords worden afgedwongen. Dit is met name belangrijk gezien de relatieve eenvoud waarmee dictionary attacks kunnen worden opgezet; door de keuze van 'moeilijke' passwords wordt de 'key-space' van potentiële passwords aanzienlijk vergroot.

2 De server geeft een 16-byte challenge (zogenaamde 'nonce'); de nonce en het gehashte password worden samen door de client geëncrypt en teruggezonden; de server encrypt ook de nonce en het password (uit de database) en vergelijkt de twee geëncrypte antwoorden.

3 Intern werkt NT met nummers in plaats van account- of groepsnamen. Deze nummers heten Security ID's.

Het op Internet beschikbare programma L0phtcrack bijvoorbeeld toont aan dat passwords met een lengte van zeven of veertien karakters relatief eenvoudig zijn te kraken. In combinatie met de snelheid van een brute force attack op passwords van zes of minder karakters betekent dit een eis dat passwords acht tot dertien karakters lang moeten zijn.
De techniek van NT staat passwords toe die veel langer zijn dan veertien karakters, maar het invoerveld op het scherm biedt niet de ruimte c.q. mogelijkheid om die dan in te voeren...

Overigens vereisen alle niet-NT-clients het gebruik van het NT Lan Manager authenticatiemechanisme, dat gebrekkig is. Zo worden user-ids in cleartext verzonden, hetgeen dictionary attacks natuurlijk eenvoudig maakt.

Toegang tot objecten

(Geautoriseerde) gebruikers zoeken toegang tot resources (objecten). Alle benoemde objecten, benoemde en anonieme processen, threads en tokenobjecten hebben in Windows NT aan de resource-objecten gekoppelde Security Descriptors, waarin Access Control Lists (ACL's) zijn opgenomen.

Een Security Descriptor is een datastructuur die de volgende elementen bevat:
- eigenaar, de SID van de gebruiker of groep die eigenaar is van het object;
- groep, de SID die aangeeft welke groep met het object wordt geassocieerd (voor POSIX-compatibiliteit);
- discretionary ACL;
- system ACL.

Er is een onderscheid te maken tussen Discretionary ACL's (DACL's) waarin de gebruikersrechten zijn opgeslagen, en System ACL's waarin de auditlogging betreffende het object is vastgelegd. Iedere ACL bestaat uit een header met de omvang, revisie en het aantal Access Control Entries (ACE's), gevolgd door een lijst ACE's. Iedere ACE bestaat zelf ook weer uit een header met de omvang, vlaggen, type, access mask en SID.

De DACL's bevatten ACE's waarin per entry een gebruikers- of groeps-SID en de bijbehorende toegangsrechten zijn vastgelegd. Er zijn twee typen DACE: Access Allowed (expliciet toestaan van toegang) en Access Denied (expliciet ontnemen van rechten).

Er is een belangrijk verschil tussen een lege DACL (zonder ACE's) en een object zonder DACL. Een lege DACL betekent dat geen rechten expliciet zijn toegekend, waarmee alle toegang wordt geweigerd. Een ontbrekende DACL betekent dat expliciet geen (selectieve) rechten zijn geweigerd, dus wordt alle toegang toegestaan.

Ieder object kent een eigenaar, die in principe de controle heeft over een object en de bijbehorende toegangsrechten. Degene die een object aanmaakt, is de eerste eigenaar. Het recht om het eigenaarschap over te nemen is apart aan gebruikers toe te kennen. Tevens is het recht tot het toekennen van toegangsrechten, apart aan gebruikers toe te kennen.

Indien een subject toegang zoekt tot een object, bouwt de Security Reference Monitor eerst een lijst op van gewenste toegang in de Desired Access Mask. Vervolgens vraagt de Security Reference Monitor de DACL op van het object, en vergelijkt het access mask met de ACE's. Dit proces loopt door totdat alle gewenste rechten in de DACL zijn voorgekomen of tot het einde van de DACL. Hierbij zijn twee kanttekeningen te plaatsen:
- de toegangsrechten zijn cumulatief: een gebruiker heeft de gecombineerde rechten van alle groepen waarin hij voorkomt. Dit kan leiden tot onbedoelde toegangsrechten;
- de Access Denied-ACE's worden vooraan in de ACL geplaatst. Zodra voor een gebruiker ten aanzien van de gewenste toegang een ACE met Access Denied wordt gedetecteerd, wordt het doorlopen van de ACL afgebroken met een Access Denied.

Passwords langer dan veertien karakters zijn technisch mogelijk, maar kunnen niet worden ingevoerd.

Toegang wordt alleen verleend indien voor het subject aldus alle gewenste toegang tot het object in de DACL is verzameld.

De registry en alle daarin aanwezige keys en subkeys zijn objecten en derhalve net als files te beveiligen. Evenzo zijn printers objecten en derhalve net als files te beveiligen.

ACE's met SID's van accounts die zijn verwijderd, worden niet geschoond. Er bestaat derhalve een (klein) risico dat malicieus gebruik van SID's waarvan de account niet meer bestaat, toegang geeft tot bepaalde objecten. SID's zijn eenvoudig af te luisteren omdat ze zo vaak in het netwerkverkeer worden gebruikt – en neem bijvoorbeeld de Recycle Bin voor gesharede disks, waarin de verwijderde files van de ingelogde gebruikers zijn opgeslagen: de Recycle Bin kent per gebruikers-SID een subdirectory en deze SID's worden bij het bekijken van de inhoud van de Recycle Bin keurig op het scherm getoond. Als later bepaalde SID's niet meer opduiken, is het zeer wel mogelijk dat die SID's behoren bij accounts die ofwel zijn geblokkeerd ofwel zijn verwijderd. In beide gevallen zullen er in de systemen nog wel files zijn waarvan de ACL's niet (handmatig...) zijn geschoond. Met een beetje 'pech' wordt de filetoegang niet goed gelogd en kan een hacker zelfs ongemerkt toegang (proberen te) krijgen tot die files.

Daarnaast is er een risico dat een gebruiker (al is hij slechts als guest ingelogd) op een Ms-Dos-machine het programma NTFSDOS.EXE kan starten, waarmee NTFS-disks op een voor Ms-Dos transparante wijze kunnen worden aangesproken. Die transparantie betekent echter ook dat geen enkele controle op toegangsrechten wordt toegepast... Linux-machines kennen eenzelfde ongelimiteerde toegang. Dit betekent welhaast een noodzaak tot het verwijderen van floppy drives (waarmee een Intel-machine met Ms-Dos of Linux zou kunnen worden gestart) en

extra maatregelen voor authenticatie op netwerkverkeer.

NT-NETWERKEN

Hiervoor was vooral sprake van de beveiliging van NT alsof het een geïsoleerd systeem betrof. Een aanzienlijk deel van het gebruik zal echter bestaan uit of zwaar leunen op gebruik van de netwerkfaciliteiten van NT. Zoals hieronder zal blijken, zitten juist daar nogal wat haken en ogen. Voor een goed begrip van de netwerkfunctionaliteiten zullen deze hier eerst worden uiteengezet.

Het is met name het gebruik van de netwerkfaciliteiten van NT dat qua beveiliging voor nogal wat problemen zorgt.

Client-servercommunicatie

De communicatie tussen clients en servers kan op NT via een zevental Interprocess Communication (IPC[4])-mechanismen verlopen:
- named pipes;
- mailslots;
- Network Basic Input/Output System (NetBIOS);
- Windows Sockets;
- Remote Procedure Calls (RPC's);
- Network Dynamic Data Exchange (NetDDE);
- Service Message Blocks (SMB's) en Common Internet File Systems (CIFS);
- Distributed Component Object Model (DCOM).

De named pipes zijn in de Microsoft-uitvoering de stukken geheugen die voor meerdere processen toegankelijk zijn. In beginsel hebben processen alleen toegang tot hun eigen virtuele geheugen; de Virtual Memory Manager bewaakt dat. Om echter uitwisseling van gegevens mogelijk te maken, kunnen named pipes worden opgezet, of OS/2 LAN Manager second class mailslots. Beide zijn geïmplementeerd als file systems en kunnen op dezelfde wijze worden afgeschermd.

De NetBIOS-, Windows Sockets en RPC-interfaces zijn API's die het bouwen van gedistribueerde applicaties mogelijk maken zonder dat de programmeur rekening hoeft te houden met specifieke netwerkprotocollen. De RPC-implementatie is compatibel met de Open Software Foundation/Distributed Computing Environment-standaard RPC. Er zijn ook NT-implementaties van DCE-services op de markt, mogelijk omdat NT tot voor kort niet als een serieus alternatief in 'grote' omgevingen werd gezien; deze hebben echter nog geen groot marktaandeel kunnen veroveren.

Het NetDDE-mechanisme is een uitbreiding van het Dynamic Data Exchange-gegevensuitwisselingsmechanisme uit vorige Windows-versies. Ook voor NetDDE dient een aparte share te bestaan; deze dient apart te worden aangemaakt en de bijbehorende NetDDE Service Data Manager-service dient apart te worden opgestart.

Het Server Message Block-protocol kent vier typen berichten om Network Control Block (NCB)-requests bij andere netwerkcomputers af te leveren:
- session control messages, die een redirectorverbinding starten en stoppen;
- file messages, die door de redirector worden gebruikt om files aan de serverzijde te benaderen;
- printer messages, waarmee de redirector data naar een print spooler kan sturen en statusinformatie terug kan ontvangen;
- message messages, waarmee applicaties berichten kunnen uitwisselen.

CIFS is een deelverzameling van het SMB-protocol, speciaal aangepast voor Internet-gebruik. CIFS is door Microsoft als Draft voorgedragen bij de Internet Engineering Taskforce om tot standaard te worden verheven.

SMB en CIFS worden gebruikt voor en in MS-Net, IBM PC Network, IBM LAN Server, IBM Warp Connect, MS OS/2 LAN Manager, LAN Manager for Unix, Unisys Advanced Server for Unix, SAMBA, SCO Unix, DEC Pathworks, 3Com 3+Open, MS Windows for Workgroups, Ungermann-Bass Net/1, Apple Macintosh en NT Networks zelf, in de ondersteuning van LAN Manager voor Ms-Dos, Windows 3.x, Windows '95 en Windows NT Server en Workstation. Verzint u er maar een die daar niet tussen staat. Een poging om de veiligheid van een NT-machine te verbeteren door SMB en CIFS uit te schakelen, betekent dus nogal wat vermindering van functionaliteit...

DCOM, ofwel Networked Object Linking en Embedding, verzorgt het gedistribueerd beschikbaar krijgen van softwareobjecten zoals sorteerroutines, random-numbergeneratoren en database-zoekalgoritmen. In een objectgeoriënteerde applicatie wordt de pointer naar een object vervangen door een pointer naar een DCOM-interfacefunctie, die bij aanroep voor verdere afhandeling (aanroep, adresresolutie, verbinding, teruggeven resultaat) zorg draagt. DCOM bouwt voort op RPC-mechanismen maar biedt uitgebreidere beveiligingsmogelijkheden. Zo kan onafhankelijk worden vastgesteld door welke user-id[5] de server(s) wordt (worden) gestart, welke user-ids de clientapplicaties mogen starten, welke user-ids de diverse serverroutines mogen aanroepen, van welke computers dat mag gebeuren, etc.

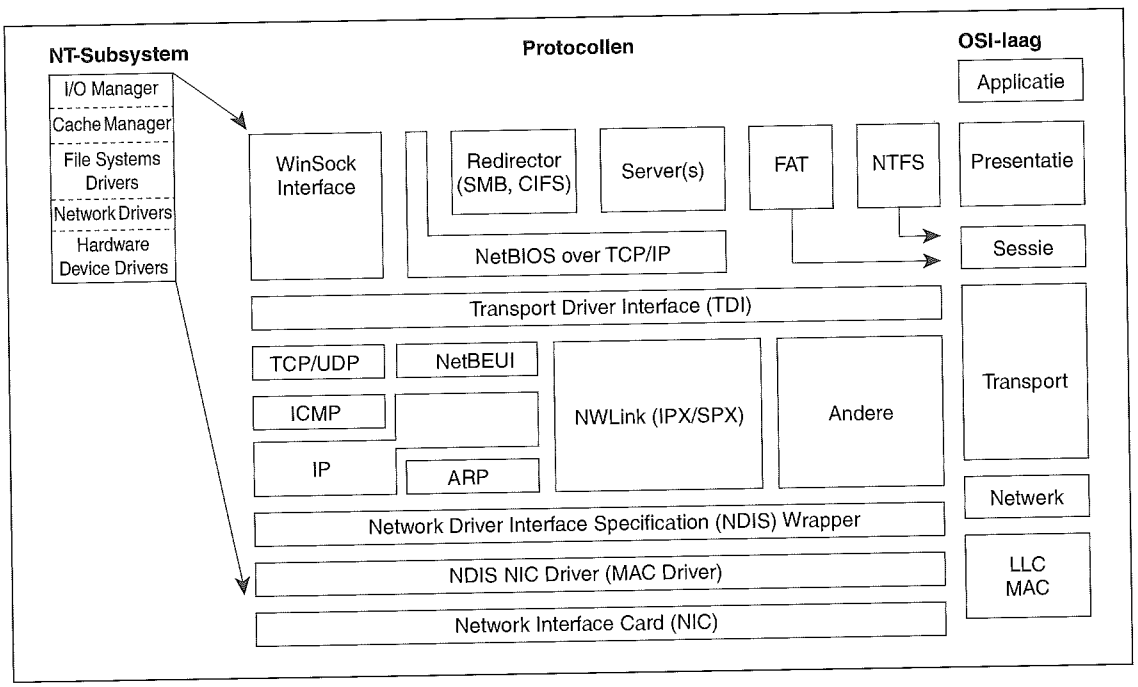
Daarnaast ondersteunt NT op de OSI-applicatielaag het gebruik van de Point-to-Point Protocol (PPP) Control-protocollen PAP, CHAP, SPAP, IPCP, IPXCP en NBFCP en ook het Point-to-Point-Tunneling Protocol (PPTP). Deze protocollen en de Remote Access Service (RAS) die onder andere PPP gebruikt, vallen echter buiten de reikwijdte van dit artikel – er valt qua beveiliging zo veel over te vertellen dat ze later nog eens in een apart artikel aan de orde zullen komen.

Protocollen

In figuur 4 is het blok 'I/O Manager' uit figuur 2 nader toegelicht, exclusief de I/O Manager zelf en de

4 Het is dan ook hiervoor dat elke NT Server en elk NT Workstation standaard een disk share IPC$ (normaliter hidden vanwege de $) aanmaken. Verwijderen van deze share verdient de voorkeur – iedere onnodige share kan immers een voet tussen de deur betekenen voor een hacker – maar dient vooraf op haalbaarheid te worden onderzocht; als de client-serverfunctionaliteit wordt gebruikt, moet de share immers behouden blijven.

5 Lees: Security ID's.



Figuur 4. Netwerkprotocollen in NT (o.a. [Stou96]).

Cache Manager, die op de OSI-applicatielaag de I/O verzorgen en opvangen. Tevens zijn rechtsboven de file systems drivers weergegeven. Deze zullen normaliter rechtstreeks door de I/O- en/of Cache Manager worden aangestuurd, en op hun beurt rechtstreeks communiceren met de disk controllers.

De figuur heeft dus met name betrekking op de netwerkprotocollen en de drivers die deze ondersteunen. En dat zijn er nogal wat. Te beginnen bij de redirector. Dat is de driver die op hoog niveau in protocol stack de IPC-calls van applicaties opvangt en, zoals de naam zegt, voor het doorsturen naar de relevante I/O-driver(s) zorgt. Microsofts implementatie van het Server Message Block (SMB)-protocol is daarin de belangrijkste. Qua abstractieniveau valt het enigszins te beschouwen als een API. Het kan en wordt overigens vervangen door het Common Internet File System (CIFS)-protocol, dat, voorzover het de functionaliteit van SMB vervangt, enkele verbeteringen met zich meebrengt. Omgekeerd worden over een netwerk behalve applicaties ook de NT file en print-services via de redirector benaderd.

De Server services uit figuur 4 ondersteunen de bekende netwerkservers zoals FTP-servers, de Windows Internet Naming Service (WINS), Dynamic Host Configuration Protocol (DHCP), TCP/IP-printing en SNMP. In NT zijn overigens ook finger, lpr, rcp, rexec, rsh, telnet, tftp, arp, hostname, ipconfig, lpq, nbtstat, netstat, ping, route, tracert, chargen, quotd, ..., etc. beschikbaar te stellen – voorzover dat gewenst is. Met het te breed in de organisatie beschikbaar stellen van dergelijke middelen komt immers gemakkelijk te veel informatie vrij die alleen nuttig kan zijn voor (beheerders of) hackers.

Zowel de redirector als de server maakt gebruik van NetBIOS. Behalve de redirector en server over NetBIOS kunnen applicaties ook gebruikmaken van de WinSocks (Windows Sockets) Interface.

Onder de Transport Driver Interface (TDI) zijn de meer bekende transport-netwerkprotocollen terug te vinden. De TDI functioneert als een soort ontkoppel-koppelpunt voor de protocollen van de presentatie- en sessielaag naar de protocollen in de transportlaag. TDI is niet een driver maar slechts een standaard voor berichtenuitwisseling.

In de transportlaag vinden we de bekende protocollen uit de TCP/IP-serie (figuur 4 is nog exclusief PPP en SLIP, die ook kunnen worden gebruikt), NWLink (de Microsoft-implementatie van IPX/SPX) en andere, zoals het inmiddels verouderde NetBEUI (NetBIOS Extended User Interface), het Data Link Control-protocol voor toegang tot onder andere IBM-mainframes, en connectivity voor AFP-verbindingen voor Apple Macintosh-ondersteuning.

Onder de transportlaag-protocollen vinden we vervolgens de NDIS-wrapper, die voor een vertaalslag zorgt van de netwerkprotocollen naar de Network Interface Card (NIC)-driver. NDIS is een de-facto-standaard van Microsoft en 3Com. De NDIS-wrapper zorgt ervoor dat op een computer een praktisch ongelimiteerd aantal netwerkkaarten kan worden aangesloten, en dat de veelheid aan netwerkprotocollen via zelfs maar één netwerkkaart op één netwerk(kabel) kan worden getransporteerd. In tegenstelling tot de TDI is de NDIS-wrapper overigens wel een stuk software, maar qua functionaliteit slechts een klein stuk.

Voorzover NT in netwerken moet opereren waarin bijvoorbeeld Novell NetWare- of SNA-systemen opereren, kunnen services worden gestart die een aanzienlijk deel van het netwerkverkeer en NT-(eigen)aardigheden transparant maken voor dergelijke systemen. Denk bijvoorbeeld aan de Client Service for NetWare, File and Print Service for NetWare, Gateway Service for NetWare en de SNA Gateway services.

NETWERKRISICO'S

De vele protocollen en stukjes software, compatibiliteiten en interoperability brengen met zich mee dat (NT-)netwerken legio zwakke punten kunnen vertonen. Voor het overzicht zijn deze onder te brengen in vier categorieën oorzaken en ook vier categorieën risico's.

Vier oorzaken, vier risico's

De risico's die kleven aan NT-netwerkgebruik kennen vier belangrijke (technische) oorzaken:

1. *De Lan Manager authenticatie- en Server Message Block (SMB)-protocollen die ervoor worden gebruikt*
Deze zijn in wezen in technische zin achterhaald. De belangrijkste reden dat deze mechanismen nog steeds worden gebruikt, ligt in de expliciete wens tot backward compatibility.

SMB geeft, al of niet gewenst, over een netwerk toegang tot juist de zaken die moeten worden afgeschermd, zoals gesharede directories, de registry en andere systeemservices. Als er iets mis gaat met SMB of het wordt misbruikt, dan is een hacker direct al relatief diep doorgedrongen tot willekeurig welk object dat hij wil bereiken.

2. *De bugs in NT en de applicaties die erop draaien*
Ten opzichte van andere operatingsystemen staat NT nog enigszins (!) in de kinderschoenen; het is derhalve niet vreemd dat er ook nog kinderziekten optreden. Met name juist de onderdelen waarvoor Microsoft moest bouwen op van buitenaf opgelegde specificaties, zoals de netwerkdrivers, gaven aanvankelijk problemen. Op dit terrein zijn ook nog steeds de meeste onvolkomenheden weg te werken.

In een eerder stadium waren er nog twijfels aan de robuustheid van NT als zodanig. Eerdere versies kenden bij vrijgave nog een groot aantal programmeerfouten, die vaak leidden tot de gevreesde Blue Screen of Death (BSOD). Dit is de gangbare benaming voor het schermbeeld na een kernel crash: een blauw scherm met in hexadecimaal een reeks hexadecimale codes die informatie zouden (kunnen) geven over de aard van de fout. De instabiliteit (terwijl NT juist was ontworpen om een robuust systeem te leveren) leidde aanvankelijk tot overzichten van vele tientallen zo niet honderden bug reports.

Er is geen sprake van een één-op-éénovereenkomst tussen oorzaak en risico.

Bovendien was een groot aantal van de gevonden fouten hardware-specifiek. Nu zo langzamerhand steeds meer componenten (hardware, drivers, etc.) in NT-compatible versies op de markt komen, vermindert het aantal van dit soort storingen aanzienlijk.

Wat resteert zijn veelal fouten die betrekking hebben op systeemreacties op onverwachte of ongedefinieerde input. In een aantal gevallen reageert NT niet met een keurige, beheerste foutmelding aan de aanroepende applicatie, maar gaat het systeem over in een instabiele status of er verschijnt een BSOD. Of het systeem gedraagt zich ogenschijnlijk correct terwijl een deel van de beveiliging ongemerkt is weggevallen.
Een probleem is tevens dat applicaties die op NT draaien, ook nog programmeerfouten bevatten; voorzover ze als gevolg daarvan 'in goed vertrouwen' (zonder de parameters op intentie te controleren) system calls doen met, in technische of beveiligingszin, verkeerde parameters, geven ze hun eigen fouten door aan het operatingsysteem of veroorzaken ze aldaar onbedoeld systeemgedrag.

3. *De inherente zwakten van TCP/IP*
De protocollen zijn gedeeltelijk connectionless, kennen geen packet signatures of iets dergelijks noch encryptie van de inhoud. TCP/IP is in de ontwikkeling gericht geweest op het herstellen van afwijkend communicatiegedrag. Het in de communicatie met opzet afwijken van normale patronen leidt dan ook tot het reconstrueren van berichten met een inhoud of werking die niet meer is te vertrouwen.

4. *Slappe implementatie van de verlening van toegangsrechten*
Dit is duidelijk niet een NT-specifieke aangelegenheid. De bevoegdheden die geautoriseerde gebruikers hebben en de bevoegdheden die niet-geautoriseerde gebruikers niet hebben, zullen altijd op geordende wijze moeten worden opgesteld, geïmplementeerd, bewaakt en gecontroleerd. Wel wordt in de praktijk met name met de bewaking, in de zin van alertheid van beheerders op ongebruikelijk systeemgedrag (het regelmatig analyseren van loggings en dergelijke), nogal eens de hand gelicht. Organisatorische efficiency-overwegingen lijken er debet aan dat beheerders er ook weinig tijd en middelen voor beschikbaar hebben.

En NT geeft uit-de-doos nogal wat rechten weg die bij een zorgvuldige inrichting niet verleend mogen worden. NT lijkt nog steeds te zeer gericht op flexibiliteit voor de eindgebruiker en het op voorhand zoveel mogelijk wegnemen van belemmeringen voor een onbekommerd systeemgebruik, hetgeen soms wel een Microsoft-mentaliteit lijkt. Indien het beheer niet is gespitst op het (blijvend) wegnemen van die te genereuze rechten, geeft dit uiteraard ten opzichte van 'veilige' operatingsystemen een relatief zwakke beveiliging.

Deze vier factoren samen leiden tot vier categorieën van risico's ([Mudg97]) – overigens is daarbij geen sprake van een één-op-éénovereenkomst tussen oorzaak en risico. De risico's zijn:

1. *Zwakke wachtwoorden en aanvallen op de authenticatiemechanismen*
Hiertoe zijn bijvoorbeeld de L0phtcrack, NTCrack en PWDump-programma's te rekenen. Deze aanvallen richten zich met name op het verkrijgen van de one-way encrypted wachtwoorden om die via een brute force-aanval te achterhalen. Hiervoor zijn twee zaken nodig: toegang tot one-way encrypted wachtwoorden en een programma dat de one-way encryptie kan naspelen.

De toegang tot de one-way versleutelde wachtwoor-

den is op twee manieren te verkrijgen: via packet sniffing – luisteren tot packets langskomen met authenticatiegegevens – of door direct de SAM-database in zijn geheel uit te lezen. Beide methoden zijn in de praktijk 'goed te doen'. Packet sniffen is niet goed te voorkomen behalve dan door organisatorische en fysieke beveiligingsmaatregelen. En constructies analoog aan de shadow-passwordfile van Unix die Microsoft op het bestand \WinNT\System32\Config\Sam heeft gebouwd, kunnen met hack-hulpmiddelen relatief eenvoudig worden omzeild.

Evenzo is software voor het uitvoeren van brute force-aanvallen – het systematisch versleutelen van alle mogelijke wachtwoorden tot een in het NT-systeem bestaande versleutelde versie wordt gevonden – in ruime mate op het Internet verkrijgbaar. Zeker als wordt begonnen met een lijst veelgebruikte wachtwoorden (dictionary attack), blijkt dat een groot aantal in gebruik zijnde wachtwoorden triviaal is; ze bestaan uit eenvoudig te raden woorden. Ook zijn wachtwoorden vaak te eenvoudig van structuur; ze kennen geen speciale karakters, ze zijn te kort, etc. Dit betekent dat het aantal mogelijke, te proberen wachtwoorden (de key space) kleiner is dan wenselijk – en wenselijk is een key space die zo groot is dat brute force-aanvallen op voorhand 'te lang' duren. Ergo, het aantal te proberen wachtwoorden is dan klein genoeg om met een moderne PC een poging te wagen. Sommige kraakprogramma's gaan uit van een gemiddelde kraaktijd van een paar uur.

2. *Oprekken van toegangsrechten van subjects*
Denk aan GetAdmin, trojaanse paarden, fouten in Internet Explorer en Internet Information Server, maar ook 'gevaarlijke' ActiveX-controls. Deze komen vaak naar voren doordat een (Internet-)gebruiker bij bepaalde handelingen met bepaalde applicaties vreemd gedrag op het spoor komt, dit onderzoekt en een systematiek ontdekt. Na eigen of andermans onderzoek blijkt dan dat onderdelen van, met name, de netwerkprotocolstack niet naar behoren functioneren; ze reageren op een 'onveilige' manier op ongedefinieerde of onverwachte input. Vervolgens valt het operatingsysteem dan vaak terug op het afbreken van een applicatie op de server terwijl de verbinding met de client nog openstaat, of de applicatie voert ongewenste commando's van de gebruiker uit alsof het zijn eigen zijn.

De client kan dan, met gebruikmaking van de authenticatie als serverapplicatie (de serverapplicatie draait nogal eens op een apart account met meer rechten dan een willekeurige gebruiker), systeemcommando's (laten) uitvoeren op de server. Daaronder kunnen dan uiteraard direct kwalijke commando's zijn zoals het wissen van files of tegelijk maar een hele harde schijf, maar ook kan de toegang gebruikt worden voor meer heimelijke activiteiten als het plaatsen van een trojaans paard of alleen al het verzamelen van meer beveiligingsinformatie (zoals de SAM-database...).

Een aantal bugs in applicaties wordt overigens op het Internet genoemd met de mededeling dat er nog geen bekende 'exploits' bij zijn. Dat wil niet zeggen dat kwaadwillende hackers die manieren van misbruik niet al toepassen zonder ze wereldkundig te maken. En, bekend of niet bekend, dergelijke programmeerfouten en ongedefinieerd systeemgedrag horen natuurlijk niet in een operatingsysteem thuis.

3. *Passieve aanvallen*
Hieronder zijn vormen van afluisteren van gegevens te vatten, maar ook de klassieke man-in-the-middle-aanvallen horen in wezen in dit rijtje thuis. Deze aanvallen kenmerken zich door de afstand die de hacker houdt ten opzichte van het systeem dat hij aanvalt. Er wordt geen inbreuk gepleegd op het systeem, er wordt alleen misbruik gemaakt van overigens geheel toegestane verbindingen – althans, toegestaan aan anderen dan de hacker.

Op deze aanvallen zal hier niet verder worden ingegaan. In wezen zijn het ook bepaald niet in alle gevallen aanvallen waar Windows NT iets tegen kan doen. Wel kunnen de ertegen te nemen maatregelen, zoals encryptie van netwerkverkeer, ook op NT worden geïmplementeerd.

4. *Denial-of-Service (DoS)-aanvallen*
Deze komen in drie smaken voor: de aanvallen die leiden tot de Blue Screen of Death (BSOD) en die daarmee de hele server buiten werking stellen, aanvallen die de server niet om zeep helpen maar wel volledig in beslag nemen en de aanvallen die de NT-server intact laten maar alle netwerkverkeer onmogelijk maken. Alledrie zijn ze natuurlijk even ernstig voor de beschikbaarheid van de NT-server als geheel – tenzij het netwerk wordt aangevallen als het nou net even niet beschikbaar zou hoeven zijn; een situatie die eigenlijk slechts hypothetisch is.

De aanvallen die leiden tot de BSOD of tot honderd procent CPU-belasting komen voornamelijk voort uit fouten in NT-programmatuur. Er valt niet veel tegen te doen, behalve dan het tijdig installeren van Service Packs en hotfixes die door Microsoft beschikbaar worden gesteld. Daarmee is tegelijkertijd een tweede risico genoemd: het te snel installeren van de hotfixes. Nogal eens is gebleken dat een hotfix op zichzelf ook weer softwarefouten bevatte; de hele Service Pack 2 bracht welhaast meer fouten met zich mee (of althans – meer en duidelijker merkbare fouten) dan ermee werden opgelost.

De aanvallen die het netwerkverkeer platleggen zijn overigens moeilijk te voorkomen. Gedeeltelijk zijn het NT-eigen fouten. Dat is het geval voorzover ze worden veroorzaakt door – alweer – een tekortschietende implementatie van netwerksoftware in NT. In andere gevallen is er soms gewoonweg niets aan te doen. De fout zit 'm dan in het netwerkprotocol en dat zal zo snel niet veranderen.

Tegenmaatregelen

Bovenstaande risico's zijn natuurlijk niet bijzonder prettig voor een client-serveromgeving als NT. De vraag is dan ook: valt er wat tegen te doen? Zoals altijd is het antwoord: ja en nee. De tegenmaatregelen vallen in drie categorieën uiteen:
- beter programmeerwerk van Microsoft;
- alleen veilige technieken voor netwerkverkeer gebruiken;
- organisatorische maatregelen, waaronder goede implementatie en monitoring van de ingestelde beveiliging.

Het betere programmeerwerk van Microsoft is natuurlijk een open deur, maar tot voor kort was het juist op dit punt dat de algemene kritiek zich richtte, en gedeeltelijk terecht. Door een doorlopende stroom verbeteringen neemt nu het aantal gemelde problemen zienderogen af.

Doordat Microsoft nu zorgvuldiger programmeert neemt het aantal gemelde problemen zienderogen af.

De meeste softwarefouten die nu nog opduiken, doen zich voor in nieuwe functionaliteiten van Windows NT of, de meerderheid, in applicaties zoals Internet Information Server. Alweer: een deel van de problemen komt voort uit de te gebruiken protocollen, waarover Microsoft geen zeggenschap heeft. Een ander deel ligt echter toch nog steeds (of weer) bij de implementatie die de toets der kritiek niet kan doorstaan. Zelfs ondanks de enorme macht op de softwaremarkt moet Microsoft op alle deelmarkten voor randproducten concurrentie dulden. Wellicht is Microsoft daar blij mee – de Amerikaanse justitie kijkt langs de zijlijn mee. Maar anderzijds kan moeilijk worden volgehouden dat men slordig werk levert om de concurrentie niet te verdringen.

Alleen veilige technieken voor netwerkverkeer gebruiken betekent in de eerste plaats een keuze voor de beschikbaar te stellen netwerkdiensten. Zo zijn er de Clipbook Viewer, de Computer Browser, de Directory Replicator en de Scheduler services die meestal toch geen nuttige bestemming hebben; ze kunnen dan ook beter worden uitgeschakeld. En de connectivity utilities (telnet, rsh, ping, etc.), SNMP en FTP kennen zo veel problemen dat ze ook beter niet aanwezig[6] kunnen zijn.

TCP/IP-protocollen zijn een bron van zorg. In plaats van de standaard ftp kan beter de FTP-service van de Internet Information Server (ja toch wel) worden gebruikt; de beveiliging is daarin beter te regelen. Met het toestaan van anonymous logon wordt dan bovendien voorkomen dat wachtwoorden in klare tekst over de lijn gaan, al moeten de accounts van de anonymous gebruikers wel in een aparte groep worden ondergebracht voor de traceerbaarheid. Bovendien, en dat geldt ook voor HTTP-diensten, laat in principe alleen verbindingen door die van binnenuit zijn geïnitieerd. En gebruik dynamische/statefull filtering op IP-niveau, een proxy minimaal op protocolniveau en content filtering voor HTTP en SMTP. En de Dynamic Name Service zou alleen 'split' DNS moeten bedienen.

Alweer wordt de Remote Access Service (RAS) buiten beschouwing gelaten; uitgangspunt voor RAS moet zijn dat er buiten de standaardinstellingen extra beveiligingsmaatregelen nodig zijn.
Bovenstaande opsomming van al of niet toegestane services geeft al aan: Windows NT is niet zo veel beter dan andere operatingsystemen dat externe toegang beveiligd zou kunnen worden zonder firewalls, gateways, routers, etc., die flink wat beheer vragen.

6 Dus niet alleen uitschakelen maar ook echt verwijderen...

Op het organisatorische vlak valt de beveiliging aanzienlijk te versterken met passieve en actieve monitoring van systemen en netwerken en met gebruikmaking van de tegenwoordig beschikbare hulpmiddelen. Daaronder zijn zeker ook de specifiek op beveiliging in engere zin gerichte hulpmiddelen als Kane Security Analyst en Security Monitor, en Axent Intruder Alert te rekenen. Al deze hulpmiddelen bieden geavanceerde mogelijkheden om de policies die in NT kunnen worden gedefinieerd, aanzienlijk uit te breiden.
Tevens valt er in veel organisaties vaak veiligheidswinst te behalen door het beleid ten aanzien van wachtwoorden aan te scherpen, te implementeren en actief te continueren. Met name aan dat laatste punt schort het nogal eens.

Een maatregel die natuurlijk een flink aantal afluisterproblemen oplost, is het gebruik van encryptie van dataverkeer. De organisatie eromheen (sleutelbeheer, etc.) maar ook de overige beveiliging van onder andere de Windows NT-systemen, zal echter wel op een hoog niveau moeten staan omdat anders een pennywise and poundfoolish beveiliging ontstaat. Ditzelfde geldt voor de fysieke beveiliging: als een hacker 'op' een systeem zelf kan komen, ter plekke of, na diefstal, rustig thuis, helpen andere maatregelen al een stuk minder.

Overigens wordt verwezen naar de binnenkort te verschijnen OTB-standaard Windows NT ([OTB98]), waarin een aantal basisnormen wordt gegeven voor adequate beveiliging van Windows NT.

En tegen een DoS-aanval zit er uiteindelijk misschien niets anders op dan de server te herstarten. Windows NT doet dat wellicht wat gemakkelijker dan andere operatingsystemen...

AFSLUITEND

Op de schaal tussen volledige flexibiliteit en vrijheid-blijheid voor de gebruiker enerzijds en een volledig dichtgetimmerd systeem anderzijds kiezen velen nu eenmaal voor een positie die dicht ligt bij het veilige eind van dat spectrum. Dat betekent dat Windows NT, ontworpen om op de flexibiliteithelft van het spectrum te staan, een flink stuk over de schaal geschoven moet worden, ofwel dat er flink wat veiligheidsmaatregelen zijn te nemen.

Windows NT is op zichzelf best veilig. Er worden inderdaad nog steeds lekken ontdekt in de NT-beveiliging maar dat worden er snel minder en met organisatorische maatregelen is veel te bereiken. Daarnaast: zolang de backward compatibility in achterhaalde authenticatiemechanismen en dergelijke behouden blijft, zal ook de backward compatibility van risico's blijven bestaan.

En ja, als de organisatorische maatregelen niet op orde zijn en worden nageleefd – zoals niet zelden in 'kleinere' IT-omgevingen waarvoor Windows NT is ontworpen, het geval is –, dan helpt natuurlijk de techniek ook nauwelijks. Ook in kleinere omgevingen zal alertheid nodig blijven; richting buitenwereld om nieuwe ontwikkelingen snel mee te

nemen en intern, om afwijkend systeemgedrag te signaleren.

Bovendien zien we uit naar versie 5.0, waarin behalve de beheerelementen ook de beveiliging een grondige renovatie ondergaat. De officiële uitgave van versie 5.0 staat gepland voor eind van het jaar, al circuleren er al ontwikkelversies in diverse gradaties van gereedheid.

Met name de introductie van authenticatie volgens het Kerberos-mechanisme betekent een verbetering van de beveiligbaarheid en maakt dat NT zal kunnen meedraaien in de kring van serieuze, robuuste operatingsystemen. Maar dan moeten we wel hopen op een kwalitatief goede implementatie. En de omvang en complexiteit van het sleutelbeheer wordt er bepaald niet minder door. Voorlopig is de algemene conclusie: NT en veilig netwerken, met wat moeite kan het best.

LITERATUUR

[Mudg97] P. Mudge en Y. Benjamin, *Déjà Vu All Over Again*, Byte, november 1997.

[NTin97] http://www.ntinternals.com/

[OTB98] Overlegorgaan Technische Beveiligingsstandaarden, *OTB-beveiligingsstandaard Windows NT*, exposure draft, te verschijnen.

[Resk97] The Microsoft Windows NT Server versie 4.0 Resource Kit, Supplement 1, Supplement 2, Microsoft Press, 1997.

[Rhin97] Rhino9 team, *The Modern Hackers Desk Reference*, http://207.98.195.250/mdh, december 1997.

[Stou96] B. Stout, *Windows NT and UNIX Network Security Mechanisms and weaknesses*, Hitachi Data Systems, www.hidata.com, november 1996.

Ir. drs. J. van der Vlugt
Is als EDP-auditor werkzaam bij KPMG EDP Auditors. Zijn aandachtsgebied ligt bij advies voor en audit van informatiebeveiligingsbeleid en de planning en beheersing van automatiseringsprojecten. Daarnaast heeft hij zich binnen de business unit Technical Auditing gespecialiseerd in de beveiliging en audit van Windows NT-systemen.

APPENDIX: OVERZICHT NT-BEVEILIGINGSGATEN

Onderstaand overzicht geeft een aantal van de tot nu toe bekende beveiligingsgaten in Windows NT (onder andere [Mudg97], [NTin97], [Rhin97] en [Stou96]). Deze behoren tot het standaardvocabulaire in NT-beveiligings- en NT-hackkringen.

Identificatie	Omschrijving	Tegenmaatregelen
PWDump, NTCrack	Programma's waarmee de user-ids en (one-way encrypted) passwords uit de SAM kunnen worden gelezen en eventueel gekraakt.	Organisatorisch.
L0phtcrack 1.5 en 2.0	Programma waarmee dictionary attacks op de user-id/password-combinaties uit de SAM kunnen worden uitgevoerd.	De Microsoft-fix tegen eerdere versies van L0phtcrack helpt niet tegen versie 1.5 en 2.0. Zorg in ieder geval voor niet-triviale passwords die niet zeven of veertien karakters lang zijn.
WINS port 84	Onzingegevens die bijvoorbeeld met Telnet naar poort 84 op een NT-server worden gestuurd, vullen de error log en eventueel de hele disk waar die op staan.	Berichten filteren.
SNMP-commando's	Met enkele SNMP-commando's kunnen alle WINS-tabellen in een netwerk worden geleegd.	SNMP stoppen, registry aanpassen, inkomende berichten filteren.
TCP/IP Flooding met Smurf	Een gespoofde ICMP echo request naar een lijst servers (bijvoorbeeld met het Smurf-programma) genereert een vloedgolf zinloze antwoorden naar de 'aanroepende' machine die daardoor overbelast kan raken.	Inherente TCP/IP-truc. Maatregelen in de technische infrastructuur.
Registry-risico's	Server Operators kunnen Administrator-rechten krijgen via verkeerde instelling van Scheduler service (waar Server Operators normaliter in kunnen grijpen). De Winlogon-service kent eenzelfde fout.	Write-toegang voor Server Operators voor deze services uitzetten.
NT crashen met NTFS	Een hackprogramma dat stukken van disk-defragmentatieprogrammatuur gebruikt, kan het (de) diskvolume(s) van een NT-systeem onbruikbaar maken.	
GetAdmin	Programma waarmee willekeurige geautoriseerde gebruiker (zoals guest...) Administrator-rechten kan krijgen.	Patch van Microsoft. Maar door eerst crash4.exe te draaien en vervolgens GetAdmin, werkt dat laatste alsnog. Maatregelen in de infrastructuur.
Ping Of Death II (SPing)	PoD II zendt (pingt) meerdere 64k packets die een NT-server kunnen ophangen (buffer overflow).	Alle inkomende ICMP-verkeer afvangen.
NT Server's DNS DoS-aanval	Het commando `$ telnet ntbox 19 | telnetntbox 53` van bijvoorbeeld een Unix-machine hangt de ntbox op.	Geen DNS gebruiken. Of blokkeer TCP-poort 53 (niet de UDP-poort). Of filter TCP-poort 53-packets op routers.
Out Of Band (OOB)-aanval (bijvoorbeeld met WinNuke)	Door out-of-band data naar een reeds opgezette verbinding te sturen, kan de NT-server zichzelf ophangen (in panic mode springen).	Inkomend verkeer op poort 139 blokkeren. Aanvallen op poorten 80 en 135 zijn met Service Pack 3 opgelost. Andere poorten zullen mogelijk nog kwetsbaar zijn.
SMB Downgrade-aanval	In de handshake voor het opzetten van een SMB-verbinding kan een client worden 'gedwongen' over te gaan op het in cleartext sturen van user-id en password. Dit wordt door een NT-server geaccepteerd, ongeacht de door de server gevraagde methode (bijvoorbeeld challenge-response) en zonder dat dit op enigerlei wijze is terug te vinden in loggings of iets dergelijks.	Alleen NT-clients gebruiken of met Service Pack 3 het gebruik van CIFS in plaats van SMB afdwingen voor het logon-proces.

Identificatie	Omschrijving	Tegenmaatregelen
RedButton	Iedereen met toegang tot poorten 137-139 kan met het RedButton-programma een disk geshared maken voor Everyone.	Hotfix van Microsoft.
IE en NTLM-authenticatie*	Internet Explorer geeft NT-domein- en password-gegevens door als een remote systeem om een NTLM-authenticatie vraagt.	Zo mogelijk de NTLM SSP service stoppen en disabelen.
Password Grabbing Trojans	Password-wijzigingen die aan een NetWare-omgeving (in cleartext) moeten worden doorgegeven, kunnen worden onderschept.	Ingewikkeld systeem van encryptie. Of koppeling met NetWare-omgeving achterwege laten.
Omkeren van een ISAPI Script	Een fout in Internet Information Server kan het aanroepende proces SYSTEM-rechten geven.	Onbekend.
Rollback.exe	Rollback.exe van Microsoft veegt een NT-configuratie vrijwel geheel schoon van instellingen; dientengevolge zijn de default accounts (waaronder Administrator zonder password) weer beschikbaar terwijl alle informatie nog wel op disk staat.	Applicatie verwijderen van alle NT-systemen en door middel van toegangsbeveiligingen voorkomen dat iemand het alsnog op een NT-systeem kan draaien.
Vervanging van systeem- dll's	Door de verkeerde (maar default) instelling van de toegang tot systeemdirectories kan iedereen systeem-dll's vervangen door zijn eigen.	Toegangsbeveiliging aanscherpen.
Executables hernoemen	Alle executables, ook die zonder extensie, kunnen vanaf de command prompt worden gedraaid. Hierdoor kan allerhande illegale programmatuur worden gebruikt.	Fysieke toegangsbeveiliging aanscherpen.
.BAT en .CMD-aanvallen	In parameters voor scripts die vanaf web pages kunnen worden gestart, kunnen commando's worden meegegeven die op de server worden uitgevoerd.	Beperking van de rechten die scripts hebben tijdens het runnen.
Afgebroken files	Zoiets als `http://www.domain.com/scripts/exploit.bat>PATH\target.exe` maakt de file `target.exe` opnieuw aan, waarmee de oude inhoud verloren gaat en mogelijk een malicieuze nieuwe `target.exe` wordt opgebouwd.	Beperking van de schrijfrechten op kritieke files.
SYN Flooding	Door een bombardement met SYN-packets van een gespoofd, niet bestaand IP-nummer zal een groot deel van de of alle capaciteit van een NT-server opgaan aan de pogingen om SYN-ACK packets terug te sturen.	TCP-fout, geen NT-oplossing mogelijk. Limieten op het aantal openstaande SYN-verzoeken aanleggen, helpt.
Land-aanval	`Land.c` stuurt SYN-packets met hetzelfde source- als destination-adres en dezelfde source- als destination-poort. Doordat NT probeert zichzelf te antwoorden gaat het systeem langzamer lopen.	Handmatig ingrijpen indien ontdekt. Maatregelen in de technische infrastructuur.
Teardrop, newtear, bonk en boink	Door twee packets te sturen die met opzet niet zijn te realigneren, wordt een systeem opgehangen of het reboot.	UDP/TCP-fout. Het blokkeren van poorten is mogelijk, maar als services van die poorten afhankelijk zijn, geeft dit natuurlijk problemen met de functionaliteit. Verder ook maatregelen in de technische infrastructuur.
NTFSDOS.EXE en Linux-systemen	Door op een Dos-machine `Ntfsdos.exe` te draaien, of via een Linux-machine op een NT-domein in te loggen, kan alle beveiliging van NTFS-volumes worden omzeild.	Beveiliging aanscherpen: geen Dos-machines met `Ntfsdos.exe` (dus zeker zonder floppy-drives), geen Linux-machines toestaan.

* (Beveiligings)fouten met applicaties, bijvoorbeeld Internet Information Server, Internet Explorer en FrontPage, blijven hier grotendeels buiten beschouwing.

Beveiligingsaspecten van Novell NetWare

Drs. M.J. van Beek RE

NetWare is nog niet verdwenen, integendeel. De auditor zal er nog steeds, wellicht meer dan hij tot nu toe deed, aandacht aan moeten schenken. Achtereenvolgens komen de structuur van NetWare en de beveiligingsaspecten, alsmede de auditaspecten en specifieke parameters aan bod.

INLEIDING

Novell NetWare is de afgelopen tien jaar onmiskenbaar marktleider geweest op de markt van (PC-)netwerkbesturingssystemen en vervult nog steeds een belangrijke rol. Desondanks hebben veel EDP-auditors geen of weinig ervaring met het beoordelen van NetWare-netwerken. Dit artikel behandelt de beveiligings- en auditaspecten van het netwerkbesturingssysteem Novell NetWare, geeft aan hoe met Novell NetWare een veilig netwerk kan worden gecreëerd en hoe een audit van een dergelijk netwerk kan plaatsvinden.

De uit Utah afkomstige firma Novell is oorspronkelijk bouwer van PC's en lanceerde in 1983 haar eerste netwerkbesturingssysteem S-NET voor de IBM PC, die tot dan toe nog nauwelijks in een netwerk kon worden opgenomen. In de jaren daarna werd een scala van versies geïntroduceerd met fantasievolle namen als Advanced NetWare, NetWare 386 3.0, etc.
In 1991 werd NetWare 3.11, later 3.12, geïntroduceerd, de eerste versie van NetWare die zowel voldoende capaciteit had (voldoende gebruikers ondersteunde) als behoorlijke beveiligingsmogelijkheden bezat.

Enkele jaren later werd NetWare 4.0, later 4.1, 4.11, geïntroduceerd; een belangrijke stap voorwaarts voor Novell bij de ondersteuning van bedrijfsbrede netwerken. Versie 4.0 bevatte veel bugs, die inmiddels echter zijn verholpen in nieuwe versies.

In de NetWare-wereld is het zeer gebruikelijk lang te wachten met de overgang naar een nieuwe versie. De auditor zal daarom nog regelmatig netwerken aantreffen die draaien onder oudere NetWare-versies. Dit is doorgaans geen probleem, daar Novell altijd minimaal één oudere versie (nu dus 3.x) blijft ondersteunen. Overigens zullen voor behoud van voldoende beveiliging wel alle security patches moeten zijn geïmplementeerd.
Tevens breidt Novell de productenportefeuille de laatste tijd weer uit met bijvoorbeeld IntraNetWare. Om dergelijke producten te kunnen controleren, is het natuurlijk belangrijk de basisstructuren te kennen.

In dit artikel zal vooral worden ingegaan op NetWare 4.x, waarbij af en toe een uitstapje terug wordt gemaakt naar de (on)mogelijkheden van oudere NetWare-versies. Daarbij komen achtereenvolgens de opzet van NetWare, netwerkbeveiligingsaspecten, algemene voorzieningen voor de beveiliging en auditattentiepunten aan de orde.

OPZET VAN NETWARE 4

Deze paragraaf behandelt de algemene beveiligingsfunctionaliteiten van NetWare 4.x. Hiertoe worden, uitgaande van een terugblik op eerdere versies, de nieuwe elementen besproken.

Security features

Inloggen op een server geschiedde vroeger per server. Werken op meerdere servers betekende het moeten gebruiken van meerdere user-ids en wachtwoorden; voor zowel beheerders als gebruikers in een groot netwerk een nauwelijks werkbare situatie. Met de introductie van NetWare 4.x is sprake van inloggen op een netwerk waarbinnen de toegang tot specifieke servers via specifieke rechteninstellingen kan worden geregeld.
Nieuw in NetWare 4.x is ook de unieke identificatie per user-loginsessie. In een bekende kraak van een oudere NetWare-versie bleek het namelijk mogelijk een netwerkpacket van een andere gebruiker te onderscheppen en op basis van het in het packet opgenomen volgnummer er een extra pakketje achteraan te sturen. Daardoor kon een bericht naar de server worden gestuurd 'namens' een andere gebruiker. Novell heeft dit in een patch direct opgelost. Om het probleem echter meer structureel op te lossen, is bij NetWare 4.x NCP Packet Signature geïntroduceerd, dat zorgt voor een unieke identificatie per sessie, zodat het afluisteren van berichten geen risico van valse packets meer oplevert.

Verschillen tussen NetWare-versies 2, 3 en 4

In tabel 1 zijn globaal de verschillen tussen enkele versies van Novell NetWare aangegeven. De verschillen in functionaliteit zijn te herleiden tot de verschillen in (de door de markt gewenste) omvang van de netwerken die konden worden ondersteund. Een aantal genoemde termen wordt hieronder in diverse paragrafen nader uitgewerkt.

Zo is duidelijk dat de versies 2.x vooral gericht waren op eenvoudige netwerkjes, terwijl pas vanaf versies 3.x werkelijke serverfunctionaliteit beschikbaar kwam. Vanaf de versies 3.x kunnen bijvoorbeeld onderlinge koppelingen tussen netwerken worden gelegd en kunnen groepen gebruikers tegelijk worden gemanaged. De techniek richt zich pas sinds de versies 3.x ook op de resourcezijde van beveiliging. Dat is ook herkenbaar in de uitbreiding van de SFT-mogelijkheden. Dat de versies 3.x nog steeds worden gebruikt, is ook niet zo vreemd als wordt beseft dat de feitelijke concurrenten ervan ook nog steeds in gebruik zijn.

Pas vanaf de wat meer recente versies 4.x is er sprake van volwaardige, multi-server netwerkoperatingsystemen die organisatiebrede, interlokale netwerken ondersteunen. De structuur van het beheer is met de nieuwe ADMIN-functie en de vernieuwde SUPERVISOR-functies op peil gebracht naar de laatste stand van de techniek en de meest recente inzichten in de inrichting van het beheer. Concurrentie ondervinden de versies 4.x vooral van Windows NT, dat vooralsnog wat sterkere applicatieserverfunctionaliteit bevat.

Met NetWare 4.x is enkele jaren geleden een groot aantal vernieuwingen geïntroduceerd, waaronder drie belangrijke:
- NetWare Directory Services (NDS);
- betere utilities voor beheer (met name de NetWare ADMINistrator);
- Memory allocation and protection (betere geheugenbescherming tegen vastlopers).

Netware Directory Services (NDS)

NDS is oorspronkelijk opgezet als manier om verschillende NetWare-netwerken op een logische en inzichtelijke manier aan elkaar te koppelen. Hierop aansluitend was NDS in een veel breder kader op sommige gebieden een de-factostandaard geworden.

Inmiddels heeft Novell ingezien dat ze geen alleenheerser meer is binnen de wereld van netwerkbesturingssystemen en is NDS als een apart product gepositioneerd, dat niet alleen voor NetWare functioneert maar ook voor andere netwerken zal worden ontwikkeld. Met name gaat het hierbij om NDS for NT on Novell (1997) (waarbij het beheer van een Windows NT-netwerk vanaf een NetWare-server onder NDS mogelijk wordt), en vanaf 1998 om NDS on NT, waarbij NDS op een Windows NT-server kan draaien.

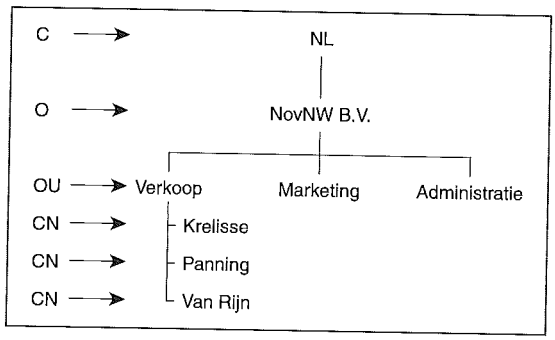
NDS maakt gebruik van een Gouden Gids-achtige hiërarchische structuur voor de naamgeving van objecten. De volgende typen objecten worden onderkend:

Aspect	2.x	3.x	4.x
Functies	Standaard	Servergericht	Multi-server, overdraagbaarheid
Maximale omvang van het netwerk	Klein	Enkele koppelingen	Organisatiebreed (interlokaal)
Beheer(der)	SUPERVISOR	SUPERVISOR, group management	ADMIN, SUPERVISORS
Doel van de beveiliging	Gebruikers	Groepen, resources, passwordencryptie	Subbomen, C2-beveiliging
Beschikbaarheid	SFT I en II	SFT I, II en III	SFT I, II en III
Concurrentie	ArcLan	Lan Manager, Unix, Banyan Vines	Windows NT Server

Tabel 1. Versies en verschillen.

- Container objecten (een container kan letterlijk andere objecten bevatten):
  - C = COUNTRY NAME,
  - O = ORGANIZATION NAME,
  - OU = ORGANIZATIONAL UNIT NAME;
- Leaf objecten:
  - CN = COMMON NAME
    De belangrijkste zijn:
    - User,
    - Volume,
    - Directory map,
    - Group,
    - NetWare server;
  - Printer;
  - Print server.

In figuur 1 is weergegeven hoe de NDS-boomstructuur (ook wel tree genoemd) kan zijn opgebouwd. Deze structuur weerspiegelt het gehele netwerk; de locatie van de objecten (waar iemand werkt) is niet van belang om te kunnen inloggen en toegang te krijgen tot servers, gegevens, etc. In de figuur is te zien hoe onder de country name NL en organization name NovNW drie organizational units zijn ondergebracht, met als voorbeeld enige common names (users) in de leafs.



Figuur 1. NDS-structuur.

Object properties

Per object kunnen properties worden bepaald, bijvoorbeeld de minimale lengte van een password. Aan groepen en users kunnen rechten worden toegekend om deze properties te benaderen. Hierdoor is onderscheid in beheer mogelijk. Een bekend voorbeeld is dat binnen een automatiseringsorganisatie een helpdesk wel wachtwoorden kan resetten (indien een gebruiker het wachtwoord niet meer weet) maar geen nieuwe gebruikers mag definiëren. Hierdoor is het mogelijk binnen één netwerk verschillende beheerfuncties te onderkennen met elk hun specifieke rechten. Onder eerdere versies van Novell NetWare was dit veel minder goed mogelijk.

ADMIN / SUPERVISOR

Tot en met NetWare 3.x bestond er één SUPERVISOR-account (de hoogste baas op het systeem met onbegrensde rechten) per server. Daarnaast was het mogelijk voor andere gebruikers of groepen een zogenaamde security equivalence ten opzichte van de SUPERVISOR te definiëren, wat betekende dat er in de praktijk een aantal, ten onrechte meestal (veel) meer dan vijf, SUPERVISOR-equivalente users bestond.

In NetWare 4 is een nieuwe hoogste baas gecreëerd, de zogenaamde ADMIN, die alle rechten heeft tot het gehele netwerk. Analoog aan versie 3.x is het creëren van een ADMIN-equivalente user mogelijk.

Onder de ADMIN is het mogelijk een SUPERVISOR (eigenaar) per NDS-onderdeel (container) aan te maken. Op deze manier kan een gedeelte van het beheer van één of meer afdelingsservers bijvoorbeeld bij de desbetreffende afdeling worden gelegd. Het beheer kan dus naar wens van de organisatie worden gecentraliseerd of gedecentraliseerd.

NLM-structuur

NLM is de afkorting voor NetWare Loadable Modules. Deze modules zijn stukjes besturingsprogrammatuur die aan het netwerkbesturingssysteem kunnen worden geplakt. Ze kunnen worden gemaakt door Novell (bijvoorbeeld om het gebruik van TCP/IP mogelijk te maken) of door derde partijen (bijvoorbeeld leveranciers van back-upprogrammatuur). De beoordeling van de beveiliging in brede zin van de gebruikte NLM's is, gegeven de mogelijkheden om het systeem te beïnvloeden, van groot belang voor een auditor.

NETWERKBEVEILIGING

Naast de specifieke structuur van NetWare is ook de 'omgeving' rond NetWare-netwerken van belang.

Een breder perspectief...

Beveiliging van een LAN staat niet op zichzelf. De basis hiervoor vormt de beveiliging van de PC's die onderdeel zijn van het LAN. Hierbij kunnen de volgende maatregelen aan bod komen:

- encryptie: het versleutelen van de gegevens op een PC dan wel het versleutelen van het berichtenverkeer tussen de PC en de server(s);
- het gebruik van beveiligingssoftware, bijvoorbeeld van een extra toegangsbeveiligingspakket dat de toegang tot de PC afschermt voor onbevoegden;
- het verwijderen of ontoegankelijk maken van een diskettestation;
- het verwijderen van de harde schijf uit een PC;
- meer uitgebreide authenticatie, bijvoorbeeld door middel van een token voor toegang tot de PC of applicatie, wat bij electronic-bankingpakketten wordt aangetroffen;
- viruscontrole op het netwerk en/of op de PC;
- een beveiligd besturingssysteem op de PC, waarbij de toegang tot de PC kan worden afgeschermd door een mechanisme dat integraal deel uitmaakt van het besturingssysteem (dus geen Ms-Dos, Windows 3.x of Windows 95).

Al deze maatregelen dragen in (veel) meerdere of mindere mate bij aan het algemene niveau van beveiliging dat wordt behaald. Derhalve is het beslist nuttig te bezien in hoeverre ze haalbaar zijn en – gerelateerd aan het vereiste beveiligingsniveau – kunnen worden voorgeschreven.

Koppelingen met andere platformen

In vroeger tijden had elk computerplatform zijn eigen hostapparatuur, bekabeling en terminals. Gebruikers werkten doorgaans met een niet-intelligente terminal om het centrale computersysteem te benaderen. De toegang kon daardoor geheel op het centrale computersysteem worden afgehandeld.

In de huidige tijd bestaan (heterogene) netwerken steeds meer uit koppelingen tussen verschillende platformen. Een voorbeeld is het opnemen van een IBM AS/400-systeem in een NetWare-netwerk. Hierdoor wordt het mogelijk het AS/400-systeem door middel van terminalemulatie te benaderen en vanaf een PC op dit systeem in te loggen. De gebruiker merkt dit doordat hij voortaan nog maar één computer en beeldscherm nodig heeft om meerdere geautomatiseerde systemen van de organisatie te benaderen.

Dit plaatst de organisatie voor de vraag in welke schil de benodigde logische toegangsbeveiliging moet worden ingebouwd. Er zijn verschillende varianten mogelijk:
- het afschermen van de toegang tot de PC;
- het afschermen van de toegang tot het PC-netwerk;
- het afschermen van de toegang tot het centrale computersysteem;
- het gebruik van 'single sign-on', met behulp van bijvoorbeeld producten van Computer Associates of Raxco.

Ook op dit punt geldt dat organisatorische aspecten een belangrijke rol spelen bij de afweging welke maatregelen worden getroffen. Daarbij is het belangrijk dat wordt vastgelegd op basis van welke argumenten de uiteindelijke beslissing(en) dienaangaande is (zijn) genomen, opdat wanneer het handhaven van de maatregelen verwatert of wordt betwist, voor wat betreft de argumenten niet telkens opnieuw het wiel behoeft te worden uitgevonden.

VOORZIENINGEN VOOR DE BEVEILIGING VAN NOVELL NETWARE-SYSTEMEN

In deze paragraaf komen enkele specifieke NetWare-beveiligingsparameters aan bod.

Inrichting van de system disk

Een NetWare-server bezit een zogenaamde system disk die de volgende standaarddirectories kent:
- LOGIN, de directory die door users wordt gebruikt om in te loggen;
- MAIL, een overblijfsel van oudere NetWare-versies. Sommige applicaties maken hier nog gebruik van;
- SYSTEM, dat NetWare-commands en -files bevat die door de ADMIN of SUPERVISOR worden gebruikt;
- PUBLIC, bevat de NetWare-files die toegankelijk zijn voor alle gebruikers.

Ieder van deze directories vereist natuurlijk zijn eigen specifieke patroon van afscherming. Omdat ze zo wezenlijk zijn voor het functioneren van NetWare, zullen de beveiligingsinstellingen dan ook nauwlettend moeten worden gecontroleerd.

Login procedures/scripts

Login scripts worden toegekend aan gebruikers en zijn de wegwijzers in het systeem. In een login script worden drive mappings van gebruikers, printerinstellingen en dergelijke opgenomen.
Qua beveiliging is het login script weinig interessant. Het is echter mogelijk in een login script allerlei statements op te nemen, waaronder het toekennen van rechten. Dit 'lek' is in het verleden door gebruikers misbruikt om zichzelf te veel rechten toe te kennen. Met name als het login script van de SUPERVISOR of ADMIN kon worden aangepast door een statement toe te voegen waarin bepaalde rechten werden doorgegeven aan andere gebruikers, kon dit ongemerkt aanzienlijke risico's opleveren. Dit 'lek' is vrij eenvoudig te dichten door de schrijfrechten van gebruikers op login scripts (en zeker het login script van de SUPERVISOR of ADMIN) af te nemen.

In het algemeen biedt het gebruik van login scripts een effectieve bijdrage aan de beveiliging, derhalve zouden er wel heel goede argumenten moeten zijn om ze niet te gebruiken!

Menubeveiliging

NetWare biedt standaard een voorziening voor menubeveiliging: de zogenaamde Saber-menu's zijn in NetWare 4.x standaard opgenomen.
Menu's werden in het verleden vooral gebruikt voor de combinatie met Ms-Dos-clients: de gebruiker werd na het inloggen op de server naar een menuschil doorgesluisd waaruit hij niet zou mogen ontsnappen. In zijn (groeps- of persoonlijke) menu stonden de programma's die hij zou mogen benaderen. Hierdoor werd zowel een simpele bewegwijzering als een beveiligingshulpmiddel verkregen: een gemakkelijke manier om geen rechten op directory- of fileniveau te hoeven definiëren.

In deze situatie werkten de gebruikers onder Ms-Dos en moest worden voorkomen dat ze, terwijl ze in het netwerk waren ingelogd, uit de applicatie naar Ms-Dos konden terugkeren. Immers, vanuit Ms-Dos was het simpel mogelijk alle directories en bestanden op de server te benaderen. Aangezien veel applicaties een ingebouwde escape-functie hadden naar Ms-Dos, moesten dergelijke functies door het systeem worden afgevangen zodat de gebruiker wel in zijn Ms-Dos-shell moest blijven.
Bij het gebruik van veel verschillende applicaties was dit zeer bewerkelijk. De standaardisatie en het beheer van programmatuur moesten welhaast perfect zijn geregeld om nog een redelijk beveiligingsniveau te kunnen halen.

In combinatie met Windows is het toepassen van menubeveiliging alléén niet aan te bevelen. Immers, onder Windows zijn meerdere Ms-Dos-vensters te activeren, waardoor de 'ontsnapping' naar Ms-Dos een simpele stap is. De noodzaak ook directories en files specifiek te gaan afschermen, wordt daarmee alleen maar groter.

Rechten

Binnen NetWare kunnen verschillende typen gebruikers worden onderscheiden. In tabel 2 staan de belangrijkste aangegeven.

Tabel 2. Typen gebruikers.

Type gebruiker	Functie
Operator	Wordt gebruikt voor printerbeheer
User	Normale gebruiker
Workgroup manager (3.x)	Beheerder van een groep gebruikers
SUPERVISOR	User met SUPERVISOR-recht op een container object in de NDS-tree
ADMIN (4.x)	Eigenaar van de gehele NDS-tree
Auditor (4.x)	Speciale gebruiker, heeft toegang tot auditfiles

Ieder operationeel systeem kent wel elk van deze typen gebruikers. Ze vormen dus een prima uitgangspunt voor het opstellen van de rechtentoekenningen.

Binnen NetWare bestaan twee soorten rechten: directory- en filerechten, waarmee gebruikers toegang tot directories en files krijgen, en object- en propertyrechten (alleen NetWare 4.x) waarmee gebruikers rechten krijgen om objecten aan te maken en de properties van objecten te beheren (login restrictions aanpassen, rechten instellen, etc.).

Directory- en filerechten kunnen bestaan uit drie soorten: trustee rights, inherited rights en effective rights.

Trustee rights zijn bestandsrechten die min of meer rechtstreeks worden toegekend. Ze worden
- ofwel rechtstreeks toegekend door een SUPERVISOR of iemand met Access Control rights;
- ofwel toegekend doordat een gebruiker Security-equivalent wordt gemaakt aan een gebruiker met de desbetreffende rechten;
- ofwel toegekend doordat een gebruiker lid wordt gemaakt van een groep die de desbetreffende rechten heeft.

Inherited rights zijn rechten die worden verkregen door het overerven van rechten van een bovenliggend niveau. Groepen en gebruikers erven immers de rechten van de groep of gebruiker die ze aanmaakt. Deze rechten stromen als een waterval door een systeem als ze op een hoog niveau (bijvoorbeeld het Root-niveau van een serverdisk) worden toegekend. Een inherited right kan worden geblokkeerd door een Inherited Right Filter (IRF-filter), wat inhoudt dat een bepaald recht kan worden tegenhouden om naar beneden door te stromen.

Effective rights zijn de uiteindelijke resultante van de trustee en inherited rights.

In figuur 2 is de combinatie van de verschillende Read-, Write-, Control- en Filescan-rechten aangegeven.

In de figuur is te zien dat uit de inherited R-, W-, C- en F-rights die user Jansen uit hoofde van zijn lidmaatschap van de groep Inkoop op een directory heeft gekregen, door een IRF-filter voor W en C worden ingeperkt, en dat deze beperking ook geldt voor een subdirectory Privé.

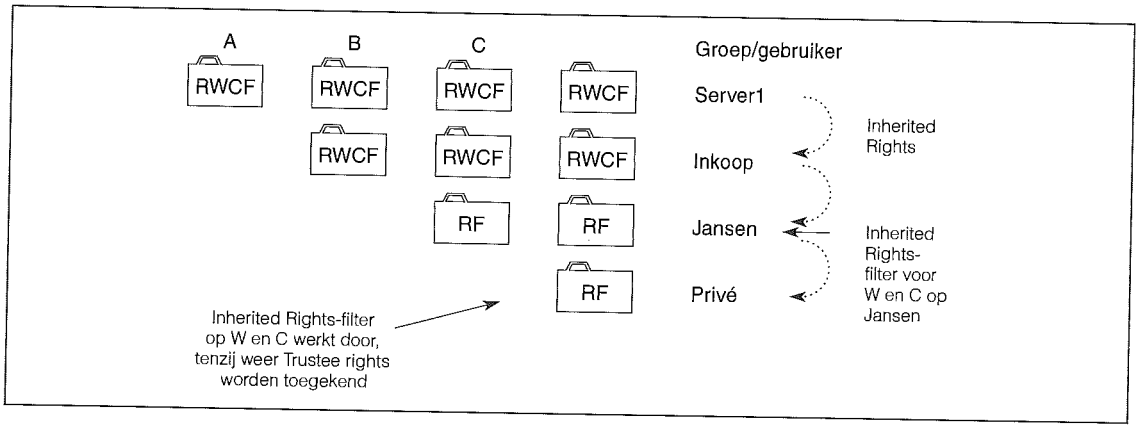
Als er geen trustee assignment is, dan is het effective right gelijk aan het effective right van de bovenliggende directory minus het IRF-filter. Als er wel een trustee assignment is, dan is het effective right gelijk aan het trustee right. Trustee-rechten zijn dus krachtiger.

Het programma Security (NetWare-versies 2 en 3) gaf aan of instellingen van gebruikers ten aanzien van een aantal systeemdirectories correct waren. Binnen NetWare 4 moet u dit zelf beoordelen. In tabel 3 is aangegeven wat de standaardinstellingen zouden moeten zijn.

Fysieke beveiliging en continuïteit

Aspecten van fysieke beveiliging en continuïteit worden slechts in beperkte mate bepaald door het netwerkbesturingssysteem in PC-netwerkomgevingen. Het in een afgesloten (computer)ruimte opstellen van een server is zeker aan te bevelen (een server-harddisk is sneller ontvreemd dan een compleet mainframe). Onderstaand enkele aanvullende zaken die NetWare-specifiek zijn.

Figuur 2. Combinaties van rechten.



Directory	Standaard-gebruikersrechten
ROOT	geen
SYS:SYSTEM	geen
SYS:PUBLIC	[RF]
SYS:LOGIN	[RF]
SYS:MAIL	[W]
eigen maildirectory per persoon	[SRWCEMF]
R = Read, F = Filescan, W = Write, S = Supervisor, C = Control, E = Erase, M = Modify	

Tabel 3. Aanbevolen standaardinstellingen.

NetWare heeft standaard back-upvoorzieningen in het programma SBACKUP, waarmee full backups, incremental backups, differential backups en custom backups kunnen worden gemaakt. In plaats van dit standaardproduct wordt overigens vanwege de meer uitgebreide functionaliteit echter veelal ARCserve gebruikt.

Bij servers worden tegenwoordig veelal RAID (Redundant Array of Inexpensive Disks)-systemen toegepast, waardoor een defecte schijf niet direct leidt tot gegevensverlies. De huidige RAID-5-systemen maken het mogelijk een defecte 'hot-swappable' schijf te verwisselen terwijl het systeem overigens normaal doordraait. De gebruiker merkt daardoor niets van het defect of de vervanging van de schijf.

Specifiek voor NetWare is de voorziening System Fault Tolerance ofwel SFT. Deze standaardoptie in het besturingssysteem kent drie niveaus:
- level I – mirroring, waarbij iedere harde-schijfeenheid dubbel is uitgevoerd;
- level II – duplexing, waarbij tevens de toegangsbus dubbel is uitgevoerd (naar beide hardeschijfeenheden);
- level III – twee onderling verbonden (gespiegelde) servers die beide dezelfde data en programmatuur bevatten.

SFT-level III wordt met name toegepast bij zeer bedrijfskritieke systemen. Producten van externe leveranciers die hetzelfde beloven zijn verkrijgbaar maar hebben als nadeel dat bij uitval van de server meestal een (kortstondige) uitval van de verbinding tussen de server en het werkstation optreedt. SFT-level III voorkomt dit.

Het Transaction Tracking System (TTS) is een voorziening waardoor bij aanpassing van een record in een database wordt vastgelegd wat de oude situatie was. Bij uitval van de server terwijl mutaties plaatsvinden (bijvoorbeeld door stroomuitval) zorgt TTS voor een herstelactie (de oude situatie wordt teruggezet). TTS werkt echter alleen indien deze functie door de gebruikte programmatuur (met name het databasemanagementsysteem) wordt ondersteund.

AUDIT VAN EEN NETWARE-NETWERK

Het proces van een audit van een NetWare-netwerk is grotendeels vergelijkbaar met een audit van een willekeurig ander netwerkplatform. In dit artikel onderscheiden we de volgende fasen, die hierna kort worden behandeld:
- inventarisatie;
- normering;
- onderzoek opzet;
- onderzoek bestaan;
- rapportage.

Fase 1: Inventarisatie

In deze fase worden de volgende zaken geïnventariseerd:
- de typologie van de organisatie;
- de organisatiestructuur;
- de belangrijkste bedrijfsprocessen;
- de afhankelijkheid van de organisatie van de LAN-automatisering (ook de koppeling met andere platformen is van belang);
- een overzicht van de aanwezige informatiesystemen (per server);
- welke soort computerapparatuur wordt gebruikt (alleen PC's en LAN's of ook mainframe en/of midrangesystemen);
- de aard en gevoeligheid van de opgeslagen gegevens;
- de gebruikte infrastructuur (aantal servers, werkstations, printers, bridges, routers, koppelingen, bekabeling, in- en uitbelvoorzieningen, protocollen);
- de automatiseringsorganisatie;
- de in gebruik zijnde versie(s) van Novell NetWare en het aantal gebruikers.

Hiermee wordt de algemene situatie rond de automatisering en de omgeving bepaald. Deze gegevens zouden voldoende moeten zijn om de soll-positie ten aanzien van de beveiliging te kunnen opstellen, hetgeen in fase 2 aan de orde komt.

Fase 2: Normering

Hierin worden normen (de soll-positie ofwel de vereisten, in wezen echter eerder minder hard: de verwachtingen) bepaald voor:
- de betrokkenheid van het management bij de automatiseringsactiviteiten;
- het beveiligingsbeleid;
- de relatie tussen gebruikersorganisatie en automatiseringsorganisatie;
- de uitvoering van het applicatie- en softwarebeheer;
- het beleid en de standaarden en procedures ten aanzien van automatiseringsactiviteiten;
- de opzet en het bestaan van functiescheidingen;
- de opzet en het bestaan van logische toegangsbeveiliging;
- de beschikbaarheid van (up-to-date) configuratieschema's;
- maatregelen ten aanzien van computervirussen;
- procedures voor de toegang tot het netwerk, de apparatuur, programma's en gegevens;
- de opzet en inrichting van groepsstructuren;
- eventuele aanvullende beveiligingsmaatregelen;
- de mogelijkheden voor toegang van buitenaf;
- test- en acceptatieprocedures;
- het functioneren van het netwerk- en systeembeheer en rapportagelijnen;

- maatregelen ter bevordering van de continuïteit;
- maatregelen ten aanzien van back-up/recovery;
- maatregelen ten aanzien van fysieke toegang;
- procedures voor het onderhoud van apparatuur.

Daarbij kan het nuttig zijn een onderscheid te maken tussen opzet en bestaan van maatregelen; in latere onderzoeksfasen kan hier dan op worden teruggevallen. Men vergete niet de normen af te stemmen met de opdrachtgever, anders kunnen er nog wel eens verschillen in verwachtingspatronen ten aanzien van de audits ontstaan die wellicht pas in de rapportagefase opduiken.

Fase 3: Beoordeling opzet beveiliging

Het doel hiervan is inzicht te verkrijgen in de opzet van de beveiliging. De uitvoering vindt veelal plaats door middel van interviews met onder anderen – of liever ten minste:
- het hoofd Automatisering;
- systeembeheerders;
- gebruikers.

In deze fase komen de 'hardere' technische parameters nog wat minder aan bod. Het is dan ook in deze fase dat nog flink wat afstemming nodig zal zijn.

Fase 4: Toetsing bestaan beveiliging

Pas in deze fase worden feitelijk de NetWare-parameters onderzocht. In sommige gevallen leidt de uitvoering van deze fase tot de misplaatste verwachting dat tevens de werking van de maatregelen wordt vastgesteld. Dit is niet het geval, hooguit kan het – bij herhaald onderzoek – waarschijnlijker worden dat de maatregelen werken zoals ze zijn bedoeld.

Attentiepunten voor fase 4 zijn:

- Voor het uitvoeren van veel controles is een ADMIN of SUPERVISOR-equivalence nodig, de auditor kan niet zelfstandig overal bij.

- Het samen met een beheerder uitvoeren van deze fase biedt diverse voordelen:
  - de beheerder krijgt de mogelijkheid iets op dit gebied te leren, de reguliere beheercursussen besteden immers slechts beperkt aandacht aan beveiligingsaspecten;
  - de auditor krijgt direct inzicht in de kennis en vaardigheden van de beheerder;
  - door de beheerder aan het toetsenbord te hebben, is deze zelf verantwoordelijk voor de ingetoetste commando's;
  - eventuele fouten kunnen (bij een groot risico) direct worden hersteld.

Overigens kan in deze fase blijken dat bijvoorbeeld de opzet van de beveiliging alleen informeel is geregeld, maar dat op basis van ervaring en bewustzijn toch een redelijke beveiliging bestaat.

Hieronder wordt een aantal technische hulpmiddelen en parameters besproken die in deze fase aan bod kunnen komen.

HULPMIDDELEN VOOR BEHEER EN AUDIT

Bij de beschikbare hulpmiddelen voor beheer en audit (vaak zijn dit dezelfde producten) kan onderscheid worden gemaakt tussen standaard Novell-hulpmiddelen en hulpmiddelen van derden. In de laatste categorie zijn bijvoorbeeld de volgende gebruikelijke hulpfuncties aan te treffen:
- antivirusprogrammatuur (op server- en werkstationniveau);
- software ten behoeve van monitoring en analyse van de audit trail (monitoring van alle acties van gebruikers op het systeem (in NetWare 4.x is dit overigens standaard opgenomen, zie de laatste paragraaf van dit artikel);
- software voor het beheren van de hard- en software-inventaris.

Onder NetWare 3.x was standaard reeds een indrukwekkend aantal utilities en commando's voor de beheerders beschikbaar – met overigens beperkte functionaliteit. Doordat een aantal utilities bestond die een min of meer vergelijkbare functionaliteit hadden, was de situatie zelfs voor ervaren beheerders behoorlijk verwarrend. Een goed voorbeeld daarvan is het gebruik van utilities om rechten te bekijken en te beheren. Hiervoor konden de utilities RIGHTS, FILER en NDIR worden gebruikt.

Utilities die bijvoorbeeld van belang zijn in een NetWare 3.x-omgeving en voor de auditor bekend moeten zijn:
- TREE, dat de directorystructuur van de disk geeft, van belang voor de bepaling van kritieke directories en bestanden;
- FILER, dat wordt gebruikt voor het nagaan van rechten voor specifieke directories of files;
- RIGHTS, dat voor een directory (en alle files) aangeeft welke *trustee*-rechten zijn toegekend en welke filters op de directories zijn geplaatst;
- NDIR, dat informatie geeft over flags, inherited rights filters en effective rights (alleen van de eigenaar van de files) voor alle files in een directory.

Bij het gebruik van bovenstaande utilities kunnen extra parameters worden toegevoegd, waarmee uitgebreidere informatie wordt verkregen. Zo kan een NDIR-overzicht worden gemaakt van een hele subdirectory, hetgeen overigens kan leiden tot een enorme stapel papier als uitdraai.

Enige tips bij het beoordelen van rechten zijn:
- de ADMIN respectievelijk SUPERVISOR zou eigenaar moeten zijn van alle standaarddirectories, waaronder de applicatiedirectories (aan gebruikers/groepen kunnen dan trustee-rechten worden toegekend). Een applicatiedirectory mag niet schrijfbaar zijn;
- een gebruiker heeft trustee-rechten op eigen mail-directory;
- een gebruiker mag alleen owner zijn van zijn eigen 'home'-directory;
- als het SUPERVISOR-recht op een object wordt verwijderd (door een ADMIN of SUPERVISOR) kan een object onbenaderbaar worden!

Security (3.x)

Security is een aparte utility onder NetWare 3.x. In de praktijk wordt deze door beheerders helaas niet gebruikt; onbekendheid ermee lijkt hieraan debet te zijn. Security controleert informatie in het systeem op basis van standaardargumenten:
- no password assigned;
- insecure passwords;
- unlimited grace logins;
- SUPERVISOR equivalence;
- root directory privileges;
- login scripts;
- excessive rights.

Indien versie 3.x in gebruik is, let er dan op dat de beheerder deze utility kent; dat duidt erop dat hij verstand van zaken heeft én waarschijnlijk dat hij 'security-minded' is. In NetWare 4.x is deze utility vervangen door de functie Search binnen de NetWare Administrator.

NetWare 4: de NetWare Administrator

Bij de ontwikkeling van NetWare 4.x heeft Novell ingezien dat het anders moest met de beheerprogrammatuur. Daarom is de NetWare Administrator ontwikkeld. Dit is een krachtig beheerprogramma, geschikt voor beheren van NDS, containers, servers, users, directories, files en rechten. Het programma werkt onder Windows en is eenvoudig te gebruiken. Ook voor auditors is dit het meest geschikte hulpmiddel.
De noodzaak voor gebruik van de 'oude' karaktergebaseerde utilities is hierdoor verdwenen (overigens zijn deze utilities nog steeds beschikbaar).

De volgende functies zijn in grafische vorm beschikbaar:
- het aanmaken en beheren van de directory tree;
- de definitie van alle soorten objecten;
- het beheer van rechten (per object en per user);
- het beheer van printfaciliteiten.

Een bijzonderheid is de NetWare Administrator Search-functie. Hiermee kan in de NDS-tree worden gezocht naar bijzondere eigenschappen van objecten (waaronder afwijkingen van de beveiligingsstandaarden). Enkele voorbeelden:
- users zonder (uniek) password;
- users die zijn gelockt als gevolg van een intruder detection;
- users met meer dan één gelijktijdige connection;
- users die security equivalent zijn aan ADMIN;
- organizational units zonder intruder detection.

Door middel van de functie 'Details on multiple Users' kan een aantal gebruikers worden beoordeeld op eventuele gemeenschappelijke eigenschappen. Afwijkingen van de standaard, bijvoorbeeld gebruikers die niet verplicht hun wachtwoord hoeven te wijzigen, kunnen nader worden onderzocht.

Een functie die per container kan worden ingesteld, is de intruder detection: het signaleren van mogelijke inbraakpogingen en de lockout-acties die hierna moeten plaatsvinden. Standaard is deze functie niet geactiveerd.

STARTUP.NCF en AUTOEXEC.NCF

Twee bijzondere bestanden zijn STARTUP.NCF en AUTOEXEC.NCF:
- STARTUP.NCF laadt de disk drivers van de file server en laadt de SET-parameters;
- AUTOEXEC.NCF bepaalt de file-servernaam, het IPX-nummer, de gewenste LAN-drivers en laadt de benodigde NLM's.

In AUTOEXEC.NCF kunnen bijzondere opties worden opgenomen. De optie 'secure console' bijvoorbeeld beveiligt het console:
- NLM's worden slechts vanaf SYS:SYSTEM geladen, de mogelijkheid NLM's vanaf bijvoorbeeld een Remote Console te laden wordt geblokkeerd;
- de toegang tot de operating system debugger wordt geblokkeerd;
- datum en tijd op de server kunnen niet worden gewijzigd;
- Ms-Dos is uit het geheugen verwijderd ten faveure van NetWare (het down brengen van een server betekent dat de server opnieuw wordt opgestart onder NetWare, niet Ms-Dos);
- in combinatie met een power-uppassword op de server wordt de toegang tot de server geblokkeerd.

De optie 'set allow unencrypted' laat het inloggen vanuit een werkstation toe dat niet in staat is geëncrypte wachtwoorden te versturen. Vrijwel altijd is dat een ongewenste situatie, dus let erop dat de optie niet wordt gebruikt.

Voor de auditor is het belangrijk te weten welke opties zijn opgenomen. Dit kan eenvoudig worden achterhaald via het programma Monitor, dat op het console draait.

Console lock

In de monitor kan de functie 'Lock File Server Console' worden geactiveerd. Hierdoor is toegang via het (remote) console tot de server alleen mogelijk met het console-password of het ADMIN-password. Voorwaar een nuttige functie, die in de praktijk ten onrechte nogal eens wordt vergeten.

NETWARE AUDITINGFUNCTIE

Binnen NetWare 3.x zijn nauwelijks auditfuncties aanwezig. Binnen NetWare 4.x is een speciale auditorfunctie geïntroduceerd. Hiermee kunnen onder andere de volgende auditfuncties worden gebruikt:
- Audit by Event (alle acties van een bepaald type kunnen worden vastgelegd);
- Audit by File/Directory (alle acties met betrekking tot bepaalde directories of bestanden worden vastgelegd);
- Audit by User (alle acties van bepaalde gebruikers kunnen worden vastgelegd).

Het is de bedoeling dat binnen de organisatie een functionaris wordt aangewezen als auditor. Deze auditor krijgt een specifiek password toegekend om de auditfunctie in het systeem te benaderen. Hier-

Drs. M.J. van Beek RE
Is bij KPMG EDP Auditors werkzaam als EDP Audit Manager. Hij is onder andere verantwoordelijk voor de productontwikkeling op het gebied van PC-netwerken en heeft de afgelopen jaren een grote reeks van advies- en auditwerkzaamheden verricht op het terrein van PC's en PC-netwerken. Hij treedt met betrekking tot dit onderwerp regelmatig op als gastdocent voor EDP-auditopleidingen.

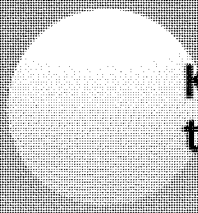
mee kan hij de auditfuncties aan- en uitzetten, instellingen aanpassen en dergelijke.

Als het auditoraccount is gedefinieerd en de auditor zijn initiële password wijzigt en geheim houdt, heeft de ADMIN of SUPERVISOR geen toegang meer tot auditing features, audit logs en dergelijke.
De ADMIN en de SUPERVISOR zijn hierdoor dus uitstekend controleerbaar geworden!

Bij het activeren van de auditingfunctie bestaat het gevaar dat een enorme hoeveelheid aan logginginformatie wordt vastgelegd. Bij het maken van rapportages zijn goede filtermogelijkheden aanwezig. Ook is output naar één van de bekende databaseformaten mogelijk.

TOT SLOT

In dit artikel is gedemonstreerd dat Novell NetWare in de nieuwste versies voldoende beveiligingsmogelijkheden heeft om kritische auditors tevreden te stellen. In de praktijk blijkt vaak dat beheerders de mogelijkheden nog onvoldoende gebruiken en dat auditors te weinig oog hebben voor het belang van PC-netwerkbesturing. Kortom, er ligt nog een wereld voor u open!



KPMG EDP Auditors
ten Hagen & Stam Uitgevers